Installing Service Packs for Avaya Aura® Session Manager

Release 6.3
Issue 5
August 2014

© 2014 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.

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 Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, 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.

Concurrent User License

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.

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.

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 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

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.

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.

Trademarks

Avaya® and Avaya Aura® are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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.

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.

Contents

Chapter 1: Introduction 5
Purpose 5
Intended audience 6
Document changes since last issue 6
Related resources 6
Documentation 6
Training 8
Viewing Avaya Mentor videos 8
Support 9
Warranty 9
Deployment options 9
Chapter 2: Installing a service pack 11
Service Pack installation checklist 11
Viewing the software release version 13
Checking the RAID Battery status 13
Downloading software from PLDS 14
Verifying Enrollment Password status 15
Denying new service 15
Verifying the Active Call Count 16
Viewing the Session Manager Entity Link Connection Status 16
Upgrading Session Manager software 16
Configuring Session Manager in a System Manager in a geographically redundant environment 19
Testing the Session Manager instance 19
Verifying Data Replication 19
Viewing Security Module status 20
Generating a test alarm 21
Accepting new service 22
Verifying the upgraded Session Managers 22
Appendix A: OS-level logins for Session Manager 23
Appendix B: Product notifications 25
Viewing PCNs and PSNs 25
Registering for product notifications 26

Chapter 1: Introduction

Purpose

This guide describes the procedures to install service packs for Avaya Aura® Session Manager. A service pack is a software package you install on top of the current software load.

This guide does not describe the procedures for installing service packs for Session Manager in a virtualized environment. To install service packs for Session Manager using VMware, see *Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment* .

You do not need to install Session Manager service packs sequentially. Each service pack contains all the changes made in the earlier service packs, so you can install any service pack on a base load without installing prior service packs. You must install the required System Manager service packs before you install any service pack of Session Manager. System Manager must have the latest VSP template installed before upgrading to the latest service pack.

You can install service packs for the following scenarios:

- If the server is running Session Manager 6.0, Session Manager 6.1 or Session Manager 6.2. In this case, you also have to upgrade the OS. For more information, see *Upgrading Avaya Aura® Session Manager*.
- If you are running Session Manager Release 6.3. In this case, follow the procedure as outlined in this document.

Note:

See the PCN issued for the specific Session Manager software release. See *Appendix : PCN and PSN notifications* for more information about PCNs and PSNs.

Schedule the service pack installation during hours of little or no system activity. You can upgrade the Session Manager server without affecting a service but redirecting the service around each Session Manager that is getting upgraded takes time. The length of time increases with increases in system activity.

Warning:

As of Session Manager Release 6.2, Access Security Gateway secures the following logins and prevents unauthorized access to the Session Manager servers by the non-Avaya services personnel.

- **sroot**
- **inads**

- `rasaccess`
- `init`
- `craft`

Using the customer login account, you can execute most of the maintenance and troubleshooting commands. You do not need root access for standard maintenance and support purposes. For details, see PSN (PSN003925U).

Intended audience

This document is intended for people who perform Avaya Aura® Session Manager upgrades.

Document changes since last issue

The following changes were made since the last issue of this document:

- Removed specific release versions and generalized steps regarding specific releases.

.

Related resources

Documentation

See the following related documents at http://support.avaya.com.

For the latest information, see the Session Manager Release Notes.

Title	Description	Audience
Overview		
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management
Implementation		

Title	Description	Audience
Deploying Avaya Aura® Session Manager	Describes how to install and configure a Session Manager instance.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager.	Services and support personnel
Deploying Avaya Aura® Communication Manager on System Platform	Describes how to install the appropriate Communication Manager template, including Branch Session Manager, on the server.	Services and support personnel
Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment	Describes how to deploy the Session Manager virtual application in a VMware environment.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade a Session Manager to the latest software release.	Services and support personnel
Installing Service Packs for Avaya Aura® Session Manager	Describes the procedures to install service packs on Session Manager.	Services and support personnel
Installing Patches for Avaya Aura® Session Manager	Describes the procedures to install patches on Session Manager.	Services and support personnel
Installing the Avaya S8800 Server for Avaya Aura® Communication Manager	Describes the installation procedures for the S8800 Server.	Services and support personnel
Installing the Avaya S8510 Server Family and Its Components	Describes the installation procedures for the S8510 Server.	Services and support personnel
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620sServer.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Maintaining		
Maintaining and Troubleshooting Avaya Aura® Session Manager	Describes the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel
Administration		
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides case studies about common administration scenarios.	System administrators

Training

The following courses are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go** .

