



Deploying Avaya Aura[®] Device Services

Release 10.2.x
Issue 10
April 2026

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 in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. 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 or on the express behalf of 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. Please refer to your agreement with Avaya 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: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA 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, <https://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.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who

installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, 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

The following applies only if the H.264 (AVC) codec is distributed with the product. 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](http://www.mpegla.com).

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC 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 FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://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, its licensors, its suppliers, 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 is a registered trademark of Avaya LLC.

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	13
Purpose	13
Changes to platform support	13
Change history	14
Chapter 2: Avaya Aura® Device Services overview	17
New in Avaya Aura® Device Services Release 10.2.1.1	17
New in Avaya Aura® Device Services Release 10.2.1	18
New in Avaya Aura® Device Services Release 10.2.0.1	18
New in Avaya Aura® Device Services Release 10.2	18
Solution topology	19
Geographically distributed system topology	20
Automatic configuration flow	21
Components	22
Data retention	24
Data encryption	24
Deployments with Avaya Aura® and without Avaya Aura®	25
Chapter 3: Planning	27
Required skills and knowledge	27
Data required for installation	27
Virtual machine requirements	30
Supported hardware for VMware	30
Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)	30
Supported servers	31
Avaya Aura® Device Services support for Avaya Solutions Platform and Avaya Common Server Release 3	31
Software requirements	31
Supported ESXi version	32
Supported ASP Server	33
Avaya Aura® Device Services virtual machine resource requirements	34
Requirements for a host machine for Hyper-V deployments	35
Resource profile specifications for Microsoft Azure virtual machines	35
Resource profile specifications for Google Cloud Platform virtual machines	36
Resources profile specifications for Avaya Aura® Device Services on Amazon Web Services	37
Virtual disk volume specifications	37
Networking considerations for Amazon Web Services	38
Connection types	38
Considerations for migrating from a standalone to a cluster environment	39
System Manager geographic redundancy	39

Considerations for large cluster deployments.....	40
Data center topology configuration in System Manager.....	40
Network latency requirements.....	41
Considerations for geographically distributed systems.....	41
Utility Server deployment considerations.....	42
LDAP authentication domain requirements.....	42
Third-party CA-signed certificates.....	42
Certificates required for an Avaya Aura [®] environment.....	43
Certificates required for an environment without Avaya Aura [®]	45
Cassandra clustering configuration on Avaya Aura [®] Device Services.....	46
Cassandra clustering and data replication configuration on System Manager.....	47
Checklist for Cassandra clustering configuration on Session Manager.....	47
Adding a data center.....	48
Assigning Session Manager to a data center on System Manager 8.x.....	48
Assigning Session Manager to a data center on System Manager 10.x or later.....	49
External load balancer requirements.....	50
Nginx load balancer requirements.....	52
Port configuration for an external load balancer.....	52
Prerequisites for SSO configuration.....	52
Prerequisites for SAML v2.0 and OAuth2 SSO configuration.....	53
Prerequisites for Device Authorization Flow configuration.....	54
Prerequisites for Workspaces SSO configuration.....	55
Configuration tools and utilities.....	56
Characters supported for Avaya Aura [®] Device Services passwords.....	56
Aliases.....	57
app commands.....	57
cdto commands.....	58
System layer commands.....	58
sys secconfig command.....	60
sys versions command.....	60
sys volmgt command.....	61
sys smcvemgt command.....	65
sys ipv6config command.....	67
passwdrules command.....	69
Data encryption commands.....	70
Using the Tmux utility.....	72
Chapter 4: Initial setup.....	73
Deployment methods.....	73
Downloading software from PLDS.....	74
Changing the administrative user password during the first login.....	75
Chapter 5: Initial setup for OVA deployments.....	77
Installation checklist for OVA-based deployments.....	77
VMware deployment options.....	78

Deploying the Avaya Aura [®] Device Services OVA using the vSphere Client.....	78
Deploying the Avaya Aura [®] Device Services OVA using the Host Client connected directly to the ESXi host.....	83
Deploying the Avaya Aura [®] Device Services OVA through Solution Deployment Manager from System Manager.....	86
Logging on to the Avaya Aura [®] Device Services console on VMware.....	92
Enabling IPv6 support at the system layer.....	93
Enabling FIPS mode.....	93
Disabling FIPS mode.....	94
Enabling additional STIG hardening.....	95
Disabling additional STIG hardening.....	95
Configuring UEFI Secure Boot for OVA-based virtual machines.....	96
Checking the UEFI Secure Boot status.....	96
Chapter 6: Initial setup for software-only deployments.....	98
Initial setup for software-only VMware deployments.....	98
Software-only installation checklist for VMware-based environment.....	99
Red Hat Enterprise Linux installation.....	101
Creating disk partitioning for VMware-based software-only deployments.....	102
Creating an administrative user.....	103
Additional packages required by Avaya Aura [®] Device Services.....	104
Enabling the Haveged service.....	105
Enabling FIPS for software-only systems.....	106
RHEL packages management.....	107
Installing the system layer.....	108
Checking the Chrony service status.....	111
Checking the connection to System Manager and Session Manager.....	111
Enabling IPv6 support for software-only deployments.....	112
Initial setup for software-only deployments on Amazon Web Services.....	113
Software-only installation checklist for Amazon Web Services.....	113
Prerequisites for software-only deployment on AWS.....	115
Creating and applying load balancer certificates.....	116
Creating a key pair.....	118
Creating security groups.....	118
Installing RHEL 8.4 or RHEL 8.10 on AWS.....	121
Configuring security groups for the secondary eth1 interface.....	123
Enabling root access.....	124
Creating disk partitioning for software-only deployments on AWS.....	124
Prerequisites for installing the system layer on AWS.....	126
Creating target groups.....	127
Creating and configuring Elastic load balancers.....	128
Configuring idle timeout.....	131
Initial setup for software-only Hyper-V deployments.....	131
Software-only installation checklist for a Hyper-V virtualized environment.....	131

