Upgrading Avaya Aura® Communication Manager to Release 6.3.6

Release 6.3
03-603560
June 2015

© 2015 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface

with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and Avaya Aura® are registered trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 14
Purpose 14
Intended audience 14
Document changes since last issue 14
Related resources 14
Documentation 14
External references to the Upgrading Communication Manager book 15
Training 17
Viewing Avaya Mentor videos 18
Support 18
Warranty 19
Communication Manager upgrades 19
Communication Manager upgrades from System Manager 20
System Platform overview 21
Communication Manager deployment options 23
Communication Manager installation on System Platform 23
Communication Manager installation in VMware environment 23
Communication Manager templates overview 24
Supported platform for survivable servers 25
License file for Communication Manager 26
Duplicated server licensing 27
Authentication files for Communication Manager 28
Security enhancements 28
Use of third-party certificates 29
Upgrade paths 29
Support for SIP Enablement Services 30
Special circumstances 30
Preupgrade requirements 31
Upgrade order 32
Upgrade process 32
Using the Upgrading to Communication Manager Release 6.3.6 book 35
Chapter 2: Upgrading from Release 6.0.x or later to Release 6.3.6 36
Upgrading from Release 6.0.x or later to 6.3.6 on the simplex template 36
Introduction 36
Preupgrade tasks 37
Prerequisites 37
Preupgrade tasks on the existing system 38
Upgrade tasks 49
Upgrading from Release 6.0.x or later to 6.3.6 on duplex template 60
Introduction 60

Preupgrade tasks..... 60
Prerequisites..... 61
Preupgrade tasks on the active server..... 62
Preupgrade tasks on the standby server..... 69
Upgrade tasks on the standby server that was active before the interchange..... 80
Postupgrade tasks on the active server running Release 6.3.6..... 87
Postupgrade tasks on the standby server running Release 6.3.6..... 92
Upgrading from Release 6.0.x or later to 6.3.6 on embedded main template..... 96
Introduction..... 96
Presite upgrade checklist..... 97
Preupgrade tasks on the existing system..... 97
Upgrade tasks..... 109
Chapter 3: Upgrading to simplex main/survivable template..... 120
Upgrading the S8500A Server to the HP DL360 G8 or Dell R620 Server..... 120
Introduction..... 120
Preupgrade tasks on the S8500A Server..... 121
State of the existing server..... 132
Upgrade tasks on a new server that supports Release 4.0.5..... 132
Upgrade tasks on the HP DL360 G8 or Dell R620 Release 6.3.6 Server..... 143
Postupgrade tasks on the HP DL360 G8 or Dell R620 Release 6.3.6 Server..... 149
Upgrading the S8500-Series Server to the HP DL360 G8 or Dell R620 Server..... 154
Introduction..... 154
Preupgrade tasks..... 155
Prerequisites..... 157
Upgrade tasks on the target server..... 169
Upgrading the S8510 Server to S8510 Server on System Platform..... 186
Introduction..... 186
Preupgrade tasks..... 186
Prerequisites..... 187
Upgrade tasks..... 204
Upgrading the S8800 Server to S8800 Server on System Platform..... 220
Introduction..... 220
Preupgrade tasks..... 221
Prerequisites..... 222
Upgrade tasks..... 244
Upgrading the S8800 Server to the HP DL360 G8 or Dell R620 Server..... 261
Introduction..... 261
Preupgrade tasks..... 262
Prerequisites..... 263
Upgrade tasks on the target server..... 275
Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform..... 292
Introduction..... 292
Preupgrade tasks..... 292

Prerequisites 293
Upgrade tasks 306
Upgrading DEFINITY SI or R Server to the HP DL360 G8 or Dell R620 Server 322
Introduction 322
Prerequisites 323
Preupgrade tasks 324
Preupgrade administration 326
Upgrade tasks 327
Postupgrade tasks on the new server 349
Chapter 4: Upgrading to simplex survivable remote template 354
Upgrading the S8500A Server to the HP DL360 G8 or Dell R620 Server 354
Introduction 354
Preupgrade tasks on the S8500A Server 355
Upgrade tasks on the Release 6.3.6 server 359
Upgrading the S8500-Series Server to the HP DL360 G8 or Dell R620 Server 368
Introduction 368
Preupgrade tasks 368
Prerequisites 370
Upgrade tasks on the HP DL360 G8 or Dell R620 Server 378
Upgrading the S8510 Server to S8510 Server on System Platform 388
Introduction 388
Preupgrade tasks 389
Prerequisites 389
Upgrade tasks 401
Upgrading the S8800 Server to S8800 Server on System Platform 411
Introduction 411
Preupgrade tasks 411
Prerequisites 412
Upgrade tasks 429
Upgrading the S8800 Server to the HP DL360 G8 or Dell R620 Server 439
Introduction 439
Preupgrade tasks 439
Prerequisites 441
Upgrade tasks on the HP DL360 G8 or Dell R620 Server 450
Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform 459
Introduction 459
Preupgrade tasks 460
Prerequisites 460
Upgrade tasks 470
Upgrading DEFINITY SI or R Server to the HP DL360 G8 or Dell R620 Server 479
Introduction 479
Prerequisites 480
Preupgrade tasks 481

Preupgrade administration 483
Upgrade tasks 484
Postupgrade tasks on the new server 500
Chapter 5: Upgrading to duplex main/survivable core template 504
Upgrading the S8500A Server to the HP DL360 G8 or Dell R620 Server 504
Introduction 504
Preupgrade tasks 505
Prerequisites 506
Preupgrade tasks on the S8500A Server 506
State of the existing server 518
Upgrade tasks on a new server that supports Release 4.0.5 519
State of the existing server 528
Upgrade tasks on the HP DL360 G8 or Dell R620 Release 6.3.6 Server 529
Completion tasks on the active S8500A Server 536
Postupgrade tasks on the first HP DL360 G8 or Dell R620 Release 6.3.6 active server 537
Upgrade tasks on the second HP DL360 G8 or Dell R620 Server 542
Upgrading the S8500B or S8500C Server to HP DL360 G8 or Dell R620 Server 552
Introduction 552
Presite preparation 553
Preupgrade tasks on the S8500B or S8500C Server 554
Installing the servers in the rack 562
Duplex main/survivable core template 562
Upgrade tasks on the first HP DL360 G8 or Dell R620 Server 562
Upgrade tasks on the second HP DL360 G8 or Dell R620 Server 575
Upgrading the S8510 server to the HP DL360 G8 or Dell R620 Server 585
Introduction 585
Presite preparation 586
Preupgrade tasks on the S8510 Server 588
Installing the servers in the rack 595
Duplex main/survivable core template 596
Upgrade tasks on the first HP DL360 G8 or Dell R620 Server 596
Upgrade tasks on the second HP DL360 G8 or Dell R620 Server 608
Upgrading the S8700-Series Servers to the HP DL360 G8 or Dell R620 Servers 618
Introduction 618
Presite preparation 620
Preupgrade tasks on the active S8700 Server 621
Preupgrade tasks on the standby S8700 Server 632
Preparing the new servers for the upgrade 642
Sequence of tasks to be performed on the staged servers 642
Staging the new servers to Communication Manager Release 5.2.1 642
Upgrade tasks on the first staged (Release 5.2.1) server 651
Upgrade tasks on the second staged (Release 5.2.1) Server 653
Upgrade tasks on the first staged (Release 5.2.1) Server 657

Completion tasks on both the staged (Release 5.2.1) servers 660
Upgrade tasks on both the new (Release 6.2) servers 663
Verification tasks on the staged servers running Release 6.3.6 670
Verification tasks on the first staged active Release 6.3.6 server 671
Completion tasks on the standby S8700 Server 672
Completion tasks on the active S8700 Server 674
Postupgrade tasks on the first staged Release 6.3.6 active server 676
Postupgrade tasks on the second staged Release 6.3.6 busied out server 681
Upgrading the S8700-Series servers to the HP DL360 G8 or Dell R620 Servers 685
Introduction 685
Presite preparation 686
Preupgrade tasks 687
Preupgrade tasks on the active S8700-Series Server 688
Preupgrade tasks on the standby S8700-Series Server 696
Installing the servers in the rack 703
Upgrade tasks on the first HP DL360 G8 or Dell R620 Server 704
Upgrade tasks on the second HP DL360 G8 or Dell R620 Server 716
Upgrading the S8800 Server to S8800 Server on System Platform 726
Introduction 726
Presite preparation 727
Preupgrade tasks 728
Preupgrade tasks on the active S8800 Server 729
Preupgrade tasks on the standby S8800 Server 737
Tasks on the active S8800 server 759
Upgrade tasks on the standby server 759
Upgrade tasks on the S8800 Server that is shutdown 761
Postupgrade tasks on the standby server 782
Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform 787
Introduction 787
Preupgrade tasks 787
Upgrading branch gateways and survivable servers 788
Survivable core servers resetting 788
Preupgrade tasks on the active HP DL360 G7 Server 789
Preupgrade tasks on the standby HP DL360 G7 Server 796
Tasks on the active HP DL360 G7 Server 809
Upgrade tasks on the standby server 810
Upgrade tasks on the server that is shutdown 812
Postupgrade tasks on the standby server 823
Upgrading the S8800 Server to HP DL360 G8 or Dell R620 Server 828
Introduction 828
Presite preparation 829
Preupgrade tasks on the active S8800 Server 830
Preupgrade tasks on the standby S8800 Server 838

Installing the servers in the rack 843
Duplex main/survivable core template 843
Upgrade tasks on the first HP DL360 G8 or Dell R620 Server 844
Upgrade tasks on the second HP DL360 G8 or Dell R620 Server 857
Upgrading DEFINITY SI or R Server to the HP DL360 G8 or Dell R620 Server 867
Introduction 867
Prerequisites 868
Preupgrade tasks 869
Preupgrade administration 870
Upgrade tasks on both the new servers 872
Verification tasks on the HP DL360 G8 or Dell R620 Servers 878
Tasks on the first HP DL360 G8 or Dell R620 Server 879
Postupgrade administration on both the servers 880
Postupgrade tasks on the first HP DL360 G8 or Dell R620 Server 893
Postupgrade tasks on the second HP DL360 G8 or Dell R620 Server 898
Chapter 6: Upgrading to embedded main template 902
Upgrading DEFINITY SI or CSI Server to the S8300D Server 902
Introduction 902
Prerequisites 903
Preupgrade tasks 904
Preupgrade administration 904
Upgrade tasks 906
Postupgrade tasks on S8300D Server 920
Upgrading the S8300A Server to S8300D Server 925
Introduction 925
Checking the FTP, SFTP, or SCP server information 926
Preupgrade tasks on the S8300 Server 926
Upgrade tasks on the S8300D (Release 4.0.1 or 5.2.1) Server 939
Upgrade tasks on the S8300D Release 6.3.6 Server 948
Upgrading the S8300 Server to the S8300D Server 965
Introduction 965
Upgrade paths 966
Required upgrade sequence 966
Onsite preparation 966
Upgrade tasks on the S8300D Server 979
Upgrading S8400 Server to the S8300D Server 995
Introduction 995
Prerequisites 997
Preupgrade tasks on the S8400 Server 998
Upgrade tasks on the S8300D Server 1008
Postupgrade tasks on S8300D Server 1022
Completion tasks on the S8400 Server 1027
Upgrading S8500 Server to the S8300D Server 1028

Introduction ... 1028
Prerequisites ... 1029
Preupgrade tasks on S8500 Server ... 1030
Upgrade tasks on the S8300D Server ... 1042
Completion tasks on S8500 Server ... 1056
Postupgrade tasks on S8300D Server ... 1056
Postupgrade tasks on the S8300E server ... 1062
Downloading patches ... 1062
Installing patches ... 1063
Restoring the upgrade dataset ... 1063
Configuring the server data ... 1064
Starting Communication Manager Messaging ... 1065
Postupgrade tasks for Communication Manager Messaging ... 1065
Downloading patches ... 1065
Installing patches ... 1066
Copying language packages to the server ... 1067
Installing language packages ... 1067
Restoring custom announcements ... 1068
Restoring Communication Manager Messaging data ... 1068
Administering the signaling group for Communication Manager and Communication Manager Messaging ... 1069
Configuring the switch link ... 1070
Rebooting the server ... 1070
Verifying the Communication Manager operation ... 1071
Enabling scheduled maintenance ... 1072
Busying out previously busied out equipment ... 1072
Saving translations ... 1072
Installing the phone message file ... 1073
Resubmitting the scheduled backups ... 1073
Resolving alarms ... 1073
Backing up the system ... 1074
Verifying the Communication Manager Messaging test data ... 1075
Backing up the Communication Manager Messaging application data from 5.2.1 ... 1075
Logging off from all administration applications ... 1076
Registering the system ... 1076
Upgrading the S8300D Server to S8300D Server on System Platform ... 1077
Introduction ... 1077
Preupgrade tasks on S8300 Server ... 1077
Upgrade tasks on the S8300D Server ... 1089
Chapter 7: Upgrading to embedded survivable remote template ... 1107
Upgrading DEFINITY SI or CSI Server to the S8300D Server ... 1107
Introduction ... 1107
Prerequisites ... 1108

Preupgrade tasks..... 1109
Preupgrade administration..... 1109
Upgrade tasks..... 1110
Postupgrade tasks on S8300D Server..... 1118
Upgrading the S8300A Server to S8300D Server..... 1123
Introduction..... 1123
Prerequisites..... 1123
Upgrade tasks on the S8300D Server..... 1130
Upgrading the S8300 Server to S8300D Server..... 1139
Introduction..... 1139
Onsite preparation..... 1140
Upgrade tasks on the S8300D Server..... 1149
Upgrading S8400 Server to the S8300D Server..... 1159
Introduction..... 1159
Prerequisites..... 1160
Preupgrade tasks on the S8400 Server..... 1161
Upgrade tasks on the S8300D Server..... 1163
Postupgrade tasks on S8300D Server..... 1170
Completion tasks on the S8400 Server..... 1174
Upgrading S8500 Server to the S8300D Server..... 1175
Introduction..... 1175
Prerequisites..... 1176
Preupgrade tasks on the S8500 Server..... 1177
Upgrade tasks on the S8300D Server..... 1180
Postupgrade tasks on S8300D Server..... 1186
Completion tasks on S8500 Server..... 1190
Upgrading the S8300D Server to S8300D Server on System Platform..... 1191
Introduction..... 1191
Preupgrade tasks on S8300 Server..... 1191
Upgrade tasks on the S8300D Server..... 1199
Chapter 8: Upgrading Communication Manager from non-VMware to VMware Virtualized Environment..... 1209
Overview..... 1209
Upgrading Communication Manager 6.x to VMware..... 1209
Upgrading Communication Manager 5.2.1 to VMware..... 1212
Chapter 9: Converting to port network..... 1215
Upgrading DEFINITY Server CSI in CMC to the HP DL360 G8 or Dell R620 Server..... 1215
Introduction..... 1215
Prerequisites..... 1216
Preupgrade tasks..... 1217
Preupgrade administration..... 1218
Upgrade tasks..... 1220
Postupgrade tasks on HP DL360 G8 or Dell R620 Server..... 1237

Upgrading DEFINITY ONE/S8100 in CMC to the HP DL360 G8 or Dell R620 Server..... 1242
Introduction..... 1242
Prerequisites..... 1243
Preupgrade tasks..... 1244
Preupgrade administration..... 1245
Upgrade tasks..... 1247
Postupgrade administration..... 1257
Postupgrade tasks on HP DL360 G8 or Dell R620 Server..... 1265
Upgrading Avaya IP600/S8100 Server in G600 to the HP DL360 G8 or Dell R620 Server..... 1269
Introduction..... 1269
Prerequisites..... 1270
Preupgrade tasks..... 1271
Preupgrade administration..... 1273
Upgrade tasks..... 1275
Postupgrade administration..... 1285
Postupgrade tasks on HP DL360 G8 or Dell R620 Server..... 1293
Upgrading S8300 Server to the HP DL360 G8 or Dell R620 Server..... 1298
Introduction..... 1298
Prerequisites..... 1299
Preupgrade tasks on the S8300 Server..... 1300
Upgrade tasks on HP DL360 G8 or Dell R620 Server..... 1311
Shutting down the S8300 Server..... 1323
Preupgrade tasks..... 1323
Postupgrade administration..... 1324
Postupgrade tasks on the HP DL360 G8 or Dell R620 Server..... 1331
Upgrading S8400 Server to the HP DL360 G8 or Dell R620 Server..... 1336
Introduction..... 1336
Prerequisites..... 1338
Preupgrade tasks on the S8400 Server..... 1339
Upgrade tasks on HP DL360 G8 or Dell R620 Server..... 1349
Upgrade tasks on the cabinet..... 1361
Completion tasks on the S8400 Server..... 1361
Postupgrade administration..... 1362
Postupgrade tasks on the HP DL360 G8 or Dell R620 Server..... 1370
Appendix A: Worksheet for upgrading Communication Manager to simplex and embedded templates..... 1376
Appendix B: Worksheet for upgrading Communication Manager to duplex template 1381
Appendix C: Worksheet for upgrading Communication Manager on simplex to duplex template..... 1391
Appendix D: Converting private control networks A and B to control network C..... 1403
Introduction..... 1403
Preparing for port network conversion..... 1403
Converting private control network to control network C..... 1404

Appendix E: Converting from fiber port networks to IP-PNC 1406
Overview 1406
Fiber-PNC configurations 1406
The starting configuration 1407
The converted configuration 1407
Prerequisites 1408
Preconversion checklist 1408
Conversion tasks checklist 1408
Changing synchronization 1408
Installing the circuit packs 1409
Addition of circuit packs 1409
Installing a circuit pack 1409
Connecting to the server 1410
Configuring the IPSI circuit pack 1410
Verifying the installation of the circuit pack 1411
Connecting the cables 1411
Cables for the new circuit packs 1411
Connecting the circuit pack cables 1411
Administering circuit packs 1412
Administration of the new circuit packs 1412
Administering the IPSI circuit pack 1412
Configuring the IPSI circuit pack 1412
Setting the VLAN parameters and diffserv parameters 1414
Verifying IPSI translations 1414
Verifying IPSI connectivity 1415
Administering the media processor circuit pack 1415
Administering the C-LAN circuit pack 1416
Firmware upgrade on the new circuit packs 1417
Upgrading IPSI firmware 1417
Removing fiber-related administration 1417
Disabling PNC duplication 1418
Removing fiber-related hardware 1418
Administering PN synchronization 1418

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® Communication Manager from the earlier releases to Release 6.3.6 on System Platform and VMware. The document includes upgrade checklist, upgrade procedures, and verification procedures for each supported upgrade path.

Intended audience

The document is intended for people who perform upgrades.

Document changes since last issue

The following change has been made to this document since the last issue:

- Added the procedure for upgrading Communication Manager to Communication Manager Release 6.3.6 running in the Avaya Aura® Virtualized Environment.
- Added support for the import of the third-party certificate that uses the SHA-2 algorithm and 2048-bit RSA keys.
- Added procedure to install the Communication Manager Release 6.3.6 patch.

Related resources

Documentation

To complete the upgrade process, you require the following documents. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Release	Notes
Installing the Dell™ PowerEdge™ R620 Server	6.x.x	To install the Dell™ PowerEdge™ R620 Server in a rack
Installing the HP ProLiant DL360p G8 Server	6.x.x	To install the HP ProLiant DL360p G8 Server in a rack
Quick Start for Hardware Installation: Avaya G250 Media Gateway, 03-300433	5.2.x	To install the S8300D Server in the G250 Branch Gateway
Quick Start for Hardware Installation: Avaya G350 Media Gateway, 03-300148	5.2.x	To install the S8300D Server in the G350 Branch Gateway
Quick Start for Hardware Installation: Avaya G430 Media Gateway, 03-603236	5.2.x	To install the S8300D Server in the G430 Branch Gateway
Quick Start for Hardware Installation: Avaya G450 Media Gateway, 03-602053	5.2.x	To install the S8300D Server in the G450Branch Gateway
Quick Start for Hardware Installation: Avaya G700 Media Gateway, 555-233-150	5.2.x	To install the S8300D Server in the G700 Branch Gateway
Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	6.x.x	To deploy System Platform, Communication Manager, license file, and authentication file
Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment	6.3.x	To deploy the Avaya Aura® Communication Manager virtual application on VMware in Virtualized Environment
Installing and Upgrading the Avaya S8300 Server, 555-234-100	5.2.x	To upgrade Communication Manager to Release 5.2 on the S8300A, B, C, or D Server
Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers, 03-602885	5.2.x	To upgrade Communication Manager to Release 5.2 on the S8500 and S8700–Series Servers

External references to the Upgrading Communication Manager book

To successfully complete the upgrade, you must refer to more books. The following table provides a reference to the specific book you must use to perform that part of the upgrade.

Table 1: Task-to-book roadmap

Task	Book to use	Notes
Upgrade Communication Manager to Release 4.0.5 or Release 5.2.1 for servers that you can upgrade directly.	*Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers*, 03-602885	You can upgrade most Linux-based servers to Release 5.2.1.

Table continues…

Task	Book to use	Notes
Upgrade Communication Manager to Release 4.0.5 or Release 5.2.1 for servers that you cannot upgrade directly.	*Upgrading Servers to the Avaya S8800 Server for Avaya Aura® Communication Manager*, 03-603446	You must upgrade the Linux-based servers, which you cannot upgrade directly to Release 4.0.5 or Release 5.2.1 to the new server first. Those servers include: • S8300A • S8500A • S8700 • S8710 with DAL1 • S8720 with DAL1
Download files from PLDS and AFS.	*Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394	
Record required data.	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	
Complete the routine preupgrade tasks on the existing server.	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	
Back up all the files on the existing server in case you need to roll back to the original release.	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	
Install the preupgrade service pack on the existing server.	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	
Back up all the data sets to be restored on the new server.	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	
Install the server in the rack.	Use one of the following books as appropriate: • *Installing the HP ProLiant DL360p G8 Server* • *Installing the Dell™ PowerEdge™ R620 Server*	
Install the S8300D Server in the branch gateway.	*Quick Start for Hardware Installation: Avaya G250 Media Gateway*, 03-300433 *Quick Start for Hardware Installation: Avaya G350 Media Gateway*, 03-300148	See the appropriate book for your Gxxx branch gateway.

Table continues…

Task	Book to use	Notes
	Quick Start for Hardware Installation: Avaya G430 Media Gateway, 03-603236 *Quick Start for Hardware Installation: Avaya G450 Media Gateway*, 03-602053 *Quick Start for Hardware Installation: Avaya G700 Media Gateway*, 555-233-150	
Install System Platform on the server.	*Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394	
Install license and authentication files.	*Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394	
Install the appropriate Communication Manager template through the System Platform Web Console.	*Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394	
(Optional) Install postupgrade service pack.	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	
Restore the datasets on the new server	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	
Configure Communication Manager through the System Management Interface.	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	Use this book to configure Communication Manager.
Complete the postupgrade administration.	*Upgrading to Avaya Aura® Communication Manager Release 6.3.6*, 03-603560 (this book)	

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
AVA00383WEN	Avaya Aura® Communication Manager Overview
AVA00279WEN	Communication Manager- Configuring Basic Features

Table continues…

Course code	Course title
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
ATI02348IEN, ATI02348VEN	Avaya Aura® Communication Manager Implementation
AVA00836H00	Communication Manager Basic Administration
5U00041I	Avaya Aura® Communication Manager Administration
AVA00834WEN	Avaya Aura® Communication Manager- System Features and Administration
5U00040I	Avaya Aura® Communication Manager Maintenance and Troubleshooting
AVA00835WEN	Avaya Avaya Aura® Communication Manager Trunk and Routing Administration

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes,

downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Communication Manager upgrades

The guide provides the process and procedures for upgrading Avaya Aura® Communication Manager to Release 6.3.6. Communication Manager is an application that resides on a virtual server.

Supported platforms

- System Platform: Communication Manager runs on System Platform as the template.
- VMware: Communication Manager runs on the VMware vSphere™ 5.0, 5.1, or 5.5 in Virtualized Environment as the OVA template.

  For instructions to upgrade Communication Manager to Release 6.3.6 in the Avaya Aura® Virtualized Environment, see *DeployingAvaya Aura® Communication Manager on VMware® in Virtualized Environment*.

Supported upgrade paths

This book provides the following upgrade procedures:

- Software-only upgrade: Upgrading Communication Manager from Release 6.0 or later to Release 6.3.6.
- Hardware and software upgrade: Replacing the existing server with the server that Communication Manager Release 6.3.6 supports.
  - For systems on Release 5.2.1, upgrading from Release 5.2.1 to Release 6.3.6.
  - For systems on Release 4.0.5, upgrading from Release 4.0.5 to Release 6.3.6.
  - For systems between Release 5.0 and Release 5.2:
    1. Upgrading from the existing release to Release 5.2.1
    2. Upgrading from Communication Manager Release 5.2.1 to Release 6.3.6

- For systems on a release earlier than 4.0.5:
  1. Upgrading from the existing release to Release 4.0.5
  2. Upgrading from Communication Manager Release 4.0.5 to Release 6.3.6

Note:

You can also use Software Management, the centralized upgrade solution, that System Manager provides to upgrade Communication Manager and the associated devices, such as Gateways, TN boards, and media modules. With Software Management, you can upgrade Communication Manager from the following releases:

- Release 5.x to Release 5.2.1
- Release 5.2.1 to Release 6.3.6
- Release 6.x to Release 6.3.6

Supported servers

You can upgrade Communication Manager from Release 5.2.1 or Release 6.0.x to Release 6.3.6 on the following servers:

- Avaya S8300D
- Avaya S8510
- Avaya S8800
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R610 1U
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R620

Note the following upgrade considerations:

- Upgrade the servers on Communication Manager Release 5.2.1 or later to Release 6.3.6 on the existing servers.
- Upgrade the servers on Communication Manager Release 5.0 or release earlier than 5.2.1 to Release 5.2.1 before you upgrade the servers to Release 6.3.6 unless otherwise noted.
- Upgrade the servers on a release earlier than 4.0.5 to Release 4.0.5 before you upgrade the servers to Release 6.3.6 unless otherwise noted.

Communication Manager upgrades from System Manager

Software Management, a centralized upgrade solution, provides an automatic upgrade of Communication Manager and associated devices, such as Gateways, TN boards, and media modules from a single view. You can upgrade Communication Manager from release 5.x to 5.2.1, 5.2.1 to Release 6.3.6, and 6.x to Release 6.3.6. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

For System Manager Release 6.3.10, you must deploy System Platform and Communication Manager 6.3.x template manually. After System Manager Release 6.3.10, Avaya will introduce an

automated process to upgrade from Communication Manager Release 5.2.1 to Communication Manager Release 6.3.6.

Using Software Management from the System Manager web console, you can perform the following:

- Get inventory: To get the inventory that you need for upgrading Communication Manager. For example, Communication Manager, gateways, media modules, and TN boards.
- Analyze software: To analyze whether the elements and components are on the latest release and to identify whether a new software is available for the inventory that you collected.
- Download files: To download files that are required for upgrading elements and components.

  You can download a new release from Avaya PLDS to the software file library and use the release to upgrade the device software.
- Preupgrade check: To ensure that conditions for successful upgrade are met. For example, if the hardware is supported by the new release, the RAID battery is sufficient, the bandwidth is sufficient, and if the files are downloaded.
- Schedule an upgrade sequence to upgrade all associated devices in a hierarchy, such as Communication Manager, Gateways, and TN boards in a flow by using job sequencing.
- Perform System Platform-based upgrades.
- Perform VMware or System Platform-based updates.

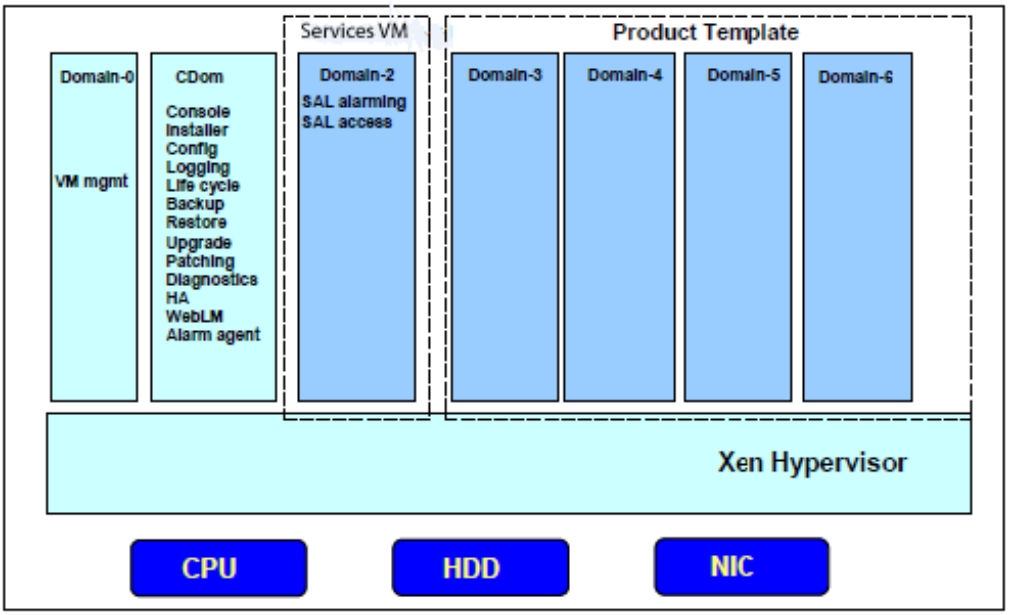
System Platform overview

Avaya Aura® System Platform technology delivers simplified deployment of Unified Communications and Contact Center applications. This framework leverages virtualization technology, predefined templates, common installation, licensing, and support infrastructure.

System Platform:

- is a software platform running CentOS plus Xen open source hypervisor for virtual machine monitoring and management
- hosts one or more Avaya products, each running on its own virtual server (virtual machine), all running on a single physical server platform
- provides a set of utilities commonly required for Avaya products, including installation, upgrade, backup/restore, licensing server, hardware monitoring and alarming, and remote access

The following figure shows an abstraction of the System Platform virtualized environment:



Avaya deploys System Platform through a *virtual appliance* model. The model includes:

- An Avaya-defined common server platform
- An Operating System (O/S) for allocating and managing server hardware resources (CPU, memory, disk storage, and network interfaces) among virtual machine instances running on the server platform
- System Platform
- An Avaya solution template containing a bundled suite of pre-integrated Avaya software applications
- A Secure Access Gateway, supporting a Secure Access Link (SAL) for remote diagnosis by Avaya or an Avaya Partner.

Advantages of System Platform

Advantages of System Platform include:

- Consolidation of servers
- Simpler maintenance
- Faster disaster recovery
- Easy installation of any Avaya Aura® solution template (bundled applications suite) on a single server platform
- Simpler and faster deployment of applications and solutions
- Efficient licensing of applications and solutions
- Security
- Portability of applications
- Reduction of operating costs

- Avaya common look-and-feel Web Console (Web Graphical User Interface) for server, virtual machine, application, and overall solution management.
- Remote access and automated alarm reporting for Network Management Systems monitored by Avaya Services and Avaya Partners personnel
- Coordinated backup and restore
- Coordinated software upgrades

Communication Manager deployment options

Communication Manager installation on System Platform

The Communication Manager installation process consists of:

- Identifying or procuring necessary hardware, software, and other equipment
- Installing the necessary hardware and equipment
- Installing Avaya Aura® System Platform on the server
- Installing the appropriate Communication Manager template on the server
- Configuring the applications on the template, including Communication Manager, Communication Manager Messaging, and Branch Session Manager
- Completing the post installation verification tasks

If Communication Manager is not running as an application in your enterprise, perform the installation. You must also install Communication Manager if one or more of your current Communication Manager executable files are corrupted.

You must upgrade Communication Manager when a new release is available. To start using the new release, shut down Communication Manager, replace the executable files with the new files, and restart Communication Manager.

For information about the upgrade process, see *Upgrading Servers to Avaya Aura® Communication Manager Templates*.

Communication Manager installation in VMware environment

You can install Communication Manager Release 6.2 and later as an Open Virtualization Program (OVA) on VMware vSphere 5.0, 5.1 or 5.5. The Communication Manager VMware virtualization environment is packaged as a virtual appliance ready for deployment on VMware certified hardware.

For more information about deploying Communication Manager on VMware, see *Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment*.

Communication Manager templates overview

Communication Manager as a template is a virtualized version that runs on System Platform. The Communication Manager template image has all the features that Communication Manager supports whether the image is on a duplicated server or a branch server. The templates support Communication Manager duplication on HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620 Server.

Note:

The Communication Manager installation and administration Web pages refer to Survivable Core as Enterprise Survivable Server (ESS) and Survivable Remote as Local Survivable Processor (LSP) respectively.

The Communication Manager templates are available in two categories: Communication Manager for Main/Survivable Core and Communication Manager for Survivable Remote.

Table 2: Applications and servers supported with Communication Manager Main and Survivable Core templates

Template name	Filename	Applications	Supported servers
Simplex CM Main/ Survivable Core	`CM_Simplex.ovf`	• Communication Manager • Communication Manager Messaging • Utility Services	• HP ProLiant DL360 G7 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R610 • Dell™ PowerEdge™ R620 • S8800
Duplex CM Main/ Survivable Core	`CM_Duplex.ovf`	• Communication Manager	• HP ProLiant DL360 G7 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R610 • Dell™ PowerEdge™ R620 • S8800
Main embedded version	`CM_onlyEmbed.ovf`	• Communication Manager • Communication Manager Messaging • Utility Services	• S8300D

Table 3: Applications and servers supported with Communication Manager Survivable Remote templates

Template Name	Filename	Applications	Supported Servers
Simplex Survivable Remote	`CM_SurvRemote.ovf`	• Communication Manager • Branch Session Manager	• HP ProLiant DL360 G7 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R610

Table continues…

Template Name	Filename	Applications	Supported Servers
		• Utility Services	• Dell™ PowerEdge™ R620 • S8800 • S8510 **Note:** You can install Simplex Survivable Remote on an HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620 Server. You can install Simplex Survivable Remote on an S8510 Server with 8-Gb memory as an upgrade only.
Embedded Survivable Remote	`CM_SurvRemoteEmbed.ovf`	• Communication Manager • Branch Session Manager • Utility Services	• S8300D **Note:** You can install Embedded Survivable Remote on S8300D Server in a G250, G350, G430, G450, or G700 Branch Gateway.

Supported platform for survivable servers

The following table defines the platforms that you can configure as a survivable remote server or survivable core server.

Important:

Beginning from Release 6.3, you can upgrade the servers from the existing platform to VMware.

Primary server	Survivable servers			
	System Platform S8300D	System Platform S8510	System Platform S8800, HP DL360 G7, Dell R610, HP DL360 G8, or Dell R620	
			Simplex	Duplex
Simplex System Platform	Survivable remote	Not applicable	Not applicable	Not applicable

Table continues…

Primary server	Survivable servers			
S8300D				
Simplex System Platform S8510	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Not applicable
Simplex System Platform S8800	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Not applicable
Duplex System Platform S8800	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Survivable core
Simplex System Platform HP DL360 G7	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Not applicable
Simplex System Platform Dell R610	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Not applicable
Duplex System Platform HP DL360 G7	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Survivable core
Duplex System Platform Dell R610	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Survivable core
Duplex System Platform HP DL360 G8	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Survivable core
Duplex System Platform Dell R620	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Survivable core

License file for Communication Manager

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager 6.0 and later. Earlier versions of Communication Manager, except Communication Manager 5.2.1 that is part of Avaya Aura® Midsize Business Template, continue to

use the Remote Feature Activation (RFA) online tool for license files. Communication Manager 5.2.1 that is part of Avaya Aura® Midsize Business Template uses PLDS to manage licenses.

PLDS is an online, Web-based tool for managing license entitlements and electronic delivery of software and related license files.

After you obtain the license file, use WebLM to install the license file. WebLM is a Web-based application for managing licenses and is installed as part of System Platform in the Console Domain.

The license file is an Extensible Markup Language (XML) file. The license file has the information regarding the product, major release, and license features and capacities.

For Communication Manager 6.0 and later, you must install license files for the Communication Manager main server, but not for survivable servers. Survivable servers receive licensing information from the main server.

A 30-day grace period applies to new installations or upgrades to Communication Manager 6.0, Collaboration Server, and Solution for Midsize Enterprise. You have 30 days from the day of installation to install a license file.

Duplicated server licensing

For a duplicated pair configuration on System Platform Console Domain WebLM, you must install the license file on both servers. The system does not synchronize the license file from active server with standby server. To activate a Communication Manager license file for a duplicated pair, provide the WebLM host ID for both servers. The license file that the system generates includes both host IDs. You must install that license file on both servers in the duplicated pair.

However, if you are using System Manager WebLM or WebLM virtual application for licensing a duplicated pair configuration, you do not need to install the license file on both servers. To activate a Communication Manager license file for a duplicated pair you do not need to provide host IDs on both servers.

Duplicated server licensing

On System Platform Console Domain WebLM, if you are licensing a duplicated pair configuration, you must install the license file on both servers. The system does not synchronize the license file from active server to standby server.

When you activate a Communication Manager license file for a duplicated pair in PLDS, you must provide the WebLM host ID for both servers. The license file that the system generates includes both host IDs. You must install that license file on both servers in the duplicated pair.

If you are using System Manager WebLM or WebLM virtual application for licensing a duplicated pair configuration, you do not need to install the license file on both servers. To activate a Communication Manager license file for a duplicated pair you do not need to provide host IDs on both servers.

Authentication files for Communication Manager

The authentication file contains Access Security Gateway (ASG) keys and the server certificate for Communication Manager. With the ASG keys, Avaya Services can securely gain access to the customer system.

System Platform and Communication Manager share the same authentication file. The system installs a default authentication file with System Platform. However, you must replace the default file with a unique file. The Authentication File System (AFS) creates unique authentication files. AFS is an online application that you can download from http://rfa.avaya.com.

Authentication files for duplicated servers and survivable servers

For duplicated pair configurations, you must install the same authentication file on both the active server and standby server. The system does not automatically synchronize the authentication file from active server to standby server.

Each survivable server must have its own unique authentication file. You must install a unique file from the System Platform Web Console of each server.

About the authentication file

AFS authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate.

Each authentication file contains an authentication file ID (AFID) that identifies the file. You need this AFID to create a new authentication file for an upgrade or to replace the current authentication file on the server.

Security enhancements

With the Communication Manager Release 6.3.6 security service patch, you can receive and validate the certificate that uses the SHA-2 signing algorithm and 2048 bit RSA keys. Using Communication Manager System Management Interface, you can import the third-party trusted certificate that uses the SHA-2 signing algorithm.

Note:

To obtain the security service pack details, go to the Avaya Support website at http://support.avaya.com.

For information about certificates, see *Avaya Aura® Communication Manager Security Design*, 03-601973 and *Administering Avaya Aura® Communication Manager*, 03-300509.

Use of third-party certificates

Many companies use third-party certificates for security. You cannot retain the third-party certificates as a part of the upgrade dataset, you must reinstall the third-party certificates after the upgrade. If you use third-party certificates, keep a copy or download new third-party certificates before you start the upgrade process.

Upgrade paths

The following table provides the supported upgrade paths from various releases of Communication Manager to Release 6.3.6.

Note:

- You cannot upgrade some servers to Release 4.0.5 or Release 5.2.1 directly. You must upgrade to Release 4.0.5 or Release 5.2.1 on a supported server before you complete the Communication Manager upgrade to Release 6.3.6.
- You can also upgrade Communication Manager from earlier releases to Release 6.3.6 on VMware vSphere™ 5.0, 5.1, or 5.5Virtualized Environment.

  For instructions to upgrade Communication Manager to Release 6.3.6 in the Avaya Aura® Virtualized Environment, see *DeployingAvaya Aura® Communication Manager on VMware® in Virtualized Environment*.

Release	Requirement
Release 1.x.x on DEFINITY R	Restore translations to a HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620 server on Release 6.3.6.
Release 2.x on DEFINITY SI	Restore translations to an S8300D, HP ProLiant DL360p G8, or Dell™ PowerEdge™ R620 server on Release 6.3.6.
Release 3.x.x on DEFINITY CSI	Restore translations to an S8300D, HP ProLiant DL360p G8, or Dell™ PowerEdge™ R620 server on Release 6.3.6.
Release 1.x.x on S8300A	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.3.6.
Release 1.x.x on S8700	Upgrade to Release 4.0.5 before you upgrade to Release 6.2.1 on HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620.
Release 2.x.x on S8300A	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.3.6.
Release 2.x.x on S8500A, S8700, S8710 wDAL1	Upgrade to Release 4.0.5 with memory upgrade before you upgrade to Release 6.3.6 on HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620.

Table continues…

Release	Requirement
	For S8710, upgrade to Release 5.2.1, before you upgrade to Release 6.3.6 on HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620, you do not require to upgrade the memory.
Release 2.x.x on all other servers	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.3.6.
Release 3.x.x on S8500A, S8700, S8710/S8720 wDAL1	Upgrade to Release 4.0.5 and then upgrade to a HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620 server on Release 6.3.6.
Release 3.x.x on all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.3.6.
Release 4.x.x on S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620 server on Release 6.3.6.
Release 4.x.x on all other servers	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.3.6.
Release 5.0.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.3.6.
Release 5.1.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.3.6.
Release 5.2.1	Install a preupgrade service pack before you upgrade to Release 6.3.6.
Release 6.0.x, 6.2, or 6.3.x	Upgrade software-only to Release 6.3.6.

Support for SIP Enablement Services

SIP Enablement Services is not compatible with Communication Manager Release 6.x. If you upgrade Communication Manager with SIP Enablement Services Release 5.2.1 or earlier to Release 6.x, you must install Avaya Aura® Session Manager for continued support of SIP stations and adjuncts. For Session Manager options, contact an Avaya salesperson.

Special circumstances

Consider the following special situations when upgrading Communication Manager to Release 6.x.

- If you have Communication Manager Messaging or Intuity Audix 770 enabled on the existing system, backup and restore that dataset separately on the upgraded system.
- If you have Communication Manager and SIP Enablement Services (SES) coresident on the S8300 Server, you cannot restore SES on the new server because Communication Manager Release 6.x does not support SES.

- If you have SES on the existing system and want to use the same SIP signaling group for Session Manager:
  - To edit the **Peer Server** field, set the **Peer Detection Enabled** field to `n`. By default, the system sets the **Peer Detection Enabled** field to `y` .
  - In the **Peer Server** field, enter `SM` or `Others`.
- If the existing system has SIP integrated Modular Messaging, the upgrade process automatically prefixes a + character to the phone number.

  Important:

  You must remove the + character manually from the phone number. For instructions, see *Messaging Application Server (MAS) Administration Guide*.
- If you use Unicode phone messages on the existing system, reinstall the Unicode phone messages file after the upgrade.

Preupgrade requirements

Make sure that you:

- Place an order for all the hardware. The hardware must be available onsite.
- Download all the software and service packs.
- Have the applications you need on the computer you will use to perform the upgrade.
- Identify a server with adequate disk space to store the datasets.
- Obtain the updated translations from the STS team. You require the updated translations for DEFINITY Server upgrades only.

Hardware requirements

- HP ProLiant DL360p G8 or Dell™ PowerEdge™ R620 Server to replace an existing standalone server that you cannot upgrade to Release 6.3.6
- S8300D Server to replace an existing embedded server that you cannot upgrade to Release 6.3.6
- Release 6.0 Migration Kit for S8510 Server, S8800 Server, HP DL360 G7, or Dell R610 to reuse the existing servers
- Required Ethernet CAT5 cables
- Five blank DVDs on which you burn the iso images.

Software requirements

Download the following software from the appropriate website:

- System Platform from PLDS
- The Communication Manager templates from PLDS

- The license file from PLDS. Obtain the MAC address from System Platform Web Console Domain, as displayed on the Server Properties page of the WebLM server.
- The authentication or password file from the Authentication File System (AFS)
- Preupgrade and postupgrade service packs from the Avaya Support website at http://support.avaya.com.

Application requirements

Install the following applications on your computer:

- Internet Explorer 7.x or 8.x browser
- Firefox 3.6 or later browser. Only System Platform supports this browser.
- A Secure Shell application such as PuTTY.

Upgrade order

If Communication Manager is part of Avaya Aura®, perform the upgrade in the following order:

1. Endpoints
2. Avaya Aura® System Manager
3. Avaya Aura® Session Manager
4. Survivable remote servers (Communication Manager and System Manager)
5. Branch gateways, formerly known as media gateways
6. Survivable core servers
7. Communication Manager, configured as feature servers and evolution servers

Upgrade process

The following list provides the key upgrade sequence for upgrade paths that start with a server running Communication Manager Release 4.0.5 and Release 5.2.1.

1. Communication Manager on any survivable remote server
2. Latest firmware on all Avaya H.248 Branch Gateway
3. Latest firmware on the media modules within the H.248 Branch Gateway
4. Communication Manager on any survivable core server
5. Latest firmware on all TN circuit packs if you are using port networks
6. Communication Manager on the main server
7. Latest firmware on all telephones

If you are upgrading Communication Manager from Release 6.0.1 or 6.2, on the survivable remote template or survivable remote embed template, the system displays the following screens. Provide the information in the appropriate fields:

- Network Settings
- Customer Login
- DHCP Basic settings
- Branch Session Manager

Important:

The system displays the screens only for the survivable remote and the survivable remote embedded template upgrades. The system does not display the screen when you upgrade the other simplex main and duplex templates.

Click **Install** and **Finish** to complete the upgrade and install the Communication Manager patches.

When you replace the server, verify the general tasks you complete on a simplex server from the following checklist:

Task	Notes	√
Ensure that the site has the server and other hardware.		
Get the required software and preupgrade and postupgrade service packs.		
Ensure that you have the server and disk space available to back up the upgrade data set. You cannot use a flashcard to restore files to System Platform.		
Keep the required documentation and release notes handy.		
For DEFINITY Servers: • Save and freeze translations. • Send the translations to the STS team a few weeks before the upgrade and obtain the updated translations from STS.		
Record the IP addresses and other data on the existing server that you need to install System Platform and Communication Manager.	Use the worksheets provided in appendices to make sure that you capture all the required information.	
Convert private control networks to the corporate LAN.	Release 6.x does not support private networks (CNA and CNB). For instructions, see Converting private control networks to corporate LAN on page 1403.	
Complete the routine preupgrade tasks on the existing server.		

Table continues…

Task	Notes	√
If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system. If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system. The upgrade fails if you do not disable or configure Messaging or Communication Manager Messaging.		
Back up all files on the existing server if you need to roll back to the original release.		
Install the preupgrade service pack on the existing server.	**Important:** To roll back the upgrade, you must deactivate the preupgrade patch.	
Create the backup of the Communication Manager data set to be restored on the new server.		
Create the backup of the Communication Manager Messaging data set that you will restore on the new server if messaging is enabled.		
For a standalone server, shut down the existing server and remove all power cords and cables. For an embedded server, remove all cables from the faceplate, shut down the existing server, and remove the server from the H.248 Branch Gateway.		
Install one of the following servers in the rack and connect the power cord and cables: • HP DL360 G8 Server • Dell R620 Server • S8300D Server. Install this embedded server in a branch gateway.	You can install a new server before completing the tasks on the existing server.	
Install System Platform on the server.	On the new server, you can install System Platform before completing the tasks on the existing server.	
Get the license file from the PLDS website at https://plds.avaya.com. Install the file on the WebLM server.	On the new server, you can perform the step before completing the tasks on the existing server.	
Using System Platform Web Console, get the authentication file from AFS and install the file.	On the new server, you can perform the step before completing the tasks on the existing server.	

Table continues…

Task	Notes	√
Using System Platform Web Console, install the appropriate Communication Manager Release 6.3 template.	On the new server, you can perform the step before completing the tasks on the existing server.	
Using System Platform Web Console, install the Release 6.3.6 service pack.		
Using System Platform Web Console, restore the Communication Manager dataset.		
Using System Management Interface, configure Communication Manager		
Restart the server by using System Platform Web Console or System Management Interface. **Important:** Check the status of other devices and applications that depend on Communication Manager, such as Call Management System (CMS) and Call Center. After you complete the Communication Manager upgrade, reboot the applications if required.		
Using System Management Interface, restore the Communication Manager Messaging data set.		
Configure Communication Manager Messaging.		
Complete the postupgrade administration.		
Create a backup of all the files.		
Register the upgraded system.		

Using the Upgrading to Communication Manager Release 6.3.6 book

This book is organized by the Communication Manager template and then by the existing server.

To upgrade Communication Manager Release 5.2.1 on an S8500 Server to the main simplex template on an HP ProLiant DL360p G8 Server, see Upgrading S8500 Server to the HP ProLiant DL360p G8 Server in Upgrading to simplex main/survivable template.

Chapter 2: Upgrading from Release 6.0.x or later to Release 6.3.6

Upgrading from Release 6.0.x or later to 6.3.6 on the simplex template

Introduction

This section describes the procedure to upgrade the Communication Manager software from Release 6.0.x or 6.2.x to Release 6.3.6 on the server running System Platform and the simplex main/survivable core template (CM_Simplex).

To perform this software-only upgrade, use one of the following methods:

- Onsite by connecting the laptop to the services port on the server
- Remotely by gaining access to the server through the corporate network

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Backing up translations, security, and system files.
- Upgrading System Platform and the Communication Manager template.
- Performing the verification tasks.
- Performing the upgrade to Release 6.3.6 as described in this section.

The upgrade procedure preserves Communication Manager translations, administrator accounts, Communication Manager Messaging files, and the server configuration. You do not require the following files during the upgrade:

- A new or updated license file
- An authentication file

Use this section to upgrade Communication Manager from Release 6.0.x or 6.2.x to Release 6.3.6 on:

- The main server
- The survivable server

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support website at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware

2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the existing system

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing System Management Interface

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.

2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

Back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

You back up the data using System Management Interface or System Platform Web Console.

Important:

If Communication Manager Messaging is enabled on your system, back up the messaging data using System Management Interface.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

   Note:

   You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

   - - https://<*IP_Address*>
   - https://<*FQDN*>

     Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Accessing the command line for System Domain

If you have physical access to the system, you can log in to the system directly. When you connect to the services port, you are connected to System Domain. You can also use an SSH (Secure Shell) client such as PuTTy to set up a remote connection from your computer. After logging in, the system prompts you with the Linux command prompt.

Note:

Administrators use the command line for System Domain to perform a small number of tasks. Access to the command line for System Domain is reserved for Avaya or Avaya Partners for troubleshooting.

Procedure

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of System Domain.

   Tip:

   You can get the IP address of Domain-0 from the Virtual Machine Management page of the Web Console. In the navigation pane of the Web Console, click **Virtual Machine Management** > **Manage**.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su – root`
6. Enter the password for the *root* user.

   Tip:

   To get to Console Domain from System Domain, type **`xm list`**, note the ID for *udom*, and then type **`xm console`** *`udom-id`*. When prompted, log in as `admin`. Then type **`su – root`** and enter the root password to log in as root.

   To exit Console Domain and return to System Domain, press `Control+]`.
7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit System Domain.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

System Platform backup

With some exceptions, you can back up configuration information for System Platform and the solution template (all template virtual machines).

Note:

The System Platform backup feature does not back up the following types of configuration data:

- System parameters (examples: SNMP Discovery, Template product ID)

- Networking parameters (examples: Template IP and host name, Console Domain IP and host name, static IP route configuration)
- Ethernet parameters (examples: Auto-negotiation, speed and port information)
- Security configuration (examples: SSH keys, Enable Advance password, Host access list)

  In scenarios where, for example, an administrator performs a system backup prior to a template or platform upgrade or platform replacement, and the system generates new unique SSH keys internally as part of the upgrade or replacement action. The SSH keys generated prior to the backup operation are of no use to the system updated or replaced.

System Platform backs up sets of data and combines them into a larger backup archive. Backup sets are related data items available for backup. When you perform a back up, the system executes the operation for all backup sets. All backup sets must succeed to produce a backup archive. If any of the backup set fails, then the system removes the backup archive. The amount of data backed up depends on the specific solution template.

The system stores the backup data in the `/vspdata/backup` directory in Console Domain. This is a default location. During an upgrade, the system does not upgrade the `/vspdata` folder, facilitating a data restore operation if required. You can change this location and back up the System Platform backup archives to a different directory in System Platform or in an external server. Optionally, send the backup data to an external e-mail address if the file size is smaller than 10 MB.

If a backup fails, the system automatically redirects to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup succeeds.

Important:

If you backup an instance of System Platform with not template installed, the server to which you restore the backup must also have no template installed. If any template is installed, the restore will fail.

Backups and restores across different versions of System Platform

You cannot restore an older version of System Platform from a backup created on a newer version of System Platform. For example, you cannot restore a System Platform 6.3 backup to System Platform 6.0. However, you can (for example), restore a System Platform 6.0 backup to System Platform 6.3, although not all templates support this ability. Confirm in your solution documentation whether or not the solution template supports restoring an older version of System Platform backup to the current version.

Utility Services settings and size of System Platform backups

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These settings apply to backups performed in Utility Services or in System Platform.

- **Include Firmware in Backup**: Use this option to create a complete backup file, which includes IP telephone firmware and Gateway firmware. Backup files are very large and take longer to generate.

- **Exclude Firmware in Backup**: Use this option to create a backup file that excludes IP telephone firmware and Gateway firmware. Backup files are smaller and are much faster to generate.

For more information about the backup and restore in Utility Services, see *Accessing and Managing Avaya Aura® Utility Services*.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        If you choose the **Full Backup** option, the resulting backup file does not include the datasets for any embedded applications, such as Communication Manager Messaging.
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**
          a. Select **Translations, Names, and Messages**.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, the system creates one or more `.tar` files.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `*.tar.gz` file to the location you specify in the **Directory** field.

6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the

language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:

   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Upgrade tasks

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

System Platform and Communication Manager upgrade

You must perform the upgrade of System Platform and Communication Manager, and install the latest service packs or patches in the following order:

- System Platform
- System Platform service pack as instructed in Installing patches
- Communication Manager
- Communication Manager service pack as instructed in Installing patches.

Related Links

Installing patches on page 51

Upgrading System Platform

Log on to System Platform Web Console.

Note:

After you upgrade System Platform, you must reconfigure the Communication Manager license server.

Procedure

1. In the left navigation pane, click **Server Management** > **Platform Upgrade**.
2. In the **Upgrade Platform From:** field, select a method you require to adopt.
3. Click **Search**.
4. Select the file to install for System Platform and click **Select**.
5. Click **Install**.
6. When the system prompts, click **Commit**.

   Note:

   If you fail to click **Commit**, the system rolls back to the existing release of System Platform.

- Install the service pack and patches for System Platform as instructed in Installing patches.
- If you upgrade from System Platform 6.0.3, configure SNMP version support on the Services virtual machine. For instructions, see *Upgrading Avaya Aura® System Platform*.
- If you upgrade from System Platform 6.2.x to Release 6.3.4, upgrade the Services virtual machine to version 3.0. For instructions, see *Upgrading Avaya Aura® System Platform*.
- Reconfigure the Communication Manager license server.

Related Links

Reconfiguring the Communication Manager license server on page 51
Installing patches on page 51

Reconfiguring the Communication Manager license server

Start an SSH session.

Procedure

At the prompt, type `weblmurl <ip address of license server>`.

By default, the system sets the IP address to the IP address of C-dom. If you use any other license server other C-dom, the system displays an error.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Upgrading the Communication Manager template

Log on to System Platform Web Console.

Procedure

1. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
2. Click **Upgrade**.
3. In the **Install Template From** field, select a method to gain access to the template file.
4. Select the Communication Manager template.

   If you are upgrading Communication Manager from Release 6.0.1 or 6.2, on the survivable remote template or survivable remote embed template, the system displays the following screens. Provide the information in the appropriate fields:

   - Network Settings
   - Customer Login

- DHCP Basic settings
- Branch Session Manager

Important:

The system displays the screens only for the survivable remote and the survivable remote embedded template upgrades. The system does not display the screen when you upgrade the other simplex main and duplex templates.

Click **Install** and **Finish** to complete the upgrade and install the Communication Manager patches.

5. Click **Upgrade**.
6. When the system prompts, click **Commit Installation**.

Note:

If you fail to click **Commit Installation**, Communication Manager remains in the current state until you click **Commit Installation**. To stay at the current Communication Manager release, click **Rollback Installation**.

The system automatically performs the following:

- Creates a back up of Communication Manager.
- Installs new Communication Manager.
- Restores Communication Manager from the backed up data.

Install the service pack and patches for Communication Manager as instructed in Installing patches.

Related Links

Installing patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.

6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system

Start a SAT session.

Procedure

Enter `list station` and verify that the stations listed after the upgrade are the same as the stations listed before the upgrade.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading from Release 6.0.x or later to 6.3.6 on duplex template

Introduction

This section describes the procedure to upgrade Communication Manager software from Release 6.0 or later to Release 6.3.6 on the servers running System Platform and the duplex CM main/survivable template (CM_Duplex).