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Session Manager and System Manager Implementation
5U00050E	Knowledge Access: Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00103W	Session Manager 6.2 Delta Overview
5U00104W	Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
ATC01840OEN	Survivable Remote Session Manager Administration
3U00100O	Designing Avaya Aura 6.2 Part 1
3U00101O	Designing Avaya Aura 6.2 Part 2

Viewing Avaya Mentor videos

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

About this task

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 Session Manager. See the sales agreement or other applicable documentation for more information about the terms of the limited warranty. In addition, see the standard warranty and details about Session Manager support during the warranty period on the Avaya Support website at https://support.avaya.com under **Help & Policies> Policies & Legal > Maintenance and Warranty Information**. See also **Help & Policies > Policies & Legal > License Terms**.

Deployment options

You can deploy Avaya Aura® Session Manager using the following methods.

Deployment Model	Documentation Reference
Session Manager on a standalone server.	*Deploying Avaya Aura® Session Manager*
Session Manager in a VMware virtualized environment.	*Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment*
Session Manager as a component of Midsize Enterprise.	*Implementing Avaya Aura® Solution for Midsize Enterprise*

Deployment Model	Documentation Reference
Branch Session Manager as a component of a Communication Manager template.	*Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394

Chapter 2: Installing a service pack

Service Pack installation checklist

Use the following checklist to install a service pack on a Session Manager or Branch Session Manager.

If you are installing a service pack on a Branch Session Manager, you can *only* install the service pack using the Network transfer procedure.

#	Action	Link/Notes	✔
1	Verify the System Manager version is the same or higher than the target service pack level of the Session Manager.	If the System Manager version is lower than the target service pack level of the Session Manager, you must upgrade System Manager first. See *Upgrading Avaya Aura® System Manager on System Platform*.	
2	Verify the Session Manager server is running Release 6.3.	Viewing the software release on page 13.	
3	Check the RAID Controller battery condition. **Note:** Do not continue if the Current Cache Policy value is **WriteThrough**. A failing RAID battery can create a write-cache problem, causing the upgrade to fail.	Checking the RAID Battery status on page 13.	
4	Download the ISO image from PLDS or https://avaya.support.com to your computer.	See Downloading software from PLDS on page 14.	
5	Copy the Session Manager ISO image to a USB thumb drive or burn the ISO image to a DVD. This step is not needed if you are planning an upgrade using the network transfer.	The USB drive needs to have a capacity of at least 4 GB.	
6	Verify the **Enrollment Password** field is still active.	Verifying Enrollment Password status on page 15	

#	Action	Link/Notes	✔
7	Change the service state of the Session Manager to **Deny New Service**.	Denying new service on page 15.	
8	Verify the **Active Call Count** is zero.	Verifying the Active Call Count on page 16.	
9	View Entity Links and note any links that are down. **Important:** Verify the entity link for the Session Manager is **UP**.	Viewing the Session Manager Entity Link Connection Status on page 16.	
10	Install the Session Manager Service Pack.	• If installing using the Network transfer, see Using Network transfer on page 16 • If using the USB thumb drive, see Using USB Thumb Drive on page 17. • If using physical media (CD or DVD), see Using a DVD on page 18.	
11	If applicable, configure the Session Manager in a System Manager Geographically Redundant environment.	Configuring Session Manager in a geographically redundant environment on page 19.	
12	Run the Session Manager tests.	Testing the Session Manager instance on page 19.	
13	Verify data replication between System Manager and Session Manager. The system synchronizes the data in about 15 minutes. Refresh the page as necessary.	Verifying Data Replication on page 19.	
14	Verify the Security Module is active for the Session Manager.	Viewing Security Module status on page 20.	
15	If SIP monitoring is provisioned for Session Manager, verify the links are active for the Session Manager instance. The system updates the status in about 10 minutes. Refresh the page as necessary. Ignore the links that you earlier noted as down.	Viewing the Session Manager Entity Link Connection Status on page 16.	
16	If the system is forwarding alarms to NMS or ADC, generate a test alarm to verify administration and connectivity.	Generating a test alarm on page 21.	
17	Change the service state to **Accept New Service** for the Session Manager server.	Accepting new service on page 22.	