Enabling the Hyper-V service.....	134
Starting Hyper-V Manager.....	134
Creating a virtual switch.....	135
Configuring network settings for the virtual switch.....	135
Creating a new virtual machine on Hyper-V.....	136
Disabling time synchronization.....	138
Creating required virtual hard disks for the virtual machine.....	138
Configuring CPU settings for a Hyper-V virtual machine.....	139
Configuring Windows Defender firewall rules for ports.....	140
Creating disk partitioning for software-only deployments on Hyper-V.....	140
Initial setup for software-only Microsoft Azure deployments.....	141
Software-only installation checklist for Microsoft Azure.....	142
Prerequisites for software-only deployment on Microsoft Azure.....	145
Red Hat Enterprise Linux virtual machine deployment in Microsoft Azure.....	146
Configuring the secondary network interface on a Microsoft Azure virtual machine.....	146
Creating required virtual hard disks for a virtual machine.....	147
Enabling root access.....	148
Creating disk partitioning for a Microsoft Azure virtual machine.....	149
Configuring security groups.....	150
Assigning security groups to network interfaces.....	152
Prerequisites for installing the system layer on Microsoft Azure.....	153
Creating a Microsoft Azure load balancer.....	154
Configuring a Microsoft Azure load balancer.....	155
Initial setup for software-only Google Cloud Platform deployments.....	157
Software-only installation checklist for Google Cloud Platform.....	157
Prerequisites for software-only deployment on Google Cloud Platform.....	160
Creating VPC peering.....	161
Configuring firewall rules.....	161
Assigning firewall rules to virtual machines.....	164
Virtual machine deployment checklist.....	164
Deploying virtual machines in Google Cloud Platform.....	165
Reimaging the operating system disk.....	167
Enabling root access.....	168
Creating an instance group for load balancers.....	169
Creating load balancers.....	170
Creating required virtual hard disks for a virtual machine.....	172
Enabling LVM on RHEL.....	173
Creating disk partitioning for a Google Cloud Platform virtual machine.....	173
Enabling editing of the /etc/hosts file	174
Prerequisites for installing the system layer on Google Cloud Platform.....	174
Configuring redirection rules for port 443.....	175
Chapter 7: Avaya Aura® Device Services installation.....	177
Avaya Aura® Device Services installation checklist.....	177

Installing Avaya Aura® Device Services.....	179
Timeout values for Cassandra and Keycloak operations.....	188
testUser validations.....	188
Utility Server VIP and FQDN in AWS cluster deployments.....	189
Installing Avaya Aura® Device Services in an environment without Avaya Aura®	189
Avaya Aura® Device Services cluster installation.....	198
Installing an Avaya Aura® Device Services cluster.....	198
Initial cluster node installation.....	199
Installing additional non-seed nodes.....	199
Installing additional non-seed nodes in an environment without Avaya Aura®	206
Configuring RSA public and private keys for SSH connections in a cluster.....	213
Changing the LDAP parameters after installing an Avaya Aura® Device Services cluster.....	214
Changing the seed node of a cluster.....	214
Configuring the virtual IP address for Avaya Aura® Device Services clusters.....	215
Configuring an additional seed node.....	217
Performing a silent installation.....	217
Enabling the Enhanced Access Security Gateway from the CLI.....	222
Running the post-installation script.....	223
Checking for DRS synchronization.....	224
Creating an AIDE baseline database.....	225
Changing the default password for automatic backups.....	226
Uninstalling Avaya Aura® Device Services.....	226
Uninstalling the system layer.....	227

Chapter 8: Initial configuration with the Avaya Aura® Device Services configuration

utility.....	228
Configuring Avaya Aura® Device Services using the configuration utility.....	229
Front-end host, System Manager, and certificate configuration.....	230
LDAP configuration.....	234
LDAP advanced parameters.....	244
Cassandra DB user and password.....	248
Clustering configuration.....	249
Utility Server configuration.....	251
Advanced configuration.....	252
Configuring the Avaya Aura® Device Services server firewall.....	254
Configuring additional ports in Avaya Aura® Device Services server firewall in 10.x releases.....	254
Enabling Open LDAP replication.....	255
Re-enabling Open LDAP replication after removing a node from a cluster.....	256
OAuth configuration.....	257
Authorization realm configuration on UC servers and Avaya Workplace Client.....	257
Configuring Keycloak settings.....	258
Logging in to the Keycloak web administration portal.....	260
Obtaining the client secret.....	260
Creating client mapping.....	260

Modifying the attribute mapping between the third-party identity provider and Keycloak.....	262
Enabling OAuth database replication in a cluster environment.....	264
Checklist to Configure Keycloak using a secure LDAP	265
Obtaining LDAP Server Certificate.....	265
Importing the Certificate into the Keycloak Truststore.....	266
Configuring LDAPS in Keycloak.....	267
Chapter 9: Configuring Session Manager for cluster environments.....	268
Managing an incoming call.....	268
Adding an Avaya Aura® Device Services instance to System Manager.....	270
Pairing Session Manager with an Avaya Aura® Device Services node.....	272
Enabling PPM rate limiting for Session Manager.....	273
Effect of Session Manager on Avaya Aura® Device Services.....	274
Session Manager operations that impact Avaya Aura® Device Services.....	274
Chapter 10: Deploying AADS on ASP R6.0.x (KVM on RHEL 8.10).....	275
Deploying Avaya Aura® Device Services on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit	275
Chapter 11: LDAP settings configuration.....	280
LDAP authentication domain requirements.....	280
LDAP attributes replication to the global catalog.....	280
Installing LDAP schema snap-in.....	280
Requirements for LDAP attribute values.....	281
Indexing an attribute.....	282
List of attributes to index.....	282
Saving existing LDAP settings.....	283
Setting up user synchronization with LDAP after deployment.....	284
LDAP configuration for Microsoft Active Directory.....	284
Configuring the binding parameters.....	287
Configuring the authentication parameters.....	288
Configuring the role search parameters.....	289
Configuring the internationalization parameters.....	289
Configuring the user management parameters.....	290
Multiple authentication and authorization domains.....	291
Creating groups in LDAP.....	292
LDAP attribute mapping.....	292
Configuration and data mapping use cases.....	293
Changing the PictureURL attribute.....	295
LDAP configuration best practices.....	296
LDAP parameter descriptions.....	296
Chapter 12: SNMP server configuration.....	299
Alarms configuration for System Manager.....	299
Setting up an SNMPv3 user profile.....	299
Setting up an SNMP target profile.....	300
Assigning the SNMPv3 user profile.....	301