The upgrade procedure involves:

- Backing up translations, security, and system files.
- Upgrading System Platform and the Communication Manager template.
- Performing the verification tasks.
- Performing the upgrade to Release 6.3.6 as described in this section.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and the server configuration. You do not require the following files during the upgrade:

- A new or an updated license file
- An authentication file

Use this section to upgrade Communication Manager from Release 6.0 or later to Release 6.3.6 on:

- The main server
- The survivable server

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support website at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the active server

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing System Management Interface

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

Back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

You back up the data using System Management Interface or System Platform Web Console.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

   Note:

   You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

   - - https://<*IP_Address*>
   - https://<*FQDN*>

     Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are

significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Connection preservation during an upgrade

When you upgrade within the same release, for example, from Release 6.3 to Release 6.3.6, Communication Manager preserves the following connections:

- The audio portion of many stable telephone calls throughout the upgrade.

- The data transmission between many stable fax, data, or multimedia endpoints.

Communication Manager does not preserve the following connections during an upgrade:

- H.323 IP trunks
- SIP trunks

  For example, trunks established for SIP endpoints that use Communication Manager and Session Manager for SIP connections.
- ISDN-BRI trunks or stations
- Unstable calls

  For example, calls that are in the ringing or dialing stage, calls that are on hold, or calls in any state that require control signaling. The system drops unstable calls, regardless of whether the calls carry voice or data transmissions.
- SAT sessions
- Adjunct links

  For example, links to a CMS, ASAI, or CDR adjunct, a link to a system printer, or any other links that are configured by using the IP Services screen.

Activating the connection preservation during an upgrade

Log on to the server using System Management Interface.

- If onsite, connect to the Services port on the back of the active server.
- If offsite, log on to Communication Manager using the IP address of Communication Manager.

Preserve connections immediately after you perform all standard preupgrade tasks.

Procedure

1. Click **Server Upgrade** > **Pre Upgrade Step**.
2. On the Pre Update/Upgrade Step window, click **Continue** to start the preupgrade process.

   The system displays the status of the preupgrade operations.

As the system locks the translations on the active server, the standby server precisely synchronizes translations and preserves connections during the interchange. When the upgrade is complete, the translations are unlocked and the normal synchronization process resumes.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Preupgrade tasks on the standby server

Accessing System Management Interface

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.

2. In your browser, choose one of the following options depending on server configuration:

   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

   - Portable computer access by IP address

     To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the

ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.

4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

Back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

You back up the data using System Management Interface or System Platform Web Console.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

   Note:

   You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

   - - https://<*IP_Address*>
   - https://<*FQDN*>

     Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Busying out the standby server

Log on to System Management Interface of the standby server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Log in as `craft` or `dadmin`.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

Upgrade tasks on the standby server

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

System Platform and Communication Manager upgrade

You must perform the upgrade of System Platform and Communication Manager, and install the latest service packs or patches in the following order:

- System Platform
- System Platform service pack as instructed in Installing patches
- Communication Manager
- Communication Manager service pack as instructed in Installing patches.

Related Links

Installing patches on page 51

Upgrading System Platform

Log on to System Platform Web Console.

Note:

After you upgrade System Platform, you must reconfigure the Communication Manager license server.

Procedure

1. In the left navigation pane, click **Server Management** > **Platform Upgrade**.
2. In the **Upgrade Platform From:** field, select a method you require to adopt.
3. Click **Search**.
4. Select the file to install for System Platform and click **Select**.
5. Click **Install**.
6. When the system prompts, click **Commit**.

   Note:

   If you fail to click **Commit**, the system rolls back to the existing release of System Platform.

- Install the service pack and patches for System Platform as instructed in Installing patches.
- If you upgrade from System Platform 6.0.3, configure SNMP version support on the Services virtual machine. For instructions, see *Upgrading Avaya Aura® System Platform*.
- If you upgrade from System Platform 6.2.x to Release 6.3.4, upgrade the Services virtual machine to version 3.0. For instructions, see *Upgrading Avaya Aura® System Platform*.
- Reconfigure the Communication Manager license server.

Related Links

Reconfiguring the Communication Manager license server on page 51
Installing patches on page 51

Reconfiguring the Communication Manager license server

Start an SSH session.

Procedure

At the prompt, type `weblmurl <ip address of license server>`.

By default, the system sets the IP address to the IP address of C-dom. If you use any other license server other C-dom, the system displays an error.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**

- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.

4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Upgrading the Communication Manager template

Log on to System Platform Web Console.

Procedure

1. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
2. Click **Upgrade**.
3. In the **Install Template From** field, select a method to gain access to the template file.
4. Select the Communication Manager template.

   If you are upgrading Communication Manager from Release 6.0.1 or 6.2, on the survivable remote template or survivable remote embed template, the system displays the following screens. Provide the information in the appropriate fields:

   - Network Settings
   - Customer Login
   - DHCP Basic settings
   - Branch Session Manager

   Important:

   The system displays the screens only for the survivable remote and the survivable remote embedded template upgrades. The system does not display the screen when you upgrade the other simplex main and duplex templates.

   Click **Install** and **Finish** to complete the upgrade and install the Communication Manager patches.
5. Click **Upgrade**.
6. When the system prompts, click **Commit Installation**.

   Note:

   If you fail to click **Commit Installation**, Communication Manager remains in the current state until you click **Commit Installation**. To stay at the current Communication Manager release, click **Rollback Installation**.

The system automatically performs the following:

- Creates a back up of Communication Manager.
- Installs new Communication Manager.
- Restores Communication Manager from the backed up data.

Install the service pack and patches for Communication Manager as instructed in Installing patches.

Related Links

Installing patches on page 51

Verifying Communication Manager operation

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay

4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Server role interchange

When the standby server is ready, from System Management Interface, interchange the roles of the standby and active servers.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrade tasks on the standby server that was active before the interchange

Tasks on the standby server

On the server that was formerly active and changed to the standby state after the server roles interchange, perform the following procedures:

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

   Note:

   You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

   - - https://<*IP_Address*>
   - https://<*FQDN*>

     Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Busying out the standby server

Log on to System Management Interface of the standby server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Log in as `craft` or `dadmin`.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

System Platform and Communication Manager upgrade

You must perform the upgrade of System Platform and Communication Manager, and install the latest service packs or patches in the following order:

- System Platform
- System Platform service pack as instructed in Installing patches
- Communication Manager
- Communication Manager service pack as instructed in Installing patches.

Related Links

Installing patches on page 51

Upgrading System Platform

Log on to System Platform Web Console.

Note:

After you upgrade System Platform, you must reconfigure the Communication Manager license server.

Procedure

1. In the left navigation pane, click **Server Management** > **Platform Upgrade**.
2. In the **Upgrade Platform From:** field, select a method you require to adopt.
3. Click **Search**.
4. Select the file to install for System Platform and click **Select**.
5. Click **Install**.
6. When the system prompts, click **Commit**.

   Note:

   If you fail to click **Commit**, the system rolls back to the existing release of System Platform.

- Install the service pack and patches for System Platform as instructed in Installing patches.

- If you upgrade from System Platform 6.0.3, configure SNMP version support on the Services virtual machine. For instructions, see *Upgrading Avaya Aura® System Platform*.
- If you upgrade from System Platform 6.2.x to Release 6.3.4, upgrade the Services virtual machine to version 3.0. For instructions, see *Upgrading Avaya Aura® System Platform*.
- Reconfigure the Communication Manager license server.

Related Links

Reconfiguring the Communication Manager license server on page 51
Installing patches on page 51

Reconfiguring the Communication Manager license server

Start an SSH session.

Procedure

At the prompt, type `weblmurl <ip address of license server>`.

By default, the system sets the IP address to the IP address of C-dom. If you use any other license server other C-dom, the system displays an error.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Upgrading the Communication Manager template

Log on to System Platform Web Console.

Procedure

1. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
2. Click **Upgrade**.

3. In the **Install Template From** field, select a method to gain access to the template file.
4. Select the Communication Manager template.

   If you are upgrading Communication Manager from Release 6.0.1 or 6.2, on the survivable remote template or survivable remote embed template, the system displays the following screens. Provide the information in the appropriate fields:

   - Network Settings
   - Customer Login
   - DHCP Basic settings
   - Branch Session Manager

   Important:

   The system displays the screens only for the survivable remote and the survivable remote embedded template upgrades. The system does not display the screen when you upgrade the other simplex main and duplex templates.

   Click **Install** and **Finish** to complete the upgrade and install the Communication Manager patches.
5. Click **Upgrade**.
6. When the system prompts, click **Commit Installation**.

   Note:

   If you fail to click **Commit Installation**, Communication Manager remains in the current state until you click **Commit Installation**. To stay at the current Communication Manager release, click **Rollback Installation**.

   The system automatically performs the following:

   - Creates a back up of Communication Manager.
   - Installs new Communication Manager.
   - Restores Communication Manager from the backed up data.

Install the service pack and patches for Communication Manager as instructed in Installing patches.

Related Links

Installing patches on page 51

Verifying the Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the active server running Release 6.3.6

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

   Note:

   You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

   - - https://<*IP_Address*>
   - https://<*FQDN*>

     Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the standby server running Release 6.3.6

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

   Note:

   You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

   - - https://<*IP_Address*>
   - https://<*FQDN*>

     Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading from Release 6.0.x or later to 6.3.6 on embedded main template

Introduction

This section describes the procedure to upgrade the Communication Manager software from Release 6.0 or later to Release 6.3.6 on the S8300D Server running System Platform and the embedded main template, CM_OnlyEmbed.

To perform this software-only upgrade, use one of the following methods:

- Onsite by connecting the laptop to the services port on the server
- Remotely by gaining access to the server through the corporate network

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Backing up translations, security, and system files.
- Upgrading System Platform and the Communication Manager template.
- Performing the verification tasks.
- Performing the upgrade to Release 6.3.6 as described in this section.

Important:

To use this section to upgrade the Communication Manager software from Release 6.0 or later to Release 6.3.6 on the S8300D Server running the embedded survivable remote template, CM_SurvRemoteEmbed, skip the following procedures:

- Communication Manager Messaging backup through Shutting down Communication Manager Messaging
- Verifying the Communication Manager Messaging test data through Backing up Communication Manager Messaging

The upgrade procedure preserves Communication Manager translations, administrator accounts, Communication Manager Messaging files, and the server configuration. You do not require the following files during the upgrade:

- A new or an updated license file
- An authentication file

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that you have the service packs and patches for the following software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Preupgrade tasks on the existing system

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing System Management Interface

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

Back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

You back up the data using System Management Interface or System Platform Web Console.

Important:

If Communication Manager Messaging is enabled on your system, back up the messaging data using System Management Interface.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

   Note:

   You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

   - - https://<*IP_Address*>

- https://<*FQDN*>

  Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Accessing the command line for System Domain

If you have physical access to the system, you can log in to the system directly. When you connect to the services port, you are connected to System Domain. You can also use an SSH (Secure Shell) client such as PuTTy to set up a remote connection from your computer. After logging in, the system prompts you with the Linux command prompt.

Note:

Administrators use the command line for System Domain to perform a small number of tasks. Access to the command line for System Domain is reserved for Avaya or Avaya Partners for troubleshooting.

Procedure

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of System Domain.

   Tip:

   You can get the IP address of Domain-0 from the Virtual Machine Management page of the Web Console. In the navigation pane of the Web Console, click **Virtual Machine Management** > **Manage**.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su – root`
6. Enter the password for the *root* user.

Tip:

To get to Console Domain from System Domain, type **xm list**, note the ID for *udom*, and then type **xm console** *udom-id*. When prompted, log in as admin. Then type **su – root** and enter the root password to log in as root.

To exit Console Domain and return to System Domain, press Control+].

7. After performing the necessary tasks, type exit to exit root login.
8. Type exit again to exit System Domain.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the /vspdata/backup/archive directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.

6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

System Platform backup

With some exceptions, you can back up configuration information for System Platform and the solution template (all template virtual machines).

Note:

The System Platform backup feature does not back up the following types of configuration data:

- System parameters (examples: SNMP Discovery, Template product ID)
- Networking parameters (examples: Template IP and host name, Console Domain IP and host name, static IP route configuration)
- Ethernet parameters (examples: Auto-negotiation, speed and port information)
- Security configuration (examples: SSH keys, Enable Advance password, Host access list)

  In scenarios where, for example, an administrator performs a system backup prior to a template or platform upgrade or platform replacement, and the system generates new unique SSH keys internally as part of the upgrade or replacement action. The SSH keys generated prior to the backup operation are of no use to the system updated or replaced.

System Platform backs up sets of data and combines them into a larger backup archive. Backup sets are related data items available for backup. When you perform a back up, the system executes the operation for all backup sets. All backup sets must succeed to produce a backup archive. If any of the backup set fails, then the system removes the backup archive. The amount of data backed up depends on the specific solution template.

The system stores the backup data in the `/vspdata/backup` directory in Console Domain. This is a default location. During an upgrade, the system does not upgrade the `/vspdata` folder, facilitating a data restore operation if required. You can change this location and back up the System Platform backup archives to a different directory in System Platform or in an external server. Optionally, send the backup data to an external e-mail address if the file size is smaller than 10 MB.

If a backup fails, the system automatically redirects to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup succeeds.

Important:

If you backup an instance of System Platform with not template installed, the server to which you restore the backup must also have no template installed. If any template is installed, the restore will fail.

Backups and restores across different versions of System Platform

You cannot restore an older version of System Platform from a backup created on a newer version of System Platform. For example, you cannot restore a System Platform 6.3 backup to System Platform 6.0. However, you can (for example), restore a System Platform 6.0 backup to System Platform 6.3, although not all templates support this ability. Confirm in your solution documentation whether or not the solution template supports restoring an older version of System Platform backup to the current version.

Utility Services settings and size of System Platform backups

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These settings apply to backups performed in Utility Services or in System Platform.

- **Include Firmware in Backup**: Use this option to create a complete backup file, which includes IP telephone firmware and Gateway firmware. Backup files are very large and take longer to generate.
- **Exclude Firmware in Backup**: Use this option to create a backup file that excludes IP telephone firmware and Gateway firmware. Backup files are smaller and are much faster to generate.

For more information about the backup and restore in Utility Services, see *Accessing and Managing Avaya Aura® Utility Services*.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        If you choose the **Full Backup** option, the resulting backup file does not include the datasets for any embedded applications, such as Communication Manager Messaging.
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.

b. Select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**
     a. Select **Translations, Names, and Messages**.

3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, the system creates one or more `.tar` files.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `*.tar.gz` file to the location you specify in the **Directory** field.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:

   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.

5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Upgrade tasks

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

System Platform and Communication Manager upgrade

You must perform the upgrade of System Platform and Communication Manager, and install the latest service packs or patches in the following order:

- System Platform
- System Platform service pack as instructed in Installing patches
- Communication Manager
- Communication Manager service pack as instructed in Installing patches.

Related Links

Installing patches on page 51

Upgrading System Platform

Log on to System Platform Web Console.

Note:

After you upgrade System Platform, you must reconfigure the Communication Manager license server.

Procedure

1. In the left navigation pane, click **Server Management** > **Platform Upgrade**.

2. In the **Upgrade Platform From:** field, select a method you require to adopt.
3. Click **Search**.
4. Select the file to install for System Platform and click **Select**.
5. Click **Install**.
6. When the system prompts, click **Commit**.

   Note:

   If you fail to click **Commit**, the system rolls back to the existing release of System Platform.

- Install the service pack and patches for System Platform as instructed in Installing patches.
- If you upgrade from System Platform 6.0.3, configure SNMP version support on the Services virtual machine. For instructions, see *Upgrading Avaya Aura® System Platform*.
- If you upgrade from System Platform 6.2.x to Release 6.3.4, upgrade the Services virtual machine to version 3.0. For instructions, see *Upgrading Avaya Aura® System Platform*.
- Reconfigure the Communication Manager license server.

Related Links

Reconfiguring the Communication Manager license server on page 51
Installing patches on page 51

Reconfiguring the Communication Manager license server

Start an SSH session.

Procedure

At the prompt, type `weblmurl <ip address of license server>`.

By default, the system sets the IP address to the IP address of C-dom. If you use any other license server other C-dom, the system displays an error.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**

- **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Upgrading the Communication Manager template

Log on to System Platform Web Console.

Procedure

1. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
2. Click **Upgrade**.
3. In the **Install Template From** field, select a method to gain access to the template file.
4. Select the Communication Manager template.

   If you are upgrading Communication Manager from Release 6.0.1 or 6.2, on the survivable remote template or survivable remote embed template, the system displays the following screens. Provide the information in the appropriate fields:

   - Network Settings
   - Customer Login
   - DHCP Basic settings
   - Branch Session Manager

   Important:

   The system displays the screens only for the survivable remote and the survivable remote embedded template upgrades. The system does not display the screen when you upgrade the other simplex main and duplex templates.

   Click **Install** and **Finish** to complete the upgrade and install the Communication Manager patches.
5. Click **Upgrade**.
6. When the system prompts, click **Commit Installation**.

   Note:

   If you fail to click **Commit Installation**, Communication Manager remains in the current state until you click **Commit Installation**. To stay at the current Communication Manager release, click **Rollback Installation**.

   The system automatically performs the following:

   - Creates a back up of Communication Manager.
   - Installs new Communication Manager.
   - Restores Communication Manager from the backed up data.

Install the service pack and patches for Communication Manager as instructed in Installing patches.

Related Links

Installing patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system

Start a SAT session.

Procedure

Enter `list station` and verify that the stations listed after the upgrade are the same as the stations listed before the upgrade.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.

11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Chapter 3: Upgrading to simplex main/ survivable template

Upgrading the S8500A Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade S8500A Server running Communication Manager releases 2.0 through 3.x to HP DL360 G8 or Dell R620 Server running Communication Manager Release 6.3.6. For the complete list of releases in this range, see the Avaya Support website at http://support.avaya.com.

In this upgrade procedure, you must replace the S8500A Server with an HP DL360 G8 or Dell R620 Server running System Platform and the simplex CM main/survivable core template (CM_Simplex). Install the Communication Manager Release 6.3.6 patch file.

The simplex CM main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Creating a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5.
- Upgrading Communication Manager to Release 4.0.5 on the existing server and restoring the backed up data.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.
- Installing System Platform and the System Platform Release 6.3.4 patch on a new server.
- Installing the Communication Manager Release 6.3 template and the Communication Manager Release 6.3.6 patch on the server.
- Restoring the data set that was created while on Release 4.0.5.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Use this section to upgrade Communication Manager from releases 2.0 through 3.x to Release 6.3.6:

- The main server
- The survivable server

Preupgrade tasks on the S8500A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Recording the configuration screens

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**

7. Click **Cancel**.

   Important:

   Do not click **Submit**.

8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.
    c. Enter `almsnmpconf` and record the output.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.

3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

To use Telnet, enable the Telnet service for Communication Manager.

If the Telnet service is disabled, use SSH to gain access to SAT.

Procedure

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     a. Click **Specify Data Sets**.
     b. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.

   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device**.
6. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.

- **Directory**. The complete directory path where the backup is stored.

7. Click **Start Backup**.
8. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Preupgrade service packs

You do not need the following preupgrade service packs to upgrade S8500A Server running Communication Manager Release 2.x to Release 4.0.5 on the new server.

- 00.0.219.0-1205 (2.0)
- 00.1.221.1-1204 (2.0.1)
- 01.0.411.7-1203 (2.1)
- 01.1.414.1-1203 (2.1.1)
- 02.0.111.4-1204 (2.2)
- 02.1.118.1-1201 (2.2.1)
- 02.2.122.0-1201 (2.2.2)

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Service pack for the current software version

You must obtain and activate the latest available service pack for the currently running Communication Manager software version before you proceed with the next upgrade steps. Depending on the release, use one of the following procedures to install the service pack.

Installing service pack updates

- Obtain the latest service pack for the currently running Communication Manager release and activate it.

Use this procedure if the server is running Communication Manager release earlier than 4.0.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. To access the `ftp` directory, enter `cd /var/home/ftp`.
5. To list the files in the `ftp` directory, at the prompt, enter `ls -ltr`.

   The system displays a list of files in the `ftp` directory.
6. Verify that the `ftp` directory contains the `*.tar.gz` file that you uploaded.
7. Enter `sudo patch_install patch.tar.gz`, where *patch* is the release or issue number of the service pack file, for example, `03.1.526.5-1003.tar.gz`.
8. Enter `patch_show` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch`, where *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name. .

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes and takes more than 2 minutes if messaging is enabled. However, wait until the restart or reset process is complete and enter additional commands.
10. Enter `patch_show` to list the files to verify that the new software file is installed.
11. To view the status of the processes, enter `statapp -c`.

    Ensure that all operations except dupmgr shows `UP`. Communication Manager should show 65/65 UP or, if Communication Manager Messaging is installed, 67/67 UP. To stop the continual refresh of the **`statapp`** command, enter `Ctrl-C`.

    Note:

    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process did not come up and should be investigated before you proceed with the next upgrade step.
12. Close the Telnet session.

Installing service pack

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     a. Select the **update ID** and click **Unpack**.
     b. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     a. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.

     b. Click **Yes**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Communication Manager backup

You must perform this backup for an upgrade to Release 4.0.5 or Release 5.2.1.

You can back up the translation files (xln), the system files (os), and the security files to:

- Flash card using the USB-connected external compact flash drive
- Localhost

  If you choose to back up the files to localhost, you must enable the FTP service.

Backing up the files to a flashcard

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter `3`.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Enabling FTP service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, in the **FTP Server** field, click **Enable**.

   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically becomes disabled.
4. Click **Submit**.

Backing up files to localhost

Enable the FTP service.

Note:

The FTP service remains enabled only for about 15 minutes and automatically becomes disabled. Therefore, complete the backup by using the anonymous user to the `/pub` location before the FTP service disables.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, select **Full Backup**.
3. In the **Backup Method** section, select **Network Device** and complete the following fields:
   - In the **Method** field, click **sftp** or **ftp**.

     The default is **scp**.
   - In the **User Name** field, type `anonymous`.
   - In the **Password** field, type `2` or `@`.
   - In the **Host Name** field, type `localhost`.
   - In the **Directory** field, type `/pub`.
4. Click **Start Backup**.
5. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Transferring files to the services laptop computer using FTP

Log on to the services laptop computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.

For example, `technician@companyname.com`.

7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget full_*
     y
     quit
     ```

   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

   The system closes the ftp session.
8. To confirm that the backup file, for example, `full_*.tar.gz` is present, enter `dir full_*`.

   If the backup file is present, proceed with the next steps of the upgrade procedure.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

State of the existing server

The S8500A server continues to provide service until later in the procedure. Do not shut down the S8500A server until instructed.

Upgrade tasks on a new server that supports Release 4.0.5

New server that supports Release 4.0.5

Complete the upgrade procedures described in the following sections on a new server that supports Communication Manager Release 4.0.5. For example, S8500 B or S8500C. At this point, you turn on the new server but you do not connect to the network.

Installing Communication Manager

Use this procedure to install Communication Manager Release 4.0.5 or Release 5.2.1.

- Install the new server, which supports Communication Manager release you want to install, in the rack.
- Insert the CD-ROM for Communication Manager Release 5.2.1 or Release 4.0.5 into the drive of the server.
- Turn on the server.

Procedure

1. On the computer, click **Start** > **Run**.
2. In the Run dialog box, enter `telnet 192.11.13.6` and press `Enter`.

   To navigate on the installation screens, use the arrow keys to move to an option and press the space bar to select the option. Press `Enter`.
3. Select **Install**, highlight **OK** and press `Enter`.
4. On the Select Release Version screen, select the appropriate release version and click **OK**.
5. At the prompts, select **SIMPLEX**.
6. Select **CM only**.

   Do not select CM with CMM or CMM standalone options.

   The installation process:

   - Installs the Linux operating system.
   - Installs Communication Manager and reports the progress.

   The installation process takes about 20 minutes. When the server is ready to restart, the DVD drive door opens and the system displays a message to check the Avaya Support Site at http://support.avaya.com for the latest software and firmware updates. Remove the DVD from the drive.

   The reboot takes about 5–8 minutes. The Telnet session ends automatically.

Checking the reboot progress

Procedure

1. On the computer, click **Start** > **Run**.
2. Enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter` to clear the ARP cache.
   - The system displays the command line prompt if the cache is cleared.
   - The system displays the message, `The specified entry was not found`, if the specified IP address does not contain an entry in the ARP cache.
4. Enter `ping -t 192.11.13.6` to access the media server.

The -t option causes the ping to repeat. When you get a response (in about 3 minutes), wait an additional 30 seconds before you access the Web interface.

5. Enter `Ctrl+c` to stop the ping.
6. Close the MS-DOS window.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Setting date, time, and time zone

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Server Date/Time**.
3. Change the date, time, and time zone as needed.
4. Click **Submit**.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

Using the steps described in this section, you can download the following files:

- The latest available service pack for Communication Manager Release 4.0.5 or Release 5.2.1
- The RFA license for Communication Manager Release 4.0.5 or Release 5.2.1
- Avaya authentication file for Communication Manager Release 4.0.5 or Release 5.2.1
- Preupgrade service pack to upgrade from Communication Manager Release 4.0.5 or Release 5.2.1

- One of the following backup sets:
  - The three-part backup, `os_*.tar.gz`, `security_*.tar.gz`, and `xln_*.tar.gz`
  - Full backup, `full_*.tar.gz`

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing service pack

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     a. Select the **update ID** and click **Unpack**.
     b. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     a. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.

4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Creating a super-user login

Note:

The craft level login can create a super-user login.

Procedure

1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a Business Partner, you can also add the dadmin login.

   Note:

   Ensure that the customer can change this login, its password, or its permissions.

2. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Administrator Accounts.**

   The system displays the Administrator Accounts page.

3. Select **Add Login**.
4. Select **Privileged Administrator** and click **Submit**.

   The system displays the Administrator Logins -- Add Login: Privileged Administrator page.

5. Type a login name for the account in the **Login name** field.
6. Verify the following:
   - `susers` appears in the `Primary group` field.
   - `prof18` appears in the `Additional groups (profile)` field. prof18 is the code for the customer superuser.
   - `/bin/bash` appears in the `Linux shell` field.
   - `/var/home/login` name appears in the `Home directory` field, where login name is the name you entered in step 5.
7. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
8. From the **Select type of authentication** option, select **password**.

   Note:

   Do not lock the account or set the password to be disabled.

9. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
10. In the section Force password/key change on next login select **no**.
11. Click **Submit**.

    The system informs you the login is added successfully.

Installing the Communication Manager license and authentication files

Caution:

A super-user login, dadmin, or other customer super-user login must exist before you install an authentication file. See Creating a super-user login on page 136.

Procedure

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > License File**.

   The system displays the License File page.
2. Select **Install the license file I previously downloaded** (radio button) and click **Submit**.

   The system displays a message indicating that the license is installed successfully.
3. Click **Restart CM**.
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that all operations are `UP`.
8. On the System Management Interface, select **Administration > Server (Maintenance) > Authentication File**.

   The system displays the Authentication File page.
9. Select **Install the Authentication file I previously downloaded** (radio button) and click **Install**.

   The system displays a message indicating that the authentication file is installed successfully.

Restoring server data

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file for survivable core server and survivable remote server.
- Copy the datasets to the server.

- Install the latest service pack for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

Depending on the release of Communication Manager of the existing system, the data you restore comes from:

- The three-part backup (os, security, and xln) or a full backup
- The backup files copied to the flashcard or the laptop

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - If the backup file is copied to the laptop, click **Local Directory**.

     The fields displays the default directory `/var/home/ftp/pub`. Keep the default directory.
   - If the backup file is copied to the flashcard, click **Local CompactFlash Card**.
4. Click **View**.
5. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
6. Select both **Force** options.
7. Click **Restore**.
8. To view the status of the restore process:
   a. Click **Restore History** and select the file you want to restore.
   b. Click **Status**.

      When the restoration is complete, the system displays the message `backup: 0: restore of <filepath/filename> completed successfully.`

You may lose connectivity between the laptop and the server. Ignore this condition and proceed to the next steps.

Rebooting the server

Use this procedure to reboot the server if the connectivity between the laptop and the server is lost after you restore the data.

Note:

If the connectivity between the laptop and the server is available after you restore the data, use **Server** > **Shutdown Server** on System Management Interface to reboot the server.

Procedure

1. Press the power control button for several seconds on the front of the server.

   The server turns off.
2. Press the power control button again.

The server turns on.

Connecting the services computer to the server

- Wait for about 5–8 minutes for the system to complete the reboot.
- Verify if ping from the portable computer to server is successful.

If the connectivity, ping test, between the portable computer and the server is functional, proceed with the section “Accessing the System Management Interface”.

Perform this procedure only if the laptop connected to the services port, the port labeled **2**, is not functional after the reboot.

Procedure

1. Disconnect the laptop from the Ethernet port labeled **2**.
2. Connect the laptop to the Ethernet port labeled **4**.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

Procedure

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.

   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Enabling FTP service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, in the **FTP Server** field, click **Enable**.

   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically becomes disabled.
4. Click **Submit**.

Backing up files to localhost

Enable the FTP service.

Note:

The FTP service remains enabled only for about 15 minutes and automatically becomes disabled. Therefore, complete the backup by using the anonymous user to the `/pub` location before the FTP service disables.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

2. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, select **Full Backup**.
3. In the **Backup Method** section, select **Network Device** and complete the following fields:
   - In the **Method** field, click **sftp** or **ftp**.

     The default is **scp**.
   - In the **User Name** field, type `anonymous`.
   - In the **Password** field, type `2` or `@`.
   - In the **Host Name** field, type `localhost`.
   - In the **Directory** field, type `/pub`.
4. Click **Start Backup**.
5. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Transferring files to the services portable computer using FTP

Log on to the services portable computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.

   For example, `technician@companyname.com`.

7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget migration-60*
     y
     quit
     ```

   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `migration-60_cmserver_172731_20100516.tar.gz`.

   The system closes the ftp session.
8. To confirm that the backup file, for example, `migration-60*.tar.gz` is present, enter `dir migration*`.

   If the backup file is present, proceed with the next steps of the upgrade procedure.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Upgrade tasks on the HP DL360 G8 or Dell R620 Release 6.3.6 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Turning on the server

Do not connect the server to the network.

Procedure

1. Insert the System Platform DVD into the CD/DVD drive of the server.
2. Turn on the server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

Procedure

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.

   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying the upgrade dataset from the laptop to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the S8500A Server

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Postupgrade tasks on the HP DL360 G8 or Dell R620 Release 6.3.6 Server

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.

5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500-Series Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 on S8500B or S8500C Server to Release 6.3.6 on HP DL360 G8 Server or Dell R620 Server.

In this upgrade procedure, you must replace the S8500B or S8500C Server by an HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex CM main/survivable template, CM_Simplex.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8500B or S8500C server to Communication Manager Release 4.0.5 or Release 5.2.1 first.
   - For servers that you can upgrade directly to Release 4.0.5 or Release 5.2.1, see *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers* (03-602885).
   - For the S8500A server, see *Upgrading Servers to the Avaya S8800 Server for Avaya Aura® Communication Manager* (03-603445).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.3.6.
3. Perform the upgrade to Release 6.3.6 as described in this section.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.3.6:

- The main server
- The survivable server

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist

You need the following additional documentation:

Sl.No	Task	Description	✔
	Obtain one of the following as appropriate: • *Installing the HP ProLiant DL360p G8 Server* • *Installing the Dell™ PowerEdge™ R620 Server*	Provides instructions for installing the server for Communication Manager.	
	Implementing *Avaya Aura® Communication Manager* , 03-603558	Provides instructions for installing and configuring Communication Manager.	

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8500 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser

to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**

   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**
     c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
     d. In the **Download size** field, enter the size of the backup `.tar` file.

        If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.

5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages,

write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:

   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**

- **Password**
- **Host Name**. The hostname or IP address.
- **Directory**. The complete directory path where the backup is stored.

9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Disconnect the laptop from the Services port.
2. Label and disconnect the power cords from the power supply at the back of the server.
3. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.
4. Disconnect the power cord from the SAMP at the back of the server.

Removing the server from the rack

Procedure

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

   For more information, see *Quick Start for Hardware Installation: Avaya S8500 Server*.

Upgrade tasks on the target server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

Note:

You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs

2. System Platform feature packs
3. Solution template service packs
4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

You change this node name in Step 4. Typically the data in this field is `msgserver`.

b. In the **Far-end Node Name** field, enter `tmp` and submit the form.

4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.

- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.

6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.

9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8510 Server to S8510 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager to Release 6.3.6 running System Platform and the simplex main/survivable core template, CM_Simplex, for existing Communication Manager on S8510 Server.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

You can reuse the existing server. However, if the current hard disks have 146 GB memory, perform the following additional tasks:

- Increase the memory.
- Remove the Server Availability Management Processor (SAMP) board.
- (Optional) Add a third hard disk drive, but only if the current hard disks are of the SAS type with 146-GB memory.
- (Optional) Reconfigure to RAID 5, but only if you add a third hard disk drive.

For servers that you can upgrade directly to Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.3.6 on:

- The main server
- The survivable server

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8510 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.

2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.

- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.

b. Select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**

c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

d. In the **Download size** field, enter the size of the backup `.tar` file.

   If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Verifying the hardware on the server

Log on to System Management Interface.

Perform the following steps to determine:

- The need to install an additional hard disk drive on the server to support Communication Manager
- RAID configuration on the server

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Server Configuration**, select **Display Configuration**.
3. Under **Disk devices**, verify the type and the number of hard disk drives (HDD) installed on the system. If the system displays:
   - SAS 146GB, you need to add a third SAS 146GB hard disk drive. You also need to convert RAID 1 to RAID 5.
   - SATA, do not add a third hard disk drive.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.

3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the

language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.

5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.

6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Removing the front bezel from the server

Caution:

Wear an antistatic wrist ground strap before you handle any server components. Connect the strap to an approved ground such as an unpainted metal surface. Also, place the hard drive on

an antistatic mat that is similarly grounded. Do not place the new or the old drive on a bare surface.

Procedure

1. If locked, unlock the bezel with the system key.

   Security alert:

   If the front bezel is locked, ensure that you lock it when you are finished with this replacement procedure.

2. Press the left tab of the bezel and rotate the left end away from the server.
3. Release the right end of the bezel and pull it away from the server.
4. Set the bezel aside.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.
3. Disconnect the power cord from the SAMP at the back of the server.
4. Disconnect the USB modem cable from the USB port on the SAMP behind the server.
5. Disconnect the LAN cable, if used, from the Ethernet port on the SAMP behind the server.

Removing the server from the rack

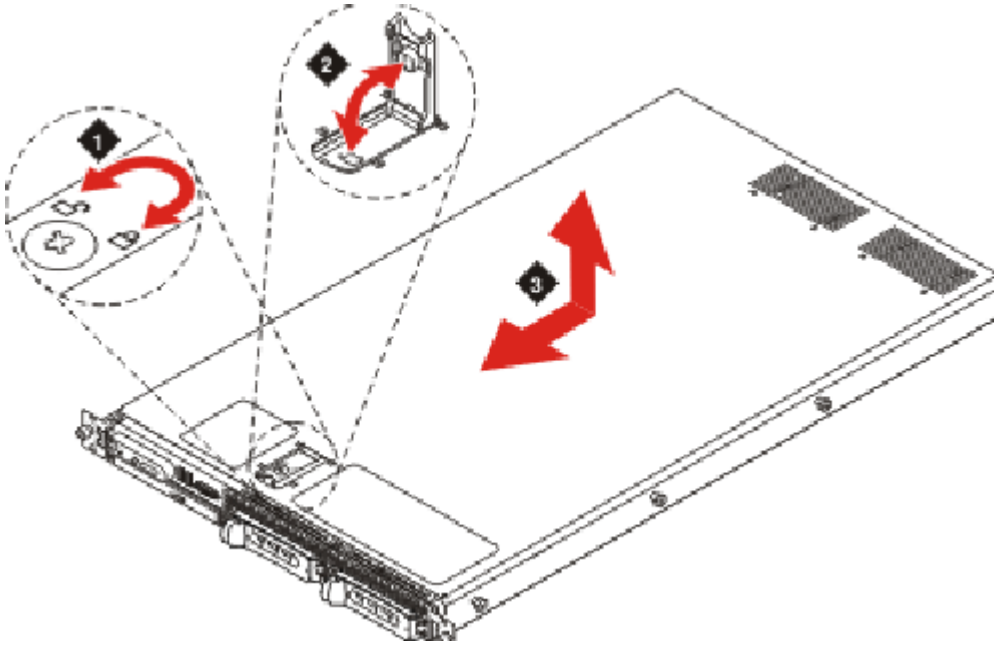
Caution:

Detach the power cords from the power source to disconnect the server completely.

Procedure

1. Loosen the captive screws on both sides of the server.
2. Slide the server clear of the rails.
3. Release the rail lock by pushing the lever in as you slide the server out of the rack.

Removing the cover of the S8510 server



Procedure

1. Turn the latch release lock counter-clockwise to the unlock position using a Phillips screwdriver. See Figure 1.
2. Lift the latch up to unlock. See Figure 2.
3. Slide the cover back and lift straight up to remove. See Figure 3.

Adding the memory modules

Caution:

Ensure that you wear electrostatic wrist ground strap on your bare wrist.

Procedure

1. Remove the protective cover over the memory modules.
2. Insert the new memory modules.

Removing the SAMP

You must remove all power from the server and the SAMP card. The SAMP has a separate power source from the server.

Electrostatic alert:

Wear a wrist strap connected to an approved ground.

The SAMP card resides in a PCI expansion card riser at the rear of the server.

Procedure

1. Lift the release latches on the PCI expansion card riser.
2. Disconnect the cable assembly from the SAMP and set the cable aside. You do not reuse the cable but return it to Avaya with the SAMP.
3. Remove the SAMP card by pulling it gently out of the expansion slot in the riser assembly.
4. Remove the ribbon cable from the motherboard.

Insert a face plate in the empty slot from where you removed the SAMP card.

This prevents any dust from entering the server through the empty slot.

Adding a third hard disk drive

- Verify if you need a third hard disk drive. For instructions, see Verifying the hardware on the server on page 193.
- Remove the front bezel and the cover of the server.

Procedure

1. Pinch together the two tabs of the drive carrier release handle.
2. Open the carrier release handle.
3. Insert the hard disk drive into the slot and push the hard disk drive inside until the drive is seated.
4. Close the hard drive carrier handle to lock the hard disk drive in place.

Replacing the S8510 Server cover

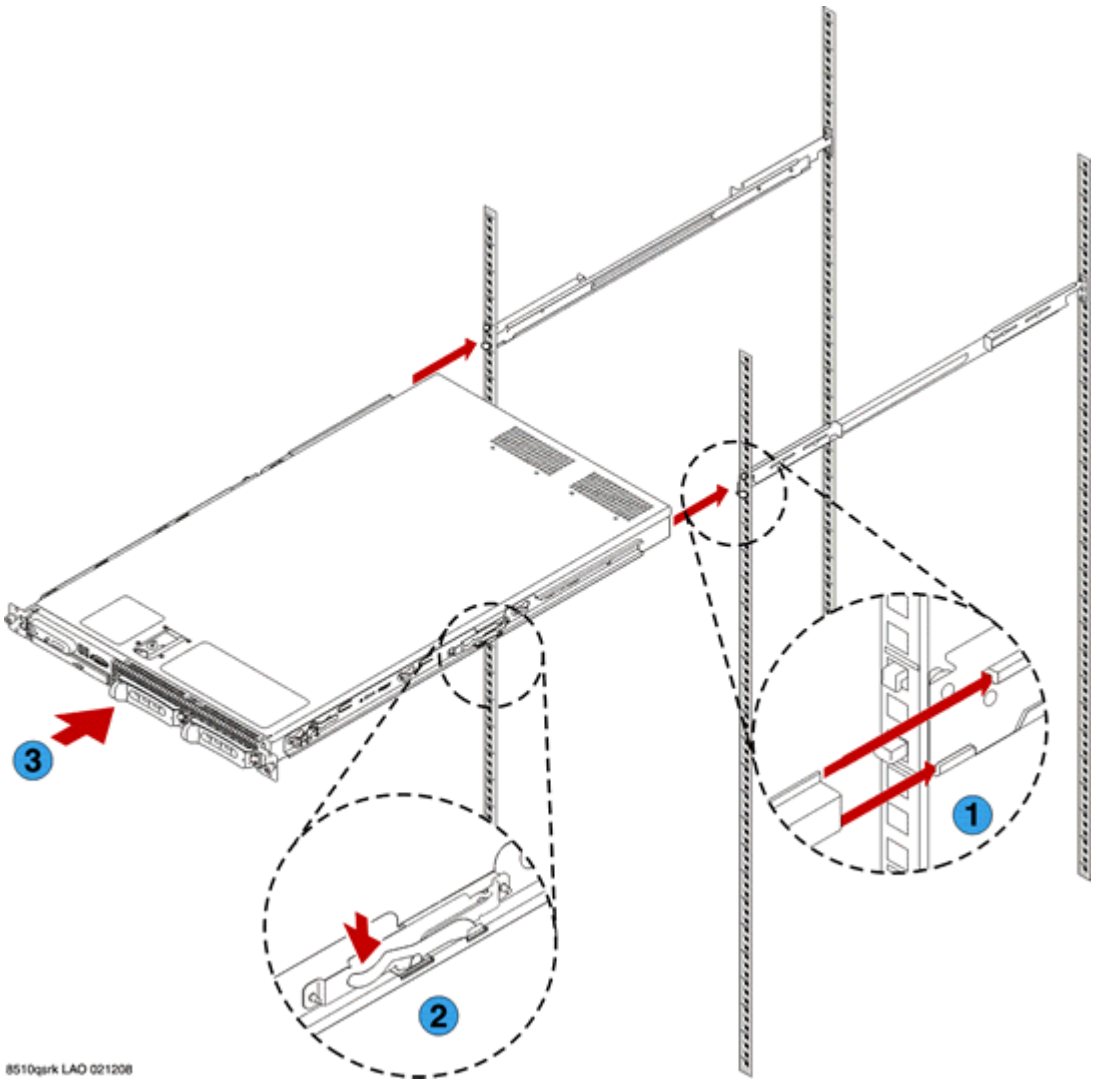
Procedure

1. Place the cover on top of the server, aligning the cover with the J hooks on the sides.
2. Slide the cover forward.
3. Push the latch down to lock.
4. Rotate the latch release lock clockwise to secure the cover.

Installing the server in the rack

The rails must be attached to the server and the rack before installing the server in the rack. If the server is being installed in a cabinet, remove the doors, following the cabinet manufacturer's instructions.

Procedure



If the server is being installed in a cabinet, reattach the doors, following the cabinet manufacturer's instructions.

Replacing the front bezel

Procedure

1. Seat the right end of the bezel in the notch on the right front of the server chassis.
2. Press the left end of the bezel into place until the tab locks in place.
3. If the bezel was originally locked, lock the bezel with the system key.

Converting the disk array to RAID 5

CD comcoded 700500415

Important:

This process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

Procedure

1. Insert the CD comcoded 700500415 into the hard disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following messages:

   ```
   2 Hard Drives Found, Applying Avaya RAID 1 Configuration & Settings
   3 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings
   4 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings
   ```

   The system automatically ejects the CD-ROM when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server, reboot the server and rerun the configuration tool. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD-ROM from the drive and press `Enter` to reboot the server.

   Alternatively, wait for 2 minutes, the system reboots automatically.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

Note:

You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Installing service pack

- Copy the latest service packs from the Avaya Support Site to the services portable computer.
- Log on to System Platform Web Console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:

You must perform this task before you proceed to the next upgrade procedures.

Procedure

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.

5. Click **Install**.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**

- **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

This step deletes the temporary node name.

8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.

8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8800 Server to S8800 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager running on S8800 Server from Release 5.2.1 to Release 6.3.6. In this procedure, you must reuse the S8800 Server and install System Platform and the simplex main/survivable core template, CM_Simplex, on the server.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure includes:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Perform the following additional tasks to reuse the existing server:

- Increase the memory.
- Add a third hard disk drive.
- Update the uEFI firmware.
- Reconfigure the RAID controller to support RAID 5.
- Update the uEFI settings.

Note:

For instructions to update the uEFI firmware and uEFI settings, download the release notes from the Avaya Support website at http://support.avaya.com.

For more information, see *Avaya S8800 Migration Kit*.

Use this section to upgrade:

- The main server
- The survivable server

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade.

✔	Task	Description
	Verify that you have the required software. • System Platform • Communication Manager template	
	Verify that you have all the necessary equipment onsite, for example: • Hard disk drive • Memory module • Services laptop and crossover cable • Electrostatic wrist ground strap and mat	For the list of required equipment, see *Avaya Migration Kit.*
	Obtain the CD-ROM to update the uEFI firmware using one of the following ways: • Order the *uEFI firmware* CD-ROM • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD-ROM.	
	Obtain the *RIAD 5 firmware* CD-ROM	
	Obtain the CD-ROM to update the uEFI settings using one of the following ways: • Order the *uEFI settings* CD-ROM	

Table continues…

✔	Task	Description
	• Download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD-ROM.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:

   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:
  a. Select **Specify Data Sets**.
  b. Select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
     - **Communication Manager Messaging (CMM)**
  c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
  d. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Verifying the hardware on the server

Log on to System Management Interface.

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.

   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the

language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.

5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.

6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server cover

Before you disconnect the server from the power source, make a note of which LEDs light up, including the LEDs that light up on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs do not light up when the power source is removed.

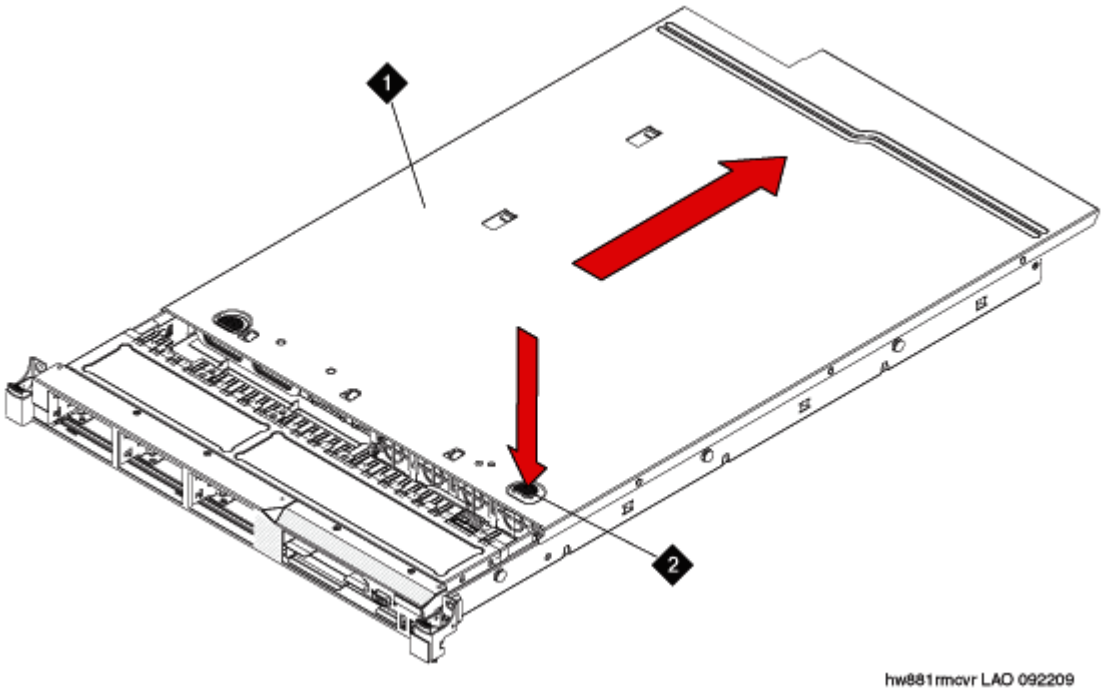
Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
   a. Turn off the server and all attached devices.
   b. Label and disconnect all power cords and external cables.
3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Press down firmly on the blue tab on the top (near the front of the server) of the cover and slide the cover toward the back of the server until the cover has disengaged from the chassis. See the following figure.



1	Cover
2	Tab

5. Lift the server cover off the server and set it aside.

Important:

For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Protecting against ESD damage

Any system component that contains transistors or integrated circuits is sensitive to electrostatic discharge (ESD). ESD damage can occur when there is a difference in charge between objects. Protect against ESD damage by equalizing the charge. The server, the part, the work mat, and the person handling the part must all be at the same charge.

Packaging materials that contain ESD-sensitive components are usually marked with a yellow and black warning symbol.

Caution:

You must observe proper grounding techniques to prevent the discharge of static electricity from your body into ESD-sensitive components.

To avoid damaging ESD-sensitive components:

- Limit your movement. Movement can cause static electricity to build up around you.
- Keep the parts in protective packages until you are ready to install them into the server. If it is necessary to set down a part, put it back into its static-protective package. Do not place the part on the server cover or on a metal surface.
- Place parts on a grounded surface before removing them from their containers.
- Handle the components only after attaching a wrist strap to your bare wrist. Attach the other end of the wrist strap to a ground that terminates at the system ground, such as any unpainted metallic chassis surface.
- Handle a circuit board by the faceplate or side edges only. Avoid touching pins, leads, or circuitry. Hold devices such as a hard disk drive in the same manner. The ESD-sensitive area of these components is located on the bottom surface.

  Caution:

  Make sure that the unprotected part of your hand is not in contact with the non-component side of the board.
- Keep components away from plastics and other synthetic materials such as polyester clothing. Most clothing is insulative and retains a charge even when you wear a wrist strap.
- Do not hand components to another person unless that person is grounded at the same potential level. In general, avoid contact with other people.
- Use the black side of a grounded work mat to provide a static-free work surface. The mat is especially useful when handling ESD-sensitive devices.

- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.
- Verify that the ESD protective devices you use are ISO 9000 certified as fully effective.

Adding the memory module

Removing the DIMM air baffle

You must remove the DIMM air baffle to replace or install a memory module.

Caution:

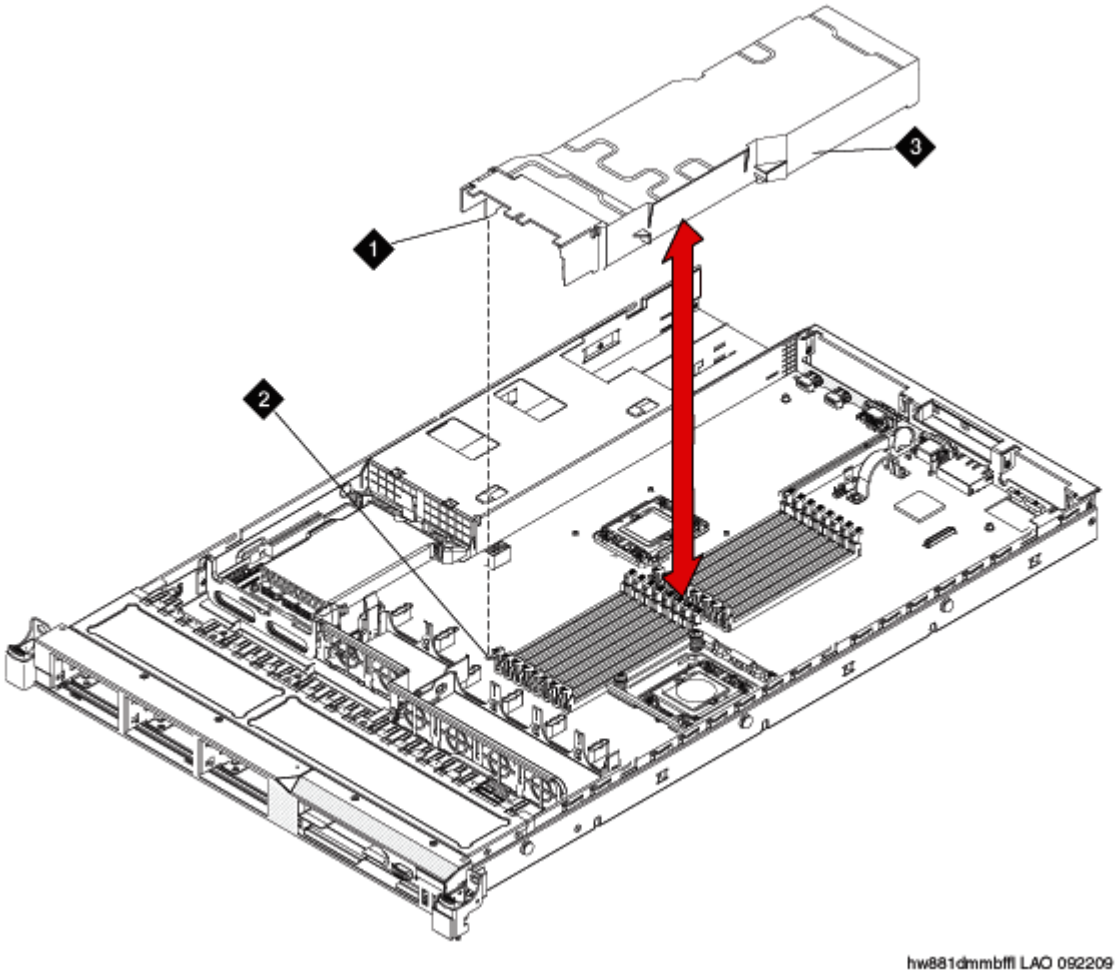
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Lift the DIMM air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Installing a memory module

Remove the DIMM air baffle.

Important:

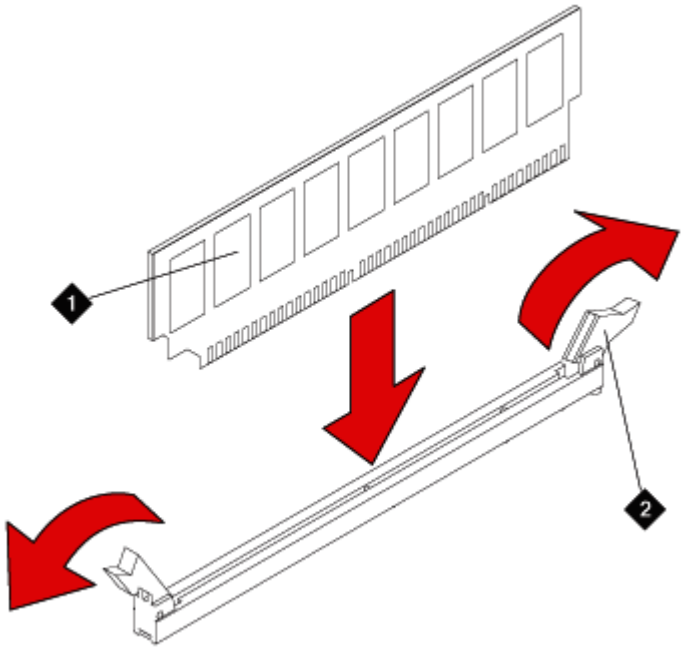
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

Important:

Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



hw88indimm LAO100209

1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.

   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

   Important:

   If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.
7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.

8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.

    When you install or remove memory modules, the server configuration information changes. When you restart the server, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

You must install the DIMM air baffle after you install a memory module.