#	Action	Link/Notes	✔
18	Install the Service Pack on the remaining Session Managers.	Repeat Steps 1 - 16 for each remaining Session Manager.	
19	Verify all upgraded Session Managers are operational.	Verifying the upgraded Session Managers on page 22	

Viewing the software release version

The format of the Session Manager software version is **w.x.y.z.#** where:

- **w** = Major release number
- **x** = Minor release number
- **y** = Service pack number
- **z** = Patch number
- **#** = Build number

For example: **6.3.1.1.620013** indicates that a Session Manager server is running Release 6.3, Service Pack 1 with Patch 1.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. The **Version** column of the **Session Manager Dashboard** page displays the installed version string.
3. **(Optional)** Select the version string to display the software version details for all the Session Manager applications.

Checking the RAID Battery status

If the RAID battery in the server is failing, a write-cache problem can cause the upgrade to fail.

Note:

This procedure does not apply to Branch Session Manager or Session Manager on Virtualized Environment. Virtual machines on System Platform or VMware cannot access the RAID controller information to determine the state of the battery. Different procedures exist for checking the RAID controller battery for VMware and System Platform. The System Platform web console displays a warning if you need to replace the battery.

Procedure

1. Log in to the Session Manager command line interface.
2. Enter the command **hardware_info –d**.

The system displays output similar to the following:

```
[Raid Information]
   Virtual Disk: 0 (Target Id: 0)
   RAID Level: Primary-1, Secondary-0, RAID Level Qualifier-0
   Size:135.972 GB
   State: Optimal
      Physical Disk: 0
          Device Id: 0
          Raw Size: 136.732 GB [0x11177328 Sectors]
          Coerced Size: 136.125 GB [0x11040000 Sectors]
      Physical Disk: 1
          Device Id: 1
          Raw Size: 136.732 GB [0x11177328 Sectors]
          Coerced Size: 136.125 GB [0x11040000 Sectors]
   Remaining Capacity: 1662 mAh
   Full Charge Capacity: 1667 mAh
   Default Cache Policy: WriteBack, ReadAdaptive, Direct, No Write Cache if Bad BBU
   Current Cache Policy: WriteBack, ReadAdaptive, Direct, No Write Cache if Bad BBU
```

3. Verify the value for the **Current Cache Policy** is `WriteBack`.

   If the value of the **Current Cache Policy** is `WriteThrough`, the RAID controller battery is degraded. You must replace the RAID controller /battery on the server.

4. Verify the value for **Remaining Capacity** is close to the value for **Full Charge Capacity**.

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads using one of the following methods:
   - By download name
   - By selecting an application type from the drop-down list
   - By download type

   After entering the search criteria, click **Search Downloads**.
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click the message, install Active X, and continue with the download.

9. When the system displays the security warning, click **Install**.

   When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Verifying Enrollment Password status

Session Manager requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and the Session Manager. The Enrollment Password is also known as the **certificate enrollment password**.

If the Enrollment Password has expired, or if you do not know the password, do one of the following:

- Ask the customer for a password.
- Make up a password.

Procedure

1. On the home page of the System Manager web console, under **Services**, select **Security** > **Certificates** > **Enrollment Password**.
2. If the value of the **Time Remaining** field is zero, you need to reset the password:
   a. In the **Password expires in** field, select a value from the drop-down menu for the time when the password must expire.
   b. Enter a password in the **Password** field.
   c. Reenter the password in the **Confirm Password** field.
   d. Make a note of the password for future reference.
   e. Click **Commit**. The system updates the **Time remaining** field.

Denying new service

When you change the state of the selected Session Manager to **Deny New Service**, the system denies any new call attempts and service requests. Existing calls remain in effect until the users terminate the calls.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. On the **Session Manager Dashboard** page, select the appropriate Session Manager check box in the **Session Manager Instances** table.
3. Click **Service State**.
4. From the drop-down list box, select **Deny New Service**.
5. On the confirmation page, click **Confirm**.

Verifying the Active Call Count

The **Active Call Count** value indicates the number of active calls on the Session Manager instance. Active calls are calls that were already active before the Session Manager was placed in the denial state. Changing the state to **Deny New Service** does not drop calls that are currently processed.

To prevent any impact on calls that are active, the **Active Call Count** must be zero before proceeding with the Session Manager upgrade. If the administrator decides to continue the upgrade if the active call count is not zero, the active calls are dropped.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Wait until **Active Call Count** is zero. Refresh the screen to update the count.

Viewing the Session Manager Entity Link Connection Status

An entity link consists of one or more physical connections between a Session Manager server and a SIP entity. If all the connections are up, then the Entity Link status is **up**. If one or more connections are down but at least one connection is up, the link status is **partially down**. If all the connections are down, the Entity Link status is **down**.