Alarms configuration for a third-party SNMP server.....	301
Setting up a third-party SNMPv3 server.....	302
Configuring Avaya Aura [®] Device Services to support a third-party SNMP server.....	302
Verifying third-party SNMP server operation.....	303
Chapter 13: Reverse proxy configuration.....	304
Checklist for reverse proxy configuration.....	304
Creating a CSR.....	305
TLS certificates field descriptions.....	306
Creating an end entity.....	308
Creating the certificate using a CSR.....	309
Uploading a certificate file.....	309
Synchronizing and installing certificate in a multi-server deployment.....	311
Downloading the System Manager PEM certificate.....	312
Installing a CA certificate.....	312
Creating a TLS server profile.....	313
TLS server profile screen field descriptions.....	313
Creating a TLS client profile.....	316
TLS client profile screen field descriptions.....	316
Adding a reverse proxy.....	318
Overriding port configuration in a cluster.....	319
Chapter 14: Remote access configuration.....	321
Configuring remote access.....	321
A10 Thunder Application Delivery Controller Configuration.....	322
Importing the A10 Client SSL Certificate.....	322
Importing the A10 Server SSL Certificate.....	323
Importing the CA root certificate.....	324
Creating the A10 server SSL template.....	324
Creating the A10 client SSL template.....	325
Creating an IP source NAT.....	326
Creating the Avaya Aura [®] Device Services backend server.....	326
Creating a virtual server.....	327
Creating a service group.....	328
Creating a virtual service.....	329
Configuring A10 for LDAP searches.....	329
Configuring A10 for LDAP authentication.....	330
Chapter 15: Troubleshooting.....	332
Avaya Workspaces Client cannot connect to Avaya Aura [®] Device Services.....	332
Service unavailable.....	333
Admin user is not prompted for password in sudo su.....	333
Avaya Workplace Client cannot connect to Avaya Aura [®] Device Services.....	334
Avaya Aura [®] Device Services installation fails if the DNS forward and reverse lookup zones are not configured properly.....	334

Avaya Aura® Device Services installation or upgrade fails due to invalid System Manager certificates.....	334
Avaya Aura® Device Services installation fails if third-party certificates are used on other Avaya Aura® elements.....	335
Avaya Aura® Device Services installation fails when using third-party CA identity certificates.....	335
app commands do not work after a failed installation.....	336
DNS entries disappear from the /etc/resolv.conf file after restarting Avaya Aura® Device Services.....	337
runUserDiagnostics tool.....	337
Data on Cassandra is corrupted.....	339
Primary System Manager fails.....	339
Open LDAP replication fails.....	340
Open LDAP replication fails if Avaya Aura® Device Services uses a custom identity certificate for server interfaces.....	340
Avaya Workplace Soft Clients are logging out due to a mismatch in the ETAG.....	341
Chapter 16: Resources	342
Documentation.....	342
Finding documents on the Avaya Support website.....	343
Avaya Documentation Center navigation.....	343
Viewing Avaya Mentor videos.....	345
Support.....	345
Using the Avaya InSite Knowledge Base.....	346
Appendix A: Avaya Aura® Device Services certificate configuration	347
Command for viewing certificate details.....	348
Importing the Avaya Aura® System Manager trusted certificate.....	349
Importing third-party CA-signed certificates.....	350
Importing intermediate CA certificates.....	352
Generating Certificate Signing Requests.....	353
Creating a Certificate Signing Request (CSR) using OpenSSL.....	354
Signing identity certificates for Avaya Aura® Device Services using third-party CA certificates...	355
Configuring System Manager to trust third-party root CA certificates.....	357
Viewing the current CA used to sign the Session Manager certificate.....	358
Importing SIP CA certificate to the Avaya Aura® Device Services trust store.....	358
LDAP certificates.....	359
Importing a trusted LDAP certificate.....	359
Configuring the client certificate policy using the command line interface.....	360
Uploading and hosting CA certificate files on Avaya Aura® Device Services server.....	361
Setting up a TLS link for Avaya Scopia® Management.....	362
Appendix B: LDAP examples and search results	364
Examples of Microsoft Active Directory LDAP property files.....	364
LDAP search results and referrals.....	365
Appendix C: FIPS validated cryptographic modules	369
Appendix D: Best Practices for VMware performance and features	370

Timekeeping.....	370
VMware Tools.....	371
VMware networking best practices.....	372
Storage.....	375
Best Practices for VMware features.....	375
VMware High Availability.....	375
VMware vMotion.....	376
VMware snapshots.....	376
VMware features supported by Avaya Aura®	378
Appendix E: Creating RHEL virtual machine on Nutanix.....	381
Uploading the RHEL ISO to Nutanix server.....	381
Installing RHEL on the Nutanix server.....	382
Appendix F: Virtual Machine Backup (clone) in ASP R6.0.x (KVM on RHEL 8.10).....	385
Virtual Machine Backups (clone) as an alternative to snapshots.....	385
Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10).....	385
Calculating space for the clone.....	388
Validating a Virtual Machine Backup (clone).....	390
Rolling back using the Virtual Machine Backup (clone).....	392
Glossary.....	395

Chapter 1: Introduction

Purpose

This document describes Avaya Aura® Device Services planning, installation, and configuration. It is intended for implementation personnel who deploy Avaya Aura® Device Services at a customer site.