Caution:

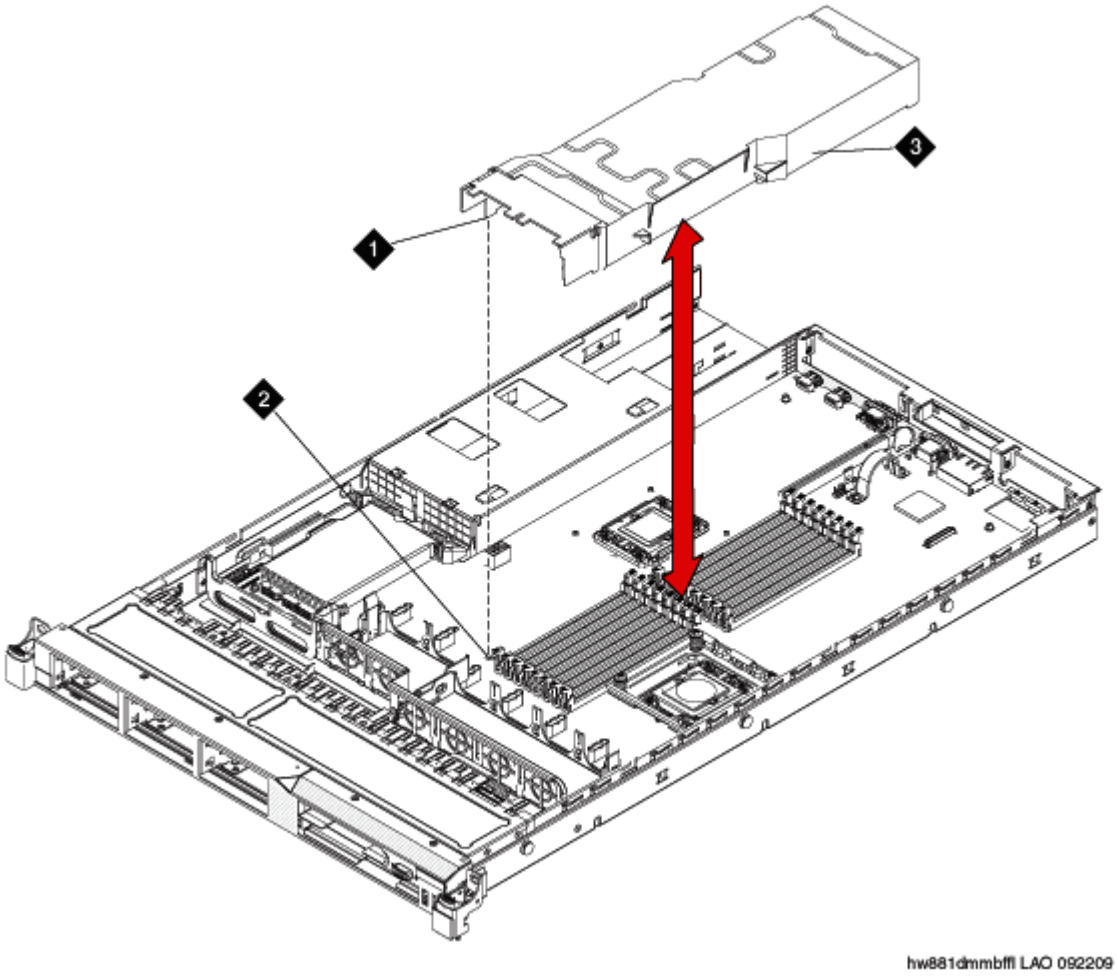
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to the DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Installing a hard disk drive

If replacing an existing hard drive, remove the hard drive that you want to replace.

Important:

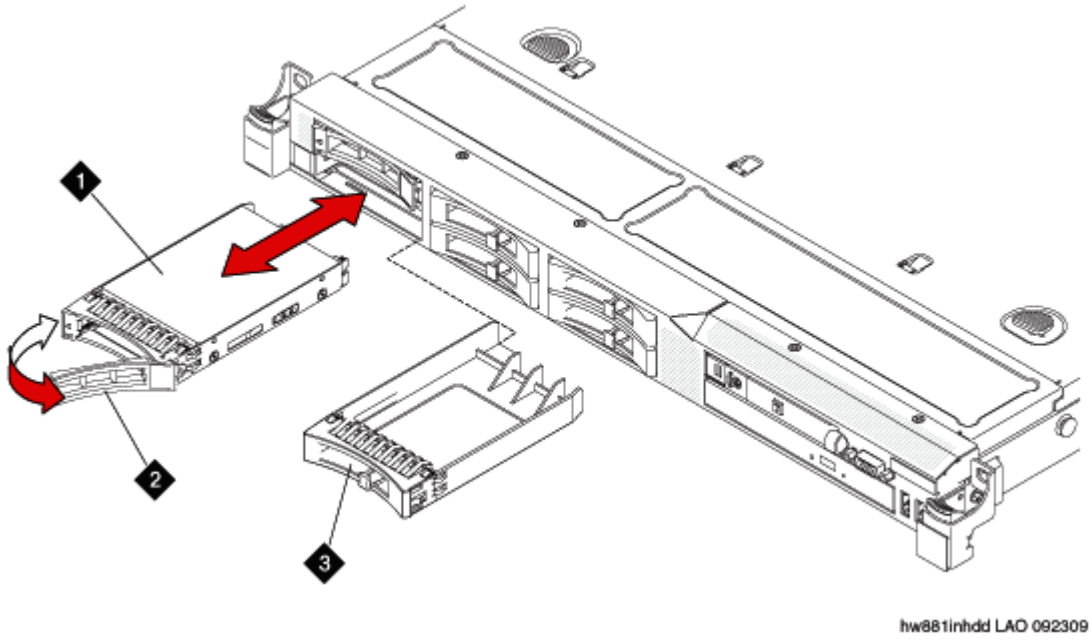
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. An amber LED that remains lit indicates a faulty drive that you must replace.

Updating S8800 server firmware

- Obtain the CO-ROM for uEFI firmware. You order the CO-ROM or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

- Obtain the CD for RAID 5 firmware. You must either order the CD or download the `S8800RAIDTool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for configuring the RAID 5 firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

The conversion process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

Procedure

1. Insert the RAID 5 firmware CD into the disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following message:

   ```
   ... 3 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings....
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server, reboot the server and run the configuration tool again. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Install the `S8800uEFITool.iso` updates.

Updating uEFI settings

- Obtain the CO-ROM for uEFI settings of S8800 Server. You order the CO-ROM or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system

Start a SAT session.

Procedure

Enter `list station` and verify that the stations listed after the upgrade are the same as the stations listed before the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.

2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading the S8800 Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 on S8800 Server to Release 6.3.6 on an HP DL360 G8Server or Dell R620 Server.

In this upgrade procedure, you:

- Replace one of the following:
  - S8800 Server with an HP DL360 G8 Server or Dell R620 Server.
  - HP DL360 G7 Server or Dell R610 Server with an HP DL360 G8 Server or Dell R620 Server.
- Install System Platform and the simplex main template, CM_Simplex, on the new server.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with the new G450 or G430 Branch Gateway.

The simplex CM main/survivable template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration.

You require a new license for Communication Manager.

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.3.6 on:

- The main server
- The survivable server

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the following software: • System Platform • the required Communication Manager template	_
	Obtain one of the following servers, as appropriate: • HP DL360 G8 • Dell R620	_
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

You need the following additional documentation:

Sl.No	Task	Description	✔
	Obtain one of the following as appropriate: • *Installing the HP ProLiant DL360p G8 Server* • *Installing the Dell™ PowerEdge™ R620 Server*	Provides instructions for installing the server for Communication Manager.	
	Implementing *Avaya Aura® Communication Manager* , 03-603558	Provides instructions for installing and configuring Communication Manager.	

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8800 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser

to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

   If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**

   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**
     c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
     d. In the **Download size** field, enter the size of the backup `.tar` file.

        If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.

5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages,

write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:

   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**

- **Password**
- **Host Name**. The hostname or IP address.
- **Directory**. The complete directory path where the backup is stored.

9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutdown tasks on S8800 Server

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

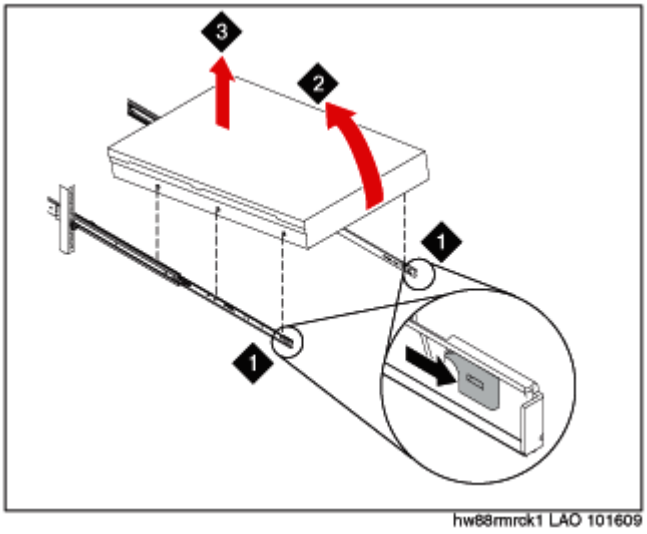
Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server from the rack

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Push the locking levers (1) forward. See the following figure.



4. Lift up the front of the server (2). See the preceding figure.
5. Pull the server out of the rack (3). See the preceding figure.

Upgrade tasks on the target server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:

   a. Start an SSH session.

b. Log in to Domain-0 as administrator.

c. In the command line, type **ip_forwarding enable**.

2. To disable IP forwarding:

a. Start an SSH session.

b. Log in to Domain-0 as administrator.

c. In the command line, enter **ip_forwarding disable**.

An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**

- **Password**
- **Host Name**
- **Directory** or **File Path**
  - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.

- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.

4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.

Comments on this document? infodev@avaya.com

b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

This step creates a node name that you use temporarily.

2. Enter `busyout signaling-group <num>`, where *<num>* is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the *<num>* is 99:
   a. Record the value of the **Far-end Node Name** field.

   You change this node name in Step 4. Typically the data in this field is `msgserver`.

   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.

4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:

   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.

7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 to Release 6.3.6 on HP DL360 G8 Server.

In this upgrade procedure, you:

- Reuse the HP DL360 G8 Server.
- Install System Platform and the simplex CM main/survivable template (CM_Simplex) on the new server.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with the new G450 or G430 Branch Gateway.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

You require a new license for Communication Manager.

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.3.6 on:

- The main server
- The survivable server

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the required software: • System Platform	_

Table continues…

✔	Task	Description
	• the required Communication Manager template	
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support website at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:
  a. Select **Specify Data Sets**.
  b. Select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
     - **Communication Manager Messaging (CMM)**
  c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
  d. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Verifying the hardware on the server

Log on to System Management Interface.

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.

   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the

language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.

5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.

6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

Note:

You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.

b. Log in to Domain-0 as administrator.
c. In the command line, type **ip_forwarding enable**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

Note:

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**

Comments on this document? infodev@avaya.com

- **Host Name**
- **Directory** or **File Path**
  - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.

5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.

6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.

4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.

Comments on this document? infodev@avaya.com

b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

This step creates a node name that you use temporarily.

2. Enter `busyout signaling-group <num>`, where *<num>* is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the *<num>* is 99:
   a. Record the value of the **Far-end Node Name** field.

   You change this node name in Step 4. Typically the data in this field is `msgserver`.

   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.

4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system

Start a SAT session.

Procedure

Enter `list station` and verify that the stations listed after the upgrade are the same as the stations listed before the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.

6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.

9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading DEFINITY SI or R Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade the following servers to Communication Manager Release 6.3.6 on an HP DL360 G8 Server or Dell R620 Server:

- DEFINITY SI Server in an SCC1 or an MCC1

- DEFINITY R Server in an MCC1

In this procedure you must:

- Discard:
  - All port networks, SCCs or MCCs
  - SI or R processor circuit pack
- Install:
  - A G650 Media Gateway and move the supported circuit packs to the media gateway.
  - An HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex CM main/survivable core template (CM_Simplex).

The simplex CM main/survivable template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- Installing translation file on Communication Manager Release 6.3.6.
- Administering IPSIs on Communication Manager Release 6.3.6.
- Installing G650 Media Gateway.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

The upgrade affects service. When you turn off the PPN stack to replace the cabinet during the upgrade process, the system drops all the calls. The system becomes operative when the new server takes control of the IPSIs. Before you turn off the cabinets, perform the following administration tasks.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following server, as appropriate: - HP DL360 G8 - Dell R620 • G650 Media Gateway • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP or later C-LAN	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

You require the following additional documentation:

Sl. no	Task	Description	✔
	Implementing Avaya Aura® Communication Manager, 03-603558	Provides instructions for installing and configuring Communication Manager.	
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.	
	Installing the Avaya G650 Media Gateway, 03-300685	Provides instructions for installing and configuring G650 Media Gateway.	

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.

- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PNs to prepare the DEFINITY system for upgrade. The changing or upgrading the hardware includes:

- Changing TN2182 Tone Clock and maintenance circuit packs for TN2312BP IP Server Interfaces (IPSI) and new TN779D maintenance circuit packs
- Connecting the IPSI circuit pack to the customer network.
- Assigning static IP address to the IPSI circuit pack.

You can perform these tasks while the existing system is in service. However, duplex-reliability configurations encounter short service interruptions when you change the tone-clock circuit pack is in IPSI-controlled PNs.

Server and IPSI cable connections

Each IPSI circuit pack must have a CAT5 cable that connects to the customer network. Cables for IPSIs are located in PN carrier A. If the system has a duplicated bearer network, the cables for IPSIs are located in PN carrier B.

In duplex configurations, each server is connected to the customer network that comprise control network A (CNA). If this system has duplicated IPSIs, each server is connected to the customer network that comprise control network B (CNB).

Saving translations

Start a SAT session.

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Replacement of circuit packs

All PNs receive IPSI circuit packs. The TN2312BP IPSI circuit pack replaces the existing TN2182 Tone Clock circuit pack and terminates control communication with the servers. Flat ribbon cables run between the IPSIs and the maintenance circuit pack. These ribbon cables provide connectivity

that is unavailable by the backplane of older carriers. After you install the IPSI circuit packs, program static IP addresses into the IPSIs.

You can complete this stage at any time before the cutover. The tone clock and the IPSI circuit packs are hot swappable, and you replace the circuit packs in the existing DEFINITY system without the need to turn off the power.

The IPSI circuit pack provides the same functionality as the tone clock circuit pack. You perform the following tasks before the cutover:

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSIs are working as tone clocks in the existing system.
- Test the connectivity between the server and the IPSI.
- Reinstall the IPSIs in the new carriers after you install the carriers.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

A cross-over cable to connect your services laptop directly to the processor.

Procedure

1. Perform one of the following tasks to connect the services laptop to the processor:
   - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Recording node names and IP addresses

Procedure

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*
- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.

b. Log in to Domain-0 as administrator.

c. In the command line, enter **ip_forwarding disable**.

An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs

2. System Platform feature packs
3. Solution template service packs
4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

Note:

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

Do not select the **Install this file on the local server** check box.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the translations

Log on to System Management Interface.

You restore the translations only on the main server. When a survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:

   Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.
6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the status of restore process.

When the restoration is complete, the system displays the following message:

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Installing G650 Media Gateway in the rack

Procedure

Install G650 Media Gateway in the rack. For instructions, see *Installing the Avaya G650 Media Gateway* (03-300685).

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit

packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.

d. Verify that the information displayed is correct.
e. Type `reset` and press `Enter`.

7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.
8. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

This jack is labeled **Port 1**.

3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.
4. For G650, if the maintenance function is used:
   a. Connect one end of the serial maintenance cable to the DB9 connector on the IPSI adapter.
   b. Connect the other end to the Emergency Transfer panel to provide 1 alarm output and 2 alarm inputs.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However,

use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Start a SAT session.

Procedure

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Port network circuit packs

Because you do not reuse the PPN after the upgrade, you must:

- Relocate the port network circuit packs to a new G650 Media Gateway.
- Remove all port network circuit pack translations related to the PPN. The STS group manages the translation changes necessary for this upgrade.

Adding IPSI information

Start a SAT session.

Procedure

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the network regions, see *Administering Network Connectivity on Avaya Aura® Communication Manager,* 555-233-504.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit pack

Start a SAT session.

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6
     - DiffServ: 46
3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`

- **DiffServ**: `46`
- **Auto** (port negotiation): `y` for the following default values:
  - `Full duplex`
  - `100mbps` speed
- **Auto** (port negotiation): `n` to modify as per the network configuration.
  - **Duplex full**
  - **Speed 100**

3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

Procedure

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

Note:

If you do not have a gateway IP address, leave the **Gateway Address** field blank.

7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint

that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.

8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.

2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Removing fiber-related administration

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

Procedure

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link` *n*, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link` *n*.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Administering PN synchronization

Start a SAT session.

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

Procedure

1. To view the synchronization information for the IP-PNC PNs, enter `list synchronization` and `status synchronization`.
2. Verify that the following fields are blank:
   - The **Primary** and the **Secondary** fields on the Synchronization Plan window.
   - The **Source Physical Location** field on the Synchronization Status window.
3. Enter `change synchronization port-network` *n*, where *n* is the PN number of the converted port network that requires synchronization.
4. Enter `list cabinet`.

   The system displays a list of all the cabinets and the PNs that the cabinets contain in the **Circuit Packs Available for Synchronization** section.
5. Obtain a location for the synchronization source circuit pack from the list in the **Circuit Packs Available for Synchronization** section for **Primary** and **Secondary** fields. Select a synchronization source that works.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, in the **Secondary** field, add another location for synchronization-source circuit pack.
8. Press `Submit`.

Wait for about 5 minutes for Communication Manager to update the synchronization plan.

9. To verify the changes, enter `list synchronization` and the `status synchronization` commands.
10. If the **Switching Capability** field for this PN is disabled on the Synchronization Status window, enter `enable synchronization all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must display `PASS` in the **Results** field. If the **Results** field does not display `PASS`, troubleshoot the synchronization error.

Completion tasks on the cabinet

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

1. Remove the fiber cables that connect the following circuit packs in the PNs:
   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Cutover to the server control

Because you do not reuse the PPN, you relocate the port network circuit packs to G650 Media Gateway.

When you relocate the circuit packs to the media gateway and you turn on the power, you want to cut over to have the new server control the existing PNs. The server can be an HP DL360 G8 Server or a Dell R620 Server. To cut over to the server, you must enable the IPSIs on the IP Server Interface (IPSI) System Parameters screen.

This stage affects service momentarily while the CSS comes up and the calls load balance across the IPSIs throughout the port networks.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

   Caution:

   The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

   Note:

   If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.

2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

   Note:

   You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or if you want to minimize out-of-service time.

4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
   - CURL - you cannot reuse this cable.
   - TDM/LAN - you can reuse this cable.
   - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on the new server

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.

- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.

11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the cabinet and the circuit packs

Discard any hardware you replaced during the upgrade.

Procedure

1. Remove the cabinet from the rack.
2. Discard all the circuit packs you removed from the cabinet.

Registering the system

Use the standard procedure to register the system.

Chapter 4: Upgrading to simplex survivable remote template

Upgrading the S8500A Server to the HP DL360 G8 or Dell R620 Server

Introduction

Use this procedure to upgrade S8500A Server running Communication Manager releases 2.0 through 3.x to an HP DL360 G8 Server or Dell R620 Server running Communication Manager Release 6.3.6. For the complete list of releases in this range, see the Avaya Support website at http://support.avaya.com.

In this upgrade procedure you must replace the S8500A Server configured as survivable remote processor with an HP DL360 G8 Server or Dell R620 Server running System Platform and the survivable remote template, CM_SurvRemote.

The upgrade procedure involves:

- Recording the configuration information from the existing S8500A Server in the upgrade worksheet.
- Shutting down the S8500A Server and installing the new server.
- Installing System Platform, the System Platform Release 6.3.6 patch, and Communication Manager survivable remote template on the new server.
- Configuring Communication Manager to be the survivable remote.

The upgrade procedure synchronizes translations and user accounts from the main Communication Manager server to the survivable remote server. You require a new authentication file for Communication Manager Release 6.3.6 configured as survivable remote server.

Preupgrade tasks on the S8500A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Recording the configuration screens

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
7. Click **Cancel**.

   Important:

   Do not click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**

- **Alarms** > **SNMP Traps**
- **Server** > **Server Date/Time**
- **Security** > **Server Access**
- **Miscellaneous** > **CM Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.
    c. Enter `almsnmpconf` and record the output.

Recording the scheduled backups

Log on to System Management Interface.

Record the backup scheduled for the existing server. You must submit the scheduled backups after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, note the details of any backup schedules.

   You submit these scheduled backups after the upgrade on the new server running Communication Manager Release 6.0.x.

Enabling the Telnet service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     a. Click **Specify Data Sets**.
     b. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.

   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device**.
6. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
7. Click **Start Backup**.
8. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

9. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Upgrade tasks on the Release 6.3.6 server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Configuring the alarming information

Log on to System Management Interface.

Configure the information provided in the worksheet available in Appendix A on page 1376.

Procedure

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter `almsnmpconf` to enter any data that you recorded earlier.

   For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.

5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Submitting the scheduled backups

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat steps 3 and 4 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500-Series Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 4.0.5 or Release 5.2.1 on S8500B or S8500C Server to Release 6.3.6.

In this upgrade procedure, you replace the S8500B or S8500C Server by an HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex survivable remote template, CM_SurvRemote.

The simplex survivable remote template supports Utility Services:

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8500 Server to Communication Manager Release 4.0.5 or Release 5.2.1.
   - For servers that you can upgrade directly to Release 4.0.5 or Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
   - For S8500A server, see *Upgrading Servers to the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603445).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.3.6.
3. Perform the upgrade to Release 6.3.6 as described in this section.

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

Comments on this document? infodev@avaya.com

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist

You need the following additional documentation:

Sl.No	Task	Description	✔
	Obtain one of the following as appropriate: • *Installing the HP ProLiant DL360p G8 Server* • *Installing the Dell™ PowerEdge™ R620 Server*	Provides instructions for installing the server for Communication Manager.	
	Implementing *Avaya Aura® Communication Manager* , 03-603558	Provides instructions for installing and configuring Communication Manager.	

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8500-Series Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser

to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:
  a. Select **Specify Data Sets**.
  b. Select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
     - **Communication Manager Messaging (CMM)**
  c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
  d. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the cables

Procedure

1. Disconnect the laptop from the Services port.
2. Label and disconnect the power cords from the power supply at the back of the server.
3. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.
4. Disconnect the power cord from the SAMP at the back of the server.

Removing the server from the rack

Procedure

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

   For more information, see *Quick Start for Hardware Installation: Avaya S8500 Server*.

Upgrade tasks on the HP DL360 G8 or Dell R620 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading the S8510 Server to S8510 Server on System Platform

Introduction

The section describes the procedure to upgrade Communication Manager to Release 6.3.6 running System Platform and the simplex survivable remote template for existing Communication Manager on S8510 Server.

The simplex survivable remote template supports Utility Services.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

You can reuse the existing server. However, if the current hard disks have 146 GB memory, perform the following additional tasks:

- Increase the memory.
- Remove the Server Availability Management Processor (SAMP) board.

- (Optional) Add a third hard disk drive, but only if the current hard disks are of the SAS type with 146-GB memory.
- (Optional) Reconfigure to RAID 5, but only if you add a third hard disk drive.

For servers that you can upgrade directly to Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8510 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**
     c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
     d. In the **Download size** field, enter the size of the backup `.tar` file.

        If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.

b. Wait until the system displays `... unpacked successfully`.

- If the status of the update file you want to activate is `unpacked`:

  a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.

  b. Click **Yes**.

4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the front bezel from the server

Caution:

Wear an antistatic wrist ground strap before you handle any server components. Connect the strap to an approved ground such as an unpainted metal surface. Also, place the hard drive on an antistatic mat that is similarly grounded. Do not place the new or the old drive on a bare surface.

Procedure

1. If locked, unlock the bezel with the system key.

   Security alert:

   If the front bezel is locked, ensure that you lock it when you are finished with this replacement procedure.
2. Press the left tab of the bezel and rotate the left end away from the server.
3. Release the right end of the bezel and pull it away from the server.
4. Set the bezel aside.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.

2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.
3. Disconnect the power cord from the SAMP at the back of the server.
4. Disconnect the USB modem cable from the USB port on the SAMP behind the server.
5. Disconnect the LAN cable, if used, from the Ethernet port on the SAMP behind the server.

Removing the server from the rack

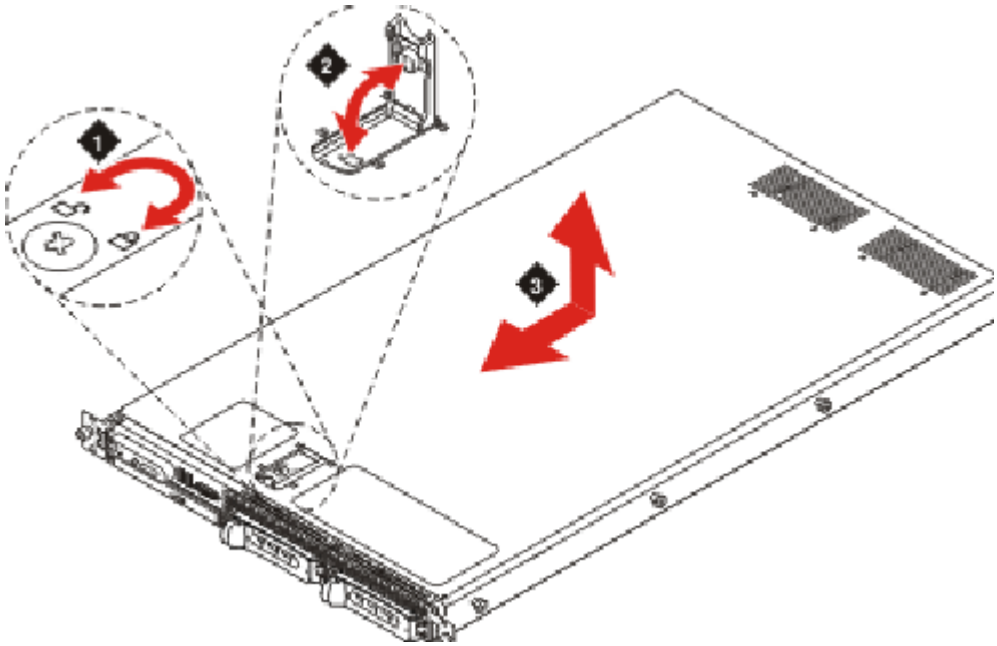
Caution:

Detach the power cords from the power source to disconnect the server completely.

Procedure

1. Loosen the captive screws on both sides of the server.
2. Slide the server clear of the rails.
3. Release the rail lock by pushing the lever in as you slide the server out of the rack.

Removing the cover of the S8510 server



Procedure

1. Turn the latch release lock counter-clockwise to the unlock position using a Phillips screwdriver. See Figure 1.
2. Lift the latch up to unlock. See Figure 2.
3. Slide the cover back and lift straight up to remove. See Figure 3.

Adding the memory modules

Caution:

Ensure that you wear electrostatic wrist ground strap on your bare wrist.

Procedure

1. Remove the protective cover over the memory modules.
2. Insert the new memory modules.

Removing the SAMP

You must remove all power from the server and the SAMP card. The SAMP has a separate power source from the server.

Electrostatic alert:

Wear a wrist strap connected to an approved ground.

The SAMP card resides in a PCI expansion card riser at the rear of the server.

Procedure

1. Lift the release latches on the PCI expansion card riser.
2. Disconnect the cable assembly from the SAMP and set the cable aside. You do not reuse the cable but return it to Avaya with the SAMP.
3. Remove the SAMP card by pulling it gently out of the expansion slot in the riser assembly.
4. Remove the ribbon cable from the motherboard.

Insert a face plate in the empty slot from where you removed the SAMP card.

This prevents any dust from entering the server through the empty slot.

Adding a third hard disk drive

- Verify if you need a third hard disk drive. For instructions, see Verifying the hardware on the server on page 193.
- Remove the front bezel and the cover of the server.

Procedure

1. Pinch together the two tabs of the drive carrier release handle.
2. Open the carrier release handle.
3. Insert the hard disk drive into the slot and push the hard disk drive inside until the drive is seated.
4. Close the hard drive carrier handle to lock the hard disk drive in place.

Replacing the S8510 Server cover

Procedure

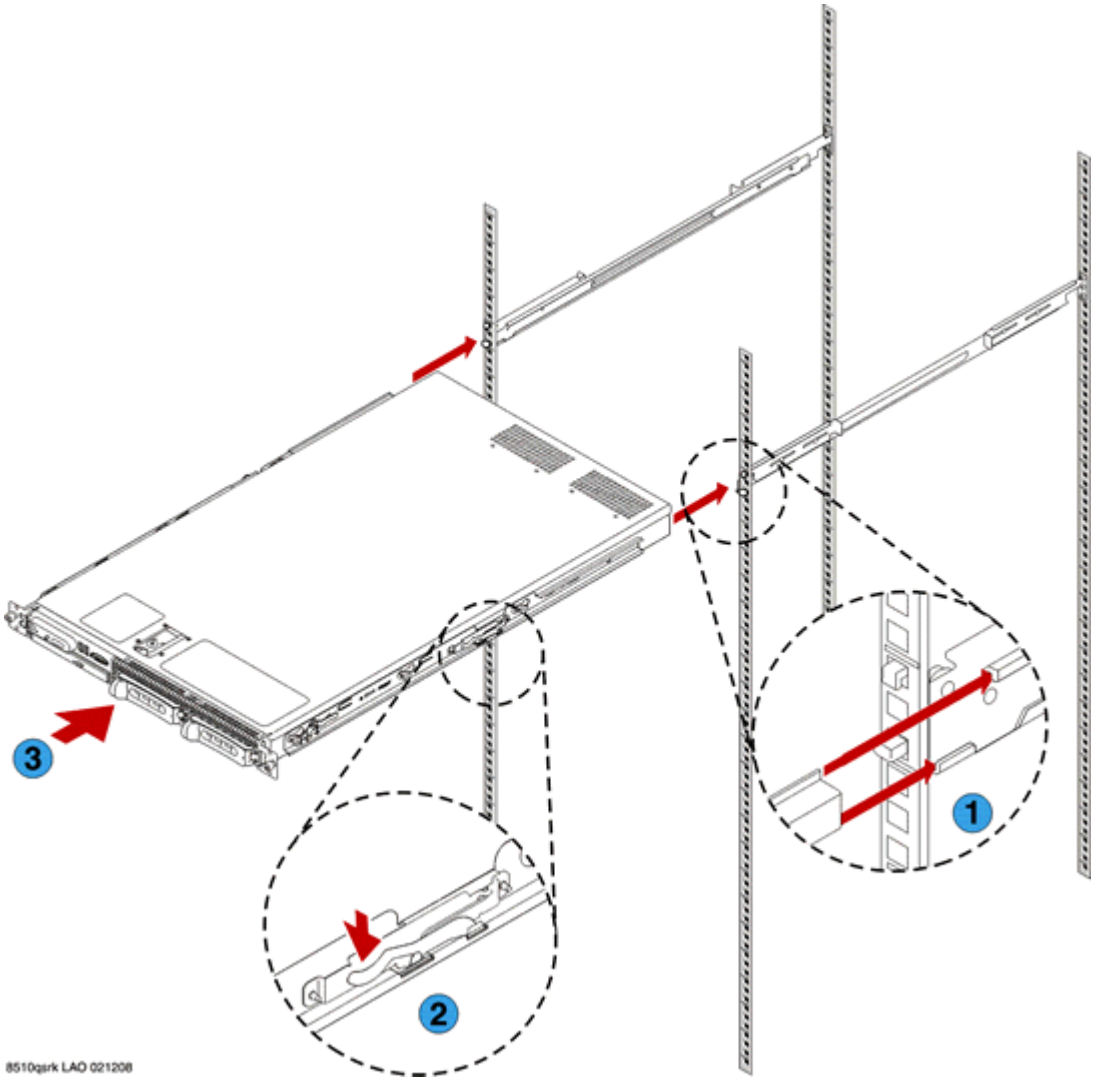
1. Place the cover on top of the server, aligning the cover with the J hooks on the sides.

2. Slide the cover forward.
3. Push the latch down to lock.
4. Rotate the latch release lock clockwise to secure the cover.

Installing the server in the rack

The rails must be attached to the server and the rack before installing the server in the rack. If the server is being installed in a cabinet, remove the doors, following the cabinet manufacturer's instructions.

Procedure



If the server is being installed in a cabinet, reattach the doors, following the cabinet manufacturer's instructions.

Replacing the front bezel

Procedure

1. Seat the right end of the bezel in the notch on the right front of the server chassis.
2. Press the left end of the bezel into place until the tab locks in place.
3. If the bezel was originally locked, lock the bezel with the system key.

Converting the disk array to RAID 5

CD comcoded 700500415

Important:

This process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

Procedure

1. Insert the CD comcoded 700500415 into the hard disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following messages:

   ```
   2 Hard Drives Found, Applying Avaya RAID 1 Configuration & Settings
   3 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings
   4 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings
   ```

   The system automatically ejects the CD-ROM when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server, reboot the server and rerun the configuration tool. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD-ROM from the drive and press `Enter` to reboot the server.

   Alternatively, wait for 2 minutes, the system reboots automatically.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading the S8800 Server to S8800 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager configured as survivable remote from Release 5.2.1 to Release 6.3.6 on the existing S8800 Server. using System Platform and the simplex survivable remote template on S8800 Server.

In this procedure, you must reuse the existing S8800 Server and install System Platform and the simplex survivable remote template, CM_SurvRemote, on the server.

The simplex survivable remote template supports Utility Services.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Perform the following additional tasks to reuse the existing server:

- Increase the memory.
- Add a third hard disk drive.
- Update the uEFI firmware.
- Reconfigure the RAID controller to support RAID 5.
- Update the uEFI settings.

Note:

For instructions to update the uEFI firmware and uEFI settings, download the release notes from the Avaya Support website at http://support.avaya.com.

For more information, see *Avaya S8800 Migration Kit*.

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade.

✔	Task	Description
	Verify that you have the required software. • System Platform • Communication Manager template	
	Verify that you have all the necessary equipment onsite, for example: • Hard disk drive • Memory module • Services laptop and crossover cable • Electrostatic wrist ground strap and mat	For the list of required equipment, see *Avaya Migration Kit.*
	Obtain the CD-ROM to update the uEFI firmware using one of the following ways: • Order the *uEFI firmware* CD-ROM • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD-ROM.	
	Obtain the *RIAD 5 firmware* CD-ROM	
	Obtain the CD-ROM to update the uEFI settings using one of the following ways: • Order the *uEFI settings* CD-ROM • Download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD-ROM.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**

- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**
- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.

- To log in from a portable computer directly connected to the services port, perform one of the following:
  - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
  - If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Verifying the hardware on the server

Log on to System Management Interface.

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.

   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server cover

Before you disconnect the server from the power source, make a note of which LEDs light up, including the LEDs that light up on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs do not light up when the power source is removed.

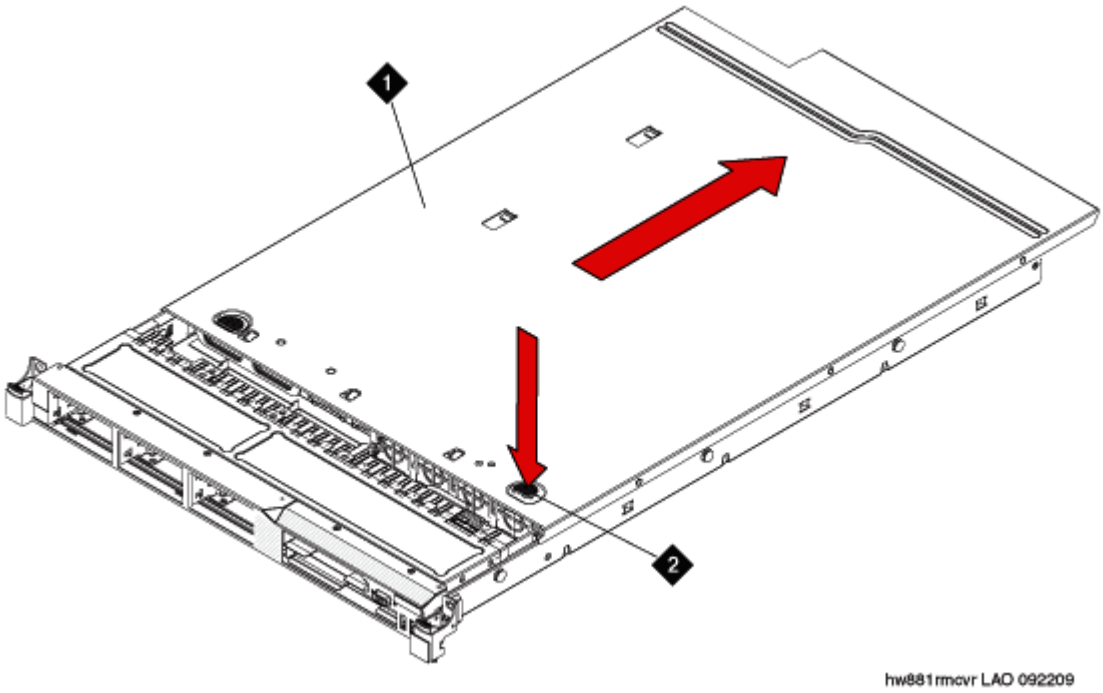
Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
   a. Turn off the server and all attached devices.
   b. Label and disconnect all power cords and external cables.
3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Press down firmly on the blue tab on the top (near the front of the server) of the cover and slide the cover toward the back of the server until the cover has disengaged from the chassis. See the following figure.



1	Cover
2	Tab

5. Lift the server cover off the server and set it aside.

Important:

For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Protecting against ESD damage

Any system component that contains transistors or integrated circuits is sensitive to electrostatic discharge (ESD). ESD damage can occur when there is a difference in charge between objects. Protect against ESD damage by equalizing the charge. The server, the part, the work mat, and the person handling the part must all be at the same charge.

Packaging materials that contain ESD-sensitive components are usually marked with a yellow and black warning symbol.

Caution:

You must observe proper grounding techniques to prevent the discharge of static electricity from your body into ESD-sensitive components.

To avoid damaging ESD-sensitive components:

- Limit your movement. Movement can cause static electricity to build up around you.

- Keep the parts in protective packages until you are ready to install them into the server. If it is necessary to set down a part, put it back into its static-protective package. Do not place the part on the server cover or on a metal surface.
- Place parts on a grounded surface before removing them from their containers.
- Handle the components only after attaching a wrist strap to your bare wrist. Attach the other end of the wrist strap to a ground that terminates at the system ground, such as any unpainted metallic chassis surface.
- Handle a circuit board by the faceplate or side edges only. Avoid touching pins, leads, or circuitry. Hold devices such as a hard disk drive in the same manner. The ESD-sensitive area of these components is located on the bottom surface.

  Caution:

  Make sure that the unprotected part of your hand is not in contact with the non-component side of the board.
- Keep components away from plastics and other synthetic materials such as polyester clothing. Most clothing is insulative and retains a charge even when you wear a wrist strap.
- Do not hand components to another person unless that person is grounded at the same potential level. In general, avoid contact with other people.
- Use the black side of a grounded work mat to provide a static-free work surface. The mat is especially useful when handling ESD-sensitive devices.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.
- Verify that the ESD protective devices you use are ISO 9000 certified as fully effective.

Adding the memory module

Removing the DIMM air baffle

You must remove the DIMM air baffle to replace or install a memory module.

Caution:

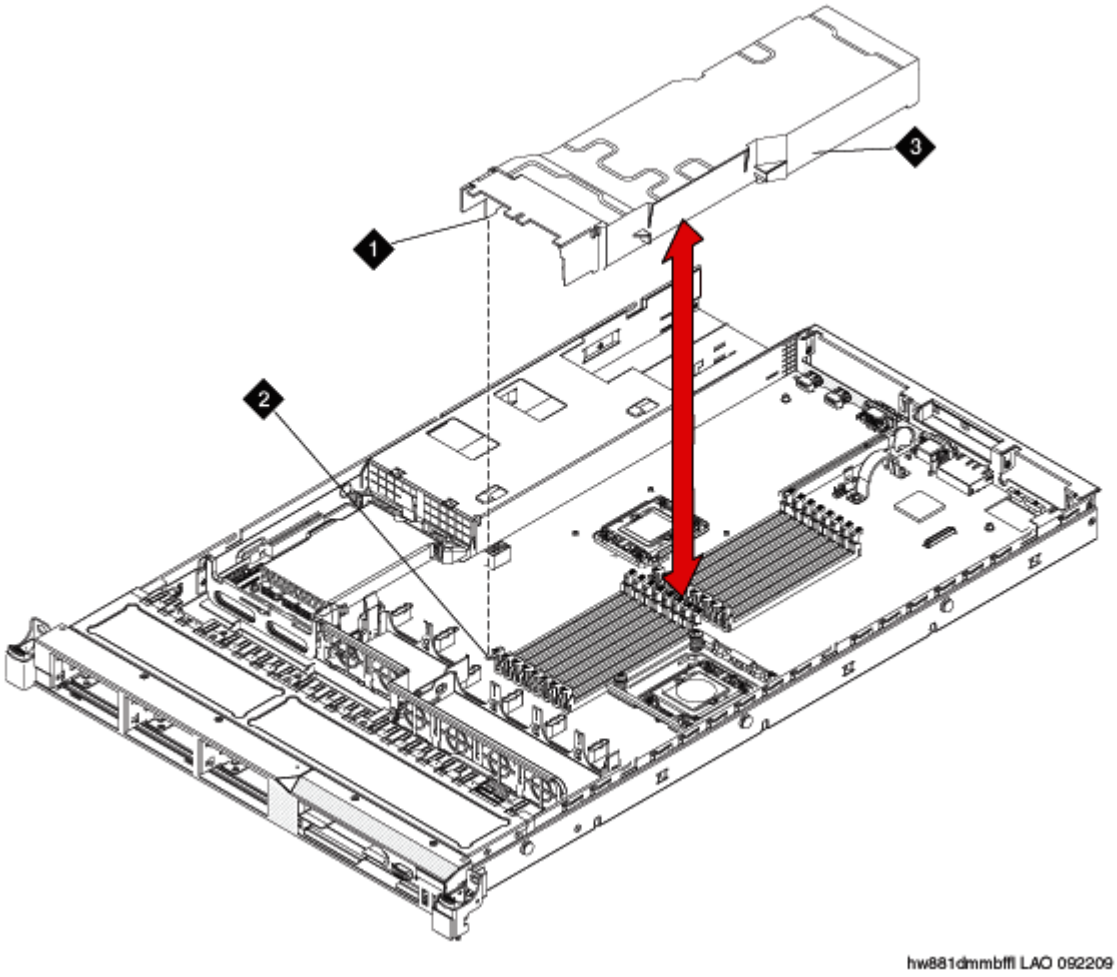
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Lift the DIMM air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Installing a memory module

Remove the DIMM air baffle.

Important:

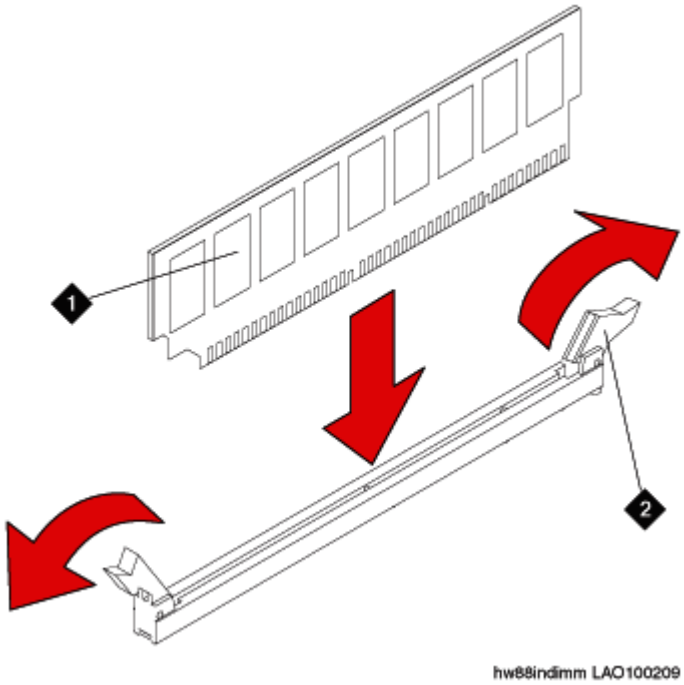
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

Important:

Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



hw88indimm LAO100209

1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.

   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

   Important:

   If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.
7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.

8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.

    When you install or remove memory modules, the server configuration information changes. When you restart the server, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

You must install the DIMM air baffle after you install a memory module.

Caution:

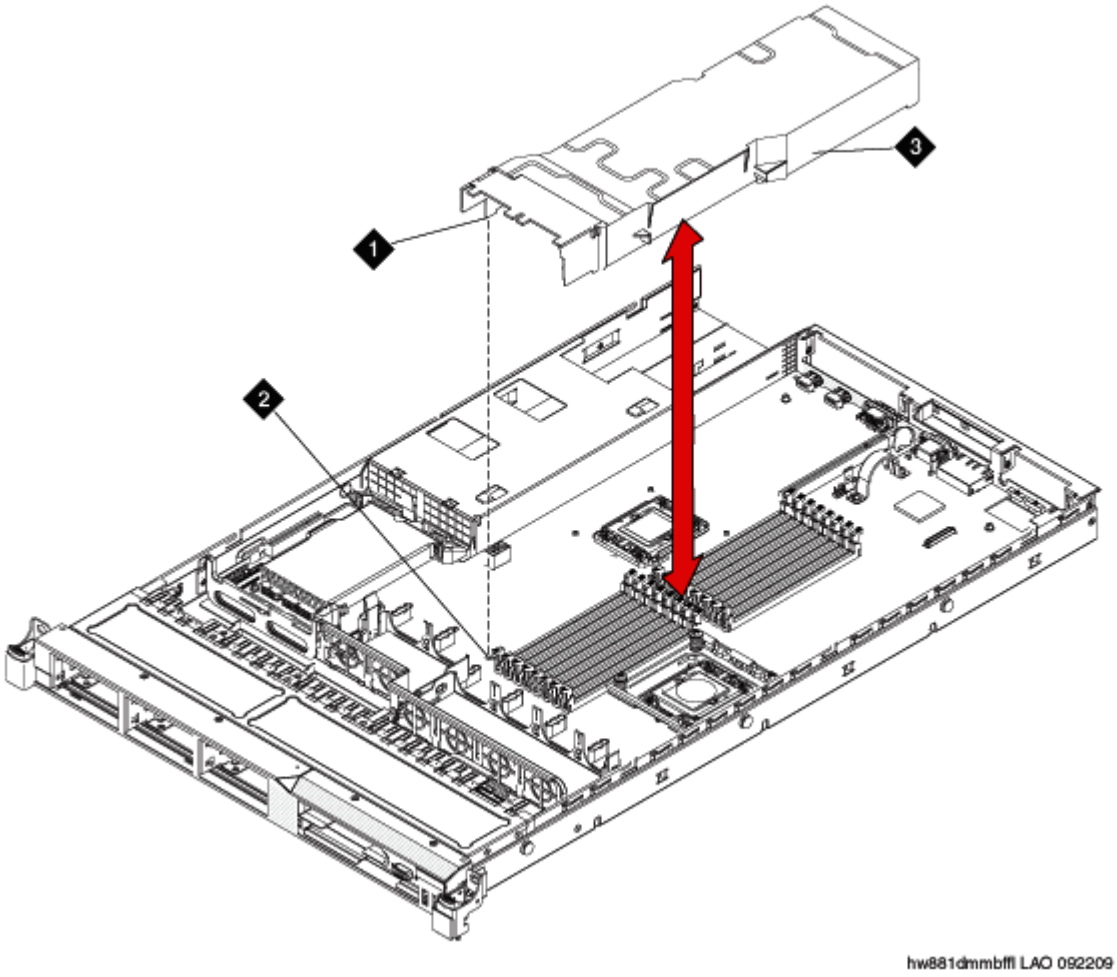
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to the DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Installing a hard disk drive

If replacing an existing hard drive, remove the hard drive that you want to replace.

Important:

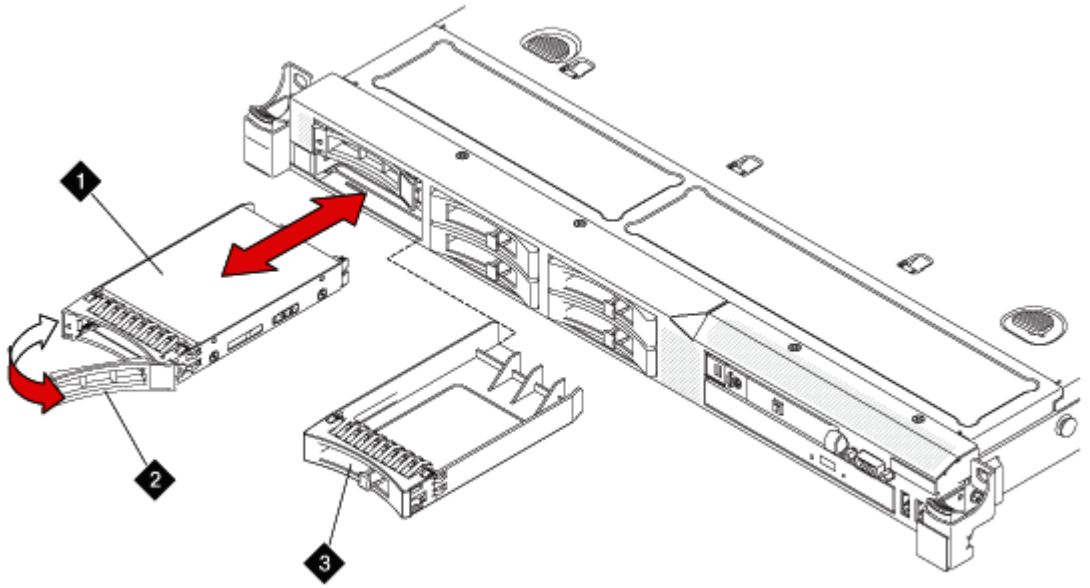
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. An amber LED that remains lit indicates a faulty drive that you must replace.

Updating S8800 server firmware

- Obtain the CO-ROM for uEFI firmware. You order the CO-ROM or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

- Obtain the CD for RAID 5 firmware. You must either order the CD or download the `S8800RAIDTool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for configuring the RAID 5 firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

The conversion process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

Procedure

1. Insert the RAID 5 firmware CD into the disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following message:

   ```
   ... 3 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings....
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server, reboot the server and run the configuration tool again. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Install the `S8800uEFITool.iso` updates.

Updating uEFI settings

- Obtain the CO-ROM for uEFI settings of S8800 Server. You order the CO-ROM or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**

- **Password**
- **Host Name**
- **Directory** or **File Path**
  - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.

c. Click **Server** > **Process Status**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:

   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading the S8800 Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 on S8800 Server to Release 6.3.6 on HP DL360 G8 Server or Dell R620 Server.

The simplex survivable remote template supports Utility Services.

In this upgrade procedure, you:

- Replace one of the following:
  - S8800 Server with an HP DL360 G8 Server or Dell R620 Server.
  - HP DL360 G7 Server or Dell R610 Server with an HP DL360 G8 Server or Dell R620 Server.
- Install System Platform and the simplex survivable remote template, CM_SurvRemote, on the new server.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with the new G450 or G430 Branch Gateway.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration.

You require a new license for Communication Manager.

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist

You need the following additional documentation:

Sl.No	Task	Description	✔
	Obtain one of the following as appropriate: • *Installing the HP ProLiant DL360p G8 Server* • *Installing the Dell™ PowerEdge™ R620 Server*	Provides instructions for installing the server for Communication Manager.	
	Implementing *Avaya Aura® Communication Manager* , 03-603558	Provides instructions for installing and configuring Communication Manager.	

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8800 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser

to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

   If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:
  a. Select **Specify Data Sets**.
  b. Select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
     - **Communication Manager Messaging (CMM)**
  c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
  d. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.

b. Click **Yes**.

4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutdown tasks on S8800 Server

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

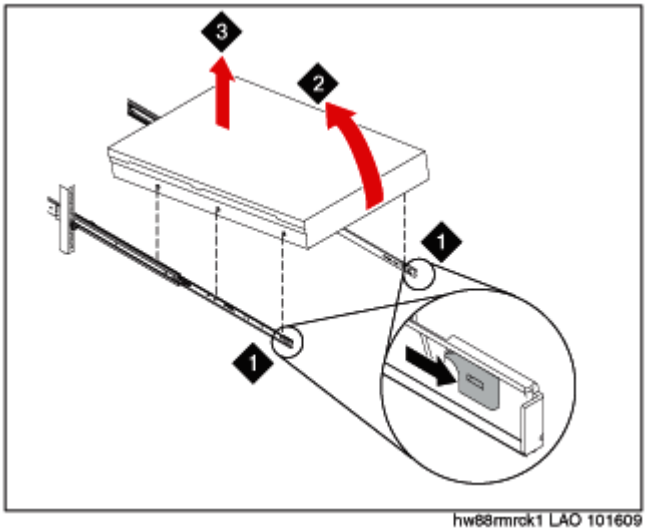
Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server from the rack

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Push the locking levers (1) forward. See the following figure.



4. Lift up the front of the server (2). See the preceding figure.

5. Pull the server out of the rack (3). See the preceding figure.

Upgrade tasks on the HP DL360 G8 or Dell R620 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**

- **Password**
- **Host Name**
- **Directory** or **File Path**
  - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.

c. Click **Server** > **Process Status**.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

For more information, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
- *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 to Release 6.3.6 on HP DL360 G8 Server.

In this upgrade procedure, you:

- Reuse the HP DL360 G8 Server.
- Install System Platform and the survivable remote template, CM_SurvRemote, on the new server.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with the new G450 or G430 Branch Gateway.

The simplex main/survivable core template supports Utility Services.

You require a new license for Communication Manager.

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support website at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server

5. Communication Manager on a main server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**

- **Configure Interfaces**
- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**
- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.

- To log in from a portable computer directly connected to the services port, perform one of the following:
  - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
  - If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**
     c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
     d. In the **Download size** field, enter the size of the backup `.tar` file.

        If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Verifying the hardware on the server

Log on to System Management Interface.

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.

   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.

3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.

6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading DEFINITY SI or R Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade the following servers to Communication Manager Release 6.3.6 on an HP DL360 G8 Server or Dell R620 Server:

- DEFINITY SI Server in an SCC1 or an MCC1
- DEFINITY R Server in an MCC1

In this procedure, you must:

- Discard:
  - All port networks, SCCs or MCCs
  - SI or R processor circuit pack

- Install:
  - A G650 Media Gateway and move the supported circuit packs to the media gateway.
  - An HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex survivable remote template (CM_SurvRemote).

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- Administering IPSIs on Communication Manager Release 6.3.6.
- Installing G650 Media Gateway.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers. You do not require to restore the translations manually.

The upgrade affects service. When you turn off the PPN stack to replace the cabinet during the upgrade process, the system drops all the calls. The system becomes operative when the new server takes control of the IPSIs. Before you turn off the cabinets, perform the following administration tasks.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	

Table continues…

✔	Task	Description
	Obtain the required hardware: • One of the following server, as appropriate: - HP DL360 G8 - Dell R620 • G650 Media Gateway • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP or later C-LAN	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

You require the following additional documentation:

Sl. no	Task	Description	✔
	Implementing Avaya Aura® Communication Manager, 03-603558	Provides instructions for installing and configuring Communication Manager.	
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.	
	Installing the Avaya G650 Media Gateway, 03-300685	Provides instructions for installing and configuring G650 Media Gateway.	

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.

- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PNs to prepare the DEFINITY system for upgrade. The changing or upgrading the hardware includes:

- Changing TN2182 Tone Clock and maintenance circuit packs for TN2312BP IP Server Interfaces (IPSI) and new TN779D maintenance circuit packs
- Connecting the IPSI circuit pack to the customer network.
- Assigning static IP address to the IPSI circuit pack.

You can perform these tasks while the existing system is in service. However, duplex-reliability configurations encounter short service interruptions when you change the tone-clock circuit pack is in IPSI-controlled PNs.

Server and IPSI cable connections

Each IPSI circuit pack must have a CAT5 cable that connects to the customer network. Cables for IPSIs are located in PN carrier A. If the system has a duplicated bearer network, the cables for IPSIs are located in PN carrier B.

In duplex configurations, each server is connected to the customer network that comprise control network A (CNA). If this system has duplicated IPSIs, each server is connected to the customer network that comprise control network B (CNB).

Saving translations

Start a SAT session.

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Replacement of circuit packs

All PNs receive IPSI circuit packs. The TN2312BP IPSI circuit pack replaces the existing TN2182 Tone Clock circuit pack and terminates control communication with the servers. Flat ribbon cables run between the IPSIs and the maintenance circuit pack. These ribbon cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit packs, program static IP addresses into the IPSIs.

You can complete this stage at any time before the cutover. The tone clock and the IPSI circuit packs are hot swappable, and you replace the circuit packs in the existing DEFINITY system without the need to turn off the power.

The IPSI circuit pack provides the same functionality as the tone clock circuit pack. You perform the following tasks before the cutover:

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSIs are working as tone clocks in the existing system.
- Test the connectivity between the server and the IPSI.
- Reinstall the IPSIs in the new carriers after you install the carriers.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

A cross-over cable to connect your services laptop directly to the processor.

Procedure

1. Perform one of the following tasks to connect the services laptop to the processor:
   - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Recording node names and IP addresses

Procedure

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

For instructions to install, see *Installing the HP DL360 G8 Server*.

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.

4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Installing G650 Media Gateway in the rack

Procedure

Install G650 Media Gateway in the rack. For instructions, see *Installing the Avaya G650 Media Gateway* (03-300685).

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.

2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.
7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.
8. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.

2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.
4. For G650, if the maintenance function is used:
   a. Connect one end of the serial maintenance cable to the DB9 connector on the IPSI adapter.
   b. Connect the other end to the Emergency Transfer panel to provide 1 alarm output and 2 alarm inputs.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Port network circuit packs

Because you do not reuse the PPN after the upgrade, you must:

- Relocate the port network circuit packs to a new G650 Media Gateway.
- Remove all port network circuit pack translations related to the PPN. The STS group manages the translation changes necessary for this upgrade.