On the Session Manager dashboard page, the number of down links and total links are shown in the **Entity Monitoring** column. The values have the format **# of Down links / # of Total links**.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Red link values indicate that at least one entity link is down. Click the link to display the Session Manager Entity Link Connection Status page.

   The Session Manager Entity Link Connection Status page displays the details for each link. If a link is down, the page displays a reason code.
3. To view the SIP Entity Link Monitoring Status Summary page, click **Summary View**.

Upgrading Session Manager software

Using Network transfer

Transfer the downloaded Session Manager ISO image to the Session Manager server and run the upgrade script.

Procedure

1. Log in as **craft** or customer to a console on the Session Manager server, or use SSH for remote login.

   Note:

   You can connect your laptop directly to the service port of the server.

2. Enter **`rm -f $HOME/asm*installer.iso`**
3. Enter **`echo $HOME`**
4. Transfer the ISO file to the directory represented by `$HOME` in the Session Manager server.

   Note:

   You can transfer the files over the network using WinSCP or another file transfer application.

5. Enter **`cd $HOME`**
6. Enter **`upgradeSM asm*installer.iso`** to mount the ISO image and run the upgrade script.
7. If prompted, accept the EULA.
8. If prompted, enter the Enrollment password. The script takes about 20 minutes to complete.

   Note:

   The upgrade process does not prompt for the Enrollment Password when upgrading from Session Manager 6.3 to Session Manager 6.3.8 and later.

Using a USB thumb drive

Transfer the Session Manager ISO file from the USB thumb drive to the Session Manager server and run the upgrade script.

Note:

This procedure does not apply to:

- Branch Session Manager
- Session Manager on Avaya Aura® Solution for Midsize Enterprise

Procedure

1. Log in as **craft** or customer to a console on the Session Manager server, or use SSH for remote login.

   Note:

   You can connect your laptop directly to the service port of the server.

2. Copy the Session Manager ISO image from a USB thumb drive to Session Manager:

   a. Insert the USB drive into the USB port of the Session Manager server.

b. Enter **mount /usbthumb/**
c. Enter **cd /usbthumb/**
d. Enter **rm –f $HOME/asm*installer.iso**
e. Enter **cp asm*installer.iso $HOME**
f. When the copy completes, enter **cd /**
g. Enter **umount /usbthumb**
h. Remove the USB drive from the server.

3. Enter **cd $HOME**
4. Enter **upgradeSM asm*installer.iso** to mount the ISO image and run the upgrade script.
5. If prompted, accept the EULA.
6. If prompted, enter the Enrollment password. The script takes about 20 minutes to complete.

Note:

The upgrade process does not prompt for the Enrollment Password when upgrading from Session Manager 6.3 to Session Manager 6.3.8 and later.

Using a DVD

Transfer the Session Manager ISO file from the DVD to the Session Manager server and run the upgrade script.

Note:

This procedure does not apply to:

- Branch Session Manager
- Session Manager on Avaya Aura® Solution for Midsize Enterprise

Procedure

1. Log in as **craft** or customer to a console on the Session Manager server or use SSH for remote login.

   Note:

   You can connect laptop directly to the service port of the server.

2. Insert the DVD into the DVD drive of Session Manager.
3. Enter **upgradeSM** to start the upgrade script.
4. If prompted, accept the End User License Agreement.
5. If prompted, enter the Enrollment password. The script takes about 20 minutes to complete.

Note:

The upgrade process does not prompt for the Enrollment Password when upgrading from Session Manager 6.3 to Session Manager 6.3.8 and later.

6. When the script completes, the Session Manager server automatically ejects the DVD and reboots. Remove the DVD and close the DVD tray.

Configuring Session Manager in a System Manager in a geographically redundant environment

In a System Manager geographic redundant environment where the Primary System Manager is down, perform this procedure *after* upgrading the Session Manager.

Procedure

1. Log in as **craft** or customer to a console on the Session Manager server, or use SSH for remote login.

   Note:

   You can connect your laptop directly to the service port of the server.

2. Enter **`changeMgmtIP`** and ensure that all fields are set correctly.
3. Enter **`dnat_failover.sh <SECONDARY_SMGR_IP>`**
4. Enter **`initTM`**

Testing the Session Manager instance

Procedure

1. On the System Manager web console, under **Elements**, select **Session Manager** > **System Tools** > **Maintenance Tests**.
2. In the **Select System Manager or a Session Manager to test** field, select the Session Manager instance from the drop-down menu.
3. Select **Execute all Tests**.
4. Verify the **Test Result** field displays **Success**.