For information about ongoing administration and maintenance, see *Administering Avaya Aura® Device Services*.

Changes to platform support

As of January 1, 2026, Avaya has refined its infrastructure support strategy for Avaya Aura® and Surround Applications. This update specifically impacts Software-Only and Infrastructure as a Service (IaaS) deployment models. To ensure your environment remains compliant and supported, review the following changes to supported platforms:

Discontinued Platforms:

- Hypervisor: Microsoft Hyper-V
- Cloud Platforms: Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud

Supported platforms for Software Only and Infrastructure as a Service (IaaS) deployment models:

- Cloud Platform: AWS
- On-premises platforms: KVM, Nutanix, VMware

Change history

Issue	Date	Summary of changes
10	April 2026	Updated the following sections: • Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10) on page 385 • Calculating space for the clone on page 388 • Validating a Virtual Machine Backup (clone) on page 390
9	March 2026	Added the section: Changes to platform support on page 13
8	February 2026	Updated the following sections: • Software requirements on page 31 • Supported ASP Server on page 33
7	April 2025	Added the following section: New in Avaya Aura Device Services Release 10.2.1.1 on page 17 Updated the following section: Supported ESXi version on page 32
6	March 2025	Added the following sections: Checklist to Configure Keycloak using a secure LDAP on page 265 Obtaining LDAP Server Certificate on page 265 Importing the Certificate into the Keycloak Truststore on page 266 Configuring LDAPS in Keycloak on page 267
5	January 2025	Added the following section: • Avaya Workplace Soft Clients are logging out due to a mismatch in the ETAG

Issue	Date	Summary of changes
4	December 2024	Added the following sections for R10.2.1: • Deploying Avaya Aura Device Services using KVM Cockpit • New in Avaya Aura® Device Services Release 10.2.1 • New in Avaya Aura® Device Services Release 10.2.0.1 • Virtual Machine Backup (clone) in KVM Updated the following sections for R10.2.1: • Initial setup-Deployment methods • Initial setup for OVA deployments-Installation checklist for OVA-based deployments • Initial setup for software-only deployments • Software-only installation checklist for VMware-based environment • Red Hat Enterprise Linux installation • Creating an administrative user • Additional packages required by Avaya Aura® Device Services • Installing additional RHEL 8.4 packages manually • Installing the system layer • Table: Software-only installation checklist for Amazon Web Services • Installing Red Hat Enterprise Linux 8.4 on AWS • Configuring security groups for the secondary eth1 interface • Software-only installation checklist for a Hyper-V virtualized environment • Creating a new virtual machine on Hyper-V • Software-only installation checklist for Microsoft Azure • Red Hat Enterprise Linux virtual machine deployment in Microsoft Azure • Virtual machine deployment checklist • TLS certificates field descriptions • Avaya Aura® Device Services virtual machine resource requirements • Requirements for a host machine for Hyper-V deployments • Enabling FIPS for software-only systems

Issue	Date	Summary of changes
3	May 2024	Updated the following sections: Data required for installation on page 27 Avaya Aura Device Services virtual machine resource requirements on page 34
2	May 2024	Update the following section: New in Avaya Aura Device Services Release 10.2 on page 18
1	December 2023	Release 10.2.

Chapter 2: Avaya Aura® Device Services overview

With Avaya Aura® Device Services, you can roll out multiple clients and seamlessly transition between devices. Avaya Aura® Device Services acts as a single point of administration for endpoints. It can also provide file server capabilities, such as firmware and settings files. Avaya Aura® Device Services can handle traditional IP phones, such as the 96xx Series Phones, and the complex configuration of SIP endpoints, such as Avaya Workplace Client. This document also uses the term “client” when referring to Avaya Workplace Client.

SIP endpoints, such as Avaya Workplace Client, integrate telephony, video, chat, email, and presence. To log in to and use all these services, the device must be configured with multiple FQDNs or IP addresses, login IDs, and passwords. Once logged in, you require the appropriately formatted contact address to initiate communication and Avaya Aura® Device Services can provide this.

Avaya Workplace Client also provides BYOD capabilities, which allow users to use their own devices. Each device has different capabilities, so the appropriate settings must be pushed to each device. Using the Dynamic Configuration service, Avaya Aura® Device Services provides dynamically created setting files that include system-wide parameters, user-specific parameters, and device-specific parameters.

As an administrator, you must maintain software-based soft clients on a limited set of versions to ensure consistent feature sets and security. With hard phones, such as 96xx Series Phones, you can initiate a firmware download by forcing the phone to reboot. With a soft phone, such as Avaya Workplace Client, you cannot manually force the software to update unless it is configured through Avaya Aura® Device Services.

New in Avaya Aura® Device Services Release 10.2.1.1

Avaya Aura® Device Services Release 10.2.1.1 supports the following new features and enhancements:

System Manager contacts filtration

With Release 10.2.1.1, Avaya Aura® Device Services restrict the display of contacts specific to System Manager upon searching the contacts.

HTTP Proxy support for client ID mapping

With Release 10.2.1.1, Avaya Aura® Device Services support HTTP Proxy configuration for client ID mapping.

Addition of a new ED signature for macOS

With Release 10.2.1.1, the Avaya Aura® Device Services support adding ED signature for macOS binary upload.