Removing port network circuit packs

Start a SAT session.

Procedure

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.

2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Start a SAT session.

Procedure

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the network regions, see *Administering Network Connectivity on Avaya Aura® Communication Manager,* 555-233-504.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit pack

Start a SAT session.

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.

- If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.

• The QoS parameters:

- 802.1p: 6
- DiffServ: 46

3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   • For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   • To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
   - **802.1p (vlan priority)**: `6`
   - **DiffServ**: `46`
   - **Auto** (port negotiation): `y` for the following default values:
     • `Full duplex`
     • `100mbps` speed
   - **Auto** (port negotiation): `n` to modify as per the network configuration.
     • **Duplex full**
     • **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

Procedure

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface UUCSS` to open the IP Interfaces screen.

b. Complete each field with the information for this circuit pack.

If you do not have a gateway IP address, leave the **Gateway Address** field blank.

5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Removing fiber-related administration

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

Procedure

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link` *`n`*, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link` *`n`*.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Administering PN synchronization

Start a SAT session.

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

Procedure

1. To view the synchronization information for the IP-PNC PNs, enter `list synchronization` and `status synchronization`.
2. Verify that the following fields are blank:
   - The **Primary** and the **Secondary** fields on the Synchronization Plan window.
   - The **Source Physical Location** field on the Synchronization Status window.
3. Enter `change synchronization port-network` *n*, where *n* is the PN number of the converted port network that requires synchronization.
4. Enter `list cabinet`.

   The system displays a list of all the cabinets and the PNs that the cabinets contain in the **Circuit Packs Available for Synchronization** section.
5. Obtain a location for the synchronization source circuit pack from the list in the **Circuit Packs Available for Synchronization** section for **Primary** and **Secondary** fields. Select a synchronization source that works.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, in the **Secondary** field, add another location for synchronization-source circuit pack.
8. Press `Submit`.

   Wait for about 5 minutes for Communication Manager to update the synchronization plan.
9. To verify the changes, enter `list synchronization` and the `status synchronization` commands.
10. If the **Switching Capability** field for this PN is disabled on the Synchronization Status window, enter `enable synchronization all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must display `PASS` in the **Results** field. If the **Results** field does not display `PASS`, troubleshoot the synchronization error.

Completion tasks on the cabinet

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

1. Remove the fiber cables that connect the following circuit packs in the PNs:
   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Cutover to the server control

Because you do not reuse the PPN, you relocate the port network circuit packs to G650 Media Gateway.

When you relocate the circuit packs to the media gateway and you turn on the power, you want to cut over to have the new server control the existing PNs. The server can be an HP DL360 G8 Server or a Dell R620 Server. To cut over to the server, you must enable the IPSIs on the IP Server Interface (IPSI) System Parameters screen.

This stage affects service momentarily while the CSS comes up and the calls load balance across the IPSIs throughout the port networks.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

   Caution:

   The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

   Note:

   If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.
2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

Note:

You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or if you want to minimize out-of-service time.

4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
   - CURL - you cannot reuse this cable.
   - TDM/LAN - you can reuse this cable.
   - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on the new server

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431

- *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.

- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the cabinet and the circuit packs

Discard any hardware you replaced during the upgrade.

Procedure

1. Remove the cabinet from the rack.
2. Discard all the circuit packs you removed from the cabinet.

Registering the system

Use the standard procedure to register the system.

Chapter 5: Upgrading to duplex main/ survivable core template

Upgrading the S8500A Server to the HP DL360 G8 or Dell R620 Server

Introduction

Use this procedure to upgrade S8500A simplex server running Communication Manager releases 2.0 through 3.x to Release 6.3.6 on HP DL360 G8 Servers or Dell R620 Servers. The complete list of releases in this range is available at http://support.avaya.com.

In this procedure, you replace the S8500A Server by a pair of HP DL360 G8 Servers or Dell R620 Servers running System Platform and the duplex main/survivable core template.

The upgrade procedure includes:

- Creating a data set with specific information of the existing simplex server that you later restore on Communication Manager Release 4.0.5.
- Installing Communication Manager Release 4.0.5 on a new server that supports Release 4.0.5 and restoring the backed up data from the existing server.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5.
- Creating a data set with specific information that you later restore on both Communication Manager Release 6.3.6 servers.
- Installing System Platform and Communication Manager duplex main/survivable core template on both the new servers that support Release 6.3.6.
- Restoring the data set that was created while on Release 4.0.5.

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Use this section to upgrade Communication Manager from releases 2.0 through 3.x to Release 6.3.6:

- The main server
- The survivable server

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • Communication Manager - CD-ROM for Communication Manager Release 5.2.1 - DVD for Communication Manager Release 6.2 template	

Documentation checklist

You need the following additional documentation:

Sl.No	Task	Description	✔
	Obtain one of the following as appropriate: • *Installing the HP ProLiant DL360p G8 Server* • *Installing the Dell™ PowerEdge™ R620 Server*	Provides instructions for installing the server for Communication Manager.	
	Implementing *Avaya Aura® Communication Manager* , 03-603558	Provides instructions for installing and configuring Communication Manager.	

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8500A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.

3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.

4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Recording the configuration screens

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.

4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
7. Click **Cancel**.

   Important:

   Do not click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.
    c. Enter `almsnmpconf` and record the output.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

To use Telnet, enable the Telnet service for Communication Manager.

If the Telnet service is disabled, use SSH to gain access to SAT.

Procedure

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up the files to a flashcard

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter `3`.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     a. Click **Specify Data Sets**.
     b. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.

   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device**.
6. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.

- **User Name**
- **Password**
- **Host Name**. The hostname or IP address.
- **Directory**. The complete directory path where the backup is stored.

7. Click **Start Backup**.
8. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.

- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Preupgrade service packs

You do not need the following preupgrade service packs to upgrade S8500A Server running Communication Manager Release 2.x to Release 4.0.5 on the new server.

- 00.0.219.0-1205 (2.0)
- 00.1.221.1-1204 (2.0.1)
- 01.0.411.7-1203 (2.1)
- 01.1.414.1-1203 (2.1.1)
- 02.0.111.4-1204 (2.2)
- 02.1.118.1-1201 (2.2.1)
- 02.2.122.0-1201 (2.2.2)

Service pack for the current software version

You must obtain and activate the latest available service pack for the currently running Communication Manager software version before you proceed with the next upgrade steps. Depending on the release, use one of the following procedures to install the service pack.

Installing service pack updates

- Obtain the latest service pack for the currently running Communication Manager release and activate it.

Use this procedure if the server is running Communication Manager release earlier than 4.0.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. To access the `ftp` directory, enter `cd /var/home/ftp`.
5. To list the files in the `ftp` directory, at the prompt, enter `ls -ltr`.

   The system displays a list of files in the `ftp` directory.
6. Verify that the `ftp` directory contains the `*.tar.gz` file that you uploaded.
7. Enter `sudo patch_install patch.tar.gz`, where *patch* is the release or issue number of the service pack file, for example, `03.1.526.5-1003.tar.gz`.
8. Enter `patch_show` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch`, where, *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name.

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes. However, wait until the restart or reset process is complete and enter additional commands.
10. Enter `patch_show` to list the files to verify that the new software file is installed.
11. Enter `statapp -c` to view the status of the processes.

    Ensure that all operations except dupmgr shows `UP`. Communication Manager should show 65/65 UP. To stop the continual refresh of the **`statapp`** command, enter `Ctrl-C`.

    Note:

    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For

example, the numbers *64/65 UP* indicates that a process has not started and you must investigate the reason before you proceed with the next upgrade step.

12. Close the Telnet session.

Installing service pack

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     a. Select the **update ID** and click **Unpack**.
     b. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     a. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.

     b. Click **Yes**.
4. Click **Continue**.

   Note:

   Do not install the pre-upgrade service pack until instructed.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Communication Manager backup

You must perform this backup for an upgrade to Release 4.0.5 or Release 5.2.1.

You can back up the translation files (xln), the system files (os), and the security files to:

- Flash card using the USB-connected external compact flash drive
- Localhost

If you choose to back up the files to localhost, you must enable the FTP service.

Backing up the files to a flashcard

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter `3`.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Enabling FTP service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, in the **FTP Server** field, click **Enable**.

   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically becomes disabled.
4. Click **Submit**.

Backing up files to localhost

Enable the FTP service.

Note:

The FTP service remains enabled only for about 15 minutes and automatically becomes disabled. Therefore, complete the backup by using the anonymous user to the `/pub` location before the FTP service disables.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, select **Full Backup**.
3. In the **Backup Method** section, select **Network Device** and complete the following fields:
   - In the **Method** field, click **sftp** or **ftp**.

     The default is **scp**.
   - In the **User Name** field, type `anonymous`.
   - In the **Password** field, type `2` or `@`.
   - In the **Host Name** field, type `localhost`.
   - In the **Directory** field, type `/pub`.
4. Click **Start Backup**.
5. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Transferring files to the services laptop computer using FTP

Log on to the services laptop computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name later in the procedure.

4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.

   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget full_*
     y
     quit
     ```
   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

   The system closes the ftp session.
8. To confirm that the backup file, for example, `full_*.tar.gz` is present, enter `dir full_*`.

   If the backup file is present, proceed with the next steps of the upgrade procedure.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Note on the server shutdown

Note:

Do not shutdown the server at this time.

State of the existing server

The S8500A server continues to provide service until later in the procedure. Do not shut down the S8500A server until instructed.

Upgrade tasks on a new server that supports Release 4.0.5

New server that supports Release 4.0.5

Complete the upgrade procedures described in the following sections on a new server that supports Communication Manager Release 4.0.5. For example, S8500 B or S8500C. At this point, you turn on the new server but you do not connect to the network.

Installing Communication Manager

Use this procedure to install Communication Manager Release 4.0.5 or Release 5.2.1.

- Install the new server, which supports Communication Manager release you want to install, in the rack.
- Insert the CD-ROM for Communication Manager Release 5.2.1 or Release 4.0.5 into the drive of the server.
- Turn on the server.

Procedure

1. On the computer, click **Start** > **Run**.
2. In the Run dialog box, enter `telnet 192.11.13.6` and press `Enter`.

   To navigate on the installation screens, use the arrow keys to move to an option and press the space bar to select the option. Press `Enter`.
3. Select **Install**, highlight **OK** and press `Enter`.
4. On the Select Release Version screen, select the appropriate release version and click **OK**.
5. At the prompts, select **SIMPLEX**.
6. Select **CM only**.

   Do not select CM with CMM or CMM standalone options.

   The installation process:

   - Installs the Linux operating system.
   - Installs Communication Manager and reports the progress.

   The installation process takes about 20 minutes. When the server is ready to restart, the DVD drive door opens and the system displays a message to check the Avaya Support Site at http://support.avaya.com for the latest software and firmware updates. Remove the DVD from the drive.

   The reboot takes about 5–8 minutes. The Telnet session ends automatically.

Checking the reboot progress

Procedure

1. On the computer, click **Start** > **Run**.

2. Enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter` to clear the ARP cache.
   - The system displays the command line prompt if the cache is cleared.
   - The system displays the message, `The specified entry was not found`, if the specified IP address does not contain an entry in the ARP cache.
4. Enter `ping -t 192.11.13.6` to access the media server.

   The -t option causes the ping to repeat. When you get a response (in about 3 minutes), wait an additional 30 seconds before you access the Web interface.
5. Enter `Ctrl+c` to stop the ping.
6. Close the MS-DOS window.

Verifying the software version

Procedure

1. At a browser on your services laptop log on to the System Management Interface (192.11.13.6).
2. Select **Administration > Server (Maintenance) > Software Version**.

   The system displays the Software Version page.
3. Verify that the server is running Release 5.2.1 software. The beginning of the CM Reports as: string should show `R015x.02.1.xxx.x`
4. Verify that the optical drive opened at the end of the software installation.

Setting date, time, and time zone

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Server Date/Time**.
3. Change the date, time, and time zone as needed.
4. Click **Submit**.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

Using the steps described in this section, you can download the following files:

- The latest available service pack for Communication Manager Release 4.0.5 or Release 5.2.1
- The RFA license for Communication Manager Release 4.0.5 or Release 5.2.1

- Avaya authentication file for Communication Manager Release 4.0.5 or Release 5.2.1
- Preupgrade service pack to upgrade from Communication Manager Release 4.0.5 or Release 5.2.1
- One of the following backup sets:
  - The three-part backup, `os_*.tar.gz`, `security_*.tar.gz`, and `xln_*.tar.gz`
  - Full backup, `full_*.tar.gz`

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing service pack

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     a. Select the **update ID** and click **Unpack**.
     b. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     a. Select the **update ID** and click **Activate**.

The system displays the status as the update progresses. The system automatically reboots, if required.

b. Click **Yes**.

4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Creating a super-user login

Note:

The craft level login can create a super-user login.

Procedure

1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a Business Partner, you can also add the dadmin login.

Note:

Ensure that the customer can change this login, its password, or its permissions.

2. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Administrator Accounts.**

The system displays the Administrator Accounts page.

3. Select **Add Login**.
4. Select **Privileged Administrator** and click **Submit**.

The system displays the Administrator Logins -- Add Login: Privileged Administrator page.

5. Type a login name for the account in the **Login name** field.
6. Verify the following:
   - `susers` appears in the `Primary group` field.
   - `prof18` appears in the `Additional groups (profile)` field. prof18 is the code for the customer superuser.
   - `/bin/bash` appears in the `Linux shell` field.
   - `/var/home/login` name appears in the `Home directory` field, where login name is the name you entered in step 5.
7. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
8. From the **Select type of authentication** option, select **password**.

Note:

Do not lock the account or set the password to be disabled.

9. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
10. In the section Force password/key change on next login select **no**.
11. Click **Submit**.

    The system informs you the login is added successfully.

Installing the Communication Manager license and authentication files

Caution:

A super-user login, dadmin, or other customer super-user login must exist before you install an authentication file. See Creating a super-user login on page 136.

Procedure

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > License File**.

   The system displays the License File page.
2. Select **Install the license file I previously downloaded** (radio button) and click **Submit**.

   The system displays a message indicating that the license is installed successfully.
3. Click **Restart CM**.
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that all operations are `UP`.
8. On the System Management Interface, select **Administration > Server (Maintenance) > Authentication File**.

   The system displays the Authentication File page.
9. Select **Install the Authentication file I previously downloaded** (radio button) and click **Install**.

   The system displays a message indicating that the authentication file is installed successfully.

Restoring server data

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file for survivable core server and survivable remote server.

- Copy the datasets to the server.
- Install the latest service pack for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

Depending on the release of Communication Manager of the existing system, the data you restore comes from:

- The three-part backup (os, security, and xln) or a full backup
- The backup files copied to the flashcard or the laptop

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - If the backup file is copied to the laptop, click **Local Directory**.

     The fields displays the default directory `/var/home/ftp/pub`. Keep the default directory.
   - If the backup file is copied to the flashcard, click **Local CompactFlash Card**.
4. Click **View**.
5. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
6. Select both **Force** options.
7. Click **Restore**.
8. To view the status of the restore process:
   a. Click **Restore History** and select the file you want to restore.
   b. Click **Status**.

      When the restoration is complete, the system displays the message `backup: 0: restore of <filepath/filename> completed successfully.`

You may lose connectivity between the laptop and the server. Ignore this condition and proceed to the next steps.

Rebooting the server

Use this procedure to reboot the server if the connectivity between the laptop and the server is lost after you restore the data.

Note:

If the connectivity between the laptop and the server is available after you restore the data, use **Server** > **Shutdown Server** on System Management Interface to reboot the server.

Procedure

1. Press the power control button for several seconds on the front of the server.

   The server turns off.

2. Press the power control button again.

   The server turns on.

Connecting the services computer to the server

- Wait for about 5–8 minutes for the system to complete the reboot.
- Verify if ping from the portable computer to server is successful.

If the connectivity, ping test, between the portable computer and the server is functional, proceed with the section “Accessing the System Management Interface”.

Perform this procedure only if the laptop connected to the services port, the port labeled **2**, is not functional after the reboot.

Procedure

1. Disconnect the laptop from the Ethernet port labeled **2**.
2. Connect the laptop to the Ethernet port labeled **4**.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

Procedure

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.

   You will be logged into the server.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Enabling FTP service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, in the **FTP Server** field, click **Enable**.

   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically becomes disabled.
4. Click **Submit**.

Backing up files to localhost

Enable the FTP service.

Note:

The FTP service remains enabled only for about 15 minutes and automatically becomes disabled. Therefore, complete the backup by using the anonymous user to the `/pub` location before the FTP service disables.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, select **Full Backup**.
3. In the **Backup Method** section, select **Network Device** and complete the following fields:
   - In the **Method** field, click **sftp** or **ftp**.

     The default is **scp**.
   - In the **User Name** field, type `anonymous`.
   - In the **Password** field, type `2` or `@`.
   - In the **Host Name** field, type `localhost`.
   - In the **Directory** field, type `/pub`.
4. Click **Start Backup**.
5. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Transferring files to the services portable computer using FTP

Log on to the services portable computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.

For example, `technician@companyname.com`.

7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget migration-60*
     y
     quit
     ```

   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `migration-60_cmserver_172731_20100516.tar.gz`.

   The system closes the ftp session.
8. To confirm that the backup file, for example, `migration-60*.tar.gz` is present, enter `dir migration*`.

   If the backup file is present, proceed with the next steps of the upgrade procedure.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

State of the existing server

The S8500A server continues to provide service until later in the procedure. Do not shut down the S8500A server until instructed.

Upgrade tasks on the HP DL360 G8 or Dell R620 Release 6.3.6 Server

Turning on the server

Do not connect the server to the network.

Procedure

1. Insert the System Platform DVD into the CD/DVD drive of the server.
2. Turn on the server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.

- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Log on to System Management Interface.

Use this procedure to copy the service packs or the upgrade data set to the server, for example, `migration-60*.tar.gz` file.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Note on restore

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the active S8500A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Service outage

Important:

Service outage begins at this point of the upgrade process.

Postupgrade tasks on the first HP DL360 G8 or Dell R620 Release 6.3.6 active server

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Perform this procedure on the main server only.

Procedure

Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Upgrade tasks on the second HP DL360 G8 or Dell R620 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the server

Procedure

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

     Important:

     Do not release the server until instructed.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing System Management Interface

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.

2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

   - Portable computer access by IP address

     To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this

computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Note on restore

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**

- **Password**
- **Host Name**
- **Directory** or **File Path**
  - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.

b. On the **Administration** menu, click **Server (Maintenance)**.

c. Click **Server** > **Process Status**.

Verifying the connection for server duplication

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. On the Ping page, in the **Endpoints to Ping** section, click **Other server via duplication link**.
4. Click **Execute Ping**.

   If the two endpoints are connected, the system displays the message `MessRecv: 1`.
5. In the navigation pane, click **Server** > **Status Summary** and perform the following:

   a. Verify that this server is in `BUSY OUT` mode.

   b. Verify that the other server is in `Active` mode.

   If the mode of the other server is `Not Ready`, it implies that the server duplication is not functional. Do not proceed until the server duplication is functional.

   If the server duplication connection is successful, the system displays, `Duplication Link: up`.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay

4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500B or S8500C Server to HP DL360 G8 or Dell R620 Server

Introduction

Use this procedure to upgrade S8500B or S8500C simplex server running Communication Manager Release 4.0.5 or Release 5.2.1 to HP DL360 G8 Servers or Dell R620 Servers running Release 6.3.6.

In this upgrade procedure, you replace the S8500B or S8500C simplex server with HP DL360 G8 Servers or Dell R620 Servers running System Platform and the duplex CM main/survivable template.

Duplex main/survivable core template on Communication Manager Release 6.x does not support Communication Manager Messaging.

Important:

If the S8500B or S8500C Server has Communication Manager Messaging installed on it, after the upgrade, messaging is not available on the system. To have messaging on your upgraded system, purchase Avaya Aura® Messaging.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8500B or S8500C server to Communication Manager Release 4.0.5 or Release 5.2.1. For instructions, see *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers* (03-602885).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.3.6.
3. Perform the upgrade to Release 6.3.6 as described in this section.

Note:

You restore the upgrade data set backed up from the existing server to both the new servers.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.3.6:

- The main server
- The survivable server

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information about the procedure and specific commands, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Media Gateways, and Servers*, 03-300431
- *Avaya Aura® Communication Manager Server Alarms* , 03-602798

Preupgrade tasks on the S8500B or S8500C Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.

3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**

- **Host Name** which is the host IP address.
- **Directory**

6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.

3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Installing the servers in the rack

Install the new servers in the rack. At this point do not connect the servers to any network. For instructions to install the servers in the rack, see the following documents:

- For Dell R620 Server, see *Installing the Dell™ PowerEdge™ R620 Server*.
- For HP DL360 G8 Server, see *Installing the HP ProLiant DL360p G8 Server*.

Duplex main/survivable core template

You are required to install duplex main/survivable core template on each server using a new host name and new IP address.

After you complete the duplex main/survivable core template installation and restore the upgrade dataset, you must configure each server in the server pair to use the Communication Manager Release 5.2.1 server host name and IP address for the Communication Manager Release 6.0.x server configuration for **Alias Host Name** and **Alias IP address**. Refer Appendix C on page 1391 for the worksheet to use for configuring the server.

Upgrade tasks on the first HP DL360 G8 or Dell R620 Server

State of the existing server

The S8500B or S8500C server continues to provide service until later in the procedure. Do not shut down the S8500B or S8500C server until instructed.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the new server

Procedure

1. Do not connect the server to the network until the procedure in this section instructs.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.

c. In the command line, type **ip_forwarding enable**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing System Management Interface

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Note on restore

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the active S8500 Server

Shutdown the active S8500 Server as outlined in the following procedure and connect the first HP DL360 G8 Server or Dell R620 Server to the network.

Important:

After you shutdown the active S8500 Server, at this point, the service is nonfunctional. To minimize this time, shut down the active S8500 Server, access the first HP DL360 G8 Server or Dell R620 Server again and release the server in the shortest amount of time possible.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the server from the rack

Procedure

1. Label and disconnect all remaining cables.

2. Disconnect the laptop from the Services port.
3. Disconnect the power cord from the UPS.
4. Disconnect USB flashcard reader or writer.
5. Disconnect any modem.
6. Remove the server from the rack, if necessary.
7. Remove the rails from the rack.

Postupgrade tasks on the first HP DL360 G8 or Dell R620 Server

Accessing the new server

Procedure

1. Clear the ARP cache on the portable computer, if necessary.
2. Open a Web browser and log onto the server using System Management Interface.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Procedures that you must skip on the survivable server

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading the survivable server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Perform this procedure on the main server only.

Procedure

Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

For more information, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
- *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Upgrade tasks on the second HP DL360 G8 or Dell R620 Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Connecting the cables to the server

Procedure

1. Connect the server to customer LAN.

2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

     Important:

     Do not release the server until instructed.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile,

Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.

3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8510 server to the HP DL360 G8 or Dell R620 Server

Introduction

Use this procedure to upgrade S8510 simplex server running Communication Manager Release 5.2.1 to HP DL360 G8 Servers or Dell R620 Servers running Release 6.3.6.

In this upgrade procedure, you must replace the S8510 simplex server with HP DL360 G8 Servers or Dell R620 Servers running System Platform and the duplex main/survivable core template.

Duplex main/survivable core template on Communication Manager Release 6.x does not support Communication Manager Messaging.

Important:

If the S8510 Server has Communication Manager Messaging installed on it, after the upgrade, messaging is not available on the system. To use messaging on your upgraded system, you must purchase Avaya Aura® Messaging.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8510 Server to Communication Manager Release 5.2.1. For instructions, see *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers* (03-602885).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.3.6.
3. Perform the upgrade to Release 6.3.6 as described in this section.

Note:

You restore the upgrade data set backed up from the existing server to both the new servers.

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.3.6 on:

- The main server
- The survivable server

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.

Table continues…

✔	Task	Description
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information about the procedure and specific commands, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Media Gateways, and Servers*, 03-300431
- *Avaya Aura® Communication Manager Server Alarms* , 03-602798

Preupgrade tasks on the S8510 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. Verify that the **CM Reports as:** field displays one of the following:

   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.

   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Installing the servers in the rack

Install the new servers in the rack. At this point do not connect the servers to any network. For instructions to install the servers in the rack, see the following documents:

- For Dell R620 Server, see *Installing the Dell™ PowerEdge™ R620 Server*.

- For HP DL360 G8 Server, see *Installing the HP ProLiant DL360p G8 Server*.

Duplex main/survivable core template

You are required to install duplex main/survivable core template on each server using a new host name and new IP address.

After you complete the duplex main/survivable core template installation and restore the upgrade dataset, you must configure each server in the server pair to use the Communication Manager Release 5.2.1 server host name and IP address for the Communication Manager Release 6.0.x server configuration for **Alias Host Name** and **Alias IP address**. Refer Appendix C on page 1391 for the worksheet to use for configuring the server.

Upgrade tasks on the first HP DL360 G8 or Dell R620 Server

State of the existing server

The S8510 server continues to provide service until later in the procedure. Do not shut down the S8510 server until instructed.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the new server

Procedure

1. Do not connect the server to the network until the procedure in this section instructs.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Note on restore

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the S8510 Server

You need to perform the following two procedures on the S8510 Server.

Important:

After you complete these two tasks, at this point, the system is out of service as the S8510 Server is shutdown. To minimize this time, shut down the S8510 Server, access the first HP DL360 G8 Server or Dell R620 Server again and release the server immediately.

You must continue to perform upgrade procedures on the first HP DL360 G8 Server or Dell R620 Server.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the server from the rack

Procedure

1. Label and disconnect all remaining cables.
2. Disconnect the laptop from the Services port.
3. Disconnect the power cord from the UPS.
4. Disconnect USB flashcard reader or writer.
5. Disconnect any modem.
6. Remove the server from the rack, if necessary.
7. Remove the rails from the rack.

Postupgrade tasks on the first HP DL360 G8 or Dell R620 Server

Accessing the new server

Procedure

1. Clear the ARP cache on the portable computer, if necessary.
2. Open a Web browser and log onto the server using System Management Interface.

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.

- To use Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Procedures that you must skip on the survivable server

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading the survivable server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Perform this procedure on the main server only.

Procedure

Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:

   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Upgrade tasks on the second HP DL360 G8 or Dell R620 Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Connecting the cables to the server

Procedure

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

     Important:

     Do not release the server until instructed.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

Comments on this document? infodev@avaya.com

- Click **Local Directory** and provide the path to the backup file on your local directory.

  Important:

  If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.

2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8700-Series Servers to the HP DL360 G8 or Dell R620 Servers

Introduction

This section describes the two-step procedure to upgrade Communication Manager from:

1. Release 1.3.x, 2.x, 3.x or 4.x on S8700–Series Servers, which are not connected to the network, to Release 4.0.5 on HP DL360 G8 Servers or Dell R620 Servers.
2. Release 5.x on S8700–Series Servers, which are not connected to the network, to Release 5.2.1 on HP DL360 G8 Servers or Dell R620 Servers.
3. Release 5.2.1 on S8800 Servers to Release 6.3.6 on HP DL360 G8 Servers or Dell R620 Servers, which you connect to the network only later during this upgrade step.

4. Release 5.2.1 on S8800 Servers to Release 6.3.6 on S8800 Servers, which you connect to the network only later during this upgrade step.

In this upgrade procedure, you replace the S8700–Series Servers with HP DL360 G8 Servers or Dell R620 Servers running System Platform and the duplex main/survivable template (CM_Duplex).

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Converting from fiber port networks to IP-PNC on page 1406.

- For Communication Manager Release 3.0 and later, perform the conversion before you upgrade the servers.
- For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

Related Links

S8700 Server upgrade procedure on page 619
High-level tasks on page 620

S8700 Server upgrade procedure

If you can upgrade the existing S8700-Series Server to Communication Manager Release 4.0.5 or Release 5.2.1 without replacing the hardware, use the procedures outlined in *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers*, 03-602885.

If you cannot upgrade the existing S8700-series Server to Communication Manager Release 4.0.5 or Release 5.2.1 without replacing the hardware, use the two-step procedure outlined in this section.

Use the following procedures for each S8700-Series Server to upgrade to Release 4.0.5 or Release 5.2.1:

Server	Upgrade procedures	Comments
S8700	Use the procedures from the current section	Communication Manager Release 5.2.1 does not support S8700 Server.
S8710 with DAL1	Use the procedures from the current section	Require DAL2 otherwise
S8710 with DAL2	Use the procedures from *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers*, 03-602885.	-
S8720	Use the procedures from *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers*, 03-602885.	-
S8730	Use the procedures from *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers*, 03-602885.	-

Related Links

Introduction on page 618

High-level tasks

Perform the following high-level tasks to upgrade the system:

- Creating a data set with specific information of the existing servers that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Installing Communication Manager Release 4.0.5 or Release 5.2.1 on both the new servers and restoring the backed up data from the existing servers.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.2.
- Installing System Platform and Communication Manager on both the new servers.
- Restoring the data set that was created while on Release 4.0.5 or Release 5.2.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.2.

Related Links

Introduction on page 618

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Preupgrade tasks on the active S8700 Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Recording the configuration screens

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
7. Click **Cancel**.

   Important:

   Do not click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.

9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.
    c. Enter `almsnmpconf` and record the output.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

To use Telnet, enable the Telnet service for Communication Manager.

If the Telnet service is disabled, use SSH to gain access to SAT.

Procedure

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     a. Click **Specify Data Sets**.
     b. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.

   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device**.
6. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
7. Click **Start Backup**.
8. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Converting fiber PNs to IP-PNC

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Converting from fiber port networks to IP-PNC on page 1406.

Note:

For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Preupgrade service packs

You do not need the following preupgrade service packs to upgrade S8500A Server running Communication Manager Release 2.x to Release 4.0.5 on the new server.

- 00.0.219.0-1205 (2.0)
- 00.1.221.1-1204 (2.0.1)
- 01.0.411.7-1203 (2.1)
- 01.1.414.1-1203 (2.1.1)
- 02.0.111.4-1204 (2.2)
- 02.1.118.1-1201 (2.2.1)
- 02.2.122.0-1201 (2.2.2)

Installing service pack updates

- Obtain the latest service pack for the currently running Communication Manager release and activate it.

Use this procedure if the server is running Communication Manager release earlier than 4.0.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. To access the `ftp` directory, enter `cd /var/home/ftp`.
5. To list the files in the `ftp` directory, at the prompt, enter `ls -ltr`.

   The system displays a list of files in the `ftp` directory.
6. Verify that the `ftp` directory contains the `*.tar.gz` file that you uploaded.
7. Enter `sudo patch_install patch.tar.gz`, where *patch* is the release or issue number of the service pack file, for example, `03.1.526.5-1003.tar.gz`.
8. Enter `patch_show` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch`, where *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name. .

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes and takes more than 2 minutes if messaging is enabled. However, wait until the restart or reset process is complete and enter additional commands.
10. Enter `patch_show` to list the files to verify that the new software file is installed.
11. To view the status of the processes, enter `statapp -c`.

    Ensure that all operations except dupmgr shows `UP`. Communication Manager should show 65/65 UP or, if Communication Manager Messaging is installed, 67/67 UP. To stop the continual refresh of the **`statapp`** command, enter `Ctrl-C`.

    Note:

    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process did not come up and should be investigated before you proceed with the next upgrade step.
12. Close the Telnet session.

Installing service pack

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     a. Select the **update ID** and click **Unpack**.
     b. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     a. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.

     b. Click **Yes**.
4. Click **Continue**.

   Note:

   Do not install the pre-upgrade service pack until instructed.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Communication Manager backup

You must perform this backup for an upgrade to Release 4.0.5 or Release 5.2.1.

You can back up the translation files (xln), the system files (os), and the security files to:

- Flash card using the USB-connected external compact flash drive
- Localhost

  If you choose to back up the files to localhost, you must enable the FTP service.

Backing up the files to a flashcard

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter `3`.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Enabling FTP service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, in the **FTP Server** field, click **Enable**.

   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically becomes disabled.
4. Click **Submit**.

Backing up files to localhost

Enable the FTP service.

Note:

The FTP service remains enabled only for about 15 minutes and automatically becomes disabled. Therefore, complete the backup by using the anonymous user to the `/pub` location before the FTP service disables.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

2. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, select **Full Backup**.
3. In the **Backup Method** section, select **Network Device** and complete the following fields:
   - In the **Method** field, click **sftp** or **ftp**.

     The default is **scp**.
   - In the **User Name** field, type `anonymous`.
   - In the **Password** field, type `2` or `@`.
   - In the **Host Name** field, type `localhost`.
   - In the **Directory** field, type `/pub`.
4. Click **Start Backup**.
5. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Transferring files to the services laptop computer using FTP

Log on to the services laptop computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.

   For example, `technician@companyname.com`.

7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget full_*
     y
     quit
     ```

   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

   The system closes the ftp session.
8. To confirm that the backup file, for example, `full_*.tar.gz` is present, enter `dir full_*`.

   If the backup file is present, proceed with the next steps of the upgrade procedure.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Note on the server shutdown

Note:

Do not shutdown the server at this time.

Preupgrade tasks on the standby S8700 Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.

3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.

4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Recording the configuration screens

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.

4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
7. Click **Cancel**.

   Important:

   Do not click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.
    c. Enter `almsnmpconf` and record the output.

Enabling the Telnet service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     a. Click **Specify Data Sets**.
     b. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

5. In the **Backup Method** section, click **Network Device**.
6. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
7. Click **Start Backup**.
8. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Preupgrade service packs

You do not need the following preupgrade service packs to upgrade S8500A Server running Communication Manager Release 2.x to Release 4.0.5 on the new server.

- 00.0.219.0-1205 (2.0)
- 00.1.221.1-1204 (2.0.1)
- 01.0.411.7-1203 (2.1)
- 01.1.414.1-1203 (2.1.1)
- 02.0.111.4-1204 (2.2)
- 02.1.118.1-1201 (2.2.1)
- 02.2.122.0-1201 (2.2.2)

Installing service pack updates

- Obtain the latest service pack for the currently running Communication Manager release and activate it.

Use this procedure if the server is running Communication Manager release earlier than 4.0.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. To access the `ftp` directory, enter `cd /var/home/ftp`.
5. To list the files in the `ftp` directory, at the prompt, enter `ls -ltr`.

   The system displays a list of files in the `ftp` directory.
6. Verify that the `ftp` directory contains the `*.tar.gz` file that you uploaded.
7. Enter `sudo patch_install patch.tar.gz`, where *patch* is the release or issue number of the service pack file, for example, `03.1.526.5-1003.tar.gz`.
8. Enter `patch_show` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch`, where *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name. .

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes and takes more than 2 minutes if messaging is enabled. However, wait until the restart or reset process is complete and enter additional commands.

10. Enter `patch_show` to list the files to verify that the new software file is installed.
11. To view the status of the processes, enter `statapp -c`.

    Ensure that all operations except dupmgr shows `UP`. Communication Manager should show 65/65 UP or, if Communication Manager Messaging is installed, 67/67 UP. To stop the continual refresh of the **`statapp`** command, enter `Ctrl-C`.

    Note:

    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process did not come up and should be investigated before you proceed with the next upgrade step.
12. Close the Telnet session.

Installing service pack

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     a. Select the **update ID** and click **Unpack**.
     b. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     a. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

   Note:

   Do not install the pre-upgrade service pack until instructed.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Communication Manager backup

You must perform this backup for an upgrade to Release 4.0.5 or Release 5.2.1.

You can back up the translation files (xln), the system files (os), and the security files to:

- Flash card using the USB-connected external compact flash drive
- Localhost

  If you choose to back up the files to localhost, you must enable the FTP service.

Backing up the files to a flashcard

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter `3`.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Enabling FTP service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Security** > **Server Access**.
3. On the Server Access page, in the **FTP Server** field, click **Enable**.

   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically becomes disabled.
4. Click **Submit**.

Backing up files to localhost

Enable the FTP service.

Note:

The FTP service remains enabled only for about 15 minutes and automatically becomes disabled. Therefore, complete the backup by using the anonymous user to the `/pub` location before the FTP service disables.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager Release 3.0 or later, select **Full Backup**.
3. In the **Backup Method** section, select **Network Device** and complete the following fields:
   - In the **Method** field, click **sftp** or **ftp**.

     The default is **scp**.
   - In the **User Name** field, type `anonymous`.
   - In the **Password** field, type `2` or `@`.
   - In the **Host Name** field, type `localhost`.
   - In the **Directory** field, type `/pub`.
4. Click **Start Backup**.
5. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Transferring files to the services laptop computer using FTP

Log on to the services laptop computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.

   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget full_*
     y
     quit
     ```
   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

   The system closes the ftp session.
8. To confirm that the backup file, for example, `full_*.tar.gz` is present, enter `dir full_*`.

   If the backup file is present, proceed with the next steps of the upgrade procedure.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Preparing the new servers for the upgrade

- Install both the staged servers to the data equipment rack. The new servers can be one of the following:
  - HP DL360 G8 Server

    For instructions to install, see *Installing the HP DL360 G8 Server.*
  - Dell R620 Server

    For instructions to install, see *Installing the Dell R620 Server*.
- Connect both the servers to the power supply. Do not turn on the servers.
- Do not connect the servers to any network until instructed.
- Do not connect the server duplication cable until instructed.

Complete the upgrade procedures on the staged servers.

Sequence of tasks to be performed on the staged servers

Complete the procedures starting from Inserting the CD for Communication Manager CD on page 642 through Completion tasks on the staged server on page 650 on the first staged server running Communication Manager release 5.2.1 first. Repeat the procedures on the second staged server running Communication Manager release 5.2.1.

Staging the new servers to Communication Manager Release 5.2.1

Inserting the Communication Manager disc

Procedure

1. Open the CD-ROM drive on the server.
2. Insert the disc for Communication Manager software in the CD/DVD drive and close the drive.

Turning on the server

Procedure

1. Plug one end of the power cord into the socket at the back of the power supply and the other end into a UPS or nonswitched outlet.

   Approximately 5 seconds after you connect the server to the power supply, one or more fans might start to provide cooling, and the power-on LED blinks quickly at three flashes per

second. About 30 seconds after you turn on the server, the power-on LED blinks slowly at one flash per second, and one or more fans might provide cooling.

Note:

Wait for the power-on LED to blink slowly before you press the power button. If you press the power button while the power-on LED blinks quickly, the server does not turn on.

2. Press the power button on the front of the server.

   When the Green power-on LED on the server is lit, but does not flash, it indicates that the server is turned on. The power-on LED can be in one of the following states:

   - Off: AC power is unavailable, or the power supply or the LED itself has failed.
   - Flashing rapidly: The server is turned off and is not ready to be turned on. The power-control button is disabled. This state lasts for about 30 seconds.
   - Flashing slowly: The server is turned off and is ready to be turned on. You can press the power-control button to turn on the server.
   - Lit: The server is turned on.

   Note:

   Do not connect the new server to the network.

   The power-on LED stops blinking and stays lit. After you press the power button, the server takes approximately 5 minutes to initialize.

Connecting the laptop to the server port

Procedure

1. Connect the laptop to the Services port on the back of the server with a cross-connect CAT5 cable.
2. On your laptop computer, click **Start** > **Run**.
3. In the Run dialog box, enter ping `-t 192.11.13.6` and press `Enter` to check connectivity between the Services laptop and the server.

Installing Communication Manager Release 5.2.1

Insert the CD-ROM for Communication Manager Release 5.2.1 or Release 4.0.5 into the drive of the server.

Procedure

1. On the computer, click **Start** > **Run**.
2. In the Run dialog box, enter `telnet 192.11.13.6` and press `Enter`.

   To navigate on the installation screens, use the arrow keys to move to an option and press the space bar to select the option. Press `Enter`.

3. Select **Install**, highlight **OK** and press `Enter`.

4. On the Select Release Version screen, select the appropriate release version and click **OK**.
5. When the system prompts you, on the Select Server Mode dialog box, select DUPLEX.
6. When the system displays the message `Private Control Network configuration using both Control Network A and Control Network B?`, select `Yes`.

   When you select Yes, the system performs a hardware check on the server to confirm if six Ethernet interfaces are available on the server. If all six Ethernet interfaces are not available, the installation will fail. The default selection is No.

   The installation process:

   - Partitions and reformats the hard drive and internal compact flash of the server.
   - Installs the Linux operating system.
   - Installs Communication Manager and reports the progress.

   The installation process takes about 20 minutes. When the server is ready to reboot, the CD/DVD drive door opens and a reminder to check the Avaya Support Site, http://support.avaya.com for the latest software and firmware updates appears on the screen. Remove the CD from the drive.

   The reboot takes about 5–8 minutes. The Telnet session ends automatically.

Checking the reboot progress

Procedure

1. On the computer, click **Start** > **Run**.
2. Enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter` to clear the ARP cache.
   - The system displays the command line prompt if the cache is cleared.
   - The system displays the message, `The specified entry was not found`, if the specified IP address does not contain an entry in the ARP cache.
4. Enter `ping -t 192.11.13.6` to access the media server.

   The -t option causes the ping to repeat. When you get a response (in about 3 minutes), wait an additional 30 seconds before you access the Web interface.
5. Enter `Ctrl+c` to stop the ping.
6. Close the MS-DOS window.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

Procedure

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.

You will be logged into the server.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying files to the server

- Obtain the service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

Use the steps described in this section to download the following files:

- The latest available service pack for Communication Manager Release 5.2.1
- The license for Communication Manager Release 5.2.1
- The Avaya authentication file for Communication Manager Release 5.2.1
- The preupgrade service pack to upgrade from Communication Manager Release 5.2.1
- The backup data sets from the original server. The data set can be a full backup (`full_*.tar.gz`), the three-part backup set (`os_*.tar.gz`, `security_*.tar.gz`, and

`xln_*.tar.gz`), or `upgrade-2.0_*.tar.gz`, if the original server is running Communication Manager Release 1.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing service pack

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     a. Select the **update ID** and click **Unpack**.
     b. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     a. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Verifying the process status

Procedure

1. In the navigation pane, click **Server** > **Process Status**.
2. In the **Frequency** section, click **Display Once**.
3. Click **View**.
4. Verify that the system displays:
   - `dupmgr` is `Down`.
   - All other operations are `UP STANDBY`.

Setting date, time, and time zone

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Server Date/Time**.
3. Change the date, time, and time zone as needed.
4. Click **Submit**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Creating a super-user login

Note:

The craft level login can create a super-user login.

Procedure

1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a Business Partner, you can also add the dadmin login.

Note:

Ensure that the customer can change this login, its password, or its permissions.

2. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Administrator Accounts.**

   The system displays the Administrator Accounts page.
3. Select **Add Login**.
4. Select **Privileged Administrator** and click **Submit**.

   The system displays the Administrator Logins -- Add Login: Privileged Administrator page.
5. Type a login name for the account in the **Login name** field.
6. Verify the following:
   - `susers` appears in the `Primary group` field.
   - `prof18` appears in the `Additional groups (profile)` field. prof18 is the code for the customer superuser.
   - `/bin/bash` appears in the `Linux shell` field.
   - `/var/home/login` name appears in the `Home directory` field, where login name is the name you entered in step 5.
7. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
8. From the **Select type of authentication** option, select **password**.

   Note:

   Do not lock the account or set the password to be disabled.
9. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
10. In the section Force password/key change on next login select **no**.
11. Click **Submit**.

    The system informs you the login is added successfully.

Installing the Communication Manager license and authentication files

Caution:

A super-user login, dadmin, or other customer super-user login must exist before you install an authentication file. See Creating a super-user login on page 136.

If the system displays any of the following messages during the installation, ignore them:

- `Filesync of new license to standby server failed.`
- `Filesync of new certificates to standby server failed.`
- `Filesync failed.`

- `License serial number mismatch.`

Procedure

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > License File**.

   The system displays the License File page.

2. Select **Install the license file I previously downloaded** (radio button) and click **Submit**.

   The system displays a message indicating that the license is installed successfully.

3. Click **Restart CM**.
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that:
   - `dupmgr` is `Down`.
   - All other operations are `UP`.
8. On the System Management Interface, select **Administration > Server (Maintenance) > Authentication File**.

   The system displays the Authentication File page.

9. Select **Install the Authentication file I previously downloaded** (radio button) and click **Install**.

   The system displays a message indicating that the authentication file is installed successfully.

Restoring server data

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file for survivable core server and survivable remote server.
- Copy the datasets to the server.
- Install the latest service pack for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

Depending on the release of Communication Manager of the existing system, the data you restore comes from:

- The three-part backup (os, security, and xln) or a full backup
- The backup files copied to the flashcard or the laptop

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - If the backup file is copied to the laptop, click **Local Directory**.

     The fields displays the default directory `/var/home/ftp/pub`. Keep the default directory.
   - If the backup file is copied to the flashcard, click **Local CompactFlash Card**.
4. Click **View**.
5. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
6. Select both **Force** options.
7. Click **Restore**.
8. To view the status of the restore process:
   a. Click **Restore History** and select the file you want to restore.
   b. Click **Status**.

      When the restoration is complete, the system displays the message `backup: 0: restore of <filepath/filename> completed successfully.`

You may lose connectivity between the laptop and the server. Ignore this condition and proceed to the next steps.

Rebooting the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Shutdown Server**.
3. Select the following check boxes:
   - **Restart server after shutdown**
   - **Shutdown even if this is the active server**
4. Click **Shutdown**.

   The system displays the `A server shutdown has been requested` message.

Completion tasks on the staged server

Procedure

1. Log off from System Management Interface.
2. Close the Web browser.
3. Disconnect the laptop from the staged server.

Upgrade tasks on the first staged (Release 5.2.1) server

Connecting a laptop to the server

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the **Host Name (or IP Address)** field, type **192.11.13.6**.
4. Select the **SSH** protocol.
5. In the **Port** field, type **10022**.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.

- Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.

4. Enter `exit`.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

Procedure

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.

   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Identifying the Ethernet interface

Log on to System Management Interface.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. On the Set Identities screen, identify the Ethernet interface assigned to Server Duplication.

   The interface assigned does not persist throughout the process to upgrade to Release 6.0.x. However, you must know the Ethernet interface assigned to complete the staging of the servers on Communication Manager Release 5.2.1.

Connecting the server duplication cable to the first staged server

Procedure

Connect the crossover Ethernet cable to the Ethernet port assigned for server duplication on the first staged server.

Important:

Do not connect the other end of the Ethernet cable to the second server until instructed.

Verifying system status

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify that `Mode` is `Active`.

   If the `Mode` is `BUSY OUT`, release the server. The server goes to the `Active` mode.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Completion tasks on the staged server

Procedure

1. Log off from System Management Interface.
2. Close the Web browser.
3. Disconnect the laptop from the staged server.

Upgrade tasks on the second staged (Release 5.2.1) Server

Connecting a laptop to the server

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

1. Connect the laptop to the services port (eth1) using a crossover cable.

If you do not have a crossover cable, you can use an IP hub.

The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.

2. Start an SSH session.
3. In the **Host Name (or IP Address)** field, type **192.11.13.6**.
4. Select the **SSH** protocol.
5. In the **Port** field, type **10022**.
6. Click **Open**.

Note:

If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.

7. Click **Yes** to accept the host key of the server.

The system displays the PuTTY window.

8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

This command produces one of the following responses:

- The command prompt displays when the cache clears.
- Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.

4. Enter `exit`.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

Procedure

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.

You will be logged into the server.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying system status

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify that `Mode` is `BUSY OUT`.
4. If the `Mode` is `Active`, perform the following steps:
   a. Log on to the server using PuTTy configured for SSH.
   b. Enter `stop -acf`.
   c. Enter `server -b`.
   d. Enter `start -ac`.
   e. Enter `exit` to log off and close PuTTY.
5. Repeat steps 2 through 4 to verify if the `Mode` is `BUSY OUT`.

Identifying the Ethernet interface

Log on to System Management Interface.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.

4. On the Set Identities screen, identify the Ethernet interface assigned to Server Duplication.

   The interface assigned does not persist throughout the process to upgrade to Release 6.0.x. However, you must know the Ethernet interface assigned to complete the staging of the servers on Communication Manager Release 5.2.1.

Connecting the server duplication cable to second staged server

One end of the Ethernet cable connected to the first server.

Procedure

Connect the other end of the Ethernet cable to the Ethernet port that is assigned for server duplication on the second server.

The crossover Ethernet cable now connects the two servers.

Verifying the connection for server duplication

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. On the Ping page, in the **Endpoints to Ping** section, click **Other server via duplication link**.
4. Click **Execute Ping**.

   If the two endpoints are connected, the system displays the message `MessRecv: 1`.
5. In the navigation pane, click **Server** > **Status Summary** and perform the following:
   a. Verify that this server is in `BUSY OUT` mode.
   b. Verify that the other server is in `Active` mode.

   If the mode of the other server is `Not Ready`, it implies that the server duplication is not functional. Do not proceed until the server duplication is functional.

   If the server duplication connection is successful, the system displays, `Duplication Link: up`.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Server states

At this point, the first server is in the active state and the second server is busied out.

Completion tasks on the staged server

Procedure

1. Log off from System Management Interface.
2. Close the Web browser.
3. Disconnect the laptop from the staged server.

Upgrade tasks on the first staged (Release 5.2.1) Server

Connecting a laptop to the server

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the **Host Name (or IP Address)** field, type **192.11.13.6**.
4. Select the **SSH** protocol.
5. In the **Port** field, type **10022**.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Starting a SAT session

Log on to the services port from a directly connected laptop.

Procedure

1. Perform one of the following:
   - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
   - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

License error message

While you log on to the server using SAT, if you see the following message, ignore it:

```
License-Error: Reference IPSI or Media-Gateway Not Responding
 System Administration Will Be Blocked in Approximately _ hours
Contact Your Service Representative Immediately
```

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

SAT error message

SAT screen displays `Success` message with Error Code `0`.

If SAT screen displays `Cannot access the standby Server at this time`, do not proceed. This error indicates that server duplication is not functional.

Resetting the system

Procedure

1. Start a SAT session.
2. Log in to the server.
3. Enter `reset system 4` and press **Enter**.

   The system initializes Communication Manager on the release 5.2.1 translations.

4. Wait for Communication Manager to restart.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Completion tasks on both the staged (Release 5.2.1) servers

Completion tasks on the staged Communication Manager Release 5.2.1 servers

Perform the procedures starting from Installing the preupgrade service packs on page 139 through Completing duplication cable connections on staged servers on page 663 on the first staged server running Communication Manager Release 5.2.1 first. Repeat the procedures on the second staged server running Communication Manager Release 5.2.1.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Enabling FTP service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, in the **FTP Server** field, click **Enable**.

The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically becomes disabled.

4. Click **Submit**.

Backing up files to the localhost

Log on to System Management Interface.

To view the **Linux Migration to CM 6.0** option in System Management Interface, install the pre-migration patch. For more information, see *Migration roadmap and limitations*.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

The FTP service remains enabled only for about 15 minutes and automatically becomes disabled. Therefore, complete the backup by using the anonymous user to the `/pub` location before the FTP service disables.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Transferring files to the services portable computer using FTP

Log on to the services portable computer.

Procedure

1. Click **Start** > **Run**.

2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.

   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget migration-60*
     y
     quit
     ```
   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `migration-60_cmserver_172731_20100516.tar.gz`.

   The system closes the ftp session.
8. To confirm that the backup file, for example, `migration-60*.tar.gz` is present, enter `dir migration*`.

   If the backup file is present, proceed with the next steps of the upgrade procedure.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Completing duplication cable connections on the staged servers

Procedure

1. Disconnect the server duplication cable.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

   Note:

   Do not connect the staged servers to the network.

Upgrade tasks on both the new (Release 6.2) servers

Sequence of tasks to be performed on the staged servers

Complete the procedures starting from Installing System Platform and Communication Manager on page 169 through Rebooting the server on page 149 on the first staged server running Communication Manager Release 6.3.6 first. Repeat the procedures on the second staged server running Communication Manager Release 6.3.6.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file

- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Connecting the cables to the new server

Procedure

1. Do not connect the server to the network until the procedure in this section instructs.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**

- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.

4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile,

Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Log on to System Management Interface.

Use this procedure to copy the service packs or the upgrade data set to the server, for example, `migration-60*.tar.gz` file.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.

3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix B on page 1381.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.

3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verification tasks on the staged servers running Release 6.3.6

Starting a SAT session

Log on to the services port from a directly connected laptop.

Procedure

1. Perform one of the following:
   - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
   - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Busying out the standby server

Log on to System Management Interface of the standby server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Log in as `craft` or `dadmin`.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

Verification tasks on the first staged active Release 6.3.6 server

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the connection for server duplication

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. On the Ping page, in the **Endpoints to Ping** section, click **Other server via duplication link**.
4. Click **Execute Ping**.

   If the two endpoints are connected, the system displays the message `MessRecv: 1`.
5. In the navigation pane, click **Server** > **Status Summary** and perform the following:
   a. Verify that this server is in `Active` mode.
   b. Verify that the other server is in `BUSY OUT` mode.

   If the mode of the other server is `Not Ready`, it implies that the server duplication is not functional. Do not proceed until the server duplication is functional.

   If the server duplication connection is successful, the system displays, `Duplication Link: up`.

Completion tasks on the standby S8700 Server

Connecting a laptop to the server

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the **Host Name (or IP Address)** field, type **192.11.13.6**.
4. Select the **SSH** protocol.
5. In the **Port** field, type **10022**.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.

- Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.

4. Enter `exit`.

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.

3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Completion tasks on the active S8700 Server

Connecting a laptop to the server

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the **Host Name (or IP Address)** field, type `192.11.13.6`.
4. Select the **SSH** protocol.
5. In the **Port** field, type `10022`.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**

2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:

   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Service outage

Important:

Service outage begins at this point of the upgrade process.

Postupgrade tasks on the first staged Release 6.3.6 active server

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Verifying the Communication Manager operation

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Administering the node name for server A for each duplex survivable core

Start a SAT session.

Complete this task on the main server only.

Perform this task after you upgrade an S8700-Series main server from Communication Manager releases earlier than 5.2.1 to Release 5.2.1 or later; and if the main server has administered survivable servers of type “ESS D” as observed on the **`list survivable-processor`** screen.

During the upgrade, the system performs the following actions on the upgraded main server:

- Transfers the server A node name on the System Parameters ESS SAT screen of the preupgrade main server to the **ACTIVE SERVER IP Address** field on the Survivable Processor screen of the upgraded main server.
- Sets the **SERVER A Node Name** field on the Survivable Processor screen to blank. Because of this action, ESS alarm 799 is generated on the main server.

Procedure

1. Enter `list survivable-processor` and search for “ESS D” to locate the servers that need administering.
2. Enter `change survivable-processor New-node-name`, where, New-node-name is the node name assigned to the survivable core server.

   You can determine the node name from the list survivable-processor screen.
3. Administer the node name of the ESS server A.

   The alarm clears after the Server A node name is administered for the duplex survivable core server.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.

6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Postupgrade tasks on the second staged Release 6.3.6 busied out server

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8700-Series servers to the HP DL360 G8 or Dell R620 Servers

Introduction

This section describes the procedure to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 on S8700-Series servers to Release 6.3.6 on HP DL360 G8 Servers or Dell R620 Servers.

In this upgrade procedure, you replace the S8700-Series servers with HP DL360 G8 Servers or Dell R620 Servers running System Platform and the duplex main/survivable core template, CM_Duplex.

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Converting from fiber port networks to IP-PNC on page 1406.

- For Communication Manager Release 3.0 and later, perform the conversion before you upgrade the servers.
- For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.

- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8700-Series servers to Communication Manager Release 4.0.5 or Release 5.2.1.
   - For servers that you can upgrade directly to Release 4.0.5 or Release 5.2.1, see *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers*, 03-602885.
   - For S8700 Servers, see *Upgrading Servers to the Avaya S8800 Server for Avaya Aura® Communication Manager*, 03-603445.
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.3.6.
3. Perform the upgrade to Release 6.3.6 as described in this section.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.3.6:

- The main server
- The survivable server

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and*

Table continues…

✔	Task	Description
		Software Updates on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information about the procedure and specific commands, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Media Gateways, and Servers*, 03-300431
- *Avaya Aura® Communication Manager Server Alarms* , 03-602798

Preupgrade tasks on the active S8700-Series Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**

   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**
     c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
     d. In the **Download size** field, enter the size of the backup `.tar` file.

        If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.

5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Converting fiber PNs to IP-PNC

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Converting from fiber port networks to IP-PNC on page 1406.

Note:

For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

Do not select the **Install this file on the local server** check box.

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.

3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Preupgrade tasks on the standby S8700-Series Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. Verify that the **CM Reports as:** field displays one of the following:

   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.

   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure

Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**

- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:
  a. Select **Specify Data Sets**.
  b. Select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
     - **Communication Manager Messaging (CMM)**
  c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
  d. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.

b. Click **Yes**.

4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the duplication cable

Procedure

1. Label and disconnect the duplication fiber cable (if present) from the server.
2. Label and disconnect the duplication interface IP cable from the server.