   If any of the tests fail, see *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Verifying Data Replication

Procedure

1. On the System Manager web console, under **Services**, click **Replication**.

2. Verify the status for the appropriate replica group is **Synchronized**.
3. If the status for the replica group is not **Synchronized**, see Troubleshooting Data Replication on page 20.

Troubleshooting Data Replication

Procedure

1. On the home page of the System Manager Web console, under **Services**, click **Replication**.
2. If the status for the replica group is not **Synchronized**:
   a. Select the check box in front of the affected replica group.
   b. Click **View Replica Nodes**.
   c. Verify that an entry for the upgraded Session Manager exists.
   d. Select the check box next to the upgraded Session Manager.
   e. Click **View Details**.
   f. Under the **Synchronization Statistics** section, wait until the **Pending Batches** number is zero. Refresh the page as necessary.
3. If the **Pending Batches** number does not change to zero, perform the following steps:
   a. Click **Done**.
   b. On the **Replica Nodes** page, click **Repair**.
   c. Click **OK** in the dialog box.
4. Wait until the status of the Session Manager is **Synchronized**. Refresh the page as necessary.

Viewing Security Module status

Procedure

1. On the System Manager Web Console, select **Elements** > **Session Manager**.

   The **Session Manager Dashboard** page displays the details and Security Module status for all the administered Session Manager servers and Survivable Remote Session Manager servers (BSM).
2. If the Security Module state of a particular Session Manager is not displayed as **Up**, see Troubleshooting Security Module Sanity failure on page 20.

Troubleshooting Security Module Sanity failure

Procedure

1. On the System Manager Web Console, select **Elements** > **Session Manager** > **System Status** > **Security Module Status**.
2. Select **Refresh** to display the current status.

3. Verify that the **Status** for the indicated Session Manager is **Up**.
4. Verify that the IP address is correct.
5. If the status is selected as **Down**, reset the security module:
    a. Select the appropriate Session Manager instance from the table.
    b. Click **Reset**.

    Warning:

    Session Manager cannot process calls while the system resets the security module.
6. Select **Refresh** to display the current status.

Generating a test alarm

Generate a test alarm to the targets assigned to the serviceability agent. These targets may include:

- A SAL Gateway (the alarm is forwarded to ADC)
- System Manager Trap Listener
- Third-party NMS
- Avaya SIG server

You can either run the **generateTestAlarmSM.sh** script using the Session Manager CLI, or you can use the **Generate Test Alarm** button on the **Serviceability Agents** screen.

Procedure

1. If using the Session Manager CLI:
    a. Login to the Session Manager server.
    b. Enter Session Manager CLI command **generateTestAlarmSM.sh**.
2. If using the **Generate Test Alarm** button on the **Serviceability Agents** screen:
    a. On the System Manager web console, under **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
    b. Select a Hostname from the list and click **Generate Test Alarm**.
3. Verify the System Manager received the test alarm message:
    a. On the System Manager Web Console, under **Services**, select **Events** > **Alarms**.
    b. Verify the message **Test alarm for testing only, no recovery action necessary** displays under the **Description** column.
4. If the serviceability agent is configured with other targets, verify the other targets also received the test alarm.

Accepting new service

Note:

Even though the Security Module displays the status as **Up**, the security module might take 5 to 10 minutes before the security module can begin routing calls.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. On the **Session Manager Dashboard** page, select the appropriate Session Manager in the **Session Manager Instances** table.
3. Click **Service State**.
4. Select **Accept New Service** from the drop-down menu.
5. Click **Confirm**.

Verifying the upgraded Session Managers

Verify:

- the software is installed and configured properly.
- the servers and applications are communicating.
- the service state is correct for the upgraded Session Managers.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. In the **Session Manager Instances** table, verify the **Security Module** is **Up** for all the upgraded Session Managers.
3. Verify the software **Version** is the same for all the upgraded Session Managers.
4. Verify the **Service State** is **Accept New Service** for all the upgraded Session Managers.