New in Avaya Aura® Device Services Release 10.2.1

Avaya Aura® Device Services Release 10.2.1 supports the following new features and enhancements:

Support for Software-Only Deployment on Nutanix Environment

With Release 10.2, Avaya Aura® Device Services Software-Only application can be deployed on Nutanix 6.5 and later.

Red Hat Enterprise Linux 8.10 support for Avaya Aura® Device Services

With Release 10.2.1, Avaya Aura® Device Services supports Red Hat Enterprise Linux Release 8.10.

Kernel-based Virtual Machine (KVM) on RHEL 8.10 hypervisor support

With Release 10.2, Avaya Aura® Device Services can be deployed on Avaya-supplied KVM on RHEL Release 8.10 hypervisor (Avaya Solutions Platform 130 R6.0).

Keycloak with FIPS support

With Release 10.2.1 Avaya Aura® Device Services provide Keycloak with FIPS support.

New in Avaya Aura® Device Services Release 10.2.0.1

The following is a summary of changes in Release 10.2.0.1 of Avaya Aura® Device Services:

- Added support to a new Enterprise-Directory Type, ActiveDirectory_2022.
- Rollback to previous AADS version below 10.2.0.1 is not supported.

New in Avaya Aura® Device Services Release 10.2

The following is a summary of new functionalities added to Avaya Aura® Device Services in Release 10.2:

Enable/Disable logging

- Before Release 10.2, AADS supported extended logging at the system level only. With AADS Release 10.2, you can enable or disable logging at an individual user level.
- LOG_VERBOSITY property is added in the AADS dynamic configuration at a user level.

Support for VMware 8.0

With Release 10.2, Avaya Aura® applications support the VMware® vSphere ESXi 8.0 and VMware® vCenter Server 8.0 in a VMware virtualized environment.

Client ID configuration

Before Release 10.2, client ID used by J100 phones was hard-coded in AADS and couldn't be configurable. With Release 10.2, you can configure the client-id in AADS, which enables IAM to apply customer-specific requirements in the access token when the client authenticates.

Dynamic configuration for telecommuter number

Using AADS auto-config service API, the administrator can configure the telecommuter number and associate it with agents using Workplace. With this release, only one telecommuter number is supported.

Upgraded Keycloak version

Upgraded Keycloak version from Release 6.0.1 to Release 22.0.4.

Added MS Graph API support

AADS now supports MS Graph API as a replacement for MS Azure API, which Microsoft retired this year.

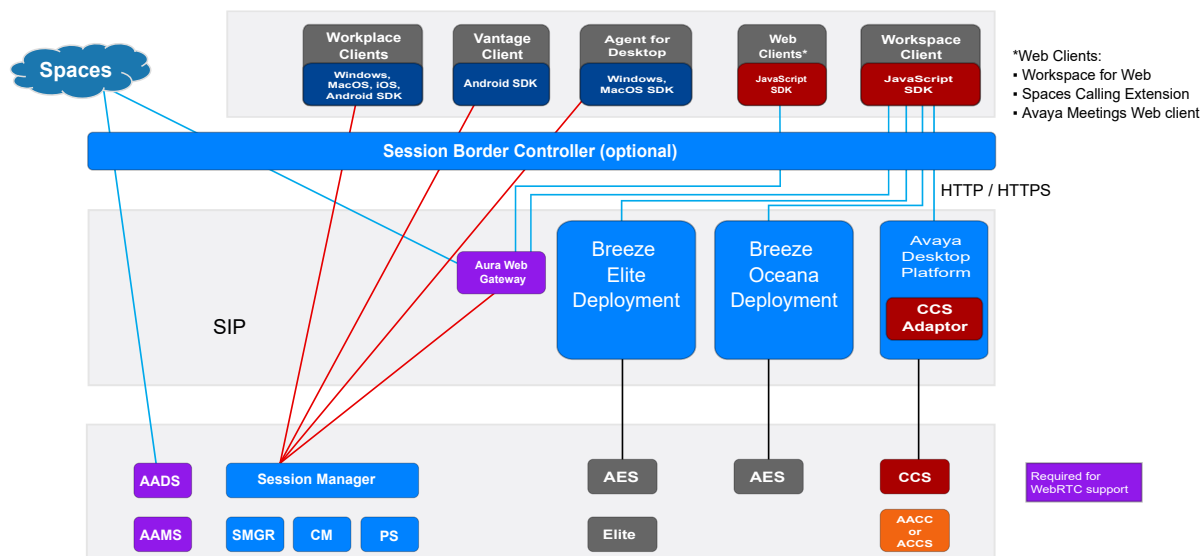
For more information on MS Graph API replacing MS Azure API, see PSN at <https://download.avaya.com/css/public/documents/101086282> for details.

* Note:

Microsoft announced EoS for Azure AD Graph API. MS Graph API will replace Azure AD Graph API.