Removing the server from the rack

Procedure

1. Label and disconnect all remaining cables.
2. Disconnect the laptop from the Services port.
3. Disconnect the power cord from the UPS.
4. Disconnect USB flashcard reader or writer.
5. Disconnect any modem.
6. Remove the server from the rack, if necessary.
7. Remove the rails from the rack.

Installing the servers in the rack

Install the new servers in the rack. At this point do not connect the servers to any network. For instructions to install the servers in the rack, see the following documents:

- For Dell R620 Server, see *Installing the Dell™ PowerEdge™ R620 Server*.
- For HP DL360 G8 Server, see *Installing the HP ProLiant DL360p G8 Server*.

Upgrade tasks on the first HP DL360 G8 or Dell R620 Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the server

Procedure

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

   Important:

   Do not release the server until instructed.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix B on page 1381.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying connectivity

To verify if the Ethernet port is working, ping the FTP server, where you saved the backup files.

Procedure

1. Under **Diagnostics**, click **Ping**.
2. Complete one of the following:
   - If the system has IPSIs configured on it, select the IPSIs and the cabinet numbers.
   - In the **Host Name or IP address** field, enter the IP address of the device on which you stored the backup files.
3. Click **Execute Ping**.

   If the ping fails, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300432).

Completion tasks on the active S8700 Server

Perform the following two procedures on the active S8700 Server.

Important:

After you complete the two mentioned tasks, at this point, the system is out of service as both the S8700 servers are shutdown. To minimize this time, shut down the active S8700 Server, access the first HP DL360 G8 Server or Dell R620 Server and release the server immediately.

Continue with the upgrade procedures on the HP DL360 G8 Server or Dell R620 Server.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.

3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the server from the rack

Procedure

1. Label and disconnect all remaining cables.
2. Disconnect the laptop from the Services port.
3. Disconnect the power cord from the UPS.
4. Disconnect USB flashcard reader or writer.
5. Disconnect any modem.
6. Remove the server from the rack, if necessary.
7. Remove the rails from the rack.

Postupgrade tasks on the first HP DL360 G8 or Dell R620 Server

Accessing the new server

Procedure

1. Clear the ARP cache on the portable computer, if necessary.
2. Open a Web browser and log onto the server using System Management Interface.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Perform this procedure on the main server only.

Procedure

Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431

- *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.

- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Upgrade tasks on the second HP DL360 G8 or Dell R620 Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Connecting the cables to the server

Procedure

1. Connect the server to customer LAN.

2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

     Important:

     Do not release the server until instructed.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile,

Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.

3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8800 Server to S8800 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager from Release 5.2.1 on duplex S8800 Servers to Release 6.3.6 by using System Platform and the duplex main/survivable template on S8800 Servers.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.2.

Perform the following additional tasks to reuse the existing server:

- Increase the memory
- Add a third hard drive
- Update the uEFI firmware
- Reconfigure the RAID controller to support RAID 5
- Update the uEFI settings

Note:

For instructions to update the uEFI firmware and uEFI settings, download the release notes for Release 6.3.6 from the Avaya Support website at http://support.avaya.com.

For more information, see the *Avaya S8800 Migration Kit*.

Use this section to upgrade:

- The main server
- The survivable server

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade.

✔	Task	Description
	Verify that you have the required software. • System Platform • Communication Manager template	
	Verify that you have all the necessary equipment onsite, for example: • Hard disk drive • Memory module • Services laptop and crossover cable • Electrostatic wrist ground strap and mat	For the list of required equipment, see *Avaya Migration Kit.*
	Obtain the CD-ROM to update the uEFI firmware using one of the following ways: • Order the *uEFI firmware* CD-ROM • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD-ROM.	
	Obtain the *RIAD 5 firmware* CD-ROM	
	Obtain the CD-ROM to update the uEFI settings using one of the following ways: • Order the *uEFI settings* CD-ROM • Download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD-ROM.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information about the procedure and specific commands, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Media Gateways, and Servers*, 03-300431
- *Avaya Aura® Communication Manager Server Alarms* , 03-602798

Preupgrade tasks on the active S8800 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

   If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
3. In the **Download size** field, enter the size of the backup `.tar` file.

   If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.

b. Click **Yes**.

4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Verifying the hardware on the server

Log on to System Management Interface.

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.

   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Preupgrade tasks on the standby S8800 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server

security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.

2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**

c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

d. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.

5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**

- **Directory**

  The backup location must be a server on the customer LAN.

4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Verifying the hardware on the server

Log on to System Management Interface.

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.

   The system opens the Display Configuration page.

3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.

3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server cover

Before you disconnect the server from the power source, make a note of which LEDs light up, including the LEDs that light up on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs do not light up when the power source is removed.

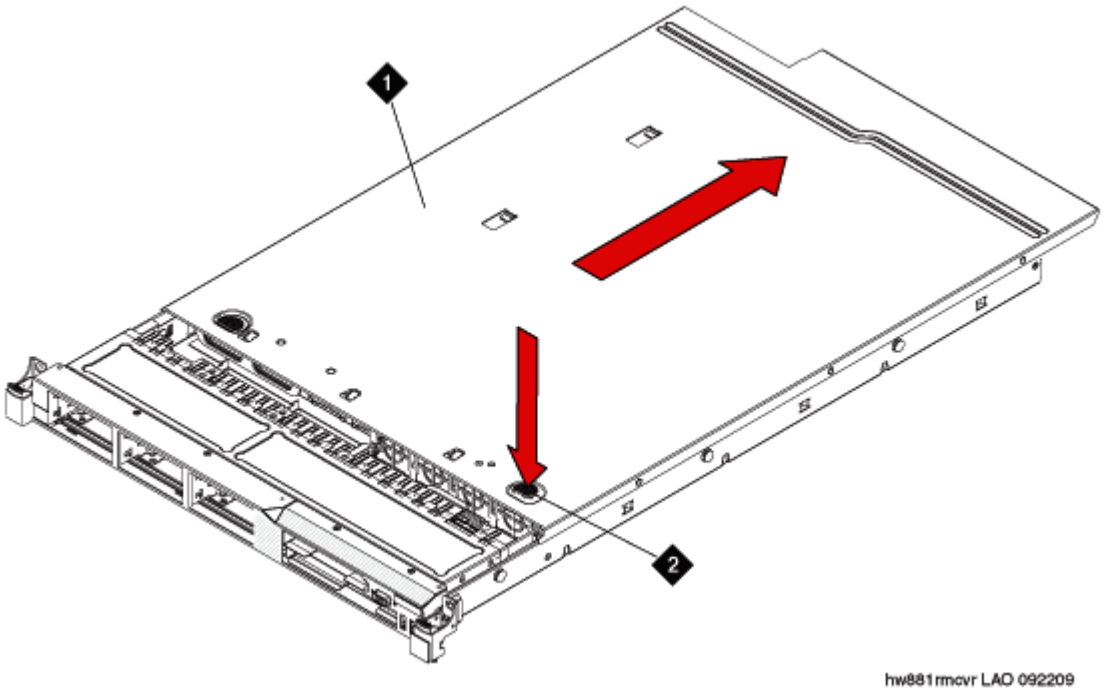
Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
   a. Turn off the server and all attached devices.
   b. Label and disconnect all power cords and external cables.
3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Press down firmly on the blue tab on the top (near the front of the server) of the cover and slide the cover toward the back of the server until the cover has disengaged from the chassis. See the following figure.



1	Cover
2	Tab

5. Lift the server cover off the server and set it aside.

Important:

For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Adding the memory module

Removing the DIMM air baffle

You must remove the DIMM air baffle to replace or install a memory module.

Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

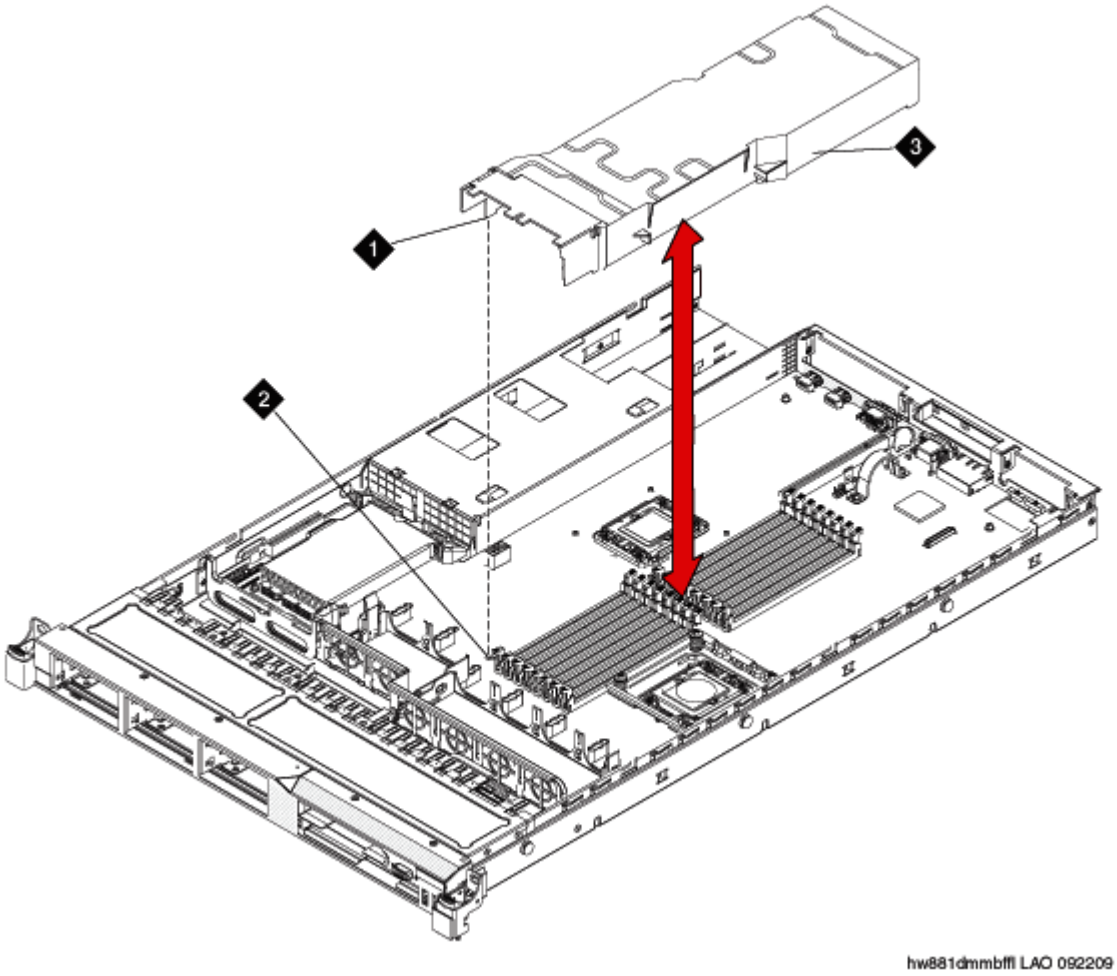
Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.

3. Remove the cover.
4. Lift the DIMM air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Installing a memory module

Remove the DIMM air baffle.

Important:

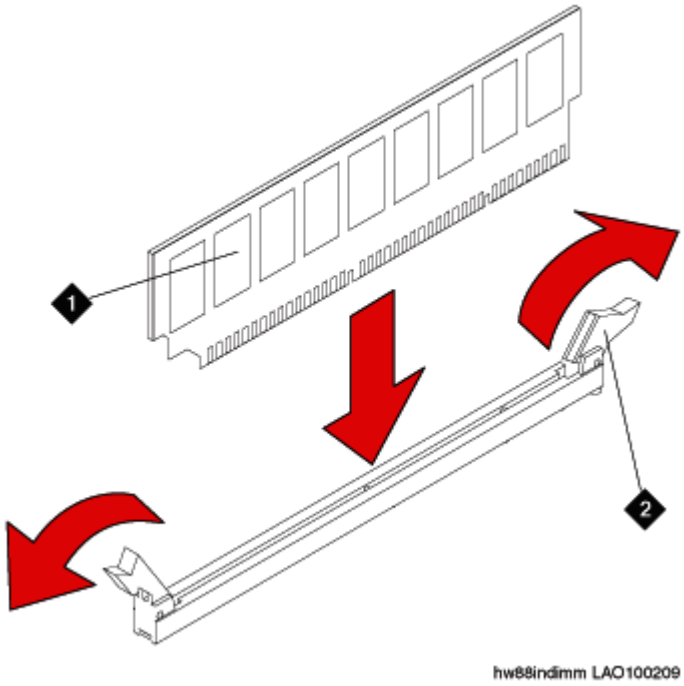
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

   Important:

   Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



hw88indimm LAO100209

1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.

   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

Important:

If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.

7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.
8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.

    When you install or remove memory modules, the server configuration information changes. When you restart the server, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

You must install the DIMM air baffle after you install a memory module.

Caution:

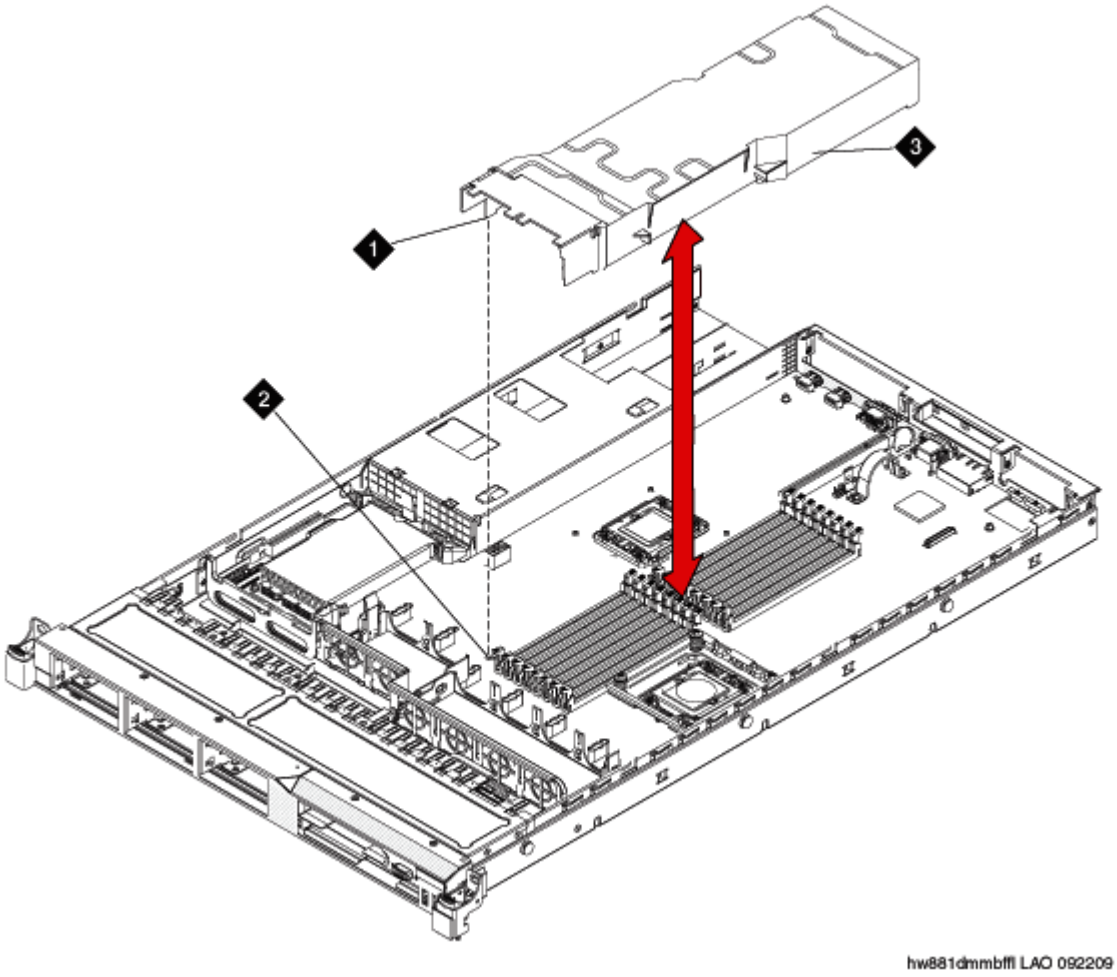
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to the DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Installing a hard disk drive

If replacing an existing hard drive, remove the hard drive that you want to replace.

Important:

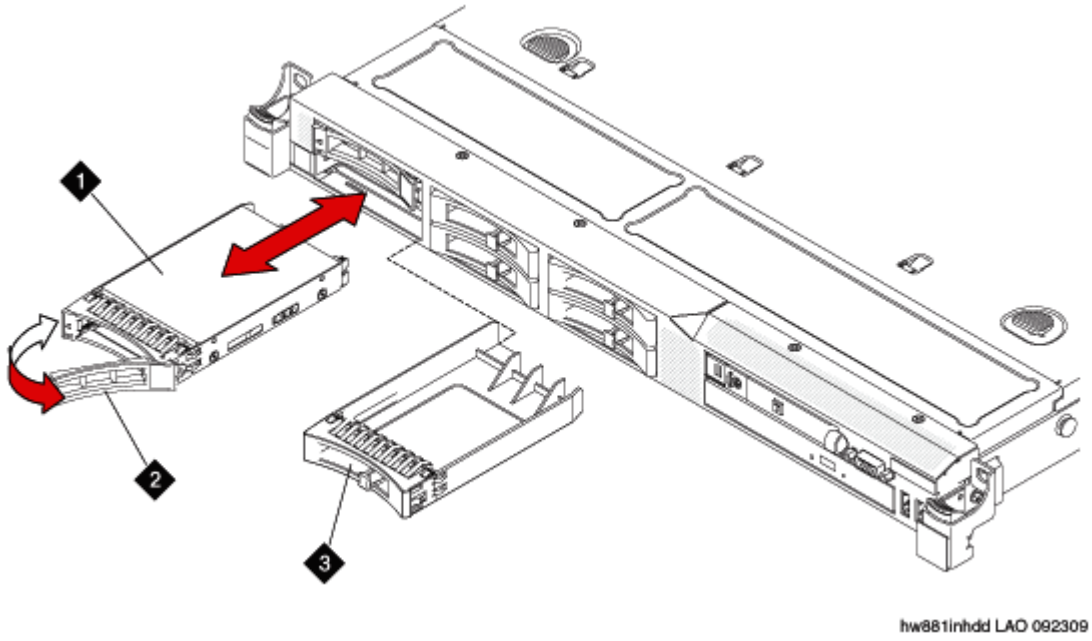
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. An amber LED that remains lit indicates a faulty drive that you must replace.

Updating S8800 server firmware

- Obtain the CO-ROM for uEFI firmware. You order the CO-ROM or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

- Obtain the CD for RAID 5 firmware. You must either order the CD or download the `S8800RAIDTool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for configuring the RAID 5 firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

The conversion process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

Procedure

1. Insert the RAID 5 firmware CD into the disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following message:

   ```
   ... 3 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings....
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server, reboot the server and run the configuration tool again. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Install the `S8800uEFITool.iso` updates.

Updating uEFI settings

- Obtain the CO-ROM for uEFI settings of S8800 Server. You order the CO-ROM or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks on the standby server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix B on page 1381.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.

7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Tasks on the active S8800 server

Completion tasks on the active S8800 Server

When you shutdown the active S8800 Server as outlined in the following procedure, the service outage begins.

Important:

To minimize the downtime, shut down the active S8800 Server, access the standby S8800 Server and release the server in the shortest amount of time possible.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Upgrade tasks on the standby server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrade tasks on the S8800 Server that is shutdown

Removing the server cover

Before you disconnect the server from the power source, make a note of which LEDs light up, including the LEDs that light up on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs do not light up when the power source is removed.

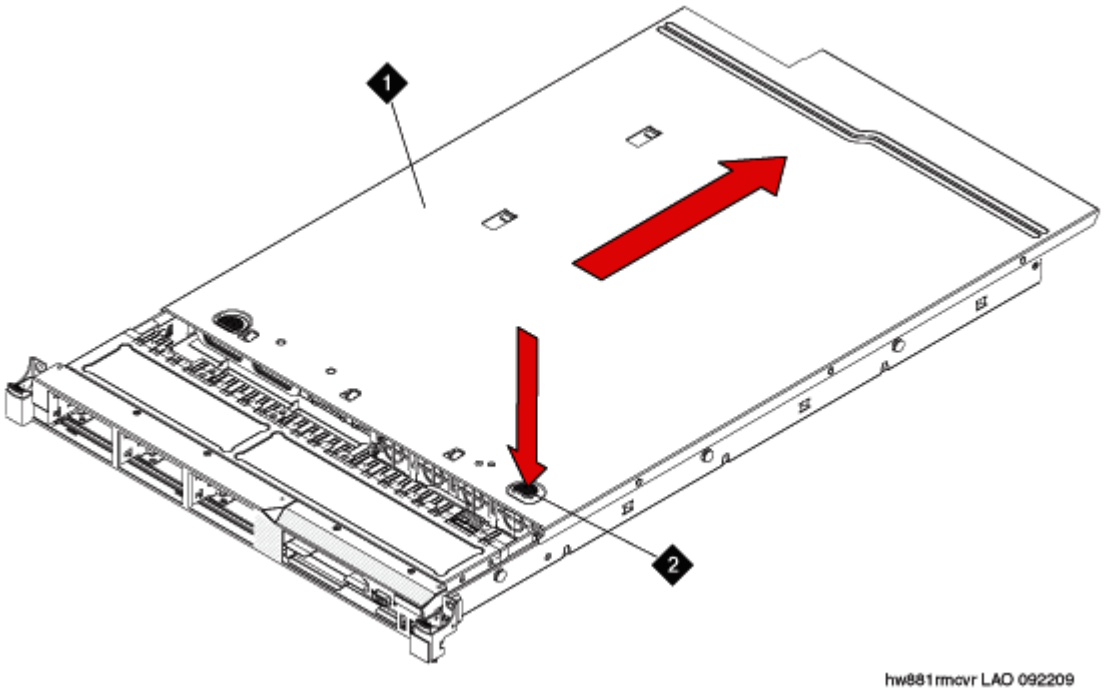
Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
   a. Turn off the server and all attached devices.
   b. Label and disconnect all power cords and external cables.
3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Press down firmly on the blue tab on the top (near the front of the server) of the cover and slide the cover toward the back of the server until the cover has disengaged from the chassis. See the following figure.



1	Cover
2	Tab

5. Lift the server cover off the server and set it aside.

Important:

For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Adding the memory module

Removing the DIMM air baffle

You must remove the DIMM air baffle to replace or install a memory module.

Caution:

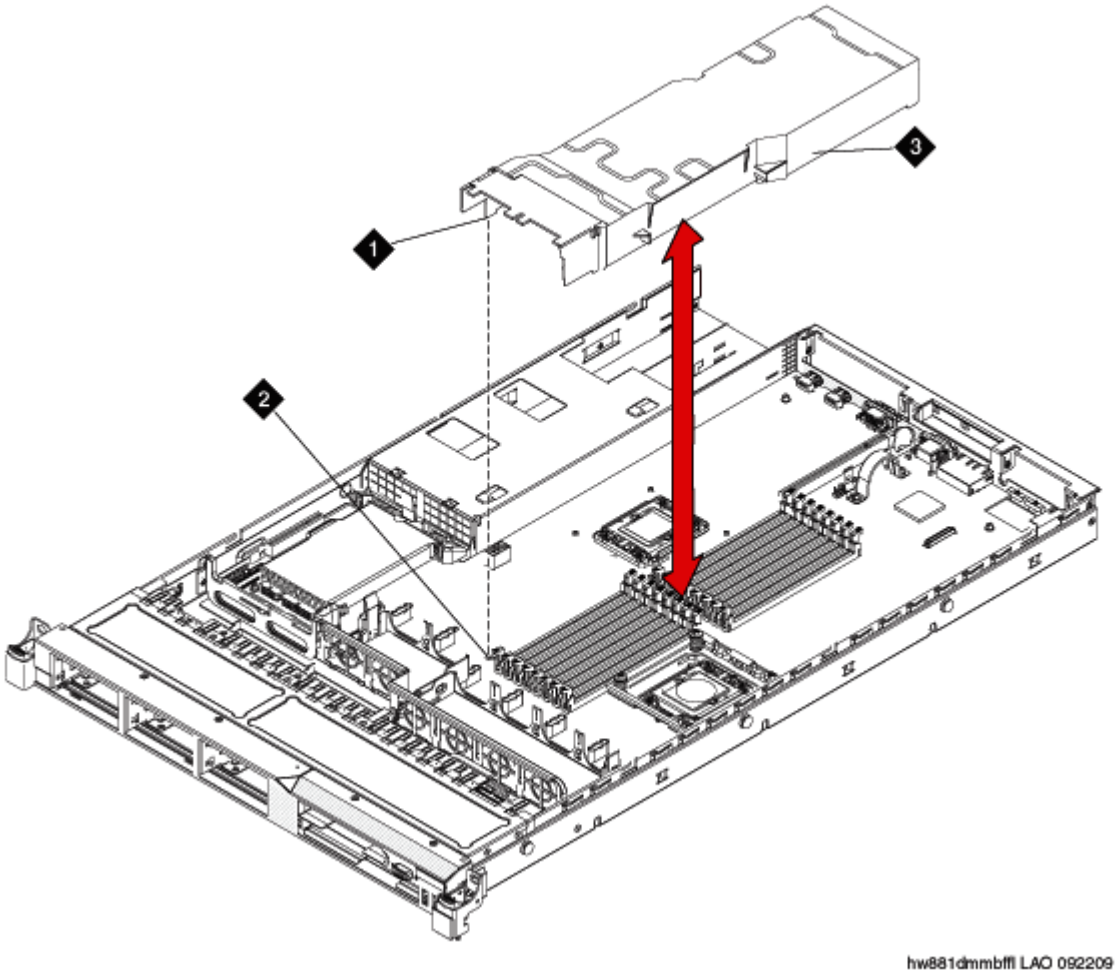
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Lift the DIMM air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Installing a memory module

Remove the DIMM air baffle.

Important:

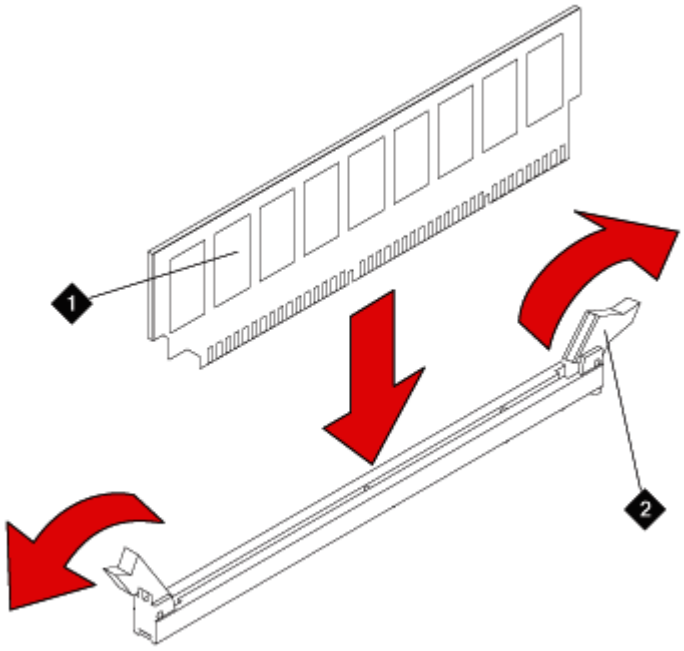
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

Important:

Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



hw88indimm LAO100209

1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.

   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

   Important:

   If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.
7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.

8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.

    When you install or remove memory modules, the server configuration information changes. When you restart the server, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

You must install the DIMM air baffle after you install a memory module.

Caution:

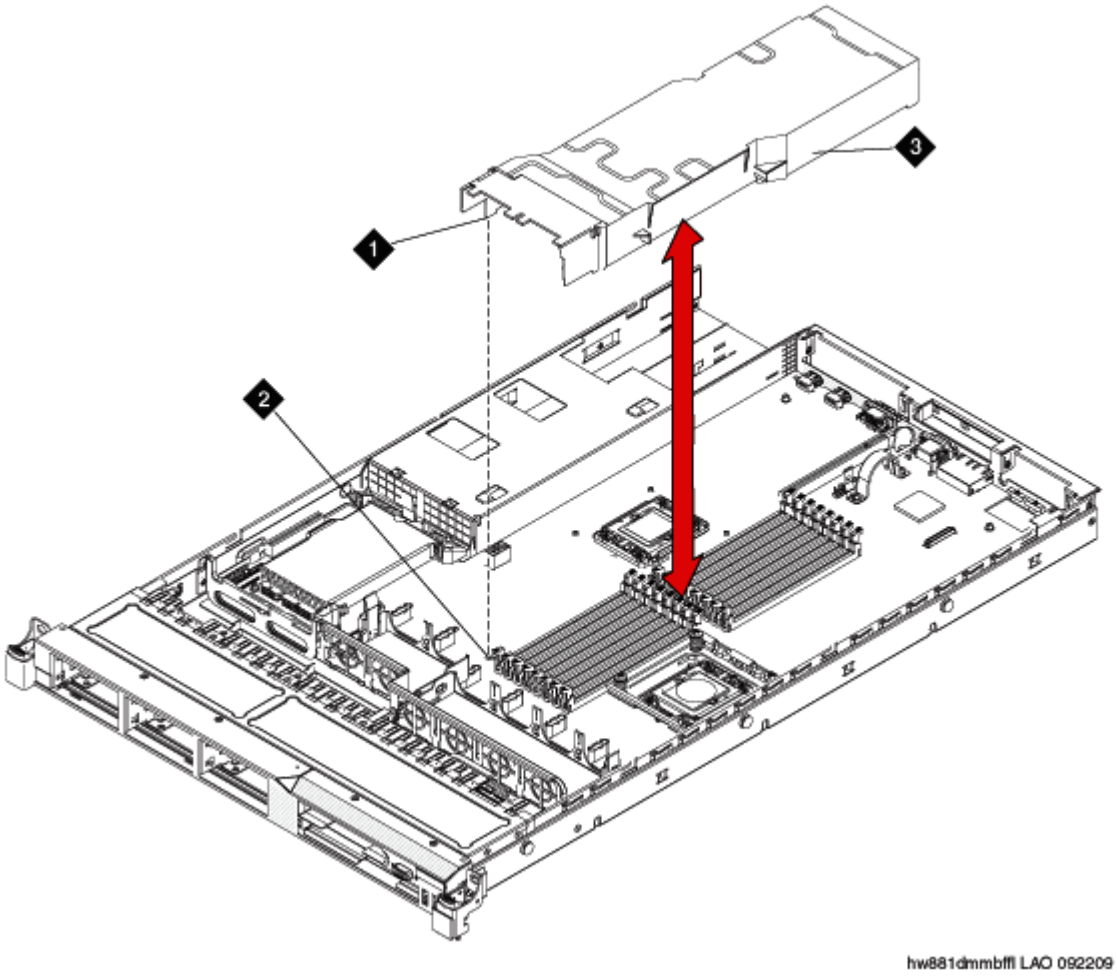
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to the DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Installing a hard disk drive

If replacing an existing hard drive, remove the hard drive that you want to replace.

Important:

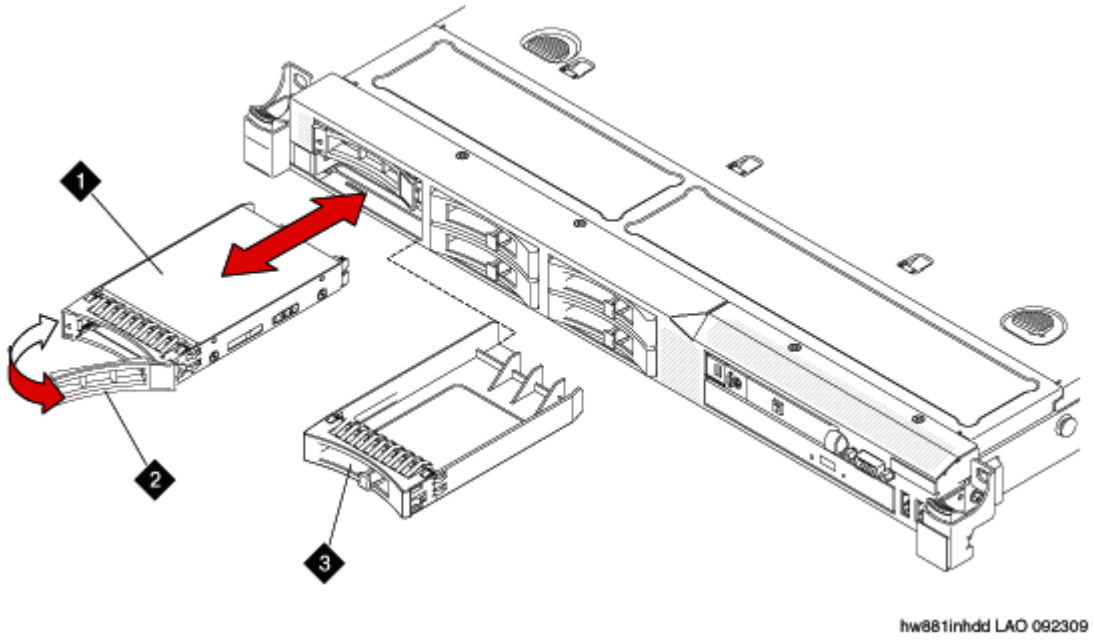
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 236.

Procedure

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. An amber LED that remains lit indicates a faulty drive that you must replace.

Updating S8800 server firmware

- Obtain the CO-ROM for uEFI firmware. You order the CO-ROM or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

- Obtain the CD for RAID 5 firmware. You must either order the CD or download the `S8800RAIDTool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for configuring the RAID 5 firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

The conversion process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

Procedure

1. Insert the RAID 5 firmware CD into the disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following message:

   ```
   ... 3 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings....
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server, reboot the server and run the configuration tool again. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Install the `S8800uEFITool.iso` updates.

Updating uEFI settings

- Obtain the CO-ROM for uEFI settings of S8800 Server. You order the CO-ROM or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800uEFITool.iso` file on the server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Connecting the cables to the server

Procedure

1. Connect the server to customer LAN.

2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

     Important:

     Do not release the server until instructed.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

   Note:

   You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

   - - https://<*IP_Address*>
   - https://<*FQDN*>

     Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Installing service pack

- Copy the latest service packs from the Avaya Support Site to the services portable computer.
- Log on to System Platform Web Console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:

You must perform this task before you proceed to the next upgrade procedures.

Procedure

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

Note:

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**

- **Host Name**
- **Directory** or **File Path**
  - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix B on page 1381.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.

c. Click **Server** > **Process Status**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the active server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site,

the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Perform this procedure on the main server only.

Procedure

Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431

- *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.

- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the standby server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

Note:

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

On the Change Current Schedule Web page, click **Change Schedule**.

- To remove the schedule backup, click **Remove**.

  The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are

significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager from Release 5.2.1 on duplex HP DL360 G8 Servers to Release 6.3.6 using System Platform and the duplex main/survivable template on HP DL360 G8 Servers.

In this upgrade procedure, you:

- Reuse the HP DL360 G8 Server.
- Install System Platform and the duplex main/survivable template, CM_Duplex, on the existing servers.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with the new G450 or G430 Branch Gateway.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Use this section to upgrade:

- The main server
- The survivable server

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.

Table continues…

✔	Task	Description
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support website at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information about the procedure and specific commands, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Media Gateways, and Servers*, 03-300431

- *Avaya Aura® Communication Manager Server Alarms* , 03-602798

Preupgrade tasks on the active HP DL360 G7 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.

7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Preupgrade tasks on the standby HP DL360 G7 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**

- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**
- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.

3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.

5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Upgrade tasks on the standby server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix B on page 1381.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.

3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Tasks on the active HP DL360 G7 Server

Completion tasks on the active HP DL360 G7 Server

When you shutdown the active HP DL360 G7 Server as outlined in the following procedure, the service outage begins.

Important:

To minimize the downtime, shut down the active server, access the standby server and release the server in the shortest amount of time possible.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Upgrade tasks on the standby server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative

uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrade tasks on the server that is shutdown

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

Note:

You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Connecting the cables to the server

Procedure

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

     Important:

     Do not release the server until instructed.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (cdom).

Note:

You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

- - https://*<IP_Address>*
- https://*<FQDN>*

  Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix B on page 1381.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the active server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

Comments on this document? infodev@avaya.com

If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Perform this procedure on the main server only.

Procedure

Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.

3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the standby server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8800 Server to HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 on duplex S8800 Servers to Release 6.3.6 on HP DL360 G8 Servers or Dell R620 Servers.

In this upgrade procedure, you:

- Replace one of the following:
  - S8800 Server with an HP DL360 G8 Server or Dell R620 Server.
  - HP DL360 G7 Server or Dell R610 Server with an HP DL360 G8 Server or Dell R620 Server.
- Install System Platform and the duplex CM main/survivable template, CM_Duplex, on the new servers.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with the new G450 or G430 Branch Gateway.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration.

You require a new license for Communication Manager.

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Converting private control networks to corporate LAN on page 1403.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information about the procedure and specific commands, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Media Gateways, and Servers*, 03-300431
- *Avaya Aura® Communication Manager Server Alarms* , 03-602798

Preupgrade tasks on the active S8800 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**

- **Set Identities**
- **Configure Interfaces**
- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**
- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Preupgrade tasks on the standby S8800 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. Verify that the **CM Reports as:** field displays one of the following:

   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.

   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.

3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.

4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Installing the servers in the rack

Install the new servers in the rack. At this point do not connect the servers to any network. For instructions to install the servers in the rack, see the following documents:

- For Dell R620 Server, see *Installing the Dell™ PowerEdge™ R620 Server*.
- For HP DL360 G8 Server, see *Installing the HP ProLiant DL360p G8 Server*.

Duplex main/survivable core template

You are required to install duplex main/survivable core template on each server using a new host name and new IP address.

After you complete the duplex main/survivable core template installation and restore the upgrade dataset, you must configure each server in the server pair to use the Communication Manager Release 5.2.1 server host name and IP address for the Communication Manager Release 6.0.x server configuration for **Alias Host Name** and **Alias IP address**. Refer Appendix C on page 1391 for the worksheet to use for configuring the server.

Upgrade tasks on the first HP DL360 G8 or Dell R620 Server

State of the existing server

The existing server continues to provide service until later in the procedure. Do not shut down the existing server until instructed.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the new server

Procedure

1. Do not connect the server to the network until the procedure in this section instructs.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.

- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing System Management Interface

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Note on restore

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

- Log on to System Management Interface.

- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the active S8800 Server

Shutdown the active S8800 Server as outlined in the following procedure and connect the first HP DL360 G8 Server or Dell R620 Server to the network.

Important:

After you shutdown the active S8800 Server, at this point, the service is nonfunctional. To minimize this time, shut down the active S8800 Server, access the first HP DL360 G8 Server or Dell R620 Server again and release the server in the shortest amount of time possible.

Shutdown tasks on S8800 Server

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

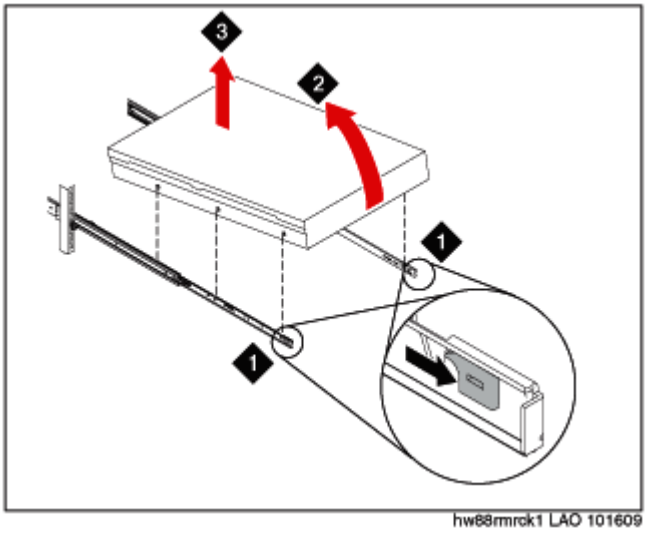
Procedure

1. Label and disconnect the power cords from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server from the rack

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Push the locking levers (1) forward. See the following figure.



4. Lift up the front of the server (2). See the preceding figure.
5. Pull the server out of the rack (3). See the preceding figure.

Postupgrade tasks on the first HP DL360 G8 or Dell R620 Server

Accessing the new server

Procedure

1. Clear the ARP cache on the portable computer, if necessary.
2. Open a Web browser and log onto the server using System Management Interface.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Procedures that you must skip on the survivable server

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading the survivable server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling the scheduled maintenance

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Perform this procedure on the main server only.

Procedure

Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.

2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Upgrade tasks on the second HP DL360 G8 or Dell R620 Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.

2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.

- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Connecting the cables to the server

Procedure

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

     Important:

     Do not release the server until instructed.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix C on page 1391.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.

3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.

3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading DEFINITY SI or R Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade the following existing DEFINITY Servers to Communication Manager Release 6.3.6 on HP DL360 G8 Servers or Dell R620 Servers:

- DEFINITY SI Server in an SCC1 or an MCC1
- DEFINITY R Server in an MCC1

In this procedure, you must discard the cabinet and move the supported circuit packs to G650 Media Gateway. You install the new servers running System Platform and the duplex CM main/survivable template (CM_Duplex).

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- Installing translation file on Communication Manager Release 6.3.6.
- Administering IPSIs on Communication Manager Release 6.3.6.
- Installing G650 Media Gateway.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

The upgrade affects service. When you turn off the PPN stack to replace the cabinet during the upgrade process, the system drops all the calls. The system becomes operative when the new

server takes control of the IPSIs. Before you turn off the cabinets, perform the following administration tasks.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following server, as appropriate: - HP DL360 G8 - Dell R620 • G650 Media Gateway • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP or later C-LAN	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

You require the following additional documentation:

Sl. no	Task	Description	✔
	Implementing Avaya Aura® Communication Manager, 03-603558	Provides instructions for installing and configuring Communication Manager.	
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.	
	Installing the Avaya G650 Media Gateway, 03-300685	Provides instructions for installing and configuring G650 Media Gateway.	

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PNs to prepare the DEFINITY system for upgrade. The changing or upgrading the hardware includes:

- Changing TN2182 Tone Clock and maintenance circuit packs for TN2312BP IP Server Interfaces (IPSI) and new TN779D maintenance circuit packs
- Connecting the IPSI circuit pack to the customer network.
- Assigning static IP address to the IPSI circuit pack.

You can perform these tasks while the existing system is in service. However, duplex-reliability configurations encounter short service interruptions when you change the tone-clock circuit pack is in IPSI-controlled PNs.

Server and IPSI cable connections

Each IPSI circuit pack must have a CAT5 cable that connects to the customer network. Cables for IPSIs are located in PN carrier A. If the system has a duplicated bearer network, the cables for IPSIs are located in PN carrier B.

In duplex configurations, each server is connected to the customer network that comprise control network A (CNA). If this system has duplicated IPSIs, each server is connected to the customer network that comprise control network B (CNB).

Saving translations

Start a SAT session.

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Replacement of circuit packs

All PNs receive IPSI circuit packs. The TN2312BP IPSI circuit pack replaces the existing TN2182 Tone Clock circuit pack and terminates control communication with the servers. Flat ribbon cables run between the IPSIs and the maintenance circuit pack. These ribbon cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit packs, program static IP addresses into the IPSIs.

You can complete this stage at any time before the cutover. The tone clock and the IPSI circuit packs are hot swappable, and you replace the circuit packs in the existing DEFINITY system without the need to turn off the power.

The IPSI circuit pack provides the same functionality as the tone clock circuit pack. You perform the following tasks before the cutover:

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSIs are working as tone clocks in the existing system.
- Test the connectivity between the server and the IPSI.
- Reinstall the IPSIs in the new carriers after you install the carriers.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

A cross-over cable to connect your services laptop directly to the processor.

Procedure

1. Perform one of the following tasks to connect the services laptop to the processor:
   - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Recording node names and IP addresses

Procedure

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

After the upgrade, the names and addresses must remain the same.

Upgrade tasks on both the new servers

Installing the servers in the rack

Install the new servers in the rack. At this point do not connect the servers to any network. For instructions to install the servers in the rack, see the following documents:

- For Dell R620 Server, see *Installing the Dell™ PowerEdge™ R620 Server*.
- For HP DL360 G8 Server, see *Installing the HP ProLiant DL360p G8 Server*.

Sequence of tasks to be performed on each of the server

Complete the procedures starting from Installing System Platform and Communication Manager through Rebooting the server on the first HP DL360 G8 Server or Dell R620 Server. Repeat the procedures on the second HP DL360 G8 Server or Dell R620 Server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

3. Click **Browse** to open the **Choose File** window on your computer.

4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the translations

Log on to System Management Interface.

You restore the translations only on the main server. When a survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:

   Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.
6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.

9. Click **Status** to view the status of restore process.

When the restoration is complete, the system displays the following message:

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix B on page 1381.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verification tasks on the HP DL360 G8 or Dell R620 Servers

Starting a SAT session

Log on to the services port from a directly connected laptop.

Procedure

1. Perform one of the following:
   - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.

- If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Busying out the standby server

Log on to System Management Interface of the standby server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Log in as `craft` or `dadmin`.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

Tasks on the first HP DL360 G8 or Dell R620 Server

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the connection for server duplication

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. On the Ping page, in the **Endpoints to Ping** section, click **Other server via duplication link**.
4. Click **Execute Ping**.

   If the two endpoints are connected, the system displays the message `MessRecv: 1`.
5. In the navigation pane, click **Server** > **Status Summary** and perform the following:
   a. Verify that this server is in `Active` mode.
   b. Verify that the other server is in `BUSY OUT` mode.

   If the mode of the other server is `Not Ready`, it implies that the server duplication is not functional. Do not proceed until the server duplication is functional.

   If the server duplication connection is successful, the system displays, `Duplication Link: up`.

Postupgrade administration on both the servers

Connecting a laptop to the server

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the **Host Name (or IP Address)** field, type **192.11.13.6**.
4. Select the **SSH** protocol.
5. In the **Port** field, type **10022**.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the host key of the server.

The system displays the PuTTY window.

8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:

   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser

to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Administering the Communication Manager system parameters for IPSI

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Installing G650 Media Gateway in the rack

Procedure

Install G650 Media Gateway in the rack. For instructions, see *Installing the Avaya G650 Media Gateway* (03-300685).

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.

7. If the IPSI circuit pack uses a default gateway, type `set control gateway gatewayaddr`, where gatewayaddr is the IP address for the network gateway that the customer-provided.
8. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack cabinetnumber` to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

4. For G650, if the maintenance function is used:
   a. Connect one end of the serial maintenance cable to the DB9 connector on the IPSI adapter.
   b. Connect the other end to the Emergency Transfer panel to provide 1 alarm output and 2 alarm inputs.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Start a SAT session.

Procedure

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Port network circuit packs

Because you do not reuse the PPN after the upgrade, you must:

- Relocate the port network circuit packs to a new G650 Media Gateway.
- Remove all port network circuit pack translations related to the PPN. The STS group manages the translation changes necessary for this upgrade.

Adding IPSI information

Start a SAT session.

Procedure

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you also adjust the administration of the network regions. Your planning documents provide the information about

changes to network regions. For more information on how to administer the network regions, see *Administering Network Connectivity on Avaya Aura® Communication Manager,* 555-233-504.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit pack

Start a SAT session.

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6
     - DiffServ: 46
3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed

- **Auto** (port negotiation): `n` to modify as per the network configuration.
  - **Duplex full**
  - **Speed 100**

3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

Procedure

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

Note:

If you do not have a gateway IP address, leave the **Gateway Address** field blank.

7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.

10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Removing fiber-related administration

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

Procedure

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link n`, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link n`.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Disabling PNC duplication

If the bearer network is duplicated, remove the duplication before you remove the fiber-optic connections. If the system does not have PNC duplication, continue with the next procedure.

Procedure

1. To check which of the duplicated PNCs is active, enter `status pnc`.
2. To busyout the standby PNC, enter `busyout pnc-standby`.
3. To open the duplication screen, enter `change system-parameters duplication`.
4. In the **Enable Operation of PNC Duplication** field, enter `n` and click **Submit**.

Administering PN synchronization

Start a SAT session.

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

Procedure

1. To view the synchronization information for the IP-PNC PNs, enter `list synchronization` and `status synchronization`.
2. Verify that the following fields are blank:
   - The **Primary** and the **Secondary** fields on the Synchronization Plan window.
   - The **Source Physical Location** field on the Synchronization Status window.
3. Enter `change synchronization port-network n`, where *n* is the PN number of the converted port network that requires synchronization.
4. Enter `list cabinet`.

   The system displays a list of all the cabinets and the PNs that the cabinets contain in the **Circuit Packs Available for Synchronization** section.

5. Obtain a location for the synchronization source circuit pack from the list in the **Circuit Packs Available for Synchronization** section for **Primary** and **Secondary** fields. Select a synchronization source that works.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, in the **Secondary** field, add another location for synchronization-source circuit pack.
8. Press `Submit`.

   Wait for about 5 minutes for Communication Manager to update the synchronization plan.
9. To verify the changes, enter `list synchronization` and the `status synchronization` commands.
10. If the **Switching Capability** field for this PN is disabled on the Synchronization Status window, enter `enable synchronization all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must display `PASS` in the **Results** field. If the **Results** field does not display `PASS`, troubleshoot the synchronization error.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

1. Remove the fiber cables that connect the following circuit packs in the PNs:
   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Cutover to the server control

Because you do not reuse the PPN, you relocate the port network circuit packs to G650 Media Gateway.

When you relocate the circuit packs to the media gateway and you turn on the power, you want to cut over to have the new server control the existing PNs. The server can be an HP DL360 G8 Server or a Dell R620 Server. To cut over to the server, you must enable the IPSIs on the IP Server Interface (IPSI) System Parameters screen.

This stage affects service momentarily while the CSS comes up and the calls load balance across the IPSIs throughout the port networks.

Decommissioning the PPN

Because you do not reuse the PPN on the upgraded system, you must relocate the port network circuit packs to the new media gateway.

Procedure

1. Turn off power to the PPN.
2. Remove all circuit packs from the PPN and place in antistatic bags. Set aside the port circuit packs for reuse.
3. Remove power supplies from the expansion control carriers.
4. Remove faceplate from the expansion control carriers.
5. Disconnect the following cables on the back of carrier A.
   - CURL
   - TDM/LAN
   - ICC-A and ICC-B
6. Remove the Current Limiter (CURL) unit from the back of the carrier. You can reuse the CURL.
7. Remove all carrier grounds.
8. Remove the expansion control carriers from the cabinet.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

   Caution:

   The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

   Note:

   If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.

2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

   Note:

   You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or if you want to minimize out-of-service time.
4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
   - CURL - you cannot reuse this cable.
   - TDM/LAN - you can reuse this cable.
   - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on the first HP DL360 G8 or Dell R620 Server

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.

3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Verifying the Communication Manager operation

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.

3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Postupgrade tasks on the second HP DL360 G8 or Dell R620 Server

Connecting the server to network

At this point, the service outage occurs.

Procedure

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Releasing the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are

significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Interchanging the servers

Log on to System Management Interface.

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Chapter 6: Upgrading to embedded main template

Upgrading DEFINITY SI or CSI Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the following DEFINITY Servers to Communication Manager Release Release 6.3.6 on S8300D Server running System Platform and the embedded main template.

- DEFINITY SI Server in a SCC1 or an MCC1
- DEFINITY CSI Server in a CMC

In this procedure, you must:

- Discard all the circuit packs and the cabinet.
- Install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded main template, CM_OnlyEmbed.

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

For the CM_OnlyEmbed template, Communication Manager supports only small memory size and does not support medium and large memory size.

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring Communication Manager Release 6.3.6 on S8300D Server.
- (optional) Installing Communication Manager Messaging.
- Installing translation file on Communication Manager Release 6.3.6.

- Decommissioning the cabinets.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

You require a new license file for Communication Manager Release 6.3.6. This upgrade affects the service.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D server.

Table continues…

✔	Task	Description
	• *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Saving translations

Start a SAT session.

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Preupgrade administration

Connecting to the processor

Cross-over cable.

Procedure

1. Connect your Services laptop directly to the processor to access the cabinet.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Upgrade tasks

Inserting the S8300D Server in the branch gateway

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

Electrostatic alert:

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.
10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the translations

Log on to System Management Interface.

You restore the translations only on the main server. When a survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.

3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:

   Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.
6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the status of restore process.

When the restoration is complete, the system displays the following message:

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.

4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:

     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list IP of CM procr / clan`.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Enter `add media-gateway <number>`, where *<number>* is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

   To obtain the serial number of the branch gateway, on the command prompt of the gateway:
   - Enter `show system`.
   - Note the serial number of the branch gateway.

     The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.
4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

Note:

The subnet mask for the branch gateway must be the same as that of the S8300D Server.

5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.

6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.

4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:

   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.

   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs

3. Solution template service packs
4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.

4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

The default is **none**.

Removing fiber-related administration

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

Procedure

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link n`, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link n`.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

1. Remove the fiber cables that connect the following circuit packs in the PNs:
   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Decommissioning the cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

Caution:

The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

Note:

If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.

2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

Note:

You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or if you want to minimize out-of-service time.

4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
   - CURL - you cannot reuse this cable.
   - TDM/LAN - you can reuse this cable.
   - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on S8300D Server

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Communication Manager Messaging procedures

Perform the procedures related to Communication Manager Messaging only if Communication Manager Messaging is enabled on this server.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.

2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the cabinet and the circuit packs

Discard any hardware you replaced during the upgrade.

Procedure

1. Remove the cabinet from the rack.
2. Discard all the circuit packs you removed from the cabinet.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300A Server to S8300D Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 1.x, 2.0, or 2.0.1 on an S8300A Server toRelease 6.3.6 on an S8300D Server.

In this procedure, you replace the S8300A Server with an S8300D Server running System Platform and the embedded main template, CM_OnlyEmbed.

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

For the CM_OnlyEmbed template, Communication Manager supports only small memory size and does not support medium and large memory size.

The upgrade procedure involves:

- Upgrading Communication Manager Release 1.x, 2.0, or 2.0.1 on S8300A Server to Release 4.0.5 on S8300D Server.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.3.6.
- Replacing the S8300A Server with an S8300D Server in the G700 Branch Gateway.
- Installing System Platform and embedded main template on S8300D Server.
- Restoring the data set that was created while on Release 4.0.5.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Checking the FTP, SFTP, or SCP server information

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

Preupgrade tasks on the S8300 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Procedure

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.

2. Verify that the **Reports as:** field displays one of the following release numbers:

   - `R011x.02.0.110.4` for release 1.2
   - `R011x.03.2.536.1` for release 1.3.2
   - `R012x.00.0.219.0` for release 2.0
   - `R012x.00.1.221.1` for release 2.0.1

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Recording the configuration screens

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
7. Click **Cancel**.

   Important:

   Do not click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**

- **Alarms** > **SNMP Traps**
- **Server** > **Server Date/Time**
- **Security** > **Server Access**
- **Miscellaneous** > **CM Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.
    c. Enter `almsnmpconf` and record the output.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

To use Telnet, enable the Telnet service for Communication Manager.

If the Telnet service is disabled, use SSH to gain access to SAT.

Procedure

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity. This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files to the FTP server.

Backing up the files

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**
     a. Select **Translations, Names, and Messages**.
3. Under **Backup Method**, select **Network Device**.
4. In the **Method** field, select `FTP`, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **Start Backup**.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

Using the steps described in this section, you can download the following files:

- The latest available service pack for Communication Manager Release 4.0.5 or Release 5.2.1

- The RFA license for Communication Manager Release 4.0.5 or Release 5.2.1
- Avaya authentication file for Communication Manager Release 4.0.5 or Release 5.2.1
- Preupgrade service pack to upgrade from Communication Manager Release 4.0.5 or Release 5.2.1
- One of the following backup sets:
  - The three-part backup, `os_*.tar.gz`, `security_*.tar.gz`, and `xln_*.tar.gz`
  - Full backup, `full_*.tar.gz`

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Service pack for the current software version

You must obtain and activate the latest available service pack for the currently running Communication Manager software version before you proceed with the next upgrade steps. Depending on the release, use one of the following procedures to install the service pack.

Installing the preupgrade service pack on a server running release earlier than 2.0

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. Enter `cd /var/home/ftp` and press `Enter` to access the ftp directory.
5. At the prompt, enter `ls -ltr` and press `Enter`.

   The system displays a list of files in the `ftp` directory.
6. Verify that the directory contains the `*.tar.gz` file you have uploaded.
7. Enter `sudo patch_install patch.tar.gz`.

Here, *patch* is the release or issue number of the service pack file. For example, `03.1.526.5-1003.tar.gz`.