Appendix A: OS-level logins for Session Manager

The following is a list of logins that are created during the Session Manager software installation:

- **craft**: An Avaya services login to gain access to the system remotely for troubleshooting purposes.
- **sroot**: An Avaya services root permission login to gain access to the system remotely for troubleshooting purposes. You cannot gain access to the sroot login directly from a login prompt except on the server console.
- **customer**: A login that the **SMnetSetup** script creates. The default name of the *customer* login is **cust**. The customer must ensure the security of this login account. The *customer* login can run software tools which do not require root access on the Session Manager servers.
- **CDR_User**: A restricted shell login for the Call Detail Recording (CDR) feature. CDR collects call data from the Session Manager server. This login is restricted to sftp access only.
- **asset**: A login created during the installation of the Security Module software. By default, access to the system using this login is disabled.
- **spirit**: A login created by the Secure Access Link remote alarming and remote access module for Avaya services.
- **postgres**: A login created by the installation of the Session Manager software PostgresSQL database system. Access to the system using this login is disabled.
- **init** : An Avaya services login that accesses the system remotely for troubleshooting purposes.
- **inads**: An Avaya services login that accesses the system remotely for troubleshooting purposes.
- **rasaccess**: An Avaya services login that accesses the system remotely for troubleshooting purposes.
- **jboss**: A login created for running the management jboss and is not a login account.
- **wsuser**: A login created for running WebSphere and is not a login account.

Warning:

As of Session Manager Release 6.2, the Access Security Gateway secures the following logins and prevents unauthorized access to the Session Manager servers by non-Avaya services personnel:

- **sroot**
- **inads**
- **rasaccess**
- **init**
- **craft**

Using the customer login account, you can run most of the maintenance and troubleshooting commands. You do not need root access for standard maintenance and support purposes. For more information, see PSN (PSN003925U).

Appendix B: Product notifications

Avaya issues a product change notice (PCN) for a software update. A PCN accompanies a service pack or patch that must be applied universally.

Avaya issues a product support notice (PSN) when there is a change in a product. A PSN provides information such as a workaround for a known problem and steps to recover software.

Both of these types of notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Enter your login credentials, if applicable.
3. On the top of the page, click **DOCUMENTS**.
4. In the **Enter your Product Here** field, enter the name of the product, then select the product from the drop-down menu.
5. In the **Choose Release** field, select the specific release from the drop-down menu.
6. In the list of filters, select the **Product Correction Notices** and/or **Product Support Notices** check box.

   Note:

   You can select multiple filters to search for different types of documents at one time.
7. Click **Enter**.

Registering for product notifications

Note:

This procedure applies only to registered Avaya customers and business partners with an SSO login.

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Log in using your SSO credentials.
3. Click on the **MY PROFILE** link.
4. Click the highlighted **HI, <username>** tab.
5. Select **E Notifications** from the menu.
6. In the **Product Notifications** section:
   a. Click **Add More Products**.
   b. Select the appropriate product.
7. In the Product box that appears on your screen:
   a. Select the appropriate release or releases for which you want to receive notifications.
   b. Select which types of notifications you want to receive. For example, **Product Support Notices** and **Product Correction Notices (PCN)**.
   c. Click **Submit**.
8. If you want notifications for other products, select another product from the list and repeat the above step.
9. Log out.

Index

A

accepting new service 22
Active Call Count
    verifying 16
alarm test 21

C

change service state
    deny new service 15
checking
    RAID battery status 13
checklist
    service pack installation 11
configuring Session Manager
    geographically redundant environment 19

D

data replication 20
deny new service 15
deployment options 9
documentation
    related 6
document changes 6
downloading software 14

E

Enrollment Password status 15
Entity Link Connection Status 16

G

generate an alarm 21

I

installed logins 23

L

legal notice .....
logins
    installed 23

N

Network transfer 16
new service
    changing state to accept 22
notifications 25

O

options for deployment 9

P

PCNs
    viewing 25
PCN updates 25
PLDS
    downloading software 14
product notification enrollment 26
product notifications
    e-notifications 26
PSNs
    viewing 25
PSN updates 25

R

RAID battery status
    checking 13
related documentation 6
replication verification 19
running maintenance tests 19

S

Security Module sanity failure
    troubleshooting 20
service pack installation checklist 11
software version
    viewing 13
status
    Enrollment Password 15
support 9

T

testing Session Manager instance 19
troubleshooting 20
    Security Module sanity failure Alarms 20

U

upgrade verification 22
USB drive
    copy ISO image 17

using
USB thumb drive 17
using a DVD 18
using physical media 18

V

verify alarm configuration 21
verifying
Active Call Count 16
data replication 19
upgraded Session Managers 22
videos 8
viewing
Entity Link Connection Status 16
PCNs 25
PSNs 25
viewing security module status 20
viewing software release
version string 13

W

warranty 9