Solution topology

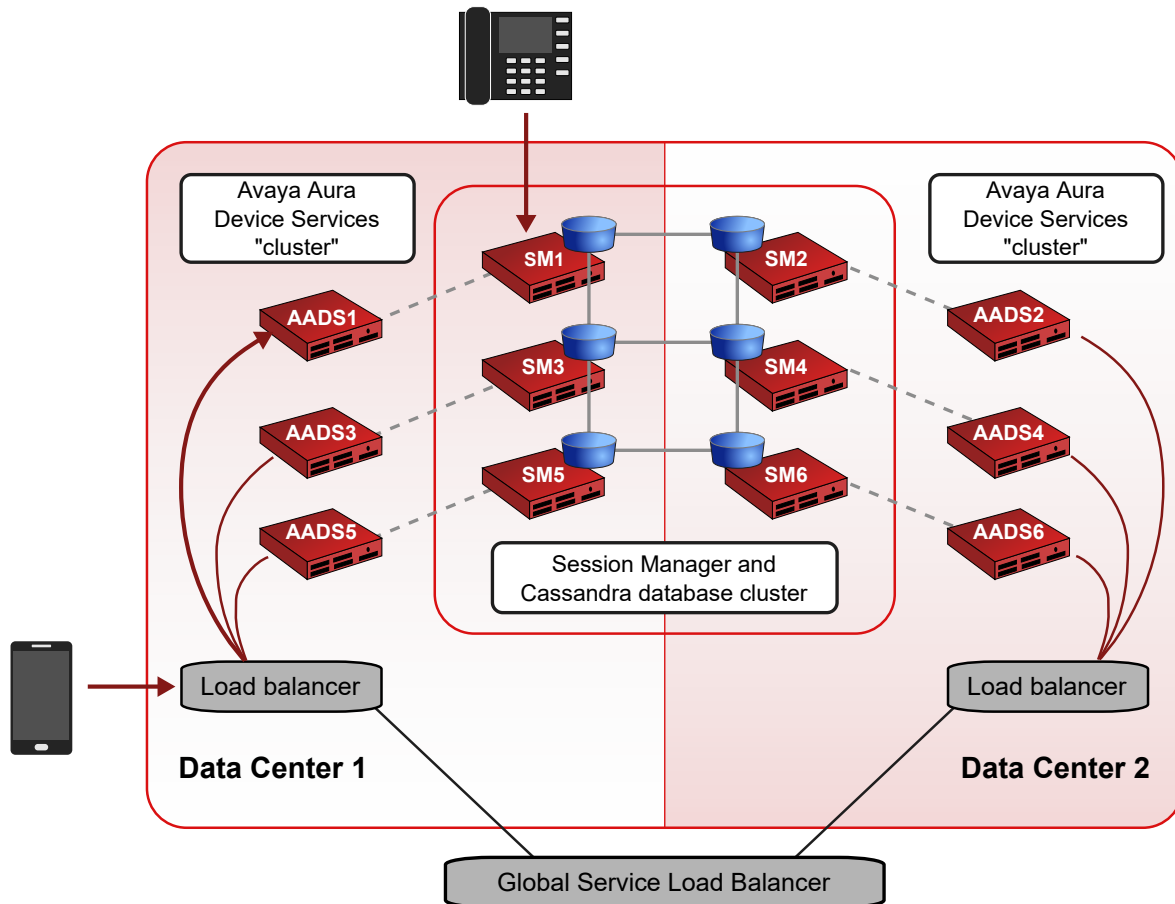
The following diagram shows a solution with Avaya Aura® Device Services.



Geographically distributed system topology

Avaya Aura® Device Services does not support multiple Avaya Aura® Device Services clusters. Instead, you can deploy a geographically distributed cluster, where resources are deployed in multiple data centers to reduce delays. For this purpose, Avaya Aura® Device Services and other components, such as Session Manager, are deployed in each data center. In a geographically distributed system, you must also use a Global Server Load Balancer (GSLB) with location-aware DNS and local or regional load balancers. GSLB provides different routes and addresses based on the location of the client. Load balancer balances traffic between two or more Avaya Aura® Device Services nodes, which may be located in the same data center or in different data centers.

In the following example, there are two data centers with three Avaya Aura® Device Services and three Session Manager servers in each data center. The cluster uses a GSLB to resolve requests to a specific regional load balancer, which then routes these requests only to the Avaya Aura® Device Services nodes within that region.