8. Enter `patch_show` and press `Enter` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch` and press `Enter`.

   Here, *patch* is the release or issue number of the service pack file. For example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name.

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes and more than 2 minutes if messaging is enabled. Wait until the restart or reset process is complete and enter additional commands.
10. Enter `patch_show again` and press `Enter` to list files to verify the new software file was applied.
11. Enter `statapp -c` to view the status of the processes.

    Make sure that all processes except dupmgr are `UP`. Communication Manager must display `65/65 UP` or, if Communication Manager Messaging is installed, must display `67/67 UP`. To stop the continual refresh of the statapp command, enter `Ctrl-C`.

    Note:

    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP indicate that a process did not come up and should be investigated before proceeding.
12. Close the Telnet session.

Installing the preupgrade service pack on a server running release 2.0

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6` and press `Enter`.
3. Log in as `craft` or `dadmin`.
4. Enter `update_unpack` and press `Enter`.
5. Select the number corresponding to the service pack file and press `Enter`.

   For example, `00.0.339.4-xxxx.tar.gz`.
6. Enter `update_show` and press `Enter` to list Communication Manager files and verify that the new service pack file is unpacked.
7. Enter `update_activate update` and press `Enter`, where update is the release or issue number of the latest service pack file.

For example, `00.0.339.4-xxxx`. Do not use the `.tar.gz` extension at the end of the file name.

If the media server reboots, it may display `/opt/ecs/sbin/drestart 2 4 command failed` message. Ignore this message. Wait until the restart or reset completes before entering additional commands. The media server displays a message that the service pack is applied.

8. Enter `update_show` and press `Enter` to list Communication Manager files and verify that the new service pack file is activated.
9. Close the Telnet session.

Backing up the files

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**
     a. Select **Translations, Names, and Messages**.
3. Under **Backup Method**, select **Network Device**.
4. In the **Method** field, select `FTP`, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **Start Backup**.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup

`os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

Recording configuration information

If you have not already completed, record the current server configuration data that you must configure on the new server. Use the worksheet provided in Worksheet for upgrading - to simplex and embedded templates on page 1376 to record the information.

Procedure

1. Click **Server Configuration** > **Configure Server**.
2. Click **Continue** on the first and second screen.
3. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
4. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
5. Select **Configure Interfaces** and record the following:
   - Server IP address
   - Gateway IP address
   - Subnet mask
   - Integrated Messaging IP address, if configured.
6. Click **Close**.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.

4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.

2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Upgrade tasks on the S8300D (Release 4.0.1 or 5.2.1) Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

Installing Communication Manager

CD/DVD for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

Procedure

1. On your laptop, click **Start** > **Run** to open the Run dialog box.
2. Enter `ping -t 192.11.13.6` and press `Enter`. Wait for the reply.

   The installation script looks for the software CD in the CD/DVD drive connected to the USB port. If the CD/DVD drive was not attached to a USB port when the server booted, the system displays the `Request Timed Out` message on the screen. You must then unseat and reseat the S8300D server in its slot.

   Tip:

   To navigate the installation screens, use the arrow keys to move to an option and press the space bar to select the option. Press `Enter`.
3. Select **Install** and press `Enter`.
4. On the Select Release Version screen, select the appropriate release version and click **OK**.

   The system displays the Run Communication Manager Messaging Installation screen. Install Communication Manager Messaging only if messaging was enabled on the S8300A.
5. Complete one of the following:
   - To install Communication Manager Messaging concurrently with Communication Manager, select **Yes**.
   - To skip the installation of Communication Manager Messaging, select **No**.

   The installation process:
   - Partitions and reformats the hard drive and internal compact flash of the server.
   - Installs the Linux operating system.
   - Installs Communication Manager and reports the progress.
   - If you select **Yes**, installs Communication Manager Messaging.

   The installation process takes about 30 minutes. When the server is ready to reboot, the DVD drive door opens and a reminder to check the Avaya Support Site at http://support.avaya.com for the latest software and firmware updates appears. Remove the DVD from the drive. The reboot takes about 5–8 minutes without Communication Manager

Messaging and takes about 8–10 minutes with Communication Manager Messaging. The Telnet session ends automatically.

6. Click **Start** > **Run** to open the Run dialog box.
7. Enter `ping -t 192.11.13.6` and press `Enter`.
8. Wait for the reply from the server to ensure connectivity to it.
9. For the remaining steps on installing Communication Manager and co-resident applications, see *Installing and Configuring the Avaya S8300 Server* (555-234-100).

Checking the reboot progress

Procedure

1. On the computer, click **Start** > **Run**.
2. Enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter` to clear the ARP cache.
   - The system displays the command line prompt if the cache is cleared.
   - The system displays the message, `The specified entry was not found`, if the specified IP address does not contain an entry in the ARP cache.
4. Enter `ping -t 192.11.13.6` to access the media server.

   The -t option causes the ping to repeat. When you get a response (in about 3 minutes), wait an additional 30 seconds before you access the Web interface.
5. Enter `Ctrl+c` to stop the ping.
6. Close the MS-DOS window.

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Setting the time, date, and time zone

Procedure

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Server Date/Time**.

   The system displays the Server Date/Time page.

2. Set the server time within five (5) minutes of the Network Timer Server (NTS) time, date and time zone so that synchronization can occur.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing service pack

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     a. Select the **update ID** and click **Unpack**.
     b. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     a. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Configuring network parameters

- Obtain the host name, subnet mask, and IP addresses of the server and default gateway.
- Log on to System Management Interface.

You can configure the server data using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Under **Installation**, click **Configure Server**.

   The system opens the Configure Server wizard.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure individual services** and click **Continue**.
4. Click **Set Identities** from the **Configure Individual IP Services** list.
5. On the Set Identities page, enter the host name of the server.
6. Click **Continue**.
7. On the Configure Interfaces page, enter the IP address for the server and gateway and the subnet mask. If Communication Manager Messaging is installed, enter the IP address.

   If these fields are already filled in, overwrite them with the correct information. Leave the **Integrated Message** field blank.
8. Click **Change** to update the system files.

   If the system displays the `Action Cancelled` message before it displays the `Success` message, refresh the screen and click **Change** again.

   When the configuration change is complete, the system displays the `Successfully configured ethernet interfaces` message.

Restoring backup data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.

5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the backup file and click **Restore**.
8. To monitor the restore progress, select **Data Backup/ Restore** > **Restore History**.

   The system displays the Restore History page.
9. Select the backup file that you want to monitor and click **Check Status**.

   The system displays the Restore History Results page.
10. Click **Refresh** periodically until the message indicates that the restore is successful.

    This refresh process takes about 5 minutes.
11. Repeat Step 3 through Step 9 to restore:
    - The security dataset, if not performed in Step 7
    - The Communication Manager translations data
    - The messaging application data in the `audix-tr-name-msg` file
    - The messaging application announcements in the `audix-ann` file

Creating a super-user login

Note:

The craft level login can create a super-user login.

Procedure

1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a Business Partner, you can also add the dadmin login.

   Note:

   Ensure that the customer can change this login, its password, or its permissions.
2. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Administrator Accounts.**

   The system displays the Administrator Accounts page.
3. Select **Add Login**.
4. Select **Privileged Administrator** and click **Submit**.

The system displays the Administrator Logins -- Add Login: Privileged Administrator page.

5. Type a login name for the account in the **Login name** field.
6. Verify the following:
   - `susers` appears in the `Primary group` field.
   - `prof18` appears in the `Additional groups (profile)` field. prof18 is the code for the customer superuser.
   - `/bin/bash` appears in the `Linux shell` field.
   - `/var/home/login` name appears in the `Home directory` field, where login name is the name you entered in step 5.
7. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
8. From the **Select type of authentication** option, select **password**.

   Note:

   Do not lock the account or set the password to be disabled.
9. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
10. In the section Force password/key change on next login select **no**.
11. Click **Submit**.

    The system informs you the login is added successfully.

Checking for the Communication Manager Messaging IP address

Procedure

1. Under **Switch Link Administration**, click **Switch Link Admin**.
2. Under **Link Addresses**, in the **Switch** field, verify the IP address of Communication Manager Messaging.

Installing the CM license and authentication files

Caution:

A super-user login, dadmin, or other customer super-user login must exist before you install an authentication file. See Creating a super-user login on page 136.

Procedure

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > License File**.

   The system displays the License File page.
2. Select **Install the license file I previously downloaded** (radio button) and click **Submit**.

   The system displays a message indicating that the license is installed successfully.

3. On the System Management Interface, select **Administration > Server (Maintenance) > Authentication File**.

   The system displays the Authentication File page.

4. Select **Install the Authentication file I previously downloaded** (radio button) and click **Install**.

   The system displays a message indicating that the authentication file is installed successfully.

5. Verify the license and authentication file installation by running the `statuslicense -v` command from the server command line:
   - The `License Mode` should be `Normal`.
   - The report should list a `License Serial Number`.

Rebooting the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Shutdown Server**.
3. Select the following check boxes:
   - **Restart server after shutdown**
   - **Shutdown even if this is the active server**
4. Click **Shutdown**.

   The system displays the `A server shutdown has been requested` message.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.

- If the status of the update file you want to activate is `unpacked`:
  a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
  b. Click **Yes**.

4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Log on the Maintenance Web page.

Procedure

1. In the navigation pane, click **Server** > **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
5. Click **OK**.
6. When the **OK to Remove LED** on the faceplate of the server is steady, it is safe to remove the server.

Upgrade tasks on the S8300D Release 6.3.6 Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.
- The Communication Manager Messaging file

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.
- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**

- **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

This step deletes the temporary node name.

8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.

8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Procedures that you must skip on the survivable server

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading the survivable server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.3.6 for existing Communication Manager on an S8300B or S8300C Server.

In this procedure, you replace the S8300B or S8300C Server by an S8300D Server running System Platform and the embedded main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

For the CM_OnlyEmbed template, Communication Manager supports only small memory size and does not support medium and large memory size.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

For S8300A Server, on Communication Manager release earlier than 5.2.1, perform the upgrade as instructed in the section Upgrading the S8300A Server to embedded main on S8300D Server.

Upgrade paths

You can upgrade the following S8300 servers running a supported release of Communication Manager to S8300D server:

- S8300C as main server
- S8300B as main server

Required upgrade sequence

Perform the upgrades in the following sequence:

- The branch gateway firmware
- The media module firmware
- Communication Manager on the survivable remote server
- Communication Manager on the main server

Onsite preparation

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.

Checking the FTP, SFTP, or SCP server information

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
    - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.

- To log in from a portable computer directly connected to the services port, perform one of the following:
  - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
  - If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.

3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

8. Select the backup file from the list and click **Check Status**.

When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.

- If the status of the update file you want to activate is `unpacked`:
  a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
  b. Click **Yes**.

4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.

- **User Name**
- **Password**
- **Host Name**. The hostname or IP address.
- **Directory**. The complete directory path where the backup is stored.

8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the devices from the server

Procedure

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the server

- Shut down the server.
- Ensure that **OK to Remove** LED on the server faceplate is steady.
- Connect the USB CD/DVD drive.
- Insert the System Platform media.

Caution:

Ensure that you wear a properly grounded ESD wrist strap when handling the server. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Loosen the two thumb screws on the faceplate of the server.
2. When removing the server, remove the LED panel (above slot V1) (G700 only) or the space bar (G250, G350 and G450) with the server.
   - For G700, disengage the LED panel and the server, and remove them together from the branch gateway.
   - For G250, G350 or G450, remove the space bar and the server.
   - For G430, remove the server from the branch gateway.
3. Perform one of the following:
   - For G700, partially reinsert the LED panel (above slot V1) and the new S8300D server (slot V1). Leave them extended from the branch gateway by about 1 inch (2.5 cm).

     Do not seat these circuit packs now.
   - For G250, G350, G430 and G450, partially reinsert the new S8300D Server (slot V1). Leave the server extended from the branch gateway by about 1 inch (2.5 cm). Do not seat this circuit pack now.
4. With the S8300D in slot V1 still extended, by about 1 inch (2.5 cm), connect the USB CD/DVD drive to any one of the USB ports.
5. When you are ready to start installing System Platform, seat the S8300D Server (for G700, also seat the LED panel) into the branch gateway by gently pressing it until the faceplate is aligned with the face of the branch gateway.
   a. Insert the System Platform media into the USB CD/DVD drive within by about 30 seconds of seating the S8300D Server.
   b. If the media is not present in the CD/DVD drive or if the USB CD/DVD drive is not connected to the server at the time of boot, you must repeat the Step 5.

      Alternatively, reboot the server by powering up and powering down the branch gateway.

      When the server starts to boot, it looks for the software on the DVD/CD-ROM. The Alarm LED of the S8300 Server is steady as it is starting. The Alarm LED starts flashing when the S8300 Server is ready to load software.
6. Secure the faceplate of the S8300D server with the thumb screws. Tighten the thumb screws with a screw driver. For G250, G350, and G450, secure the space bar above slot V1
7. Reconnect the laptop to the services port of the new S8300D server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

Note:

You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.

b. Log in to Domain-0 as administrator.

c. In the command line, type **ip_forwarding enable**.

2. To disable IP forwarding:

a. Start an SSH session.

b. Log in to Domain-0 as administrator.

c. In the command line, enter **ip_forwarding disable**.

An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**

- **Password**
- **Host Name**
- **Directory** or **File Path**
  - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.

- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.

4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.

b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

This step creates a node name that you use temporarily.

2. Enter `busyout signaling-group <num>`, where *<num>* is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the *<num>* is 99:
   a. Record the value of the **Far-end Node Name** field.

   You change this node name in Step 4. Typically the data in this field is `msgserver`.

   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.

4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.

6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.

9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading S8400 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the existing S8400 Server running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.3.6 on S8300D Server.

In this procedure, you must:

- Discard:
  - All circuit packs
  - The G600, G650 Media Gateway or the CMC cabinet
- Install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded CM main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

For the CM_OnlyEmbed template, Communication Manager supports only small memory size and does not support medium and large memory size.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Restoring the data set on Communication Manager Release 6.3.6.
- (Optional) Restoring Communication Manager Messaging data set.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

You require a new license for Communication Manager Release 6.3.6.

You can upgrade Communication Manager releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first before you upgrade to Release 6.3.6. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on S8300D Server and restore the system data from the existing server.
- Continue to perform the procedures described in this section.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D server.

Preupgrade tasks on the S8400 Server

Connecting to the server

A CAT5 cross-over cable to connect your services laptop to the server.

Procedure

1. Plug one end of the CAT5 cross-over cable into the services access port on the server faceplate.
2. Plug the other end of the cross-over cable into the services laptop.
3. Start a SAT session.
4. Log in as `craft`.

Accessing System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. If you log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

To use Telnet, enable the Telnet service for Communication Manager.

If the Telnet service is disabled, use SSH to gain access to SAT.

Procedure

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Recording node names and IP addresses

Procedure

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

Back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

If Communication Manager Messaging is enabled on your system, back up the messaging data.

Backing up the files

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**
     a. Select **Translations, Names, and Messages**.

3. In the **Backup Method** section, click **Network Device**.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
5. Click **Start Backup**.
6. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
7. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Recording configuration information

If you have not already completed, record the current server configuration data that you must configure on the new server. Use the worksheet provided in Worksheet for upgrading - to simplex and embedded templates on page 1376 to record the information.

Procedure

1. Click **Server Configuration** > **Configure Server**.
2. Click **Continue** on the first and second screen.
3. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
4. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
5. Select **Configure Interfaces** and record the following:
   - Server IP address
   - Gateway IP address
   - Subnet mask
   - Integrated Messaging IP address, if configured.
6. Click **Close**.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:

   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.

5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

Electrostatic alert:

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides

6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

Note:

Media modules are restricted to certain slots.

9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.
10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.

c. In the command line, type **ip_forwarding enable**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the upgrade dataset

- Log on to System Management Interface.

- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:

     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Enter `add media-gateway <number>`, where *<number>* is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

To obtain the serial number of the branch gateway, on the command prompt of the gateway:

- Enter `show system`.
- Note the serial number of the branch gateway.

  The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.

4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.

5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.

6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.

4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:

   a. Click **Miscellaneous** > **Messaging Software**.

The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.

- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.

4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.

b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

This step creates a node name that you use temporarily.

2. Enter `busyout signaling-group <num>`, where *<num>* is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the *<num>* is 99:
   a. Record the value of the **Far-end Node Name** field.

   You change this node name in Step 4. Typically the data in this field is `msgserver`.

   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.

4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Procedures that you must skip on the survivable server

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading the survivable server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are

significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.

3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Removing the G650 Media Gateway and the circuit packs

Discard any hardware you replaced during the upgrade.

Procedure

1. Remove the G650 Media Gateway from the rack.
2. Discard all the circuit packs you removed from the gateway or the port network.

Registering the system

Use the standard procedure to register the system.

Completion tasks on the S8400 Server

Shutting down the server

Procedure

1. Push and hold the **Shutdown** button on the faceplate of the server for more than 2 seconds.

   The **OK to Remove LED** in green flashes to indicate that shutdown is in progress.
2. When the green **OK to Remove LED** is steady, unlatch the circuit pack, slide it out of its slot.
3. Leave the compact flash card with translations in the slot.
4. Leave cable adapter of the server attached at the rear of the carrier and its cable connections in place during the entire replacement procedure.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Turning off the power to the port network

Procedure

1. From the bash prompt on the services laptop, enter `shutdown system` and press `Enter`.

   This shuts down the server gracefully.

2. Wait until the **Shutdown Complete** LED on the lower portion of the faceplate of the server is solid green.
3. Turn off the power to the media gateway for safety purpose.

   Danger:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the media gateway, pull the AC power cord from the back of the media gateway.
4. Unplug the power cord for safety purpose.

Upgrading S8500 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the existing S8500 main server running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.3.6 on S8300D Server.

In this procedure, you must:

- Discard:
  - All port networks (CMCs, SCCs, MCCs or IP600)
  - All circuit packs and any gateways above 50
  - The S8500 Server and the G650 Media Gateway
- Install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded main template, CM_OnlyEmbed.

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

For the CM_OnlyEmbed template, Communication Manager supports only small memory size and does not support medium and large memory size.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.

- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Restoring the data set on Communication Manager Release 6.3.6.
- (Optional) Restoring Communication Manager Messaging data set.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

You require a new license for Communication Manager Release 6.2.

You can upgrade Communication Manager running releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first, before you upgrade to Release 6.3.6. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on S8300D Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D server.

Preupgrade tasks on S8500 Server

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.

- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

Important:

Do not click **Submit**.

9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.

2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Checking the clock synchronization

Start a SAT session.

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Procedure

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:
  a. Select **Specify Data Sets**.
  b. Select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
     - **Communication Manager Messaging (CMM)**
  c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
  d. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.

b. Click **Yes**.

4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.

2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.

- **Directory**. The complete directory path where the backup is stored.

8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

Electrostatic alert:

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.

7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.
10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the upgrade dataset

- Log on to System Management Interface.

- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:

     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Enter `add media-gateway <number>`, where *<number>* is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

To obtain the serial number of the branch gateway, on the command prompt of the gateway:

- Enter `show system`.
- Note the serial number of the branch gateway.

  The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.

4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.

5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.

6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.

4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:

   a. Click **Miscellaneous** > **Messaging Software**.

The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.

- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.

4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.

b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

This step creates a node name that you use temporarily.

2. Enter `busyout signaling-group <num>`, where *<num>* is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the *<num>* is 99:
   a. Record the value of the **Far-end Node Name** field.

   You change this node name in Step 4. Typically the data in this field is `msgserver`.

   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.

4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on S8500 Server

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the server from the rack

Procedure

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

   For more information, see *Quick Start for Hardware Installation: Avaya S8500 Server*.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Procedures that you must skip on the survivable server

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading the survivable server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Removing the G650 Media Gateway and the circuit packs

Discard any hardware you replaced during the upgrade.

Procedure

1. Remove the G650 Media Gateway from the rack.
2. Discard all the circuit packs you removed from the gateway or the port network.

Registering the system

Use the standard procedure to register the system.

Postupgrade tasks on the S8300E server

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**

- **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

The system displays a list of packages available for installation.

4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**

- **Password**
- **Host Name**
- **Directory**

5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.

b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.

- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.

9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300D Server to S8300D Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager from Release 5.2.1 to Release 6.3.6 on an S8300D Server.

In this procedure, you reuse the existing S8300D Server and install System Platform and the embedded main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

For the CM_OnlyEmbed template, Communication Manager supports only small memory size and does not support medium and large memory size.

Communication Manager does not support upgrading SIP Enablement Services (SES) to Release 6.x.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

For S8300D Server on Communication Manager release earlier than 5.2.1, upgrade to Release 5.2.1 before you upgrade it to Release 6.3.6. For more information, see *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers* (03-602885).

Preupgrade tasks on S8300 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

   If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

b. Enter `productid` and copy the value for the product ID.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.

- If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**

- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:
  a. Select **Specify Data Sets**.
  b. Select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
     - **Communication Manager Messaging (CMM)**
  c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
  d. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test

message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:

   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.

4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.

9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Verify that you selected the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.

Disconnecting the devices from server

Procedure

Disconnect the USB CD/DVD reader from the server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Communication Manager Messaging file

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After you install the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you to.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**

- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.

4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile,

Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.

6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.

2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**

- **Host Name**
- **Directory**

5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.

3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.

3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Verifying the destination for scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

You must change or remove the scheduled backups with USB flash card as the destination.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     On the Change Current Schedule Web page, click **Change Schedule**.
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Log on to System Management Interface.

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make the backups compatible with Release 6.x.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.

- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.

11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Chapter 7: Upgrading to embedded survivable remote template

Upgrading DEFINITY SI or CSI Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the following DEFINITY servers to Communication Manager Release 6.3.6 on S8300D Server running System Platform and the embedded survivable remote template (CM_SurvRemoteEmbed).

- DEFINITY SI Server in a SCC1 or an MCC1
- DEFINITY CSI Server in a CMC

In this procedure, you must:

- Discard all the circuit packs and the cabinet.
- Install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded remote template.

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring Communication Manager Release 6.3.6 on S8300D Server.
- Decommissioning the cabinets.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers. You do not require to restore the translations manually.

You require a new authentication file for Communication Manager Release 6.3.6 that is configured as survivable remote server.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D server.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Saving translations

Start a SAT session.

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Preupgrade administration

Connecting to the processor

Cross-over cable.

Procedure

1. Connect your Services laptop directly to the processor to access the cabinet.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Upgrade tasks

Inserting the S8300D Server in the branch gateway

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

Electrostatic alert:

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.
10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:

     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Enter `add media-gateway <number>`, where *<number>* is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

To obtain the serial number of the branch gateway, on the command prompt of the gateway:

- Enter `show system`.
- Note the serial number of the branch gateway.

  The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.

4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.

5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.

6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Removing fiber-related administration

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

Procedure

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link n`, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link n`.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

1. Remove the fiber cables that connect the following circuit packs in the PNs:
   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

Caution:

The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

Note:

If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.

2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

Note:

You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or if you want to minimize out-of-service time.

4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
   - CURL - you cannot reuse this cable.
   - TDM/LAN - you can reuse this cable.
   - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on S8300D Server

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:

   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the cabinet and the circuit packs

Discard any hardware you replaced during the upgrade.

Procedure

1. Remove the cabinet from the rack.
2. Discard all the circuit packs you removed from the cabinet.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300A Server to S8300D Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 1.x, 2.0, or 2.0.1 on an S8300A Server to Release 6.3.6on an S8300D Server.

In this procedure, you must replace the S8300A Server that is configured as survivable remote server with an S8300D Server. The S8300D Server must be running System Platform and the embedded survivable remote template, CM_SurvRemoteEmbed.

The upgrade procedure involves:

- Recording the configuration information from the existing S8300A Server in the upgrade worksheet.
- Upgrading the branch gateway firmware to make it compatible with Release 6.3.6.
- Replacing the S8300A Server with an S8300D Server in the G700 Branch Gateway.
- Installing System Platform and the embedded survivable remote template on the S8300D Server.
- Configuring Communication Manager to work as the survivable remote server.

The upgrade procedure synchronizes translations and user accounts from the main Communication Manager server to the survivable remote processor. You require a new authentication file for Communication Manager Release 6.3.6 configured as survivable remote server.

Prerequisites

USB DVD/CD-ROM drives

To upgrade S8300 Server to S8300D Server, you must install System Platform and Communication Manager on the new server. You need a USB DVD/CD-ROM drive at the site to do this.

S8300 Server supports Avaya approved Panasonic Digistor 73082 or 73322 external CD/DVD-ROM drives.

- The switch must be set to ON.
- The Panasonic Digistor CD/DVD-ROM drives draw more power than the USB port can supply. Therefore, instead of AC power, the Panasonic Digistor drives use a Lithium ION battery to supply the additional power. If the Lithium ION battery is depleted, the LED turns red and the system displays the message `failed to mount CD-ROM`. You can charge the Lithium ION battery by plugging the CD-ROM drive into a USB port for approximately 30 minutes. The Lithium ION battery charges faster if the switch is set to OFF.

Note:

The Lithium ION battery supplies the extra power only to Panasonic Disgistor CD/DVD-ROM drives.

Checking the FTP, SFTP, or SCP server information

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

Preupgrade tasks on the S8300A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.

3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Verifying the current software release

Procedure

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **Reports as:** field displays one of the following release numbers:
   - `R011x.02.0.110.4` for release 1.2
   - `R011x.03.2.536.1` for release 1.3.2
   - `R012x.00.0.219.0` for release 2.0
   - `R012x.00.1.221.1` for release 2.0.1

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Recording the configuration screens

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.

5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
7. Click **Cancel**.

   Important:

   Do not click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.
    c. Enter `almsnmpconf` and record the output.

Recording configuration information

If you have not already completed, record the current server configuration data that you must configure on the new server. Use the worksheet provided in Worksheet for upgrading - to simplex and embedded templates on page 1376 to record the information.

Procedure

1. Click **Server Configuration** > **Configure Server**.
2. Click **Continue** on the first and second screen.
3. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
4. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
5. Select **Configure Interfaces** and record the following:
   - Server IP address
   - Gateway IP address
   - Subnet mask
   - Integrated Messaging IP address, if configured.
6. Click **Close**.

Recording the scheduled backups

Log on to System Management Interface.

Record the backup scheduled for the existing server. You must submit the scheduled backups after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, note the details of any backup schedules.

   You submit these scheduled backups after the upgrade on the new server running Communication Manager Release 6.0.x.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity. This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files to the FTP server.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     a. Click **Specify Data Sets**.
     b. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.

   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device**.
6. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
7. Click **Start Backup**.
8. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on the Maintenance Web page.

Procedure

1. In the navigation pane, click **Server** > **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
5. Click **OK**.
6. When the **OK to Remove LED** on the faceplate of the server is steady, it is safe to remove the server.

Disconnecting the devices from the server

Procedure

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the S8300A Server

- Shut down the server.
- Ensure that **OK to Remove** LED on the server faceplate is steady.

Warning:

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Loosen the two thumb screws on the faceplate of the server.
2. Disengage the LED panel and the server, and remove them together from the gateway.
3. Partially reinsert the LED panel (above slot V1) and the new S8300D Server (slot V1). Leave them extended from the gateway by about 1 inch (2.5 cm).

   Do not seat these circuit packs now.
4. With the S8300D Server in slot V1 still extended, connect the USB CD/DVD drive to any one of the USB ports.
5. When you are ready to start installing System Platform, seat the S8300D Server and the LED panel into the gateway by gently pressing it until the faceplate is aligned with the face of the gateway.
6. Insert the System Platform media into the USB CD/DVD drive within by about 30 seconds of seating the S8300D Server.

Note:

If the media is not present in the CD/DVD drive or if the USB CD/DVD drive is not connected to the server at the time of boot, repeat Step 5.

Alternatively, reboot the S8300D Server by powering up and powering down the gateway.

When the server starts to boot, it looks for the software on the DVD/CD-ROM. The Alarm LED of the S8300D Server is steady as it is starting. The Alarm LED starts flashing when the S8300D Server is ready to load software.

7. Secure the faceplate of the S8300D Server with the thumb screws. Tighten the thumb screws with a screw driver.
8. Reconnect the laptop to the services port of the S8300D Server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring the alarming information

Log on to System Management Interface.

Configure the information provided in the worksheet available in Appendix A on page 1376.

Procedure

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter `almsnmpconf` to enter any data that you recorded earlier.

   For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.

8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Submitting the scheduled backups

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, select the scheduled backup and click **Change**.

4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat steps 3 and 4 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300 Server to S8300D Server

Introduction

This section describes the procedure to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.3.6 for existing Communication Manager on S8300B or S8300C Server.

In this upgrade procedure, replace the S8300B or S8300C Server with an S8300D Server running System Platform and the embedded survivable remote template, CM_SurvRemoteEmbed.

The embedded survivable remote template supports Utility Services.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8300 Server to Communication Manager Release 4.0.5 or Release 5.2.1.

   For servers that you can upgrade directly to Release 4.0.5 or Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

   S8300A servers require special procedures to upgrade.
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.3.6.
3. Perform the upgrade to Release 6.3.6 as described in this section.

Onsite preparation

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for the product ID.

Checking the FTP, SFTP, or SCP server information

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
    - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.

- To log in from a portable computer directly connected to the services port, perform one of the following:
  - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
  - If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**
     c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
     d. In the **Download size** field, enter the size of the backup `.tar` file.

        If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.

- **Directory**. The complete directory path where the backup is stored.

When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.

6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the devices from the server

Procedure

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the server

- Shut down the server.
- Ensure that **OK to Remove** LED on the server faceplate is steady.
- Connect the USB CD/DVD drive.
- Insert the System Platform media.

Caution:

Ensure that you wear a properly grounded ESD wrist strap when handling the server. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Loosen the two thumb screws on the faceplate of the server.

2. When removing the server, remove the LED panel (above slot V1) (G700 only) or the space bar (G250, G350 and G450) with the server.
   - For G700, disengage the LED panel and the server, and remove them together from the branch gateway.
   - For G250, G350 or G450, remove the space bar and the server.
   - For G430, remove the server from the branch gateway.
3. Perform one of the following:
   - For G700, partially reinsert the LED panel (above slot V1) and the new S8300D server (slot V1). Leave them extended from the branch gateway by about 1 inch (2.5 cm).

     Do not seat these circuit packs now.
   - For G250, G350, G430 and G450, partially reinsert the new S8300D Server (slot V1). Leave the server extended from the branch gateway by about 1 inch (2.5 cm). Do not seat this circuit pack now.
4. With the S8300D in slot V1 still extended, by about 1 inch (2.5 cm), connect the USB CD/DVD drive to any one of the USB ports.
5. When you are ready to start installing System Platform, seat the S8300D Server (for G700, also seat the LED panel) into the branch gateway by gently pressing it until the faceplate is aligned with the face of the branch gateway.
   a. Insert the System Platform media into the USB CD/DVD drive within by about 30 seconds of seating the S8300D Server.
   b. If the media is not present in the CD/DVD drive or if the USB CD/DVD drive is not connected to the server at the time of boot, you must repeat the Step 5.

      Alternatively, reboot the server by powering up and powering down the branch gateway.

      When the server starts to boot, it looks for the software on the DVD/CD-ROM. The Alarm LED of the S8300 Server is steady as it is starting. The Alarm LED starts flashing when the S8300 Server is ready to load software.
6. Secure the faceplate of the S8300D server with the thumb screws. Tighten the thumb screws with a screw driver. For G250, G350, and G450, secure the space bar above slot V1
7. Reconnect the laptop to the services port of the new S8300D server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring the alarming information

Log on to System Management Interface.

Configure the information provided in the worksheet available in Appendix A on page 1376.

Procedure

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter `almsnmpconf` to enter any data that you recorded earlier.

   For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.

4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Submitting the scheduled backups

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat steps 3 and 4 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.

- A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading S8400 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the existing S8400 Server configured as survivable remote processor, formerly Local Survivable Processor (LSP) running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.3.6 on S8300D Server.

In this procedure, you must:

- Discard:
  - All circuit packs
  - The G600, G650 Media Gateway or the CMC cabinet
- Install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded survivable remote template, CM_SurvRemoteEmbed.

The upgrade procedure involves:

- Creating a data set to use if you have to back out of the upgrade.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers. You do not require to restore the translations manually.

You require a new license for Communication Manager Release 6.3.6.

You can upgrade Communication Manager releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first before you upgrade to Release 6.3.6. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on S8300D Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.

Table continues…

✔	Task	Description
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D server.

Preupgrade tasks on the S8400 Server

Connecting to the server

A CAT5 cross-over cable to connect your services laptop to the server.

Procedure

1. Plug one end of the CAT5 cross-over cable into the services access port on the server faceplate.
2. Plug the other end of the cross-over cable into the services laptop.
3. Start a SAT session.
4. Log in as `craft`.

Accessing System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. If you log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.
4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

Back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

If Communication Manager Messaging is enabled on your system, back up the messaging data.

Backing up the files

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**
     a. Select **Translations, Names, and Messages**.
3. In the **Backup Method** section, click **Network Device**.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
5. Click **Start Backup**.
6. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
7. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

Electrostatic alert:

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.
10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:

     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Enter `add media-gateway <number>`, where *<number>* is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

To obtain the serial number of the branch gateway, on the command prompt of the gateway:

- Enter `show system`.
- Note the serial number of the branch gateway.

  The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.

4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.

5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.

6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.

3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.

c. Click **Server** > **Process Status**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site,

the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Removing the G650 Media Gateway and the circuit packs

Discard any hardware you replaced during the upgrade.

Procedure

1. Remove the G650 Media Gateway from the rack.
2. Discard all the circuit packs you removed from the gateway or the port network.

Registering the system

Use the standard procedure to register the system.

Completion tasks on the S8400 Server

Shutting down the server

Procedure

1. Push and hold the **Shutdown** button on the faceplate of the server for more than 2 seconds.

   The **OK to Remove LED** in green flashes to indicate that shutdown is in progress.
2. When the green **OK to Remove LED** is steady, unlatch the circuit pack, slide it out of its slot.
3. Leave the compact flash card with translations in the slot.
4. Leave cable adapter of the server attached at the rear of the carrier and its cable connections in place during the entire replacement procedure.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Turning off the power to the port network

Procedure

1. From the bash prompt on the services laptop, enter `shutdown system` and press `Enter`.

   This shuts down the server gracefully.
2. Wait until the **Shutdown Complete** LED on the lower portion of the faceplate of the server is solid green.
3. Turn off the power to the media gateway for safety purpose.

   Danger:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the media gateway, pull the AC power cord from the back of the media gateway.
4. Unplug the power cord for safety purpose.

Upgrading S8500 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the existing S8500 Server configured as survivable remote processor running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.3.6 on S8300D Server.

In this upgrade procedure, you must:

- Discard:
  - All port networks (CMCs, SCCs, MCCs or IP600)
  - All circuit packs and any gateways above 50
  - The S8500 Server and the G650 Media Gateway
- Install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded survivable remote template (CM_SurvRemoteEmbed).

The embedded survivable remote template supports Utility Services.

The upgrade procedure involves:

- Creating a data set to use if you have to back out of the upgrade.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers. You do not require to restore the translations manually.

You require a new license for Communication Manager Release 6.3.6.

You can upgrade Communication Manager running releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first, before you upgrade to Release 6.3.6. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on S8300D Server and restore the system data from the existing server.

- Continue with the procedures described in this section.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D server.

Preupgrade tasks on the S8500 Server

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 Branch Gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server you want to upgrade is the main server of a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.

b. Select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**

c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

d. In the **Download size** field, enter the size of the backup `.tar` file.

   If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

Electrostatic alert:

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

Procedure

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.
10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**

- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click a patch ID to view the details.

4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:

     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1376.

Procedure

1. Enter `add media-gateway <number>`, where *<number>* is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

   To obtain the serial number of the branch gateway, on the command prompt of the gateway:

   - Enter `show system`.
   - Note the serial number of the branch gateway.

     The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.
4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.
5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.
6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.

2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.

3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Removing the G650 Media Gateway and the circuit packs

Discard any hardware you replaced during the upgrade.

Procedure

1. Remove the G650 Media Gateway from the rack.
2. Discard all the circuit packs you removed from the gateway or the port network.

Registering the system

Use the standard procedure to register the system.

Completion tasks on S8500 Server

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the server from the rack

Procedure

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

   For more information, see *Quick Start for Hardware Installation: Avaya S8500 Server*.

Upgrading the S8300D Server to S8300D Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager from Release 5.2.1 to Release 6.3.6 on an S8300D Server.

In this procedure, you upgrade the existing S8300D to run System Platform and the embedded survivable remote template, CM_SurvRemoteEmbed.

The embedded survivable remote template supports the Utility Services.

Communication Manager does not support upgrading SIP Enablement Services (SES) to Release 6.x.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.3.6.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.3.6.

For S8300D servers on releases of Communication Manager earlier than 5.2.1, upgrade to Release 5.2.1 first before you upgrade them to Release 6.3.6. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Preupgrade tasks on S8300 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.

3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for the product ID.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, perform one of the following:
   - If Communication Manager Messaging is not enabled:
     a. Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:

        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
   - If Communication Manager Messaging is enabled:
     a. Select **Specify Data Sets**.
     b. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**
     c. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.
     d. In the **Download size** field, enter the size of the backup `.tar` file.

        If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer before you proceed with the upgrade.
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.

b. Wait until the system displays `... unpacked successfully`.

- If the status of the update file you want to activate is `unpacked`:

  a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.

  b. Click **Yes**.

4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Verify that you selected the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.

Disconnecting the devices from server

Procedure

Disconnect the USB CD/DVD reader from the server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring the alarming information

Log on to System Management Interface.

Configure the information provided in the worksheet available in Appendix A on page 1376.

Procedure

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter `almsnmpconf` to enter any data that you recorded earlier.

   For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.

3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Submitting the scheduled backups

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat steps 3 and 4 for all the scheduled backups.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Chapter 8: Upgrading Communication Manager from non-VMware to VMware Virtualized Environment

Overview

The upgrade to VMware procedure requires several different organizations such as the customer, Avaya Professional Services, Avaya Technical Support, and Avaya Registration Team to perform certain steps in parallel. The customer cannot gain access to the registration forms. SAL Gateway testing and configuration must be in synchronization with the record updates or changes in Seibel.

Important:

Current users with embedded Communication Manager Messaging must use another way to host messaging for migrating Communication Manager to Virtualized Environment because Communication Manager Messaging has not been virtualized and is not supported in Virtualized Environment.

If you must reuse the existing IP addresses, the Communication Manager non-VMware environment and the Communication Manager Virtualized Environment *cannot* exist on the customer network at the same time. If you turn on a server, you must turn off the other server.

As the upgrade process does not migrate the administrator accounts, you must add the accounts on the upgraded system. If SNMP is implemented, note the SNMP settings and re-enter on the upgraded system.

Upgrading Communication Manager 6.x to VMware

VMware is not supported on the S8300D server. Therefore, you must upgrade to Communication Manager on System Platform. You *must* upgrade survivable remote servers to System Platform 6.2.1.0.9 or later before you can upgrade the Communication Manager template to the survivable embedded remote template. Survivable servers must have the same version or later than the main server.

Important:

Ensure any the survivable remote server has the same version as the Communication Manager virtual application version. The survivable remote version must remain at 6.2. Use the 6.2 media if you must update the version.

Procedure

1. Download and save the *Migrating from Avaya Aura® Communication Manager 6.x to VMware® Workbook* from the Avaya support website at https://downloads.avaya.com/css/P8/documents/100167658. In the Security Warning dialog box, click **Enable Macros**.
2. Record the required Communication Manager data in the workbook.
3. Navigate to the Communication Manager SMI page of the existing main Communication Manager server.
4. Backup the existing translations from the SMI page:
   - Communication Manager 6.x translation files
   - Utility Services translations files if applicable. Utility Services is only available in 6.2 and later. For instructions to create a backup, see the Utility Services deployment guide.
5. If using Utility Services 6.1:
   a. Note the DHCP server settings if in use.
   b. Note any special firmware that has been loaded and ensure that you have a copy of the firmware that you must upload to the new server. The firmware includes Branch Gateway, ADVD, and IP phone firmware.
   c. Note the Communication Manager server IP address, login, and password so Utility Services can interrogate the system to understand the IP phone firmware.
6. Download and install the following virtual application OVA files.
   - Communication Manager

     See the appropriate deployment guide for downloading and installing the virtual application OVA file.
   - Utility Services if applicable
   - WebLM if applicable
   - Secure Access Link. You do not require if a standalone SAL Gateway exists

   Note:

   Do not turn on the applications.
7. If SAL is in use on System Platform:
   a. Log in to the SAL Gateway.
   b. Capture settings using screen capture.
8. Turn off the existing server.

9. If a Standalone SAL Gateway is *not* in place, turn on and configure the SAL virtual application. Reuse the details on the screen captures from the existing SAL Gateway.
10. Turn on the following virtual applications:
    - Communication Manager. Provision the initial IP address as required by the deployment guide.
    - Utility Services if applicable
    - WebLM if applicable
11. Download and activate the latest Communication Manager service pack.
12. Navigate to SMI of Communication Manager and perform the following:
    a. Set the date and time.
    b. Set the NTP. You must reboot to synchronize all processes to NTP.
    c. Add a superuser login.
    d. Restore existing Communication Manager call processing translations (XLN file only). Re-enter the SNMP data if required.
    e. Click **Administration** > **Licensing** > **WebLM Configuration,** and retranslate the WebLM server destination if applicable.
13. Restore Utility Services 6.2 and later or retranslate Utility Services as applicable.
14. Retranslate the Utility Services server destination if applicable.
15. Set up System Manager or WebLM as applicable to provide licensing support for Communication Manager.

    You cannot use the MAC address from the previously used server. See the appropriate deployment guide for the licensing procedures. You require a new PLDS license. Log in to WebLM and click **Properties** to get the MAC address information or equivalent.
16. Complete the SAL registration spreadsheet in the migration workbook.
17. Reregister Communication Manager as a virtual application.
18. Avaya Registration Team must perform the following:
    a. Remove records for Communication Manager as System Platform.
    b. Add records.
19. Verify the SAL connectivity after the new SAL Gateway starts communicating with the data center.
20. Test an alarm and verify that the alarming is working properly.
21. Verify the survivability with existing survivable servers.

22. If System Platform used multiple SAL Gateways before the upgrade, and you require to consolidate SAL Gateways into a single SAL Gateway virtual application, perform the following steps:
    a. Choose settings for one SAL Gateway virtual application that carries forward. Make a screen capture of the administration settings and export managed elements for the primary SAL Gateway.
    b. Export managed elements for each existing System Platform-based SAL Gateway to the virtual application-based SAL Gateway.
    c. Update the virtual SEID and Product IDs for each System Platform-based SAL Gateway that is no longer used.
23. Remove the Ethernet cables from the decommissioned server as a network safety measure.

    If IP addresses were reused, the pre-VMware Communication Manager environment cannot be running on the customer's network at the same time as the VMware-based Communication Manager.
24. Determine the disposition of the server on which applications were previously running. The server cannot be reused for any other Avaya applications unless the server has the same comcode as the Communication Manager server. If the server will not be used, submit the appropriate forms to the Avaya Customer Care Center to remove the server from the installed base record.
    - For Avaya personnel, the forms can be found at Avaya Personnel Forms.
    - For Business Partners, the forms can be found at Business Partner Forms.
25. Remove the physical server from the maintenance contract if it is no longer utilized. The customer contacts the Avaya Customer Care Center and requests removal from the installed base record of the Functional Location (FL). The adjustment becomes effective with the next contract renewal or true-up because the contract is prepaid by the customer.

Upgrading Communication Manager 5.2.1 to VMware

Procedure

1. Download and save the *Migrating from Avaya Aura® Communication Manager 5.2.1 to VMware® Workbook* from the Avaya support website at https://downloads.avaya.com/css/P8/documents/100167657. In the Security Warning dialog box, click **Enable Macros**.
2. Record the required Communication Manager data in the workbook.
3. Log on to the existing main Communication Manager server from SMI.
4. Backup the Communication Manager data from SMI.

   For instructions, see Backing up Communication Manager.

5. Download and install the following virtual application OVA files but *do not* turn on the applications. See the appropriate deployment guide for downloading and installing the virtual application OVA file.
   - Communication Manager
   - Utility Services if applicable
   - WebLM if applicable
   - Secure Access Link. You do not require if a Standalone SAL Gateway exists.
6. Turn off the existing server.
7. If a Standalone SAL Gateway is *not* in place, turn on and configure the SAL virtual application. Reuse the details on the screen captures from the existing SAL Gateway.
8. Turn on the following virtual applications:
   - Communication Manager. Provision the initial IP address as required by the deployment guide.
   - Utility Services if applicable
   - WebLM if applicable
9. Download and activate the latest Communication Manager service pack.
10. Navigate to SMI of Communication Manager and perform the following steps:
    a. Set the date and time.
    b. Set the NTP. You must reboot to synchronize all processes to NTP.
    c. Add a superuser login.
    d. Restore the Communication Manager data of the existing server that you created in Step 4, and re-enter the SNMP data if required.
    e. Click **Administration** > **Licensing** > **WebLM Configuration,** and retranslate the WebLM server destination if applicable.
11. Set up System Manager or WebLM as applicable to provide licensing support for Communication Manager.

    You cannot use the MAC address from the previously used server. See the appropriate deployment guide for the licensing procedures. You require a new PLDS license. Log in to WebLM and click **Properties** to obtain the MAC address information or equivalent.
12. Complete the SAL registration spreadsheet in the migration workbook if you installed SAL.
13. Reregister Communication Manager as a virtual application.
14. Avaya Registration Team must perform the following:
    a. Remove records for Communication Manager as System Platform.
    b. Add records.
15. Verify the SAL connectivity after the new SAL Gateway starts communicating with the data center.

16. Test an alarm and verify that the alarming is working properly.
17. Verify the survivability with existing survivable server, LSP or ESS.
18. Remove the Ethernet cables from the decommissioned server as a network safety measure.

    If IP addresses were reused, the pre-VMware Communication Manager environment cannot be running on the customer's network at the same time as the VMware-based Communication Manager.
19. Determine the disposition of the server on which applications were previously running. The server cannot be reused for any other Avaya applications unless the server has the same comcode as the Communication Manager server. If the server will not be used, submit the appropriate forms to the Avaya Customer Care Center to remove the server from the installed base record.
    - For Avaya personnel, the forms can be found at Avaya Personnel Forms.
    - For Business Partners, the forms can be found at Business Partner Forms.
20. Remove the physical server from the maintenance contract if it is no longer utilized. The customer contacts the Avaya Customer Care Center and requests removal from the installed base record of the Functional Location (FL). The adjustment becomes effective with the next contract renewal or true-up because the contract is prepaid by the customer.

Chapter 9: Converting to port network

Upgrading DEFINITY Server CSI in CMC to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade the existing DEFINITY Server CSI in a CMC to Communication Manager Release 6.3.6 on an HP DL360 G8 Server or Dell R620 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.3.6. You reuse the cabinet in the new system.

In this procedure, you replace the DEFINITY Server CSI with an HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex main/survivable core template, CM_Simplex.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Installing translation file on Communication Manager Release 6.3.6.
- Administering IPSIs on Communication Manager Release 6.3.6.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

You require a new license for Communication Manager Release 6.3. This upgrade affects service because you turn off the cabinets to replace the processor and tone-clock circuit packs. The system drops all calls and the service returns when the server takes control of the IPSIs.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Send the translations to the STS team few weeks before the upgrade and obtain the updated translations from STS.	STS updates the translations to the latest version. This process can take two weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For information on where and how to send the translations and forms to be used, contact the STS scheduling desk at 720-444-9418.
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following servers, as appropriate: - HP DL360 G8 - Dell R620 • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP C-LAN	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://avaya.com/support.
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. Changing or upgrading the hardware includes:

- Adding new TN2312BP IPSI, TN799D C-LAN, and TN2302 or TN2602 Media Processor circuit packs.
- Connecting the IPSI circuit pack to the customer network.
- Assigning static IP address to the IPSI circuit pack.

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Saving translations

Start a SAT session.

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Replacement of circuit packs

The TN2312BP IPSI circuit pack in the PN replaces the existing circuit packs and terminates control communication with the server. CAT5 Ethernet cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit pack, program static IP addresses into the IPSI.

You can complete this task at any time before the cutover. IPSI circuit pack is hot swappable, and you replace the circuit pack in the existing DEFINITY system without the need to turn off the power.

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSI is working in the existing system.

- Test the connectivity between the server and the IPSI.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

Cross-over cable.

Procedure

1. Connect your Services laptop directly to the processor to access the cabinet.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Recording node names and IP addresses

Procedure

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the translations

Log on to System Management Interface.

You restore the translations only on the main server. When a survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:

   Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.
6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the status of restore process.

When the restoration is complete, the system displays the following message:

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.
7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.

8. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Start a SAT session.

Procedure

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Start a SAT session.

Procedure

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the network regions, see *Administering Network Connectivity on Avaya Aura® Communication Manager,* 555-233-504.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit pack

Start a SAT session.

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.

2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6
     - DiffServ: 46
3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

Procedure

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.

3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on HP DL360 G8 or Dell R620 Server

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:

   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading DEFINITY ONE/S8100 in CMC to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade the existing S8100 Server in a CMC to Communication Manager Release 6.3.6 on an HP DL360 G8 Server or Dell R620 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.3.6. You reuse the cabinet in the new system.

In this procedure, you must replace:

- The TN2314 or TN795 circuit pack with a TN2312BP IPSI circuit pack
- The S8100 Server with an HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex CM main/survivable core template (CM_Simplex)

You install Communication Manager Messaging on the new system because you discard the processor circuit pack that has the Audix feature embedded in it.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Installing translation file on Communication Manager Release 6.3.6.
- Administering IPSIs on Communication Manager Release 6.3.6.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

You require a new license for Communication Manager Release 6.3.6. This upgrade affects service because you turn off the cabinets to replace the processor circuit pack. The system drops all calls, the service returns when the new server takes control of the IPSIs.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Send the translations to the STS team few weeks before the upgrade and obtain the updated translations from STS.	STS updates the translations to the latest version. This process can take two weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For information on where and how to send the translations and forms to be used, contact the STS scheduling desk at 720-444-9418.
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following servers, as appropriate: - HP DL360 G8 - Dell R620 • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP C-LAN	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://avaya.com/support.
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. Changing or upgrading the hardware includes:

- Adding new TN2312BP IPSI, TN799D C-LAN, and TN2302 or TN2602 Media Processor circuit packs.
- Connecting the IPSI circuit pack to the customer network.
- Assigning static IP address to the IPSI circuit pack.

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Saving translations

Start a SAT session.

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Replacement of circuit packs

The TN2312BP IPSI circuit pack in the PN replaces the existing circuit packs and terminates control communication with the server. CAT5 Ethernet cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit pack, program static IP addresses into the IPSI.

You can complete this task at any time before the cutover. IPSI circuit pack is hot swappable, and you replace the circuit pack in the existing DEFINITY system without the need to turn off the power.

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSI is working in the existing system.
- Test the connectivity between the server and the IPSI.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

A cross-over cable to connect your services laptop directly to the processor.

Procedure

1. Perform one of the following tasks to connect the services laptop to the processor:
   - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

3. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Recording node names and IP addresses

Procedure

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Recording IP settings

Start a Telnet session to access the processor circuit pack that is connected to the service laptop.

You must view and record the IP settings assigned to the processor that you must configure on the new server. For this, use the worksheet provided in Appendix A.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log on as `craft` or `dadmin`.

4. Enter `setip`. The system displays the list of IP settings.
   - cust: IPaddress, subnet mask, gateway
   - dns: server name, domain name, 2 DNS server IP addresses
   - wins: two WINS server IP addresses
   - ras: one remote access server IP address
5. Record this information exactly as displayed.

   Important:

   Include any periods, commas, or other punctuation marks. Record this information in lowercase or uppercase as the information appears.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*
- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the translations

Log on to System Management Interface.

You restore the translations only on the main server. When a survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:

   Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.
6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the status of restore process.

When the restoration is complete, the system displays the following message:

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.

b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Tasks performed on the cabinet

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.
7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.
8. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Turning off the power to the control cabinet

Procedure

1. On the faceplate of the processor, press and hold the shutdown button until the system starts the shutdown process.

   The green light indicates that the cabinet is shut down.

   Important:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane.

2. Remove the power cord from the back of the cabinet.

   The cabinet turns off.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Start a SAT session.

Procedure

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Start a SAT session.

Procedure

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administering the IPSI circuit pack

Start a SAT session.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Set the **Switch Identifier** field for the IPSI on this system.
3. Set the QoS parameters:
   - 802.1p: 6
   - DiffServ: 46

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.

- To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
  - **802.1p (vlan priority)**: `6`
  - **DiffServ**: `46`
  - **Auto** (port negotiation): `y` for the following default values:
    - `Full duplex`
    - `100mbps` speed
  - **Auto** (port negotiation): `n` to modify as per the network configuration.
    - **Duplex full**
    - **Speed 100**

3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

Procedure

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

Note:

If you do not have a gateway IP address, leave the **Gateway Address** field blank.

7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface UUCSS` to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Postupgrade tasks on HP DL360 G8 or Dell R620 Server

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.
4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading Avaya IP600/S8100 Server in G600 to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade the existing S8100 Server in G600 Media Gateway to Communication Manager Release 6.2 on a HP DL360 G8 Server or Dell R620 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.3.6. You reuse the cabinet in the new system.

In this procedure, you replace:

- The TN2314 or TN795 circuit pack with a TN2312BP IPSI circuit pack
- The S8100 Server with an HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex CM main/survivable core template (CM_Simplex)

You install Communication Manager Messaging on the new system because you discard the processor circuit pack that has the Audix feature embedded in it.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- Installing Communication Manager Messaging (optional).
- Installing translation file on Communication Manager Release 6.3.6.
- (Optional) Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.3.6.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

You require a new license for Communication Manager Release 6.3.

The upgrade affects service. When you turn off the PPN stack to replace the cabinet during the upgrade process, the system drops all the calls. The system becomes operative when the new server takes control of the IPSIs. Before you turn off the cabinets, perform the following administration tasks.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Send the translations to the STS team few weeks before the upgrade and obtain the updated translations from STS.	STS updates the translations to the latest version. This process can take two weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For information on where and how to send the translations and forms to be used, contact the STS scheduling desk at 720-444-9418.
	Verify that you have the required software: • System Platform	

Table continues…

✔	Task	Description
	• Communication Manager	
	Obtain the required hardware: • One of the following servers, as appropriate: - HP DL360 G8 - Dell R620 • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP C-LAN	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://avaya.com/support.
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Provides instructions for administering network regions.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.

- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. Changing or upgrading the hardware includes:

- Adding new TN2312BP IPSI, TN799D C-LAN, and TN2302 or TN2602 Media Processor circuit packs.
- Connecting the IPSI circuit pack to the customer network.
- Assigning static IP address to the IPSI circuit pack.

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Saving translations

Start a SAT session.

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Replacement of circuit packs

The TN2312BP IPSI circuit pack in the PN replaces the existing circuit packs and terminates control communication with the server. CAT5 Ethernet cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit pack, program static IP addresses into the IPSI.

You can complete this task at any time before the cutover. IPSI circuit pack is hot swappable, and you replace the circuit pack in the existing DEFINITY system without the need to turn off the power.

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSI is working in the existing system.

- Test the connectivity between the server and the IPSI.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

A cross-over cable to connect your services laptop directly to the processor.

Procedure

1. Perform one of the following tasks to connect the services laptop to the processor:
   - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
3. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Recording node names and IP addresses

Procedure

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Recording IP settings

Start a Telnet session to access the processor circuit pack that is connected to the service laptop.

You must view and record the IP settings assigned to the processor that you must configure on the new server. For this, use the worksheet provided in Appendix A.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log on as `craft` or `dadmin`.
4. Enter `setip`. The system displays the list of IP settings.
   - cust: IPaddress, subnet mask, gateway
   - dns: server name, domain name, 2 DNS server IP addresses
   - wins: two WINS server IP addresses
   - ras: one remote access server IP address
5. Record this information exactly as displayed.

   Important:

   Include any periods, commas, or other punctuation marks. Record this information in lowercase or uppercase as the information appears.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the translations

Log on to System Management Interface.

You restore the translations only on the main server. When a survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:

   Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.
6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the status of restore process.

When the restoration is complete, the system displays the following message:

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Tasks performed on the G600 gateway

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

The system displays the IP address, the subnet mask, and the default gateway information.

d. Verify that the information displayed is correct.

e. Type `reset` and press `Enter`.

7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.

8. Perform the following steps to close the IPSI session and log in to IPSI:

a. Type `exit`.

The system saves the changes and ends the IPSI session.

b. Type `192.11.13.6` and log in to IPSI.

c. Type `show control interface`.

The system displays the IP address, the subnet mask, and the default gateway information.

d. Verify that the information displayed is correct.

e. Type `reset` and press `Enter`.