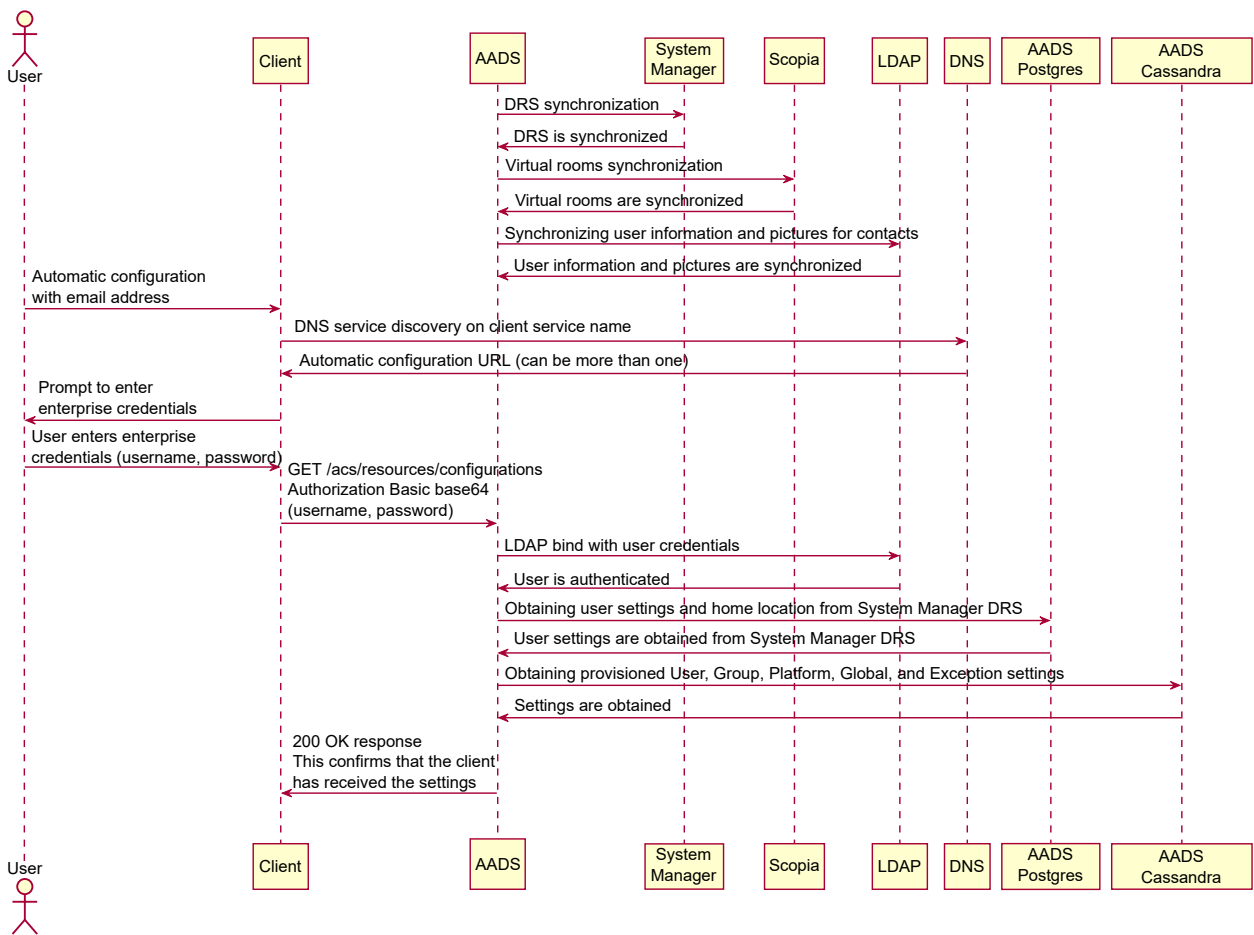


Related links

- [External load balancer requirements](#) on page 50
- [Considerations for geographically distributed systems](#) on page 41
- [System Manager geographic redundancy](#) on page 39
- [Utility Server deployment considerations](#) on page 42

Automatic configuration flow

The following diagram shows the automatic client configuration flow.



Components

The following table lists key components that Avaya Aura® Device Services requires. Avaya Aura® Device Services can also integrate with other products and solutions, such as Avaya Workplace Client, Avaya Spaces, and Avaya Workspaces for Avaya Oceana®. For more information about interoperability and supported product versions, see <https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=Avaya+Aura+Device+Services>.

Components	Description
Avaya Aura® core	Avaya Aura® Device Services requires the following Avaya Aura® key components: • System Manager: For centralized management. System Manager also enables other capabilities, including licensing with Avaya WebLM.  Note: Avaya Aura® Device Services does not support the System Manager Geographic Redundancy mode. • Session Manager: For registration and telephony functions, such as call escalation. • Communication Manager: For organizing and routing voice, data, image, and video transmissions. • Presence Services: For Presence and IM functionality.  Note: Starting from Release 10.1.1, you can deploy Avaya Aura® Device Services in an environment without Avaya Aura®. When deployed in an environment without Avaya Aura®, Avaya Aura® Device Services does not require Avaya Aura® solution components.
Avaya Session Border Controller (Avaya SBC)	Avaya SBC provides a common element to enable secure access to the Avaya infrastructure from untrusted networks, such as the internet. In addition to SIP firewall services, this component provides the Reverse Proxy services required for HTTP signaling, media traversal, and access to other data services.
Enterprise Directory	The corporate LDAP server. For example, Microsoft Active Directory.

Virtualized components	Description
ESXi Host	A virtual machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer simultaneously.
vSphere Client	An application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface.
vCenter Server	An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.
Avaya Solutions Platform	A platform that is a customized OEM version of VMware ESXi. With Avaya Solutions Platform, customers can run any combination of supported applications on Avaya-supplied servers. Avaya Solutions Platform provides greater flexibility in scaling customer solutions to individual requirements.

Virtualized components	Description
Solution Deployment Manager	The centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
Open Virtualization Appliance	The virtualized operating system and application packaged in a single file that is used to deploy a virtual machine.

You can deploy Avaya Aura® Device Services if you have any of the following:

- Solution Deployment Manager
- vSphere Client
- vCenter server
- Avaya Solutions Platform

Data retention

The following Avaya Aura® Device Services locations can contain private or sensitive user data:

- Log files.
- Avaya Aura® Device Services Cassandra database.

To maximize data privacy and security, you can specify how long you want to keep log files and user data on Avaya Aura® Device Services from the Data Retention page.

Data retention — log files

Avaya Aura® Device Services encrypts all log files that can contain personal information if they are older than the configured retention period.

Data retention — Cassandra database

When a user is deleted from data sources, such as the enterprise LDAP directory, iView, or System Manager, Avaya Aura® Device Services deletes the corresponding records for that user from the Cassandra database after the retention period elapses. The process of deleting data can take up to one hour. For example, if the retention period is one day and the user is deleted from the LDAP directory today, then the user information is removed from the Cassandra database within 24 hours.

Data encryption

You can enable or disable data encryption when deploying the Avaya Aura® Device Services OVA. When data encryption is enabled, all operational data and log files are encrypted.

You can only enable data encryption on Avaya Aura® Device Services if you use Avaya Solutions Platform or a VMware Virtualized Environment. For software-only deployments, you must enable data encryption on the virtualization platform itself. For more information about enabling data

encryption on Amazon Web Services, see [How to Protect Data at Rest with Amazon EC2 Instance Store Encryption](#).

Once data encryption is enabled, you cannot disable it using the configuration utility or the Avaya Aura® Device Services administration portal. To disable data encryption, you must redeploy the Avaya Aura® Device Services OVA.

If you enabled data encryption and selected the **Require Encryption Pass-Phrase at Boot-Time** option, then you will need to enter the data encryption passphrase after every Avaya Aura® Device Services reboot. If you do not select this option, Avaya Aura® Device Services enables the local key store to store encryption keys, so you do not need to enter the passphrase manually. However, this is a less secure solution. Alternatively, you can set up a remote key server to store encryption keys.