Add or copy the login portion before you add the control gateway.

9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Turning off the power to the control cabinet

Procedure

1. On the faceplate of the processor, press and hold the shutdown button until the system starts the shutdown process.

The green light indicates that the cabinet is shut down.

Important:

The latch on the power supply acts as the DC power switch and removes only DC power from the backplane.

2. Remove the power cord from the back of the cabinet.

The cabinet turns off.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Replacing I/O cables

Turn off power to the carrier or the media gateway.

Caution:

Failure to turn off the power can result in electric shock.

On older G600 cabinets you must replace the existing I/O cables (WP-90753, LI), which connect the backplane to the rear connector panel, with twisted pair I/O cables. The existing I/O cables have straight wires. They may be white with two red wires, or multicolored wires. If the cables have multicolored, tightly twisted wires do not replace them.

Electrostatic alert:

When you add or replace any hardware and associated cables and adapters, wear a grounded wrist strap to ground yourself against electrostatic discharge (ESD). Failure to follow ESD procedures can result in system damage or service disruption.

Procedure

1. For the G600 Media Gateway, remove the fan assembly to access the cables.
   a. Loosen the thumb screws on the fan assembly and pull it out.
   b. Leave the fan assembly off until all the wires are installed.
2. Note the orientation of the existing I/O cables.

   The existing I/O cables may be white and red or multicolored. They are not twisted.
3. Remove the nontwisted pair of existing I/O cables from the backplane and the connector panel slots.

4. Install the 10 tight-twisted pair I/O cables onto the backplane.

   Observe the white outline printed on the backplane for the location of each connector.

5. When you view from the side with twin connectors (that is, while plugging them into the backplane) and with the connectors oriented properly for plug-in, they should look like

   The connector panel contains some pin locations that have no wires in them. Top of the connector panel contains an orange-black pair on the right and a violet-brown pair on the left. The 50-position metal shell D connectors should be installed into the connector panel with the longer side of the D (pins 1–25) toward the right when viewed from the rear of the media gateway.

6. For the G600 Media Gateway, perform one of the following:
   - If you do not have to install any other gateway, replace the fan unit .
   - If you have to add more gateways to the rack, leave the fan units off until all of the TDM cables are installed.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Start a SAT session.

Procedure

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Start a SAT session.

Procedure

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administering the IPSI circuit pack

Start a SAT session.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Set the **Switch Identifier** field for the IPSI on this system.
3. Set the QoS parameters:
   - 802.1p: 6
   - DiffServ: 46

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

Procedure

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.

3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Postupgrade tasks on HP DL360 G8 or Dell R620 Server

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms that you must clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:

   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Note:

Contact Avaya Support at http://support.avaya.com/ if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.

7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading S8300 Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade the embedded S8300 Server in G430 or G450 Branch Gateway to Communication Manager Release 6.3.6 on an HP DL360 G8 Server or Dell R620 Server.

In this upgrade scenario:

- You must discard the embedded S8300 Server and the H.248 Branch Gateway.
- You must install a G650 Media Gateway and move the supported circuit packs to the media gateway that becomes a port network on the new system running Communication Manager Release 6.3.6.
- Install the stand-alone HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex CM main/survivable core template (CM_Simplex).

You install Communication Manager Messaging on the new system because you discard the processor circuit pack that has the Audix feature embedded in it.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Restoring the data set on Communication Manager Release 6.3.6.
- (Optional) Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.3.6.
- Installing G650 Media Gateway.
- Adding circuit packs to the media gateway.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

You require a new license for Communication Manager Release 6.3.6.

You can upgrade Communication Manager releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first before you upgrade to Release 6.3.6. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on the HP DL360 G8 Server or Dell R620 Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the following software: • System Platform • the required Communication Manager template	
	Obtain the required hardware: • One of the following servers, as appropriate: - HP DL360 G8 - Dell R620 • Circuit packs: - TN2312BP IPSI - TN799DP C-LAN	
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Preupgrade tasks on the S8300 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying the current software release

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You must record the configuration information that is available on System Management Interface of the existing release of Communication Manager. You can use this information to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information.

Copy the information from each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1376 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.

b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for the product ID.

Checking the FTP, SFTP, or SCP server information

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address

- Directory on the FTP server

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - To log in from a portable computer directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network, such as an SCP, SFTP, or FTP server. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device**.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
8. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

Do not select the **Install this file on the local server** check box.

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.

3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.

4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.

2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Upgrade tasks on HP DL360 G8 or Dell R620 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*
- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **`ip_forwarding enable`**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **`ip_forwarding disable`**.

      An alternative to the previous command is **`service_port_access disable`**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.

6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:
   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs

2. System Platform feature packs
3. Solution template service packs
4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

You change this node name in Step 4. Typically the data in this field is `msgserver`.

b. In the **Far-end Node Name** field, enter `tmp` and submit the form.

4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Shutting down the S8300 Server

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Turning off the power to the control cabinet

Procedure

1. On the faceplate of the processor, press and hold the shutdown button until the system starts the shutdown process.

   The green light indicates that the cabinet is shut down.

   Important:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane.
2. Remove the power cord from the back of the cabinet.

   The cabinet turns off.

Preupgrade tasks

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. Changing or upgrading the hardware includes:

- Adding the TN2312BP IPSI and TN799D C-LAN circuit packs

- Connecting the IPSI circuit pack to the customer network.
- Assigning static IP address to the IPSI circuit pack.

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.

4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Tasks performed on the cabinet

Installing G650 Media Gateway in the rack

Procedure

Install G650 Media Gateway in the rack. For instructions, see *Installing the Avaya G650 Media Gateway* (03-300685).

Installing the circuit packs

Addition of circuit packs

Port network (PN) must have an IPSI circuit pack. Add the circuit pack to the PN if it has not already have one.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.

4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.

5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.

6. Perform the following steps to close the IPSI session and log in to IPSI:

   a. Type `exit`.

      The system saves the changes and ends the IPSI session.

   b. Type `192.11.13.6` and log in to IPSI.

   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.

   d. Verify that the information displayed is correct.

   e. Type `reset` and press `Enter`.

7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.

8. Perform the following steps to close the IPSI session and log in to IPSI:

   a. Type `exit`.

      The system saves the changes and ends the IPSI session.

   b. Type `192.11.13.6` and log in to IPSI.

   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.

   d. Verify that the information displayed is correct.

   e. Type `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.

9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Tasks performed on the new server

Administering the gateway on Communication Manager

Start a SAT session.

Procedure

1. Enter `add media-gateway` *`number`*, where *number* is gateway number from 1 to n.

   The system displays the Media Gateway screen.
2. In the **Name** field, enter the hostname assigned to the media gateway.
3. In the **Serial No** field, enter the serial number of the media gateway.

   Tip:

   To get the serial number, enter `show system` command at the media gateway command line interface.

   Caution:

   Be sure the serial number for the media gateway you enter in this procedure matches the serial number displayed in the `show system` command. The serial number is case-sensitive, and if entered incorrectly, prevents the server from communicating with the media gateway.
4. In the **Network Region** field, enter the appropriate value.
5. If required, in the **V9** field, enter `gateway-announcements`.

This field allows you to enable announcements on the media gateway. V9 is a virtual slot. No announcement board is associated the slot. The announcements for the media gateway are available in the media gateway firmware.

6. Press **Enter**.

   If properly administered, the media gateway registers with the main server within 1–2 minutes. The system populates the **IP Address**, **MAC Address**, and **Module Type** fields once the media gateway gets registered with the server.

7. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the media gateway number.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Adding IPSI information

Start a SAT session.

Procedure

1. Enter `add ipserver-interface` *`PNnumber`*, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administering the IPSI circuit pack

Start a SAT session.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Set the **Switch Identifier** field for the IPSI on this system.
3. Set the QoS parameters:
   - 802.1p: 6
   - DiffServ: 46

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

   Important:

   Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

If you do not have a gateway IP address, leave the **Gateway Address** field blank.

5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Postupgrade tasks on the HP DL360 G8 or Dell R620 Server

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.

8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Procedures that you must skip on the survivable server

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading the survivable server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.

4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.

- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**

- **Host Name**. The hostname or IP address.
- **Directory**. The complete directory path where the backup is stored.

10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.

11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Upgrading S8400 Server to the HP DL360 G8 or Dell R620 Server

Introduction

This section describes the procedure to upgrade the existing S8400 Server running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.3.6 on an HP DL360 G8 Server or Dell R620 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.3.6. You reuse the cabinet in the new system.

In this procedure, you must:

- Discard:
  - The TN8400AP or TN8400BP circuit pack

  - The TN8412AP (SIPI) circuit pack
- Retain the following circuit packs:
  - The TN2312 BP IPSI
  - The TN799 DP CLAN
  - The TN2302 or TN2602 Media Processor
- Install the stand-alone HP DL360 G8 Server or Dell R620 Server running System Platform and the simplex CM main/survivable core template (CM_Simplex).

You install Communication Manager Messaging on the new system because you discard the processor circuit pack that has the Audix feature embedded in it.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.3.6.
- Installing and configuring System Platform and Communication Manager Release 6.3.6 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Restoring the data set on Communication Manager Release 6.3.6.
- (Optional) Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.3.6.
- Adding circuit packs to the media gateway.
- Completing the postupgrade administration tasks on Communication Manager Release 6.3.6.

You require a new license for Communication Manager Release 6.3.6.

Use this section to upgrade Communication Manager on the following servers:

- The main server
- The survivable server

You can upgrade Communication Manager releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first before you upgrade to Release 6.3.6. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on the HP DL360 G8 Server or Dell R620 and restore the system data from the existing server.
- Continue with the procedures that are provided in this section.

Prerequisites

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the following software: • System Platform • the required Communication Manager template	_
	Obtain one of the following servers, as appropriate: • HP DL360 G8 • Dell R620	_
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, get *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 from the Avaya Support website at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Preupgrade tasks on the S8400 Server

Connecting to the server

A CAT5 cross-over cable to connect your services laptop to the server.

Procedure

1. Plug one end of the CAT5 cross-over cable into the services access port on the server faceplate.
2. Plug the other end of the cross-over cable into the services laptop.
3. Start a SAT session.
4. Log in as `craft`.

Accessing System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. If you log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Verifying system status

Start a SAT session.

Verify the groups that are in-service and the groups that are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

Procedure

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Clearing alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms that you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms using the SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

To use Telnet, enable the Telnet service for Communication Manager.

If the Telnet service is disabled, use SSH to gain access to SAT.

Procedure

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

Start a SAT session.

Procedure

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Recording node names and IP addresses

Procedure

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Disabling the scheduled maintenance

Start a SAT session.

The scheduled daily maintenance might interfere with the server upgrade. To prevent the interference, you must reschedule the daily maintenance activity.

Procedure

1. Enter `change system-parameters maintenance`.
2. Press `Enter`.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is stopped, set the **Start Time** field to a time later than the server upgrade completion time.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

Back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

If Communication Manager Messaging is enabled on your system, back up the messaging data.

Backing up the files

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**
     a. Select **Translations, Names, and Messages**.

3. In the **Backup Method** section, click **Network Device**.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
5. Click **Start Backup**.
6. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
7. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Recording configuration information

If you have not already completed, record the current server configuration data that you must configure on the new server. Use the worksheet provided in Worksheet for upgrading - to simplex and embedded templates on page 1376 to record the information.

Procedure

1. Click **Server Configuration** > **Configure Server**.
2. Click **Continue** on the first and second screen.
3. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
4. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
5. Select **Configure Interfaces** and record the following:
   - Server IP address
   - Gateway IP address
   - Subnet mask
   - Integrated Messaging IP address, if configured.
6. Click **Close**.

Copying files to the server

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

- Log on to System Management Interface.

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Installing the preupgrade service pack

Log on to System Management Interface.

To prepare the system for an upgrade to Communication Manager Release 6.3.6, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. Perform one of the following:
   - If the status of the update file you want to activate is `packed`:
     a. Select the **Update ID** and click **Unpack**.
     b. Wait until the system displays `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:
     a. Select the **Update ID** and click **Activate**. The system displays the status as the update progresses. The system automatically reboots, if required.
     b. Click **Yes**.
4. Click **Continue**.

Important:

To roll back the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Log on to System Management Interface.

Perform this procedure to generate a backup file that you later restore on the Release 6.3.6 system after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Checking for backed up files

Procedure

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

- If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system.
- If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.

Language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support website at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called the *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Log on to System Management Interface.

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Log on to System Management Interface.

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying the language packages on page 47.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device**.
8. Fill in the following fields:

   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
9. Click **Start Backup**.
10. To view the backup history, click **Status**.

    The system displays the Backup History page and a list of recent backups.
11. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.

5. Call the test station and record a message.

Shutting down Communication Manager Messaging

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device**.
7. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
8. Click **Start Backup**.
9. To view the backup history, click **Status**.

The system displays the Backup History page and a list of recent backups.

10. Select the backup file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Upgrade tasks on HP DL360 G8 or Dell R620 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you must turn on the new server, but do not connect the server to the network.

The new server can be one of the following:

- HP DL360 G8 Server

  For instructions to install, see *Installing the HP DL360 G8 Server.*

- Dell R620 Server

  For instructions to install, see *Installing the Dell R620 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Deploying Avaya Aura® Communication Manager on System Platform, 18-604394*.

- System Platform
- The Communication Manager license file
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on Domain-0. You must enable IP forwarding to access both SSH and the System Platform Web Console.

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Accessing the System Platform Web Console

To access the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 38.

Important:

You cannot get to Console Domain until the system finishes the first boot process.

You can get to the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

Note:

This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Accessing the System Management Interface

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Firefox 3.6 and later.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.

2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.

   The system copies the files to the default file location.

Restoring the upgrade dataset

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.3.6.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **File Path**
       - If you select `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you select `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.

5. Select the files to restore.

   For example, `migration-60_*.tar.gz` where, * is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Log on to System Management Interface.

Configure the server data using the information provided in the worksheets in Appendix A on page 1376.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.

4. Ensure that the system displays the `UP` status for Messaging. If not, start the messaging service:

   a. Click **Miscellaneous** > **Messaging Software**.

      The Messaging Software page displays `Internal messaging is disabled`.

   b. Click **Enable**.

      The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Postupgrade tasks for Communication Manager Messaging

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.

2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the URL to navigate to the patch.

   If required, click **Configure Proxy** to specify a proxy server.
5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

Related Links

Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51
Installing patches on page 51

Installing patches

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

Perform the following steps to install all System Platform and solution template service packs and feature packs with the System Platform Web Console.

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.

   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Commit the patch.

Related Links

Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51
Downloading patches on page 51

Copying language packages to the server

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 47.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.

   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Log on to System Management Interface.

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 48.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. In the **Method** field, select ftp.

4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

- Start a SAT session.
- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far-end node name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor Ethernet interface (PROCR) using the `status link procr` command.

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

      This step creates a node name that you use temporarily.
2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.

      You change this node name in Step 4. Typically the data in this field is `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.

4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node name.
8. Enter `save translation`.

Configuring the switch link

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Upgrade tasks on the cabinet

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. Changing or upgrading the hardware includes:

- Removing the TN8400AP or TN8400BP and TN8412AP (SIPI) circuit packs from the existing system.
- Connecting the IPSI circuit pack to the customer network.
- Assigning static IP address to the IPSI circuit pack.

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Completion tasks on the S8400 Server

Shutting down the server

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Tasks performed on the cabinet

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Port network (PN) must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to the PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

The system displays the IP address, the subnet mask, and the default gateway information.

d. Verify that the information displayed is correct.

e. Type `reset` and press `Enter`.

7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.

8. Perform the following steps to close the IPSI session and log in to IPSI:

a. Type `exit`.

The system saves the changes and ends the IPSI session.

b. Type `192.11.13.6` and log in to IPSI.

c. Type `show control interface`.

The system displays the IP address, the subnet mask, and the default gateway information.

d. Verify that the information displayed is correct.

e. Type `reset` and press `Enter`.

Add or copy the login portion before you add the control gateway.

9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Turning off the power to the control cabinet

Procedure

1. On the faceplate of the processor, press and hold the shutdown button until the system starts the shutdown process.

The green light indicates that the cabinet is shut down.

Important:

The latch on the power supply acts as the DC power switch and removes only DC power from the backplane.

2. Remove the power cord from the back of the cabinet.

The cabinet turns off.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.

5. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Start a SAT session.

Procedure

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Start a SAT session.

Procedure

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.

6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administering the IPSI circuit pack

Start a SAT session.

Procedure

1. Enter `change system-parameters ipserver-interface`.
2. Set the **Switch Identifier** field for the IPSI on this system.
3. Set the QoS parameters:
   - 802.1p: 6
   - DiffServ: 46

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **set port** commands.

Administering the media processor circuit pack

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

Procedure

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Postupgrade tasks on the HP DL360 G8 or Dell R620 Server

Verifying the Communication Manager operation

Performing an integrity check

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click **Display Once**.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Ping the IP address of Communication Manager by using SSH or Telnet.

Starting a SAT session

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If the system displays the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Procedures that you must skip on the survivable server

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading the survivable server.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling scheduled maintenance

Start a SAT session.

Procedure

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Related Links

Disabling the scheduled maintenance on page 41

Saving translations

Start a SAT session.

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Installing the phone message file

If the phone message file is installed on the existing system, identify the file.

Procedure

Install the phone message file. For instructions, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Resolving alarms

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade.

   For more information, see *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 44.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Important:

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These Utility Services settings apply to backups performed in Utility Services or in System Platform. Backup files are significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

   The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up the Communication Manager Messaging application data from 5.2.1

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.
7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.
   - **Directory**. The complete directory path where the backup is stored.
10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.
11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    Important:

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Registering the system

Use the standard procedure to register the system.

Appendix A: Worksheet for upgrading Communication Manager to simplex and embedded templates

Use this worksheet to record the information from the Communication Manager Release 5.2.1 server. Use the completed worksheet to configure the Communication Manager Release 6.3.6 server on a simplex survivable template, simplex survivable remote template, embedded survivable template, or embedded survivable remote template.

When you restore the upgrade dataset, on the Server Role webpage, the system automatically populates the following fields:

- **Server Role**
- **SID**
- **MID**
- **Memory Setting**
- **Media Gateway serial number**

In all the blank fields, enter the values using this worksheet.

Note:

IPv6 has restricted usage. Therefore, unless instructed otherwise, leave IPv6 disabled and do not enter information in the IPv6 fields.

Server Role

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server Role	MAIN, ESS, or LSP	**Configure Server > Server Role**	-
SID		`statuslicense -v`	RFA System ID
MID		`statuslicense -v`	RFA Module ID

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Registration address		**Configure Server > Configure LSP/ESS**	-
Registration address IPv6		Does not exist in Release 5.2.1	-
File Synch address		**Configure Server > Configure LSP/ESS**	-
File Synch address		**Configure Server > Configure LSP/ESS**	If MAIN is duplicated
File Synch address IPv6		Does not exist in Release 5.2.1	-
File Synch address IPv6		Does not exist in Release 5.2.1	If MAIN is duplicated
File Synch address		**Configure Server > Configure LSP/ESS**	Optional
File Synch address		**Configure Server > Configure LSP/ESS**	Optional, if MAIN is duplicated
File Synch address IPv6		Does not exist in Release 5.2.1	Optional
File Synch address IPv6		Does not exist in Release 5.2.1	Optional, if MAIN is duplicated
This server's memory setting	Small, Medium, or Large		The system populates with upgrade dataset restore. Also, see Help on Server Role webpage.
Media gateway serial number		Does not exist in Release 5.2.1	See, Help on Server Role webpage on Release 6.3.6.

Network Configuration

When you restore the upgrade dataset, on the Network Configuration webpage, the system automatically populates the following fields:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**
- System Platform Web Console, **Server Management** > **Network Configuration**.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server > Set Identities**	View only. Populated during the installation of System Platform.
DNS Domain		**Configure Server > DNS**	If you configured **CM Hostname** on System Platform: • As an FQDN, the webpage automatically populates the **CM Hostname** field in Communication Manager. • As simple hostname, you can configure the **CM Hostname** field in Communication Manager.
Search Domain list 1		**Configure Server > DNS**	In Communication Manager Release 6.3.6, **Domain Search list** is a single field and accepts comma-separated values. Combine the values obtained from **Search Domain list 1** to **Search Domain list 5** fields from Communication Manager Release 5.2.1 into a single comma-separated list for Communication Manager Release 6.3.6. If you configured **Domain Search list** on System Platform, the system populates the **Domain Search list** field

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			automatically in Communication Manager. If **Domain Search list** is not configured on System Platform, you can configure the **Domain Search list** in Communication Manager.
Search Domain list 2		**Configure Server > DNS**	-
Search Domain list 3		**Configure Server > DNS**	-
Search Domain list 4		**Configure Server > DNS**	-
Search Domain list 5		**Configure Server > DNS**	-
Primary DNS		**Configure Server > DNS**	Entered on the System Platform Web Console at the time of installation.
Secondary DNS		**Configure Server > DNS**	Entered on the System Platform Web Console at the time of installation.
Tertiary DNS		**Configure Server > DNS**	System Platform supports only two DNS values. System Platform does not automatically populate the third DNS value.
Server ID		**ID** field on Status Summary page	-
Default Gateway		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only. Populated during the installation of System Platform.
eth0 IP address IPv4		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only. Populated during the installation of the Communication Manager template.

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth0 mask IPv4		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only. Populated during the installation of the Communication Manager template.
eth0 IP address IPv6		Does not exist in Release 5.2.1	View only. Populated during the installation of the Communication Manager template.
eth0 functional assignment	PE assigned or PE unused	**Configure Server > Set Identities**	-

Appendix B: Worksheet for upgrading Communication Manager to duplex template

Use this worksheet to record the information from the Communication Manager Release 5.2.1 server. You must use the completed worksheet to configure the Communication Manager Release 6.3.6 server on a duplex main/survivable template.

When you restore the upgrade dataset, on the Server Role webpage, the system automatically populates the following fields:

- **Server role**
- **SID**
- **MID**
- **Memory Setting**

In all the blank fields, enter the values using this worksheet.

Note:

IPv6 has restricted usage. Therefore, unless instructed otherwise, leave IPv6 disabled and do not enter information in the IPv6 fields.

Server Role

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server Role	MAIN or ESS	**Configure Server > Server Role**	-
SID		`statuslicense -v`	RFA System ID
MID		`statuslicense -v`	RFA Module ID
Only for survivable core (ESS) server			
Registration address		**Configure Server > Configure ESS**	-
Registration address IPv6		Does not exist in Release 5.2.1	-

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
File Synch address		**Configure Server > Configure ESS**	-
File Synch address		**Configure Server > Configure ESS**	If MAIN is duplicated
File Synch address IPv6		Does not exist in Release 5.2.1	-
File Synch address IPv6		Does not exist in Release 5.2.1	If MAIN is duplicated
File Synch address		**Configure Server > Configure ESS**	Optional
File Synch address		**Configure Server > Configure ESS**	Optional, if MAIN is duplicated
File Synch address IPv6		Does not exist in Release 5.2.1	Optional
File Synch address IPv6		Does not exist in Release 5.2.1	Optional, if MAIN is duplicated
This server's memory setting	Small, Medium, or Large		The system populates after you restore the dataset. Also, see the Help on the Server Role Web page.

Network Configuration Server 1

When you restore the upgrade dataset, on the Network Configuration webpage, the system automatically populates the following fields:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**

- System Platform Web Console, **Server Management** > **Network Configuration**.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server** > **Identities**	View only. Populated during the installation of System Platform.
Alias Host Name		**Configure Server** > **Identities**	-
DNS Domain		**Configure Server** > **DNS**	If you have configured **CM Hostname** on System Platform: • As an FQDN, the webpage automatically populates this field in Communication Manager. • As simple hostname, you can configure this field in Communication Manager.
Search Domain list 1		**Configure Server** > **DNS**	In Communication Manager Release 6.3.6, **Domain Search List** is a single field and accepts comma separated values. Combine the values obtained from **Search Domain list 1** to **Search Domain list 5** fields from Communication Manager Release 5.2.1 into a single comma separated list for Communication Manager. If you configured **Domain Search List** on System Platform, the system automatically populates **Domain Search List** field in Communication Manager. If you did not configure **Search Domain list 1** on System Platform, you can configure the **Search**

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			Domain list 1 in Communication Manager.
Search Domain list 2		**Configure Server** > **DNS**	-
Search Domain list 3		**Configure Server** > **DNS**	-
Search Domain list 4		**Configure Server** > **DNS**	-
Search Domain list 5		**Configure Server** > **DNS**	-
Primary DNS		**Configure Server** > **DNS**	Entered on System Platform at the time of installation.
Secondary DNS		**Configure Server** > **DNS**	Entered on System Platform at the time of installation.
Tertiary DNS		**Configure Server** > **DNS**	System Platform supports only two DNS values. System Platform does not automatically populate the third DNS value.
Server ID		**ID** field on Status Summary page	-
Default Gateway		**Configure Server** > **Set Identities** and **Configure Server** > **Configure Interfaces**	View only. Populated during the installation of System Platform.
Default Gateway IPv6		Does not exist in Release 5.2.1	-

Table 4: etho

eth0 represents the IP interface for Corporate LAN, Control Network or Processor Ethernet functionality. On the existing Communication Manager 5.2.1 server, the Corporate LAN, Control Network, and Processor Ethernet may have been assigned to an ethernet interface other than eth0.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth0 IP address IPv4		**Configure Server** > **Set Identities** and **Configure**	View only. Populated during the installation of

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
		Server > **Configure Interfaces**	the Communication Manager template.
eth0 mask IPv4		**Configure Server** > **Set Identities** and **Configure Server** > **Configure Interfaces**	View only. Populated during the installation of the Communication Manager template.
eth0 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of the Communication Manager template.
eth0 Alias IP address		**Configure Server** > **Set Identities** and **Configure Server** > **Configure Interfaces**	-
eth0 functional assignment	PE assigned or PE unused	**Configure Server** > **Set Identities**	For MAIN, you can make the Processor Ethernet available.

Table 5: eth1

eth1 represents the IP interface for duplication functionality of Communication Manager. On the existing Communication Manager 5.2.1 server, the Duplication Interface may have been assigned to an Ethernet interface other than eth1.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 IP address IPv4		**Configure Server** > **Configure Interfaces**	This field is the Duplication Interface IP address for this server. Typically: • 192.11.13.13 for server 1 • 192.11.13.14 for server 2
eth1 mask IPv4		**Configure Server** > **Configure Interfaces**	Typically 255.255.255.252.
eth1 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of the Communication Manager template.
eth1 Alias IP address	Leave this field blank	Not applicable	Leave the field blank.
eth1 functional assignment	select **Duplication Link**	Not applicable	Select **Duplication Link**.

Duplication Parameters

Table 6: Server 1

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server Duplication	Encrypted or un-Encrypted	**Configure Server** > **Set Identities** and	See the worksheets for **Network Configuration**
Hostname		**Configure Server** > **Set Identities**	Enter the hostname of the other server.
Server ID		**Configure Server** > **Set Identities**	Enter the server ID of the other server.
Corporate LAN/PE IP address		**Configure Server** > **Configure Interfaces**	Enter the eth0 IP address of the other server.
Corporate LAN/PE IP address IPv6		Does not exist in Release 5.2.1	Enter the eth0 IP (IPv6) address of the other server.
Duplication IP address		**Configure Server** > **Configure Interfaces**	Enter the eth1 IP address of the other server.
Duplication IP address, IPv6		Does not exist in Release 5.2.1	Enter the eth1 IP (IPv6) address of the other server.
PE Interchange Priority	HIGH, EQUAL, LOW, or IGNORE	**Configure Server** > **Configure Interfaces**	Must be the same for both servers.
IP address for PE Healthcheck		**Configure Server** > **Configure Interfaces**	-
IP address for PE Healthcheck IPv6		Does not exist in Release 5.2.1	-

Network Configuration Server 2

When you restore the upgrade dataset, on the Network Configuration webpage, the system automatically populates the following fields:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**
- System Platform Web Console, **Server Management** > **Network Configuration**.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server** > **Set Identities**	View only. Populated during the installation of System Platform.
Alias Host Name		**Configure Server** > **Set Identities**	-
DNS domain		**Configure Server** > **DNS**	If you have configured **CM Hostname** on System Platform: • As an FQDN, the webpage automatically populates thisCommunication Manager. • As simple hostname, you can configure this field in Communication Manager
Search Domain list 1		**Configure Server** > **DNS**	In Communication Manager Release 6.3.6, **Domain Search List** is a single field and accepts comma separated values. Combine the values obtained from **Domain Search List** to **Search Domain list 5** fields from Communication Manager Release 5.2.1 into a single comma separated list for Communication Manager Release 6.3.6. If you have configured **Domain Search List** on System Platform, the

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			system automatically populates the **Domain Search List** field in Communication Manager. If you have not configured **Search Domain list 1** on System Platform, you can configure the **Search Domain list 1**.in Communication Manager.
Search Domain list 2		**Configure Server** > **DNS**	-
Search Domain list 3		**Configure Server** > **DNS**	-
Search Domain list 4		**Configure Server** > **DNS**	-
Search Domain list 5		**Configure Server** > **DNS**	-
Primary DNS		**Configure Server** > **DNS**	Enter these values on the System Platform web console.
Secondary DNS		**Configure Server** > **DNS**	Enter these values on the System Platform web console.
Tertiary DNS		**Configure Server** > **DNS**	System Platform supports only two DNS values. System Platform does not automatically populate the third DNS value.
Server ID		**Status Summary** > **ID**	-
Default Gateway		**Configure Server** > **Set Identities**	View only. Populated during the installation of System Platform.
Default Gateway IPv6		Does not exist in Release 5.2.1	

Table 7: eth0

eth0 represents the IP interface for Corporate LAN, Control Network or Processor Ethernet functionality. On the existing Communication Manager 5.2.1 server, the Corporate LAN, Control Network, and Processor Ethernet may have been assigned to an ethernet interface other than eth0.

Field	Value	Method for obtaining from CM Release 5.2.1	Note
eth0 IP address IPv4		**Configure Server** > **Configure Interfaces**	View only. Populates during the installation of Communication Manager template.
eth0 mask IPv4		**Configure Server** > **Configure Interfaces**	View only. Populates during the installation of the Communication Manager template.
eth0 IP address, IPv6		Does not exist in Release 5.2.1	If present, populates during the installation of the Communication Manager template.
eth0 Alias IP address		**Configure Server** > **Configure Interfaces**	-
eth0 functional assignment	PE assigned or PE unused	**Configure Server** > **Set Identities**	For main, you can make the Processor Ethernet available.

Table 8: eth1

eth1 represents the IP interface for duplication functionality of Communication Manager. On the existing Communication Manager 5.2.1 server, the Duplication Interface may have been assigned to an ethernet interface other than eth1.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 IP address IPv4		**Configure Server** > **Configure Interfaces**	This field is the Duplication Interface IP address for this server. Typically: • 192.11.13.13 for server 1 • 192.11.13.14 for server 2
eth1 mask IPv4		**Configure Server** > **Configure Interfaces**	Typically 255.255.255.252.
eth1 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of the Communication Manager template.
eth1 Alias IP address	Leave this field blank	**Configure Server** > **Configure Interfaces**	Leave this field blank.
eth1 functional assignment	select **Duplication Link**	**Configure Server** > **Set Identities**	Select **Duplication Link**

Duplication Parameters

Table 9: Server 2

Field	Value	Method for obtaining from 5.2.1	Notes
Server Duplication	Encrypted or un-Encrypted	**Configure Server** > **Set Identities**	See the worksheets for **Network Configuration**.
Hostname		**Configure Server** > **Set Identities**	Enter the host name of the other server
Server ID		**Configure Server** > **Set Identities**	Enter the server ID of the other server
Corporate LAN/PE IP address		**Configure Server** > **Configure Interfaces**	Enter the eth0 IP address of the other server
Corporate LAN/PE IP address IPv6		Does not exist in Release 5.2.1	Enter the eth0 IP (IPv6) address of the other server
Duplication IP address		**Configure Server** > **Configure Interfaces**	Enter the eth1 IP address of the other server
Duplication IP address, IPv6		Does not exist in Release 5.2.1	Enter the eth1 IP (IPv6) address of the other server
PE Interchange Priority	HIGH, EQUAL, LOW, or IGNORE	**Configure Server** > **Configure Interfaces**	Must be the same for both servers.
IP address for PE Healthcheck		**Configure Server** > **Configure Interfaces**	-
IP address for PE Healthcheck IPv6		Does not exist in Release 5.2.1	-

Appendix C: Worksheet for upgrading Communication Manager on simplex to duplex template

Use this worksheet to record the information from a simplex server running Communication Manager Release 5.2.1. You must use the completed worksheet to configure the Communication Manager Release 6.3.6 server on a duplex main/survivable core template.

When you restore the upgrade dataset, on the Server Role webpage, the system automatically populates the following fields:

- **Server role**
- **SID**
- **MID**
- **Memory Setting**

In all the blank fields, enter the values using this worksheet.

Note:

IPv6 has restricted usage. Therefore, unless instructed otherwise, leave IPv6 disabled and do not enter information in the IPv6 fields.

Server Role
Server 1 and Server 2

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server Role	MAIN or ESS	**Configure Server** > **Server Role**	-
SID		`statuslicense -v`	RFA System ID
MID		`statuslicense -v`	RFA Module ID
This server's memory setting	Small, Medium, or Large		Auto populates with upgrade dataset restore. Also, see Help on Server Role Web page.
Only for survivable core (ESS) server			

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Registration address		**Configure Server** > **Configure ESS**	-
Registration address IPv6		Does not exist in Release 5.2.1	-
File Synch address Main		**Configure Server** > **Configure ESS**	-
File Synch address Main duplicate		**Configure Server** > **Configure ESS**	If MAIN is duplicated
File Synch address IPv6 Main		Does not exist in Release 5.2.1	-
File Synch address IPv6 Main duplicate		Does not exist in Release 5.2.1	If MAIN is duplicated
File Synch address Alternate		**Configure Server** > **Configure ESS**	Optional
File Synch address Alternate duplicate		**Configure Server** > **Configure ESS**	Optional, if Alternate is duplicated
File Synch address IPv6 Alternate		Does not exist in Release 5.2.1	Optional
File Synch address IPv6 Alternate duplicate		Does not exist in Release 5.2.1	Optional, if Alternate is duplicated

Network Configuration Server 1

You must assign a unique server ID to both the servers. The original simplex server has a server ID assigned to it. You can assign the same server ID to one of the new server pair. For example, if the server ID of the original simplex server is 1, assign *1* to one server and *2* to the other server.

For duplicated survivable core server, the server ID on the Network Configuration Web page must also correspond to Communication Manager translations on the corresponding survivable-processor SAT screen. See *Avaya Aura® Communication Manager Survivable Options* (03-603633) for more information on administering Communication Manager for survivable processors.

When you restore the upgrade dataset, on the Network Configuration webpage, the system automatically populates the following fields:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**
- System Platform Web Console, **Server Management** > **Network Configuration**.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server** > **Identities**	View only. Populated during the installation of System Platform. The hostname must be a new name specific to server 1 of the new pair of servers. Do not use the hostname of the Communication Manager Release 5.2.1 server. You use Release 5.2.1 hostname in another field.
Alias Host Name		**Configure Server** > **Identities**	Use the hostname of the Communication Manager Release 5.2.1 server.
DNS Domain		**Configure Server** > **DNS**	If you have configured **CM Hostname** on System Platform Web Console: • As an FQDN, the Web page automatically populates this field in Communication Manager. • As simple hostname, you can configure this field in Communication Manager.
Search Domain list 1		**Configure Server** > **DNS**	In Communication Manager Release 6.3.6, **Domain Search List** is a single field and accepts comma-separated values. Combine the

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			values obtained from **Search Domain list 1** to **Search Domain list 5** fields from Communication Manager Release 5.2.1 into a single comma-separated list for Communication Manager Release 6.3.6. If you have configured **Domain Search List** on System Platform, the system automatically populates the **Domain Search List** field in Communication Manager. If you have not configured the **Search Domain list 1** on System Platform, you can configure the **Search Domain list 1** in Communication Manager.
Search Domain list 2		**Configure Server** > **DNS**	-
Search Domain list 3		**Configure Server** > **DNS**	-
Search Domain list 4		**Configure Server** > **DNS**	-
Search Domain list 5		**Configure Server** > **DNS**	-
Primary DNS		**Configure Server** > **DNS**	Entered on System Platform Web Console at the time of installation
Secondary DNS		**Configure Server** > **DNS**	Entered on System Platform Web Console at the time of installation
Tertiary DNS		**Configure Server** > **DNS**	System Platform supports only two DNS values, it does not automatically populate the third DNS value.

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server ID		**ID** field on Status Summary page	-
Default Gateway		**Configure Server** > **Set Identities** and **Configure Server** > **Configure Interfaces**	View only. Populated during the installation of System Platform.
Default Gateway IPv6		Does not exist in Release 5.2.1	-

Table 10: eth0

eth0 represents the IP interface for Corporate LAN, Control Network or Processor Ethernet functionality. On the existing Communication Manager 5.2.1 server, the Corporate LAN, Control Network, and Processor Ethernet may have been assigned to an ethernet interface other than eth0.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth0 IP address IPv4		**Configure Server** > **Set Identities** and **Configure Server** > **Configure Interfaces**	View only. Populated during the installation of the Communication Manager template. Use the IP address assigned for server 1. Do not use the IP address of the Communication Manager Release 5.2.1 server. You use this IP address in another field.
eth0 mask IPv4		**Configure Server** > **Set Identities** and **Configure Server** > **Configure Interfaces**	View only. Populated during the installation of the Communication Manager template.
eth0 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of the Communication Manager template.
eth0 Alias IP address IPv4		**Configure Server** > **Set Identities** and **Configure Server** > **Configure Interfaces**	Use the IP address of the Communication Manager Release 5.2.1 server.
eth0 Alias IP address IPv6		Does not exist in Release 5.2.1	-
eth0 functional assignment	PE assigned or PE unused	**Configure Server > Set Identities**	For MAIN, you can make the Processor Ethernet available.

Table 11: eth1

eth1 represents the IP interface for duplication functionality of Communication Manager. On the existing Communication Manager 5.2.1 server, the Duplication Interface may have been assigned to an Ethernet interface other than eth1.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 IP address IPv4		**Configure Server > Configure Interfaces**	This field is the Duplication Interface IP address for this server. Typically: • 192.11.13.13 for server 1 • 192.11.13.14 for server 2
eth1 mask IPv4		**Configure Server > Configure Interfaces**	Typically 255.255.255.252.
eth1 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of the Communication Manager template.
eth1 Alias IP address	Leave this field blank	Not applicable	Leave the field blank
eth1 functional assignment	select **Duplication Link**	Not applicable	Select **Duplication Link**

Duplication Parameters

Table 12: Server 1

Field	Value	Notes
Server Duplication	Encrypted or un-Encrypted	See the worksheets for **Network Configuration**.
Hostname		Enter the host name of the other server
Server ID		Enter the server ID of the other server
Corporate LAN/PE IP address		Enter the eth0 IP address of the other server
Corporate LAN/PE IP address IPv6		Enter the eth0 IP (IPv6) address of the other server
Duplication IP address	192.11.13.14	Enter the eth1 IP address of the other server
Duplication IP address, IPv6		Enter the eth1 IP (IPv6) address of the other server

Table continues…

Field	Value	Notes
PE Interchange Priority	HIGH, EQUAL, LOW, or IGNORE	Must be the same for both servers
IP address for PE Healthcheck		The network gateway router is the default address. You can also use the IP address of other device on the network that responds. For more information, see the Help on the Duplication Parameters page.
IP address for PE Healthcheck IPv6		The network gateway router is the default address. You can also use the IP address of other device on the network that responds. For more information, see the Help on the Duplication Parameters page.

Network Configuration Server 2

Server ID for a server must be unique. The original simplex server has a server ID assigned to it. You can assign the same server ID to one of the new server pair. For example, if the server ID of the original simplex server is 1, assign *1* to one server and *2* to the other server.

For duplicated survivable core server, the server ID on the Network Configuration page must also correspond to Communication Manager translations on the corresponding survivable-processor SAT screen. For more information on administering Communication Manager for survivable processors, see *Avaya Aura® Communication Manager Survivable Options*, 03-603633.

When you restore the upgrade dataset, on the Network Configuration page, the system automatically populates the following information:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**
- System Platform Web Console, **Server Management** > **Network Configuration**.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server** > **Identities**	View only. Populated during the installation of System Platform. The host name must be a new name specific to server 1 of the new pair of servers. Do not use the host name of the Communication Manager Release 5.2.1 server. You use this host name in another field.
Alias Host Name		**Configure Server** > **Identities**	Use the exact host name of the Communication Manager Release 5.2.1 server.
DNS domain		**Configure Server** > **DNS**	If you have configured **CM Hostname** on System Platform: • As an FQDN, the Web page automatically populates this field in Communication Manager. • As simple hostname, you can configure this field in Communication Manager.
Search Domain list 1		**Configure Server** > **DNS**	In Communication Manager Release 6.3.6, **Domain Search List** is a single field and accepts comma-separated values. Combine the values obtained from **Domain Search List** to **Search Domain list 5** fields from Communication Manager Release 5.2.1 into a single comma-separated list for Communication Manager Release 6.3.6.

Table continues…

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			If you have configured **Domain Search List** on System Platform, the **Domain Search List** field is automatically populated in Communication Manager. If you have not configured **Search Domain list 1** on System Platform, you can configure the **Search Domain list 1** in Communication Manager.
Search Domain list 2		**Configure Server** > **DNS**	-
Search Domain list 3		**Configure Server** > **DNS**	-
Search Domain list 4		**Configure Server** > **DNS**	-
Search Domain list 5		**Configure Server** > **DNS**	-
Primary DNS		**Configure Server** > **DNS**	Enter these values on the System Platform Web Console.
Secondary DNS		**Configure Server** > **DNS**	Enter these values on the System Platform Web Console.
Tertiary DNS		**Configure Server** > **DNS**	System Platform supports only two DNS values, it does not automatically populate the third DNS value.
Server ID		**Status Summary** > **ID**	-
Default Gateway		**Configure Server** > **Set Identities**	View only. Populated during the installation of System Platform.
Default Gateway IPv6		Does not exist in Release 5.2.1	-

Table 13: eth0

eth0 represents the IP interface for Corporate LAN, Control Network or Processor Ethernet functionality. On the existing Communication Manager Release 5.2.1 server, the Corporate LAN, Control Network, and Processor Ethernet may have been assigned to an ethernet interface other than eth0.

Field	Value	Method for obtaining from CM Release 5.2.1	Note
eth0 IP address IPv4		**Configure Server** > **Configure Interfaces**	View only. Populated during the installation of Communication Manager template. Use the IP address assigned for server 1. Do not use the IP address of the Communication Manager Release 5.2.1 server. You must use this IP address in another field.
eth0 mask IPv4		**Configure Server** > **Configure Interfaces**	View only. Populated during the installation of Communication Manager template.
eth0 IP address, IPv6		Does not exist in Release 5.2.1	If present, populates during the installation of Communication Manager template.
eth0 Alias IP address IPv4		**Configure Server** > **Configure Interfaces**	Use the IP address of the Communication Manager Release 5.2.1 server.
eth0 Alias IP address IPv6		Does not exist in Release 5.2.1	-
eth0 functional assignment	PE assigned or PE unused	**Configure Server** > **Set Identities**	For main, you can choose to make the Processor Ethernet available.

Table 14: eth1

eth1 represents the IP interface for duplication functionality of Communication Manager. On the existing Communication Manager 5.2.1 server, the Duplication Interface may have been assigned to an ethernet interface other than eth1.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 IP address IPv4		**Configure Server** > **Configure Interfaces**	This field is the Duplication Interface IP address for this server. Typically: • 192.11.13.13 for server 1 • 192.11.13.14 for server 2
eth1 mask IPv4		**Configure Server** > **Configure Interfaces**	Typically 255.255.255.252.
eth1 IP address IPv6		Does not exist in Release 5.2.1	If present, the system populates during the installation of the Communication Manager template.
eth1 Alias IP address	Leave this field blank	**Configure Server** > **Configure Interfaces**	Leave the field blank.
eth1 functional assignment	select **Duplication Link**	**Configure Server** > **Set Identities**	Select **Duplication Link**.

Duplication Parameters

Table 15: Server 2

Field	Value	Notes
Server Duplication	Encrypted or un-Encrypted	See the worksheets for **Network Configuration**.
Hostname		Enter the hostname of the other server.
Server ID		Enter the server ID of the other server.
Corporate LAN/PE IP address		Enter the eth0 IP address of the other server.
Corporate LAN/PE IP address IPv6		Enter the eth0 IP (IPv6) address of the other server.
Duplication IP address	192.11.13.13	Enter the eth1 IP address of the other server.
Duplication IP address, IPv6		Enter the eth1 IP (IPv6) address of the other server.
PE Interchange Priority	HIGH, EQUAL, LOW, or IGNORE	Must be the same for both servers.

Table continues…

Field	Value	Notes
IP address for PE Healthcheck		The network gateway router is the default address. You can also use the IP address of other device on the network that responds. For more information, see Help on the Duplication Parameters page.
IP address for PE Healthcheck IPv6		The network gateway router is the default address. You can also use the IP address of other device on the network that responds. For more information, see Help on the Duplication Parameters page.

Appendix D: Converting private control networks A and B to control network C

Introduction

Before you upgrade the system to Communication Manager Release 6.3.6, you must remove private control networks, and place all IPSI on the network that connects the Communication Manager server to the corporate LAN.

This procedure applies to duplicated Communication Manager servers with the following conditions:

- Servers that are not yet upgraded to Communication Manager Release 6.3.6.
- Port networks with duplicated IPSI circuit pack, HP DL360 G8 or Dell R620 Server in the duplex configuration.
- Port networks with simplex IPSI circuit pack.

Preparing for port network conversion

Procedure

1. Collect the location of all IPSI circuit packs in control network A (CN-A) and control network B (CN-B).
2. On a worksheet, assign a new public (static) control network IP addresses to each CN-A and CN-B IPSI in the system.
3. Verify that all port networks have duplicated IPSI circuit packs.

   This activity determines whether the changes impacts the service. Duplicate IPSIs infer the changes may be executed on each circuit pack as the IPSI is in standby mode.

   Note:

   If an IPSI contains only one IPSI (not duplicated IPSI, which may be the case for some port networks), the conversion to CN-C affects the service for that port network.
4. Assign a port to the network switches supporting the IPSIs to connect to the public network routing system.

5. Obtain required cables for connecting the switch. Do not use the cables from the former dedicated (private) control network.

Converting private control network to control network C

- Ensure that IPSIs are running the latest firmware.
- Disable the DHCP service for private control networks on Communication Manager servers.
- Start the SAT session.

Convert the duplicated IPSI systems on the public control network to control network C.

Procedure

1. Connect the network switch devices supporting IPSIs to the public control network.

   Note:

   Do not disconnect the Ethernet switch private network from Communication Manager servers until instructed.

2. If a public network is not assigned to the server community, perform the following actions:
   a. Log in to the server.
   b. Type `cnc on`.

      Run this command on:

      - Both Communication Manager servers.
      - Any survivable core servers that are part of the system.

3. Type `set ipserver-interface b-all`.
4. Type `list ip-server-interface` to confirm that all b-side boards are active.

   If all b-side boards are not active, interchange the boards individually and debug issues until the b-side boards in all port networks are in service.

5. Type `change ipserver-interface X`.
   a. In the **Secondary IPSI** field, enter the new IP addresses.
   b. Continue to change all b-side IPSI addresses.
   c. Type `list ipserver-interface` command to verify that all b-side IPSIs are in service.

      Because the network switch is connected to the public network, IPSIs display `0.0.0.0`, that indicates that all aspects of connectivity are good and IPSIs are in service.

6. Type `set ipserver-interface a-all` to interchange IPSIs.

   All a-side IPSIs must be in the standby and in service. Debug IPSIs if IPSIs are inactive.

7. Repeat the address changes for all a-side IPSIs.
8. Type `list ipserver-interface` and verify that all IPSI interfaces display `0.0.0.0`.
9. Type `list sys-link` and verify that EAL links are functional.
10. Make some IP and TDM type calls and exercise a couple of IPSI interchanges to confirm reliability.
11. Change the management IP addresses of the CN-A and CN-B Ethernet switches to an available address in the newly connected public control network.
    a. On Ethernet switches, restart to make the new address active.

       To prevent the service interruption, restart only when IPSIs are in the standby mode.

    b. Disconnect and remove Ethernet cables from CN-A and CN-B ports of the server and the former CN-A and CN-B switches.

Related Links

Configuring the IPSI circuit pack on page 339

Appendix E: Converting from fiber port networks to IP-PNC

Overview

Fiber port network connectivity (fiber-PNC) uses the circuit-switched (TDM) protocol to transport bearer traffic (voice, fax, video) between port networks (PN) over fiber-optic cables. IP-PNC uses the packet-switched Internet Protocol to transport bearer traffic over Ethernet cables.

Note:

The term fiber-PNC used in this document has almost the same meaning as the term multiconnect. Multiconnect implies a dedicated control network and fiber-PNC that carry the bearer traffic. The term fiber-PNC applies to configurations with a dedicated or a nondedicated control network.

You are required to change the MCC1, SCC1, and G650 cabinets present in the current fiber-PNC configuration to IP-PNC configuration.

When you convert a system to IP-PNC, the **Internet Protocol (IP) PNC** field on the Customer Options screen is set to y.

The conversion procedures apply to individual PNs in a communications system that is composed of one or more PNs. In the final converted system, the PNs are 100% IP-PNC.

Use these procedures to convert the fiber-PNC to IP-PNC. These procedures are applicable for PNs controlled by servers running Communication Manager Release 3.0 and later.

Fiber-PNC configurations

The conversion procedures cover the following three fiber-PNC configurations:

- Direct connect

  In this configuration, one PN, the control PN, is IPSI-connected to the control network, and one or two additional PNs are fiber-connected to the control PN. The fiber connections are between the TN570 Expansion Interface (EI) circuit packs in the PNs.

- Center Stage Switch (CSS)

In this configuration, all PNs are fiber-connected through the CSS and one or more PNs are connected to the control network through the TN2312 IP Server Interface (IPSI) circuit pack. The fiber connections are between the TN573 Switch Node Interface (SNI) circuit packs and the TN570 Expansion Interface (EI) circuit packs. The SNI circuit packs reside in a switch node carrier. The EI circuit packs reside in a PN. The fiber also can connect SNIs in two switch-node carriers.

- Asynchronous Transmission Mode (ATM)

  In this configuration, all PNs are fiber-connected through the ATM switch, and one or more PNs are connected to the control network through the TN2312 IP Server Interface (IPSI) circuit pack. The fiber connections are between the ATM switch and the TN2305B or TN2306B ATM Interface circuit packs in the PNs.

The starting configuration

The starting configuration consists:

- Two or three fiber-PNC PNs in a direct connect configuration
- Up to 64 fiber-PNC PNs that use CSS or an ATM switch

All PNs are fiber-connected, and one or more PNs are IPSI-connected to the control network. For Communication Manager release 3.0 and later, the starting configuration may include some IP-PNC components in addition to the fiber-PNC components. Each PN may be implemented in an MCC1, an SCC1 stack, or a G650 stack. The overall system may be any combination of MCC1, SCC1, or G650 Media Gateways.

The starting configuration can be any of the following:

- Simplex or duplex servers
- Simplex or duplex control networks
- Simplex or duplex bearer networks

The converted configuration

The final converted configuration is all IP-PNC. Fiber-PNC does not exist after the conversion.

The final configuration can only be on port networks controlled by a server running Communication Manager on a simplex or a duplex template.

For systems that are controlled by a server running a simplex or a duplex template, the IP-PNC components can have a simplex or a duplex control networks and a simplex or a duplex bearer network.

Prerequisites

Preconversion checklist

Before you start the conversion, ensure that you have the conversion specific hardware:

✔	Task	Description
	Obtain the following circuit packs: • TN2312BP IPSI • TN2302AP HW11 (or later) or TN2602AP Media Processor • TN799DP C-LAN	

Conversion tasks checklist

Conversion procedure involves the following major tasks:

#	Task
1	Changing synchronization
2	Adding new circuit packs
3	Upgrading firmware on circuit packs
4	Disabling PNC duplication
5	Removing fiber-related administration
6	Enabling PNC duplication
7	Removing fiber-related hardware
8	Administering PN synchronization
9	Completing post-conversion tasks

Changing synchronization

Use this procedure only if you are converting the PN that contains the direct-connect, CSS or ATM synchronization source. Perform the following steps to remove or change the synchronization source:

Synchronization for a direct connect configuration is derived from a fiber-PNC. Synchronization for the ATM is derived from a connection through an ATM-connected PN.

Procedure

1. Perform one of the following:
   - For direct connect and CSS, enter `change synchronization css`.
   - For ATM, enter `change synchronization atm`.
2. Leave the **Primary** and **Secondary** fields blank.
3. Click **Submit**.
4. Verify that the synchronization sources are updated correctly.
5. Enter `list synchronization`.
6. Verify that the **Primary** field and the **Secondary** field are blank.

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

Procedure

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

Procedure

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.
7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.
8. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.

c. Type `show control interface`.

   The system displays the IP address, the subnet mask, and the default gateway information.

d. Verify that the information displayed is correct.

e. Type `reset` and press `Enter`.

   Add or copy the login portion before you add the control gateway.

9. Type `exit`.

Verifying the installation of the circuit pack

Start a SAT session.

Procedure

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

Procedure

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.

3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the network regions, see *Administering Network Connectivity on Avaya Aura® Communication Manager,* 555-233-504.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit pack

Start a SAT session.

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6
     - DiffServ: 46
3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Configuring the IPSI circuit pack

For static addressing, perform the procedure on the circuit pack.

Procedure

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Type `telnet 192.11.13.6` to access the IPSI circuit pack.
3. At the prompt, type `ipsilogin` to log in to IPSI IP Administration Utility.
4. Log in as `craft` and type the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, type `set control interface` *`ipaddr netmask`*.
6. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.
7. If the IPSI circuit pack uses a default gateway, type `set control gateway` *`gatewayaddr`*, where gatewayaddr is the IP address for the network gateway that the customer-provided.
8. Perform the following steps to close the IPSI session and log in to IPSI:
   a. Type `exit`.

      The system saves the changes and ends the IPSI session.
   b. Type `192.11.13.6` and log in to IPSI.
   c. Type `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information.
   d. Verify that the information displayed is correct.
   e. Type `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Type `exit`.

Setting the VLAN parameters and diffserv parameters

Start a SAT session.

Procedure

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Verifying IPSI translations

Procedure

1. Enter `list ipserver-interface`.
2. Verify that the IPSI circuit packs are translated.

   The system displays `0.0.0.0` in the **State of Health - C P E G** field for each healthy IPSI. If the system displays `1` in any position, troubleshoot the problem.

   The pattern `0.1.1.0` indicates that a cabinet type is administered incorrectly or a connectivity problem such as an incorrectly terminated cable exists.

Verifying IPSI connectivity

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Administering the media processor circuit pack

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

Procedure

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.

7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

Procedure

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface UUCSS` to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Firmware upgrade on the new circuit packs

The IPSI, the media processor, and the C-LAN circuit packs that you add must have the latest available firmware installed. Check the version of the firmware that is installed on each circuit pack and compare with the latest version that is available on the Avaya Support Web site. If a circuit pack does not have the latest version installed, upgrade the firmware on the circuit pack. If you have not already copied the latest firmware to your laptop, download the latest firmware files from the Avaya Support Web site available at http://avaya.com/support.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Procedure

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing fiber-related administration

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

Procedure

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link n`, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link n`.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Disabling PNC duplication

If the bearer network is duplicated, remove the duplication before you remove the fiber-optic connections. If the system does not have PNC duplication, continue with the next procedure.

Procedure

1. To check which of the duplicated PNCs is active, enter `status pnc`.
2. To busyout the standby PNC, enter `busyout pnc-standby`.
3. To open the duplication screen, enter `change system-parameters duplication`.
4. In the **Enable Operation of PNC Duplication** field, enter `n` and click **Submit**.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

1. Remove the fiber cables that connect the following circuit packs in the PNs:
   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Administering PN synchronization

Start a SAT session.

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

Procedure

1. To view the synchronization information for the IP-PNC PNs, enter `list synchronization` and `status synchronization`.
2. Verify that the following fields are blank:
   - The **Primary** and the **Secondary** fields on the Synchronization Plan window.
   - The **Source Physical Location** field on the Synchronization Status window.

3. Enter `change synchronization port-network n`, where *n* is the PN number of the converted port network that requires synchronization.
4. Enter `list cabinet`.

   The system displays a list of all the cabinets and the PNs that the cabinets contain in the **Circuit Packs Available for Synchronization** section.
5. Obtain a location for the synchronization source circuit pack from the list in the **Circuit Packs Available for Synchronization** section for **Primary** and **Secondary** fields. Select a synchronization source that works.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, in the **Secondary** field, add another location for synchronization-source circuit pack.
8. Press `Submit`.

   Wait for about 5 minutes for Communication Manager to update the synchronization plan.
9. To verify the changes, enter `list synchronization` and the `status synchronization` commands.
10. If the **Switching Capability** field for this PN is disabled on the Synchronization Status window, enter `enable synchronization all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must display `PASS` in the **Results** field. If the **Results** field does not display `PASS`, troubleshoot the synchronization error.

Index

A

accessing
the server 659
Accessing
the new server 570, 603, 711, 851
accessing System Management Interface 998, 1161, 1339
Accessing the first new server 570, 603, 711, 851
accessing the server 659
activate
connection preservation during an upgrade 68
adding
cables for new circuit packs
.....340, 491, 884, 1232, 1260, 1288, 1327, 1365, 1411
memory modules 201, 399
adding a branch gateway .913, 1015, 1049, 1115, 1168, 1184
adding a third hard drive 202, 399
adding cables for new circuit packs
.....340, 491, 884, 1232, 1260, 1288, 1327, 1365, 1411
adding IPSI information
.....342, 494, 886, 1234, 1262, 1290, 1329, 1366
Adding memory modules 201, 399
addition
of new circuit packs
.....338, 489, 882, 1230, 1258, 1285, 1325, 1362, 1409
add new circuit packs
.....338, 489, 882, 1230, 1258, 1285, 1325, 1362, 1409
administer
new circuit packs 343, 494, 886, 1234, 1412
administering
C-LAN circuit pack
.....345, 496, 889, 1236, 1264, 1292, 1330, 1369, 1416
media processor circuit pack
.....344, 495, 888, 1236, 1263, 1292, 1368, 1415
the gateway 1327
the IPSIs ...338, 488, 882, 1230, 1257, 1285, 1324, 1362
Administering
the IPSI circuit pack
.....343, 494, 887, 1234, 1262, 1291, 1329, 1367, 1412
the IPSI circuit packs
.... 339, 489, 883, 1231, 1259, 1286, 1325, 1363, 1410, 1412
Administering PN synchronization 346, 497, 890, 1418
administering the C-LAN circuit pack
.....345, 496, 889, 1236, 1264, 1292, 1330, 1369, 1416
Administering the for server A for each
duplex survivable core 677
node name 677
Administering the gateway 1327
Administering the IPSI circuit pack
.....343, 494, 887, 1234, 1262, 1291, 1329, 1367, 1412
Administering the IPSI circuit packs
.....339, 489, 883, 1231, 1259, 1286, 1325, 1363, 1410, 1412
administering the IPSIs
.....338, 488, 882, 1230, 1257, 1285, 1324, 1362
administering the media processor circuit pack
.....344, 495, 888, 1236, 1263, 1292, 1368, 1415
Administering the node name for server A for each duplex survivable core 677
Administering the signaling group for Communication Manager and Communication Manager Messaging
.... 179, 213, 253, 285, 315, 336, 917, 958, 988, 1020, 1054, 1069, 1099, 1228, 1256, 1283, 1321, 1359
alarm activation level
.....345, 497, 889, 918, 1117, 1237, 1265, 1293, 1331, 1369
alarms
clear
....39, 63, 70, 99, 123, 159, 190, 225, 265, 296, 372, 392, 415, 443, 463, 509, 557, 590, 623, 690, 732, 791, 832, 929, 969, 999, 1033, 1080, 1143, 1194, 1303, 1340
resolve
....153, 217, 366, 540, 551, 679, 683, 784, 825, 896, 899, 962, 992, 1024, 1059, 1073, 1103, 1138, 1157, 1172, 1188, 1207, 1333, 1372
and
IP addresses
.....327, 484, 871, 1000, 1219, 1246, 1274, 1341
node names
....179, 213, 253, 285, 315, 327, 336, 484, 871, 917, 958, 988, 1000, 1020, 1054, 1069, 1099, 1219, 1228, 1246, 1256, 1274, 1283, 1321, 1341, 1359
Recording . 327, 484, 871, 1000, 1219, 1246, 1274, 1341
announcement sets
.... 47, 107, 165, 196, 231, 271, 302, 936, 974, 1005, 1039, 1086, 1308, 1346
application data
.... 47, 106, 165, 196, 231, 271, 302, 935, 974, 1004, 1039, 1085, 1307, 1345
applications
log off
..59, 92, 95, 119, 154, 185, 219, 261, 291, 322, 353, 367, 388, 410, 438, 459, 479, 503, 542, 552, 575, 585, 608, 618, 681, 685, 716, 726, 786, 828, 856, 867, 898, 901, 925, 965, 995, 1027, 1061, 1076, 1106, 1122, 1139, 1159, 1173, 1190, 1208, 1241, 1269, 1297, 1336, 1374
authentication 137, 523, 648, 945
authentication files
about 28
Avaya S8xxx Servers
accessing System Management Interface
....38, 62, 69, 98, 139, 147, 525, 546, 566, 644, 652, 654, 847
accessing the Maintenance Web Interface
.....121, 355, 507, 536, 621, 633, 1124

Avaya S8xxx Servers *(continued)*
accessing the System Management Interface
.... 53, 77, 82, 88, 92, 113, 157, 173, 187, 207, 222, 247, 263, 279, 293, 309, 331, 363, 370, 382, 390, 405, 412, 432, 441, 453, 461, 473, 491, 532, 554, 579, 588, 600, 612, 667, 673, 675, 688, 696, 707, 720, 729, 737, 755, 760, 774, 778, 782, 789, 796, 806, 810, 816, 819, 824, 830, 838, 860, 875, 881, 910, 926, 940, 952, 966, 982, 1012, 1030, 1046, 1077, 1093, 1120, 1133, 1140, 1153, 1170, 1177, 1186, 1191, 1203, 1223, 1251, 1278, 1300, 1315, 1352

B

backed up files
...165, 196, 231, 271, 302, 378, 397, 419, 448, 469, 562, 595, 696, 702, 736, 743, 796, 802, 837, 843, 934, 947, 973, 1004, 1038, 1085, 1148, 1199, 1307, 1345
backing
Communication Manager Messaging application data
..47, 106, 165, 196, 231, 271, 302, 935, 974, 1004, 1039, 1085, 1307, 1345
backing up
System Platform and solution template
43, 57, 66, 72, 90, 94, 103, 117, 153, 183, 217, 258, 289, 320, 350, 366, 387, 409, 437, 458, 478, 502, 541, 574, 583, 607, 616, 680, 683, 715, 724, 781, 784, 822, 826, 855, 865, 896, 899, 922, 962, 993, 1024, 1059, 1074, 1103, 1121, 1138, 1157, 1172, 1188, 1207, 1239, 1266, 1295, 1334, 1372
Backing up
announcements
..48, 107, 166, 197, 232, 272, 303, 936, 975, 1005, 1040, 1086, 1308, 1346
files to a flashcard 129, 510, 516, 629, 639
files to another server
.... 48, 107, 125, 162, 166, 167, 192, 197, 198, 227, 232, 233, 268, 272, 273, 298, 303, 304, 358, 374, 393, 417, 445, 465, 511, 559, 593, 625, 635, 693, 699, 734, 740, 794, 799, 835, 840, 936, 938, 971, 975, 976, 1005, 1007, 1035, 1040, 1041, 1082, 1086, 1088, 1128, 1145, 1178, 1195, 1305, 1308, 1310, 1346, 1348
files to server 46, 105
the files 931, 934, 1001, 1162, 1342
to localhost 130, 140, 516, 526, 630, 640
using Linux migration procedure
....164, 195, 230, 270, 301, 377, 396, 419, 448, 468, 561, 594, 661, 695, 702, 736, 742, 795, 801, 836, 842, 947, 973, 1004, 1038, 1085, 1147, 1198, 1306, 1345
backing up,
destinations
..41, 65, 71, 101, 125, 161, 192, 227, 267, 298, 357, 374, 393, 416, 445, 465, 510, 559, 592, 624, 635, 692, 699, 734, 740, 793, 799, 834, 840, 931, 971, 1001, 1035, 1082, 1127, 1144, 1162, 1178, 1195, 1304, 1342
the data
..41, 65, 71, 101, 125, 161, 192, 227, 267, 298, 357, 374, 393, 416, 445, 465, 510, 559, 592, 624, 635, 692, 699, 734, 740, 793, 799, 834, 840, 931, 971, 1001, 1035, 1082, 1127, 1144, 1162, 1178, 1195, 1304, 1342
Backing up Communication Manager
.41, 65, 71, 101, 125, 161, 192, 227, 267, 298, 357, 374, 393, 416, 445, 465, 510, 559, 592, 624, 635, 692, 699, 734, 740, 793, 799, 834, 840, 931, 971, 1001, 1035, 1082, 1127, 1144, 1162, 1178, 1195, 1304, 1342
Backing up Communication Manager Messaging application data
...58, 118, 184, 218, 260, 290, 321, 352, 924, 964, 994, 1026, 1060, 1075, 1105, 1240, 1268, 1296, 1335, 1373
Backing up the Communication Manager Messaging data
.....661
Backing up the files 931, 934, 1001, 1162, 1342
Backing up the files to restore
...164, 195, 230, 270, 301, 377, 396, 419, 448, 468, 561, 594, 695, 702, 736, 742, 795, 801, 836, 842, 947, 973, 1004, 1038, 1085, 1147, 1198, 1306, 1345
Backing up to localhost 130, 140, 516, 526, 630, 640
backing up using Linux migration 661
backing up using Linux migration procedure
...164, 195, 230, 270, 301, 377, 396, 419, 448, 468, 561, 594, 695, 702, 736, 742, 795, 801, 836, 842, 947, 973, 1004, 1038, 1085, 1147, 1198, 1306, 1345
backup
about 44, 104
backup data; restore 943
book organization 15, 35
busying out
busied-out equipment
56, 89, 115, 151, 256, 318, 539, 572, 605, 678, 713, 779, 820, 853, 895, 961, 991, 1023, 1058, 1072, 1102, 1333, 1371
busying out previously busied-out equipment
.... 56, 89, 115, 151, 256, 318, 539, 572, 605, 678, 713, 779, 820, 853, 895, 961, 991, 1023, 1058, 1072, 1102, 1333, 1371
busying out server 73, 83, 670, 879

C

changing synchronization 1408
check
translation corruption
..40, 55, 64, 100, 115, 151, 161, 181, 191, 215, 226, 256, 267, 287, 297, 317, 349, 365, 373, 385, 393, 408, 416, 435, 444, 456, 465, 476, 501, 538, 558, 571, 591, 605, 658, 659, 670, 677, 692, 712, 733, 793, 834, 853, 879, 894, 921, 960, 990, 1023, 1034, 1057, 1071, 1081, 1101, 1119, 1137, 1144, 1156, 1171, 1188, 1195, 1206, 1238, 1266, 1294, 1332, 1370
Checking
availability of the FTP, SFTP, or SCP server
.....926, 969, 1124, 1143, 1302
the reboot progress 133, 519, 644, 940

checking clock synchronization
.... 40, 64, 100, 160, 190, 226, 266, 297, 464, 558, 591, 691, 733, 792, 833, 1034
Checking for backed up files
...165, 196, 231, 271, 302, 378, 397, 419, 448, 469, 562, 595, 696, 702, 736, 743, 796, 802, 837, 843, 934, 947, 973, 1004, 1038, 1085, 1148, 1199, 1307, 1345
checking for IP address; CMM 945
checking for the CMM IP address 945
Checking hardware
on the server 193, 229, 300, 417, 467, 737, 743
checking media modules
...151, 215, 539, 677, 894, 960, 991, 1023, 1058, 1072, 1101, 1332, 1371
Checking the reboot progress 133, 519, 644, 940
checklist
conversion tasks 1408
documentation 156, 262, 324, 369, 440, 481, 505, 868
onsite server upgrade
.....156, 186, 221, 369, 389, 411, 440, 505, 687, 728
presite upgrade 37, 60, 292, 460, 787
checklist,
Preconversion checklist 1408
Presite upgrade
.... 97, 155, 262, 368, 439, 505, 553, 586, 620, 686, 727, 829, 1299, 1338
preupgrade 323, 480, 868, 1216, 1243, 1270
Preupgrade checklist .. 903, 997, 1029, 1108, 1160, 1176
circuit packs 342, 493, 886
administer 343, 494, 886, 1234, 1412
Clearing
the ARP cache on the laptop computer
....121, 355, 506, 536, 621, 632, 651, 654, 658, 672, 674, 881, 1124
Clearing alarms
...39, 63, 70, 99, 123, 159, 190, 225, 265, 296, 372, 392, 415, 443, 463, 509, 557, 590, 623, 690, 732, 791, 832, 929, 969, 999, 1033, 1080, 1143, 1194, 1303, 1340
Clearing the ARP cache on the laptop computer
...121, 355, 506, 536, 621, 632, 651, 654, 658, 672, 674, 881, 1124
clock synchronization; check
.... 40, 64, 100, 160, 190, 226, 266, 297, 464, 558, 591, 691, 733, 792, 833, 1034
cold standby server; pre-upgrade activation 932
command line
accessing System Domain 42, 102
Communication Manager 1391
installation on System Platform 23
installation on VMware platform 23
license file 26
migrate to Virtualized Environment 1209, 1212
security SHA-2
enhancements 28
upgrades 19
Communication Manager 5.2.1 backup
...164, 195, 230, 270, 301, 377, 396, 419, 448, 468, 561, 594, 695, 702, 736, 742, 795, 801, 836, 842, 947, 973, 1004, 1038, 1085, 1147, 1198, 1306, 1345
Communication Manager data
backup 661
Communication Manager Messaging
backup
.... 58, 118, 184, 218, 260, 290, 321, 352, 924, 964, 994, 1026, 1060, 1075, 1105, 1240, 1268, 1296, 1335, 1373
Communication Manager Messaging data
.... 58, 118, 184, 218, 259, 290, 321, 352, 923, 964, 994, 1025, 1060, 1075, 1105, 1240, 1268, 1296, 1335, 1373
backup 661
Communication Manager Messaging IP address 945
Communication Manager survivable servers 25
Communication Manager template 24
Communication Manager upgrade 261, 292, 459
Communication Manager upgrade from Software Management 20
Communication Manager upgrade from System Manager ..20
Communication Manager upgrade paths 29
Communication Manager upgrade to VMware 1209
Completing duplication cable connections on staged servers 663
Completion tasks on the staged server 650, 653, 657
configurations 1406
configuration screens
copy 122, 356, 507, 622, 633, 928, 1125
record 122, 356, 507, 622, 633, 928, 1125
configure
server data
....148, 175, 208, 249, 281, 311, 384, 406, 434, 455, 475, 953, 984, 1014, 1048, 1064, 1095, 1135, 1155, 1204, 1317, 1355
Configure
server data
....535, 548, 568, 581, 602, 614, 669, 709, 722, 757, 776, 807, 817, 849, 862, 878
configure server data 364, 1135, 1155, 1205
Configure server data
...148, 175, 208, 249, 281, 311, 384, 406, 434, 455, 475, 535, 548, 568, 581, 602, 614, 669, 709, 722, 757, 776, 807, 817, 849, 862, 878, 953, 984, 1014, 1048, 1064, 1095, 1135, 1155, 1204, 1317, 1355
Configuring
network parameters 943
configuring a branch gateway
.....912, 1015, 1049, 1115, 1168, 1184
configuring Communication Manager
..169, 204, 244, 276, 306, 663, 752, 770, 812, 948, 979, 1089
configuring Communication Manager Release
.....907, 1009, 1043, 1220, 1247, 1275, 1311, 1349
configuring Communication Manager Release 6.0 ....328, 485
Configuring network parameters 943
Configuring switch link
.... 180, 214, 255, 286, 316, 337, 918, 959, 989, 1021, 1055, 1070, 1100, 1229, 1257, 1284, 1322, 1360

configuring the System Platform
...169, 204, 244, 276, 306, 328, 485, 663, 752, 770, 812, 907, 948, 979, 1009, 1043, 1089, 1220, 1247, 1275, 1311, 1349
connect cables to new server 563, 597, 664, 844
connect cables to server
.....543, 578, 612, 704, 719, 770, 812, 860
connect cables to the server 139, 525
connecting
to the processor
.....326, 483, 870, 904, 1109, 1218, 1245, 1273
to the server
339, 489, 883, 998, 1161, 1231, 1258, 1286, 1325, 1339, 1363, 1410
Connecting
the circuit pack cables
.....340, 491, 884, 1232, 1260, 1288, 1327, 1365, 1411
the laptop 643
the server to network
.....149, 537, 570, 603, 676, 681, 852, 893, 898
to the server port 643
connecting cables to the server
...139, 525, 543, 563, 578, 597, 612, 664, 704, 719, 770, 812, 844, 860
Connecting Ethernet cables to the Ethernet port 653, 656
Connecting the cables to the Ethernet switch
.....325, 482, 869, 1217, 1244, 1272, 1324, 1361
Connecting the circuit pack cables
.....340, 491, 884, 1232, 1260, 1288, 1327, 1365, 1411
Connecting the laptop to the server port 643
Connecting the server to network
.....149, 537, 570, 603, 676, 681, 852, 893, 898
Connecting to the
Ethernet cables 653, 656
Ethernet port 653, 656
connecting to the processor
.....326, 483, 870, 904, 1109, 1218, 1245, 1273
connecting to the server
.....339, 489, 883, 1231, 1258, 1286, 1325, 1363, 1410
connection preservation during an upgrade 68
connect service computer to server
.....80, 87, 92, 142, 528, 759, 778, 782, 810, 819, 823
control network C 1404
conversion tasks checklist 1408
Converting
the disk array to RAID 5 ..... 203, 401
Converting control network 1404
Converting fiber PNs to IP-PNC 626, 694
Converting PNs to IP-PNC
overview 1406
Converting the
disk array to RAID 5 ..... 243, 428, 751, 769
Converting the disk array to RAID 5 ..... 243, 428, 751, 769
Converting the disk array to RAID 5 (if required) 203, 401
convert port network 1403
copy
the configuration screens
....158, 188, 224, 264, 295, 371, 391, 414, 442, 462, 555, 589, 689, 698, 730, 738, 790, 798, 831, 839, 967, 1031, 1078, 1141, 1192, 1301
copy configuration information
...122, 158, 188, 223, 264, 294, 355, 371, 390, 414, 442, 462, 507, 555, 588, 621, 633, 689, 697, 730, 738, 790, 798, 831, 838, 927, 967, 1031, 1078, 1125, 1141, 1192, 1301
copy files to the server 533, 668
copy information from each screen
...122, 158, 188, 223, 264, 294, 355, 371, 390, 414, 442, 462, 507, 555, 588, 621, 633, 689, 697, 730, 738, 790, 798, 831, 838, 927, 967, 1031, 1078, 1125, 1141, 1192, 1301
copying
configuration information from System Management Interface
....122, 158, 188, 223, 264, 294, 355, 371, 390, 414, 442, 462, 507, 555, 588, 621, 633, 689, 697, 730, 738, 790, 798, 831, 838, 927, 967, 1031, 1078, 1125, 1141, 1192, 1301
copying files
332, 876, 911, 1013, 1047, 1224, 1252, 1279, 1316, 1353
server 134, 520, 645, 931
copying files; server
...127, 147, 163, 194, 229, 269, 300, 376, 395, 418, 447, 467, 513, 560, 593, 627, 636, 694, 701, 735, 741, 794, 800, 835, 841, 941, 972, 1002, 1037, 1084, 1146, 1197, 1305, 1343
copying files to the server
...127, 134, 163, 194, 229, 269, 300, 332, 376, 395, 418, 447, 467, 513, 520, 560, 593, 627, 636, 645, 694, 701, 735, 741, 794, 800, 835, 841, 876, 911, 931, 941, 972, 1002, 1013, 1037, 1047, 1084, 1146, 1197, 1224, 1252, 1279, 1305, 1316, 1343, 1353
Copying files to the server 533, 668
copying the upgrade dataset 147
copy language packages
.... 177, 211, 252, 283, 313, 335, 916, 956, 986, 1018, 1052, 1067, 1097, 1227, 1255, 1282, 1319, 1357
cover
removing 235, 420, 744, 761
custom announcements
...178, 212, 252, 284, 314, 957, 987, 1019, 1053, 1068, 1098, 1320, 1358

D

date 941
decommissioning the cabinet 919
decommissioning the PPN 892
DEFINITY CSI 902
DEFINITY R 867
DEFINITY Server CSI in a CMC to port network 1215
DEFINITY SI 322, 479, 867, 902, 1107
DIMM air baffle
installing 240, 425, 748, 766
removing 237, 422, 745, 763
DIMMs
installing 238, 423, 746, 764

direct connection 651, 653, 657, 672, 674, 880
Disabling
PNC duplication 890, 1418
scheduled maintenance
41, 65, 100, 126, 160, 191, 226, 266, 297, 373, 444, 464, 512, 558, 592, 626, 691, 733, 792, 834, 930, 970, 1001, 1034, 1081, 1304, 1342
Disabling PNC duplication 890, 1418
discard the cabinet
.....353, 503, 925, 1027, 1061, 1122, 1173, 1190
discard the circuit packs
.....353, 503, 925, 1027, 1061, 1122, 1173, 1190
disconnect
the cables 200, 397
disconnecting
from the server
60, 68, 80, 87, 92, 95, 119, 185, 220, 261, 291, 322, 347, 353, 388, 410, 438, 459, 479, 498, 503, 759, 761, 777, 782, 786, 809, 811, 819, 823, 828, 891, 919, 925, 1056, 1122, 1190, 1237, 1241, 1269, 1297
the cables
....169, 234, 275, 305, 378, 420, 449, 469, 737, 744, 796, 802, 851
the devices 977, 1089, 1129, 1148, 1199
the portable computer from the server
....132, 359, 518, 562, 595, 632, 641, 663, 696, 837, 843, 1027, 1174, 1311, 1323, 1361
disconnecting modem 977, 1129, 1148
disconnecting USB CD/DVD reader 1089, 1199
documentation checklist
.....156, 262, 324, 369, 440, 481, 505, 868
Documentation checklist
.... 37, 61, 187, 222, 293, 389, 412, 460, 553, 587, 621, 687, 727, 788, 829, 903, 997, 1030, 1108, 1160, 1176, 1216, 1243, 1271, 1300, 1338
documentation required 14
duplex CM main/survivable template ...60, 504, 726, 787, 867
upgrade 685
Duplex main/survivable core template 562, 596, 843
duplicated server
licensing 27
duplication cable; remove 703
duplication cable connections on staged servers 663
duplication parameters
...535, 548, 568, 581, 602, 614, 669, 709, 722, 757, 776, 807, 817, 849, 862, 878
DVD/CD-ROM drive 1123

E

embedded main template 96, 902
embedded survivable remote template 1107
embedded survivable remote template on S8300D server
.....1191
enable
FTP service 130, 140, 516, 526, 630, 639, 660
scheduled maintenance
55, 89, 115, 151, 215, 256, 318, 539, 572, 605, 678, 713, 779, 820, 853, 894, 961, 991, 1023, 1058, 1072, 1102, 1333, 1371
Enabling
Telnet service 123, 357, 509, 623, 635, 999, 1340
Enabling Telnet service ... 123, 357, 509, 623, 635, 999, 1340
enhancements
Communication Manager 28
security SHA-2 28
error message 658
existing hardware
.....325, 482, 869, 1217, 1244, 1272, 1323, 1361
Existing hardware upgrade
.....325, 482, 869, 1217, 1244, 1272, 1323, 1361
external references 15

F

Fiber-PNC configurations
Fiber-PNC 1406
firmware upgrade
.....341, 493, 885, 1233, 1261, 1290, 1329, 1366, 1417
flashcard 129, 515, 629, 639
front benzel; remove 199, 397
front bezel; replace 203, 401
FTP, SFTP, or SCP 926, 969, 1124, 1143, 1302
FTP service
enable 130, 140, 516, 526, 630, 639, 660

H

hard disk drive
installing 241, 426, 749, 767
high-level tasks 620

I

identify
language packages
..47, 107, 166, 196, 231, 272, 302, 936, 974, 1005, 1039, 1086, 1308, 1346
Identifying
the Ethernet interface 652, 655
Identifying the Ethernet interface 652, 655
identify the language packages
.... 47, 107, 166, 196, 231, 272, 302, 936, 974, 1005, 1039, 1086, 1308, 1346
Inserting
Communication Manager disc 642
Inserting Communication Manager disc 642
install
phone message file
....152, 181, 216, 257, 288, 318, 350, 365, 436, 476, 501, 539, 550, 572, 582, 606, 615, 679, 682, 713, 723, 779, 783, 821, 825, 854, 864, 895, 899, 922, 961, 992, 1024,

install *(continued)*
1059, 1073, 1102, 1119, 1137, 1157, 1172, 1188, 1206, 1238, 1266, 1294, 1333, 1372
installing
.... 143, 169, 204, 244, 276, 306, 328, 359, 379, 401, 429, 450, 470, 485, 529, 542, 563, 575, 596, 608, 663, 704, 716, 752, 770, 802, 812, 844, 857, 872, 907, 948, 979, 1009, 1043, 1089, 1111, 1130, 1149, 1164, 1181, 1199, 1220, 1247, 1275, 1311, 1349
G650 Media Gateway in the rack 338, 489, 882, 1325
Installing
a circuit pack
.....339, 489, 883, 1231, 1258, 1286, 1325, 1363, 1409
Communication Manager 133, 519, 643, 939
language packages
178, 211, 252, 284, 314, 336, 917, 956, 987, 1019, 1053, 1067, 1097, 1228, 1255, 1283, 1320, 1357
S8300D Server 906, 1008, 1042, 1110, 1163, 1180
service pack 129, 135, 515, 521, 628, 638, 646, 942
service pack updates 128, 206, 514, 627, 637, 774
the preupgrade service pack on the server running release 2.0 933
Installing a circuit pack
.....339, 489, 883, 1231, 1258, 1286, 1325, 1363, 1409
installing Communication Manager
...143, 359, 379, 401, 429, 450, 470, 529, 542, 563, 575, 596, 608, 704, 716, 802, 844, 857, 872, 1111, 1130, 1149, 1164, 1181, 1199
Installing Communication Manager 133, 519, 643, 939
installing G650 Media Gateway in the rack
.....338, 489, 882, 1325
Installing preupgrade service pack 127, 514, 932
Installing S8300D Server in the gateway
.....906, 1008, 1042, 1110, 1163, 1180
Installing service pack 129, 135, 515, 521, 628, 638, 646, 942
Installing service pack updates ..128, 206, 514, 627, 637, 774
installing the preupgrade service pack
...139, 164, 194, 229, 270, 300, 376, 395, 418, 447, 468, 526, 560, 594, 660, 695, 701, 735, 742, 795, 800, 836, 842, 932, 946, 972, 1003, 1037, 1084, 1146, 1197, 1306, 1344
Installing the preupgrade service pack on the server running release 2.0 933
installing the server in the rack 562, 595, 703, 843, 872
Installing the service pack 127, 514, 932
installing the System Platform
...143, 359, 379, 401, 429, 450, 470, 529, 542, 563, 575, 596, 608, 704, 716, 802, 844, 857, 872, 1111, 1130, 1149, 1164, 1181, 1199
Install phone message file
...152, 181, 216, 257, 288, 318, 350, 365, 436, 476, 501, 539, 550, 572, 582, 606, 615, 679, 682, 713, 723, 779, 783, 821, 825, 854, 864, 895, 899, 922, 961, 992, 1024, 1059, 1073, 1102, 1119, 1137, 1157, 1172, 1188, 1206, 1238, 1266, 1294, 1333, 1372
install server in rack 202, 400
install the new server 562, 595, 703, 843, 872
install the new server in the rack 562, 595, 703, 843, 872
integrity check
.... 54, 114, 150, 214, 255, 317, 364, 407, 435, 475, 959, 990, 1022, 1056, 1071, 1100, 1136, 1156, 1171, 1187, 1205, 1331, 1370
interchange servers
.....79, 551, 584, 617, 684, 725, 785, 827, 866, 900
Introduction 1403
IP forwarding
disabling
.... 38, 62, 70, 80, 97, 144, 170, 205, 245, 276, 306, 328, 360, 379, 402, 429, 450, 470, 485, 529, 543, 563, 576, 597, 609, 664, 704, 717, 753, 771, 803, 813, 844, 857, 872, 907, 949, 979, 1009, 1043, 1090, 1112, 1130, 1150, 1165, 1181, 1200, 1220, 1248, 1275, 1312, 1350
enabling
.... 38, 62, 70, 80, 97, 144, 170, 205, 245, 276, 306, 328, 360, 379, 402, 429, 450, 470, 485, 529, 543, 563, 576, 597, 609, 664, 704, 717, 753, 771, 803, 813, 844, 857, 872, 907, 949, 979, 1009, 1043, 1090, 1112, 1130, 1150, 1165, 1181, 1200, 1220, 1248, 1275, 1312, 1350
IPSI information; add
.....342, 494, 886, 1234, 1262, 1290, 1329, 1366

L

label
...200, 234, 275, 305, 397, 420, 449, 469, 737, 744, 796, 802, 851
language packages
.... 47, 107, 165, 166, 178, 196, 211, 231, 252, 271, 272, 284, 302, 314, 336, 917, 936, 956, 974, 987, 1005, 1019, 1039, 1053, 1067, 1086, 1097, 1228, 1255, 1283, 1308, 1320, 1346, 1357
language packages; copy
.... 177, 211, 252, 283, 313, 335, 916, 956, 986, 1018, 1052, 1067, 1097, 1227, 1255, 1282, 1319, 1357
latest changes in the document 14
legal notice .....
license 137, 523, 648, 945
license error message 658
licensing
Communication Manager 26
duplicated server 27
Linux Migration to CM 6.0
...164, 195, 230, 270, 301, 377, 396, 419, 448, 468, 561, 594, 695, 702, 736, 742, 795, 801, 836, 842, 947, 973, 1004, 1038, 1085, 1147, 1198, 1306, 1345
localhost 129, 515, 629, 639
backup 130, 140, 516, 526, 630, 640
Log off
applications
..59, 92, 95, 119, 154, 185, 219, 261, 291, 322, 353, 367, 388, 410, 438, 459, 479, 503, 542, 552, 575, 585, 608, 618, 681, 685, 716, 726, 786, 828, 856, 867, 898, 901, 925, 965, 995, 1027, 1061, 1076, 1106, 1122, 1139, 1159, 1173, 1190, 1208, 1241, 1269, 1297, 1336, 1374

M

Manage Software 20
media modules; check
...151, 215, 539, 677, 894, 960, 991, 1023, 1058, 1072, 1101, 1332, 1371
memory module air baffle
installing 240, 425, 748, 766
removing 237, 422, 745, 763
memory modules
installing 238, 423, 746, 764
migrating
Communication Manager to Virtualized Environment
....1212
Communication Manager to VMware 1209

N

network configuration
...148, 175, 208, 249, 281, 311, 384, 406, 434, 455, 475, 535, 548, 568, 581, 602, 614, 669, 709, 722, 757, 776, 807, 817, 849, 862, 878, 953, 984, 1014, 1048, 1064, 1095, 1135, 1155, 1204, 1317, 1355
new server
.132, 143, 169, 275, 327, 378, 450, 484, 519, 542, 939, 1220, 1247, 1275, 1311, 1349
node names
...179, 213, 253, 285, 315, 327, 336, 484, 871, 917, 958, 988, 1000, 1020, 1054, 1069, 1099, 1219, 1228, 1246, 1256, 1274, 1283, 1321, 1341, 1359
non-VMware to VMware upgrades 1209

O

overview
System Platform 21
Overview 1406

P

patches
downloading
..51, 74, 84, 110, 145, 171, 176, 209, 246, 250, 278, 282, 307, 312, 330, 334, 361, 380, 403, 431, 452, 471, 486, 531, 544, 565, 577, 598, 610, 665, 706, 718, 754, 772, 804, 814, 846, 859, 874, 908, 915, 950, 954, 981, 985, 1011, 1017, 1045, 1051, 1062, 1065, 1091, 1095, 1113, 1132, 1151, 1166, 1182, 1201, 1222, 1226, 1249, 1253, 1277, 1281, 1313, 1318, 1351, 1355
installing
..51, 75, 85, 111, 146, 172, 176, 210, 247, 251, 278, 282, 308, 312, 330, 335, 362, 381, 404, 431, 452, 472, 487, 531, 545, 565, 578, 599, 611, 666, 707, 719, 755, 773, 805, 815, 846, 859, 875, 909, 915, 951, 955, 981, 985, 1011, 1017, 1045, 1051, 1063, 1066, 1092, 1096, 1114, 1133, 1152, 1167, 1183, 1202, 1222, 1227, 1250, 1254, 1277, 1282, 1314, 1318, 1352, 1356
performing
integrity check
.... 54, 114, 150, 214, 255, 317, 364, 407, 435, 475, 959, 990, 1022, 1056, 1071, 1100, 1136, 1156, 1171, 1187, 1205, 1331, 1370
Performing
an integrity check
..78, 79, 87, 537, 549, 551, 571, 582, 584, 604, 615, 618, 682, 712, 723, 725, 758, 761, 777, 786, 808, 811, 819, 827, 852, 863, 866, 898
Performing an integrity
.... 78, 87, 549, 582, 615, 682, 723, 758, 761, 777, 808, 811, 819, 863, 898
Performing an integrity check
.... 79, 537, 551, 571, 584, 604, 618, 712, 725, 786, 827, 852, 866
Platform Upgrade 50, 73, 83, 109
PN synchronization 346, 497, 890, 1418
port network circuit packs
....342, 493, 886, 1233, 1261, 1290, 1366
prepare
the server for the upgrade 642
Preparing for
port network conversion 1403
Preparing for port network conversion 1403
preparing the server 642
preupgrade
checklist 37, 60, 292, 460, 787
Preupgrade
service packs 127, 513, 627, 637
setup 324, 481, 869, 904, 1109, 1217, 1244, 1271
preupgrade checklist 323, 480, 868, 1216, 1243, 1270
preupgrade requirements 31
preupgrade service pack
...139, 164, 194, 229, 270, 300, 376, 395, 418, 447, 468, 526, 560, 594, 660, 695, 701, 735, 742, 795, 800, 836, 842, 932, 946, 972, 1003, 1037, 1084, 1146, 1197, 1306, 1344
Preupgrade service packs 127, 513, 627, 637
Preupgrade setup
....324, 481, 869, 904, 1109, 1217, 1244, 1271

R

rack
removing server 275, 449, 851
Rebooting the server
...138, 149, 180, 214, 255, 286, 316, 364, 384, 407, 434, 455, 475, 524, 535, 548, 569, 581, 602, 614, 650, 669, 709, 722, 758, 776, 808, 818, 850, 863, 878, 946, 959, 989, 1021, 1055, 1070, 1100, 1136, 1155, 1169, 1185, 1205, 1322, 1360
Reconfigure the Communication Manager server
....51, 74, 84, 110
Recording 327, 484, 871, 1000, 1219, 1246, 1274, 1341
configuration information 935, 1002, 1127, 1343

Recording *(continued)*
configuration screens to copy or print 122, 356, 507, 622, 633, 928, 1125
IP settings 1246, 1274
the scheduled backup 357, 1127
Recording all busyouts .40, 64, 99, 124, 160, 190, 226, 266, 297, 327, 464, 484, 509, 558, 591, 624, 691, 732, 792, 833, 871, 905, 930, 970, 1000, 1033, 1081, 1110, 1219, 1246, 1273, 1303, 1341
Recording configuration information 935, 1002, 1127, 1343
Recording IP settings 1246, 1274
Recording node names and IP addresses 327, 484, 871, 1000, 1219, 1246, 1274, 1341
Registering 60, 96, 119, 154, 185, 220, 291, 353, 367, 503, 552, 585, 618, 685, 726, 786, 828, 867, 901, 925, 965, 995, 1027, 1062, 1076, 1106, 1122, 1139, 1159, 1174, 1190, 1208, 1241, 1269, 1297, 1336, 1375
the system 60, 96, 119, 154, 185, 220, 291, 353, 367, 503, 552, 585, 618, 685, 726, 786, 828, 867, 901, 925, 965, 995, 1027, 1062, 1076, 1106, 1122, 1139, 1159, 1174, 1190, 1208, 1241, 1269, 1297, 1336, 1375
release 4.0.5 ....133, 519
release 5.2.1 ....133, 519
Release 5.2.1 ....643, 939
releasing server 78, 87, 537, 549, 570, 581, 603, 614, 647, 653, 656, 671, 682, 711, 722, 761, 777, 811, 818, 851, 863, 879, 898
releasing the server 78, 87, 537, 549, 570, 581, 603, 614, 647, 653, 656, 671, 682, 711, 722, 761, 777, 811, 818, 851, 863, 879, 898
remove
the cabinet and the circuit packs 353, 503, 925, 1027, 1061, 1122, 1173, 1190
remove server from rack 569, 603, 703, 711
Remove the cabinet and the circuit packs 353, 503, 925, 1027, 1061, 1122, 1173, 1190
remove the front benzel 199, 397
remove the server from the rack 200, 398
Removing
fiber-related administration 346, 497, 890, 919, 1117, 1417
fiber-related hardware 347, 498, 891, 919, 1117, 1418
S8500–Series Server from the rack 169, 378, 1056, 1190
removing duplication cable 703
Removing fiber-related administration 346, 497, 890, 919, 1117, 1417
Removing fiber-related hardware 347, 498, 891, 919, 1117, 1418
Removing port network circuit packs 342, 493, 886, 1233, 1261, 1290, 1366
removing processor port network control cabinet 347, 499, 892, 919, 1117
removing S8510 server cover 201, 398
removing the SAMP 201, 399
removing the server 569, 603, 703, 711
replace
the S8510 Server cover 202, 399
replace the cover 202, 399
replacing
I/O cables 1288
Replacing
a server 977, 1129, 1148
Replacing a server 977, 1148
Replacing circuit packs 325, 482, 870, 1218, 1245, 1272
replacing I/O cables 1288
Replacing S8300A Server 1129
replacing the cover on S8510 server 202, 399
replacing the front bezel 203, 401
required sequence 966
Resetting the system 659
resolve alarms ...153, 217, 366, 540, 551, 679, 683, 784, 825, 896, 899, 962, 992, 1024, 1059, 1073, 1103, 1138, 1157, 1172, 1188, 1207, 1333, 1372
Resolving
alarms ..56, 89, 93, 115, 182, 258, 288, 319, 350, 386, 409, 437, 457, 477, 501, 573, 607, 714, 780, 822, 855, 922, 1121, 1239, 1266, 1294
Restoring
Communication Manager Messaging data 178, 212, 253, 285, 315, 957, 988, 1020, 1054, 1068, 1098, 1320, 1358
custom announcements 178, 212, 252, 284, 314, 957, 987, 1019, 1053, 1068, 1098, 1320, 1358
server data 137, 523, 649
the translations 332, 877, 911, 1224, 1252, 1279
upgrade dataset 147, 174, 208, 248, 280, 310, 383, 406, 433, 454, 474, 534, 547, 567, 580, 601, 613, 668, 708, 721, 756, 775, 807, 817, 848, 861, 953, 983, 1013, 1047, 1063, 1094, 1134, 1154, 1204, 1316, 1354
restoring backup data 943
Resubmitting
scheduled backups 152, 182, 216, 257, 288, 319, 386, 408, 436, 457, 477, 540, 550, 573, 583, 606, 616, 679, 683, 714, 724, 780, 784, 821, 825, 854, 864, 896, 962, 992, 1073, 1103

S

S8100 Server in a CMC to port network 1242
S8100 Server in G600 to port network 1269
S8300D server upgrade to embedded main template 1077
S8510 server cover removal 201, 398
S8510 Server on simplex CM main/survivable template ... 186
S8700 Server upgrade procedure 619
S8700 Server upgrade tasks 620
S8800 server firmware 243, 428, 751, 769

safety 236, 421
ESD 236, 421
SAMP; remove 201, 399
SAT session
... 40, 55, 64, 99, 114, 124, 150, 160, 180, 190, 215, 225, 256, 266, 287, 296, 317, 338, 365, 373, 384, 392, 408, 415, 435, 444, 456, 463, 476, 488, 509, 538, 557, 571, 591, 604, 624, 658, 670, 677, 691, 712, 732, 792, 833, 853, 878, 894, 918, 929, 960, 969, 990, 1000, 1022, 1033, 1057, 1071, 1080, 1101, 1116, 1137, 1143, 1156, 1171, 1187, 1194, 1206, 1230, 1257, 1285, 1303, 1324, 1332, 1341, 1362, 1370
saving
translations
..... 124, 126, 161, 191, 227, 510, 512, 626, 1035
saving translations
... 41, 56, 65, 89, 101, 115, 151, 181, 216, 257, 267, 287, 298, 318, 325, 350, 374, 385, 393, 416, 445, 456, 465, 482, 539, 558, 572, 592, 605, 624, 659, 678, 692, 713, 733, 779, 793, 821, 834, 854, 869, 895, 904, 921, 930, 961, 970, 991, 1000, 1024, 1058, 1072, 1082, 1102, 1109, 1144, 1195, 1217, 1244, 1272, 1304, 1333, 1341, 1371
schedule daily maintenance
..... 89, 256, 318, 572, 605, 713, 779, 820, 853
second server 656
server
reboot 650, 946
removing from the rack 275, 449, 851
server; busy out 73, 83, 670, 879
server; release
.... 78, 87, 537, 549, 570, 581, 603, 614, 647, 653, 656, 671, 682, 711, 722, 761, 777, 811, 818, 851, 863, 879, 898
server; remove 569, 603, 703, 711
server; remove from rack 200, 398
server cover
removing 235, 420, 744, 761
server data
configure 364, 1135, 1155, 1205
server duplication cable 656
server role
... 148, 175, 208, 249, 281, 311, 384, 406, 434, 455, 475, 535, 548, 568, 581, 602, 614, 669, 709, 722, 757, 776, 807, 817, 849, 862, 878, 953, 984, 1014, 1048, 1064, 1095, 1135, 1155, 1204, 1317, 1355
servers
accessing System Management Interface
.... 38, 53, 62, 69, 77, 82, 88, 92, 98, 113, 139, 147, 173, 207, 247, 279, 309, 331, 363, 382, 405, 432, 453, 473, 491, 525, 532, 546, 566, 579, 600, 612, 644, 652, 654, 667, 707, 720, 755, 760, 774, 778, 782, 806, 810, 816, 819, 824, 847, 860, 875, 910, 952, 982, 998, 1012, 1046, 1093, 1120, 1133, 1153, 1161, 1170, 1186, 1203, 1223, 1251, 1278, 1315, 1339, 1352
accessing the System Management Interface
.... 121, 157, 187, 222, 263, 293, 355, 370, 390, 412, 441, 461, 507, 536, 554, 588, 621, 633, 673, 675, 688, 696, 729, 737, 789, 796, 830, 838, 881, 926, 940, 966, 1030, 1077, 1124, 1140, 1177, 1191, 1300
interchange
..... 79, 551, 584, 617, 684, 725, 785, 827, 866, 900
service
outage 569, 602, 710, 759, 809, 850
service outage 569, 602, 710, 759, 809, 850
services port
accessing System Platform through
.... 38, 62, 70, 80, 97, 144, 170, 205, 245, 276, 306, 328, 360, 379, 402, 429, 450, 470, 485, 529, 543, 563, 576, 597, 609, 664, 704, 717, 753, 771, 803, 813, 844, 857, 872, 907, 949, 979, 1009, 1043, 1090, 1112, 1130, 1150, 1165, 1181, 1200, 1220, 1248, 1275, 1312, 1350
SES 30
set
date and time 134, 520, 647
the time, date, and time zone 134, 520, 647
Set Identities 943
Set the time, date, and time zone 134, 520, 647
setting
VLAN parameters and diffserv parameters
..... 343, 495, 887, 1235, 1262, 1291, 1329, 1367, 1414
setting alarm activation level
..... 345, 497, 889, 918, 1117, 1237, 1265, 1293, 1331, 1369
setting the VLAN parameters and diffserv parameters
..... 343, 495, 887, 1235, 1262, 1291, 1329, 1367, 1414
setting up test data
.... 49, 108, 167, 198, 233, 273, 304, 937, 976, 1006, 1040, 1087, 1309, 1347
set up
test data
.. 49, 108, 167, 198, 233, 273, 304, 937, 976, 1006, 1040, 1087, 1309, 1347
shut down
Communication Manager Messaging
.. 49, 109, 167, 198, 233, 273, 304, 937, 976, 1007, 1041, 1088, 1309, 1348
Shutting down
Communication Manager Messaging
.. 49, 109, 167, 198, 233, 273, 304, 937, 976, 1007, 1041, 1088, 1309, 1348
the server 948, 1128
Shutting down Communication Manager Messaging
.... 49, 109, 167, 198, 233, 273, 304, 937, 976, 1007, 1041, 1088, 1309, 1348
Shutting down the server
... 142, 149, 168, 199, 234, 274, 305, 359, 376, 397, 419, 449, 469, 528, 536, 569, 602, 662, 673, 676, 703, 710, 743, 759, 802, 809, 850, 977, 1027, 1056, 1089, 1148, 1174, 1190, 1199, 1310, 1323, 1361
signaling-groups
.... 179, 213, 253, 285, 315, 336, 917, 958, 988, 1020, 1054, 1069, 1099, 1228, 1256, 1283, 1321, 1359
simplex CM main/survivable template 220
simplex CM main/survivable template upgrade 186
simplex main/survivable core template 120, 322
simplex main/survivable template 36, 154
simplex S8510 Server 388

simplex survivable remote template 354, 388, 479
upgrade 411
simplex to duplex upgrade 1391
simplex to duplex upgrade template 1391
SIP Enablement Services 30
SNMP Agents 364, 1135, 1155, 1205
SNMP Traps 364, 1135, 1155, 1205
Software Inventory 20
Software Management 20
software release
...134, 223, 294, 413, 461, 556, 590, 645, 688, 697, 730, 738, 789, 797, 832, 840, 927, 941, 967, 1080, 1125, 1141, 1193, 1300
Special
circumstances 30
Special circumstances 30
stage server 642
start a
SAT session on active server
..... 124, 509, 624, 929, 1000, 1341
starting
SAT session
....40, 55, 64, 99, 114, 150, 180, 215, 256, 287, 317, 338, 365, 384, 408, 435, 456, 476, 488, 538, 571, 604, 677, 712, 853, 894, 918, 960, 990, 1022, 1057, 1071, 1101, 1116, 1137, 1156, 1171, 1187, 1206, 1230, 1257, 1285, 1324, 1332, 1362, 1370
SAT session on active server
....160, 190, 225, 266, 296, 373, 392, 415, 444, 463, 557, 591, 658, 670, 691, 732, 792, 833, 878, 969, 1033, 1080, 1143, 1194, 1303
Starting Communication Manager Messaging
.... 175, 209, 250, 281, 311, 333, 914, 954, 984, 1016, 1050, 1065, 1095, 1225, 1253, 1280, 1317, 1355
static IP address
..... 326, 483, 870, 1218, 1245, 1273, 1324, 1361
Status Summary
.... 54, 114, 150, 214, 255, 317, 364, 407, 435, 475, 959, 990, 1022, 1056, 1071, 1100, 1136, 1156, 1171, 1187, 1205, 1331, 1370
Submitting
scheduled backups 365, 1137, 1157, 1207
super-user login 136, 522, 647, 944
support 18
supported Communication Manager upgrade paths 29
Supported USB DVD/CD-ROM drives 1123
survivable core servers
resetting 554, 587, 687, 729, 788, 830
survivable servers 25
switch link
.... 180, 214, 255, 286, 316, 337, 918, 959, 989, 1021, 1055, 1070, 1100, 1229, 1257, 1284, 1322, 1360
System Domain
accessing command line 42, 102
System Platform
overview 21
upgrade 50, 73, 83, 109
System Platform Web Console
accessing
..42, 56, 65, 71, 81, 90, 93, 101, 116, 144, 171, 205, 245, 277, 307, 329, 360, 380, 402, 430, 451, 471, 486, 530, 544, 564, 576, 597, 609, 664, 705, 717, 753, 771, 803, 813, 845, 858, 873, 908, 949, 980, 1010, 1044, 1090, 1112, 1131, 1151, 1165, 1181, 1200, 1221, 1248, 1276, 1312, 1350

T

tasks on active server 809
tasks on existing server 850
tasks on S8510 602
tasks on S8700 ..... 569, 710, 759
Testing
the system using SAT commands
.... 55, 114, 151, 181, 215, 256, 287, 318, 349, 365, 385, 436, 456, 476, 500, 538, 572, 605, 670, 677, 713, 853, 879, 894, 920, 960, 991, 1023, 1057, 1072, 1101, 1118, 1137, 1157, 1172, 1188, 1206, 1237, 1265, 1293, 1332, 1371
The converted configuration 1407
The starting configuration 1407
third-party certificates 29
time 941
time zone 941
to check media modules
...151, 215, 539, 677, 894, 960, 991, 1023, 1058, 1072, 1101, 1332, 1371
training 17
Transferring
files using FTP 131, 141, 517, 527, 631, 641, 661
to the services laptop computer 131, 517, 631, 641
to the services portable computer 141, 527, 661
Transferring files to the services laptop computer
..... 131, 517, 631, 641
Transferring files to the services portable computer
..... 141, 527, 661
Transferring files using FTP
..... 131, 141, 517, 527, 631, 641, 661
translations; save
...41, 56, 65, 89, 101, 115, 151, 181, 216, 257, 267, 287, 298, 318, 325, 350, 374, 385, 393, 416, 445, 456, 465, 482, 539, 558, 572, 592, 605, 624, 659, 678, 692, 713, 733, 779, 793, 821, 834, 854, 869, 895, 904, 921, 930, 961, 970, 991, 1000, 1024, 1058, 1072, 1082, 1102, 1109, 1144, 1195, 1217, 1244, 1272, 1304, 1333, 1341, 1371
turning off
the power to the control cabinet
..... 1027, 1174, 1260, 1287, 1323, 1364
Turning off the power to the control cabinet
..... 1027, 1174, 1260, 1287, 1323, 1364
Turning on
the server 642
turning on the server 143, 529
Turning on the server 642

U

uEFI settings 244, 429, 752, 770
Updating
S8800 server firmware 243, 428, 751, 769
uEFI settings of S8800 ..... 244, 429, 752, 770
upgrade
Communication Manager 50, 73, 83, 109
Communication Manager to VMware 1209
non-VMware to VMware 1209
paths 966
S8300 Server 1298
S8400 Server 995, 1159, 1336
S8500 Server 1028, 1175
S8700 Server 619, 620
sequence 966
System Platform 50, 73, 83, 109
upgrade Communication Manager 19
Upgrade Communication Manager 52, 76, 85, 112
upgrade order 32
upgrade paths 29, 966
upgrade prerequisites for Communication Manager 1376, 1381
upgrade process 32
upgrade S8300 Server in port network 1298
upgrade S8400 Server in port network 1336
upgrade S8400 Server to S8300D Server 995, 1159
upgrade S8500 Server to S8300D Server 1028, 1175
upgrade sequence 966
upgrade worksheet 1381
upgrading
firmware on the new circuit packs 1417
System Platform 50, 73, 83, 109
Upgrading
Communication Manager template 52, 76, 85, 112
S8510 Server to the simplex survivable remote template 388
upgrading an S8300A server to
embedded survivable remote template 1123
upgrading an S8300A Server to
embedded main template 925
upgrading an S8300A Server to embedded main embedded template 925
upgrading an S8300A server to embedded survivable remote template 1123
upgrading an S8300 Server to
embedded main template 965
embedded survivable remote template 1139
upgrading an S8300 Server to embedded main template . 965
upgrading an S8300 Server to embedded survivable remote template 1139
Upgrading branch gateways and survivable servers 37, 61, 157, 187, 222, 263, 293, 370, 389, 441, 460, 506, 554, 587, 687, 728, 788, 829, 1030, 1177
Upgrading DEFINITY R 867
Upgrading DEFINITY SI 322, 479, 902, 1107
upgrading firmware 341, 493, 885, 1233, 1261, 1290, 1329, 1366, 1417
Upgrading firmware on the new circuit packs 1417
upgrading S8300D server to embedded main template .. 1077
upgrading S8300D server to embedded survivable remote template 1191
Upgrading S8510 Server to the simplex CM main/survivable template 186
upgrading to
duplex CM main/survivable template 552
duplex main/survivable core template 585, 828
duplex main/survivable template 618
simplex survivable remote template 368, 439
upgrading to CM duplex main/survivable template 726, 787
upgrading to duplex CM main/survivable template 60, 552
upgrading to duplex main/survivable template 504, 585, 618, 685
upgrading to duplex template 828
upgrading to embedded main template 96
upgrading to simplex CM main/survivable template .. 154, 220
upgrading to simplex main/survivable template 36, 120
upgrading to simplex survivable remote template 354, 368, 411, 439
USB CD/DVD reader 977, 1089, 1129, 1148, 1199
USB flashcard drive 977, 1129, 1148
using the book 35

V

verify 520
destination for scheduled backups 152, 182, 216, 257, 288, 319, 385, 408, 436, 457, 477, 540, 550, 573, 582, 606, 615, 679, 682, 713, 723, 779, 783, 821, 825, 854, 864, 895, 961, 992, 1102
IPSI connectivity 78, 86, 150, 341, 492, 537, 570, 581, 604, 615, 676, 681, 711, 722, 758, 777, 808, 818, 852, 863, 885, 893, 898, 1232, 1260, 1289, 1328, 1365, 1415
system status 653, 655
verifying
Communication Manager Messaging test data 58, 118, 184, 218, 259, 290, 321, 352, 923, 964, 994, 1025, 1060, 1075, 1105, 1240, 1268, 1296, 1335, 1373
connection for server duplication 549, 656, 671, 879
current software release 134, 223, 294, 413, 461, 556, 590, 645, 688, 697, 730, 738, 789, 797, 832, 840, 927, 941, 967, 1080, 1125, 1141, 1193, 1300
system status 326, 349, 483, 500, 871, 905, 921, 998, 1109, 1119, 1162, 1218, 1238, 1245, 1265, 1273, 1293, 1339
Verifying
firmware version 341, 493, 885, 1233, 1261, 1289, 1328, 1365
IPSI translations 1414
the installation of the circuit pack 340, 490, 884, 1232, 1260, 1287, 1326, 1364, 1411

Verifying *(continued)*
the process status 647
the software version
..49, 73, 81, 109, 145, 171, 206, 247, 277, 309, 329, 361, 380, 403, 431, 452, 471, 486, 531, 544, 564, 577, 598, 610, 665, 706, 718, 754, 774, 804, 814, 846, 858, 874, 908, 950, 980, 1010, 1045, 1091, 1113, 1132, 1151, 1166, 1182, 1201, 1222, 1249, 1277, 1313, 1351
verifying connectivity 710
verifying current software release
...134, 223, 294, 413, 461, 556, 590, 645, 688, 697, 730, 738, 789, 797, 832, 840, 927, 941, 967, 1080, 1125, 1141, 1193, 1300
Verifying firmware version
.....341, 493, 885, 1233, 1261, 1289, 1328, 1365
Verifying IPSI translations 1414
Verifying the connection for server duplication
.....549, 656, 671, 879
Verifying the installation of the circuit pack
.....340, 490, 884, 1232, 1260, 1287, 1326, 1364, 1411
Verifying the process status 647
Verifying the software version
.49, 73, 81, 109, 145, 171, 206, 247, 277, 309, 329, 361, 380, 403, 431, 452, 471, 486, 531, 544, 564, 577, 598, 610, 665, 706, 718, 754, 774, 804, 814, 846, 858, 874, 908, 950, 980, 1010, 1045, 1091, 1113, 1132, 1151, 1166, 1182, 1201, 1222, 1249, 1277, 1313, 1351
verify IPSI connectivity
.... 78, 86, 150, 341, 492, 537, 570, 581, 604, 615, 676, 681, 711, 722, 758, 777, 808, 818, 852, 863, 885, 893, 898, 1232, 1260, 1289, 1328, 1365, 1415
videos 18
view
the configuration screens
....158, 188, 224, 264, 295, 371, 391, 414, 442, 462, 555, 589, 689, 698, 730, 738, 790, 798, 831, 839, 967, 1031, 1078, 1141, 1192, 1301
Viewing
configuration screens to copy or print
.....122, 356, 507, 622, 633, 928, 1125

W

Warranty 19
Web Console
accessing
..42, 56, 65, 71, 81, 90, 93, 101, 116, 144, 171, 205, 245, 277, 307, 329, 360, 380, 402, 430, 451, 471, 486, 530, 544, 564, 576, 597, 609, 664, 705, 717, 753, 771, 803, 813, 845, 858, 873, 908, 949, 980, 1010, 1044, 1090, 1112, 1131, 1151, 1165, 1181, 1200, 1221, 1248, 1276, 1312, 1350
worksheet for simplex to duplex template upgrade 1391