Encryption of Avaya Aura® Device Services partitions

When you enable data encryption for Avaya Aura® Device Services, the following partitions are encrypted:

- sdb: /var/log/Avaya
- sdc: /media/data
- sdd: /media/cassandra

The sda boot disk is always unencrypted.

Data encryption management

After deploying the Avaya Aura® Device Services OVA with data encryption enabled, you can manage data encryption settings using system layer commands. For information about managing data encryption settings, see the “Security options” chapter in *Administering Avaya Aura® Device Services*.

Deployments with Avaya Aura® and without Avaya Aura®

Starting from Release 10.1.1, you can choose whether Avaya Aura® Device Services requires Avaya Aura® components, such as System Manager or Session Manager, to operate. Avaya Aura® Device Services supports the following deployment options:

- Avaya Aura® deployments, where Avaya Aura® Device Services requires the functionality that Avaya Aura® components provide, such as System Manager or Session Manager. Avaya Aura® Device Services cannot operate if your environment does not include these components.
- Deployments without Avaya Aura®, where Avaya Aura® Device Services does not require any Avaya Aura® components and operates as an independent server. Your environment can include other Avaya Aura® components, but Avaya Aura® Device Services do not use them by default.

You can choose the deployment type when installing the Avaya Aura® Device Services application on a virtual machine. The initial virtual machine deployment process remains the same for both deployment options.

! Important:

You cannot switch the deployment type after installing Avaya Aura® Device Services or when you upgrade Avaya Aura® Device Services to the latest release. To switch to another deployment type, uninstall the Avaya Aura® Device Services application and select the required deployment type when reinstalling Avaya Aura® Device Services.

Considerations and limitations

Avaya Aura® Device Services deployed in an environment without Avaya Aura® cannot use features that System Manager or Session Manager provide. Therefore, certain features work differently in deployments with Avaya Aura® and deployments without Avaya Aura®. For example:

- Identity certificates for Avaya Aura® Device Services interfaces and internode communication. In Avaya Aura® deployments, Avaya Aura® Device Services by default uses identity certificates signed by the System Manager. In deployments without Avaya Aura®, System Manager is unavailable, so you must obtain and use identity certificates provided by a third-party CA.
- Dynamic configuration service. In Avaya Aura® deployments, Avaya Aura® Device Services automatically retrieves certain endpoint configuration settings from System Manager. In deployments without Avaya Aura®, you must manually configure and publish these settings on Avaya Aura® Device Services.
- Alarms. When operating, Avaya Aura® Device Services can trigger various alarms. In Avaya Aura® deployments, you can view these alarms on System Manager. In deployments without Avaya Aura®, you must configure a separate SNMP server to view Avaya Aura® Device Services alarms.
- LDAP and contact search. In deployments without Avaya Aura®, Avaya Aura® Device Services does not perform contact search on System Manager and does not synchronize LDAP data with System Manager.

Deployments without Avaya Aura® do not support the following Avaya Aura® components and their features:

- System Manager and all its features, such as data center topology configuration or DRS synchronization.
- Session Manager and all its features, such as Session Manager Cassandra clustering.

If deployments without Avaya Aura® do not support a particular feature or require a specific setup for a feature, this document mentions it explicitly.

Chapter 3: Planning

Required skills and knowledge

Before deploying the product, ensure that you know how to do the following:

- Manage VMware or AWS deployments.
 - For VMware deployments, you must be familiar with virtual machines using vCenter and vSphere.
 - For AWS deployments, you must be familiar with Amazon Machine Images (AMIs) and with the AWS Management console. For a list of supported browsers in AWS, see https://aws.amazon.com/console/faqs/#browser_support.
- Install, deploy, and use key Avaya Aura[®] components.
- Install, set up, and use the enterprise LDAP directory.
- Use basic Linux commands.

Data required for installation

Gather and keep the following data ready before you attempt Avaya Aura[®] Device Services installation. For the latest Avaya Aura[®] Device Services compatibility matrix, see <https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=Avaya+Aura+Device+Services>.

Parameter	Notes	Value	✓
LDAP type	Avaya Aura [®] Device Services supports the following LDAP types: • Microsoft Active Directory 2012, 2016, and 2019 • Microsoft Active Directory Lightweight Directory Services (LDS) 2012 • IBM Domino Server 7.0 and 8.5.3 • Novell e-Directory 8.8 • Open LDAP 2.4.44 and 2.4.46		

Parameter	Notes	Value	✓
	• Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1.7.0) • ActiveDirectory_2022 • Azure Active Directory		
Additional LDAP parameters	• LDAP URL • Bind DN • Bind Credential • UID Attribute ID • Base Context DN • Role Filter • Role Context DN • Role Attribute ID • Role Recursion • Search Scope • User IDs for administrator role, users role, and auditor role • Active users filter For examples of LDAP parameters, see LDAP configuration on page 234 or Examples of Microsoft Active Directory LDAP property files on page 364.		
System Manager FQDN	If you deploy Avaya Aura® Device Services in an environment with Avaya Aura®, you must know the System Manager FQDN. If you deploy Avaya Aura® Device Services in an environment without Avaya Aura®, this parameter is not required.		
System Manager enrollment password	If you use System Manager for enrolling certificates, ensure that you have the enrollment password. To view the enrollment password, go to the System Manager home page, and click Security > Enrollment Password to check whether the enrollment password expired. If the Time Remaining field displays zero, the password expired and must be changed. If you deploy Avaya Aura® Device Services in an environment without Avaya Aura®, this parameter is not required.		

Parameter	Notes	Value	✓
Session Manager Asset IP	If you deploy Avaya Aura® Device Services in an environment with Avaya Aura®, you must know the Session Manager Asset IP address. To view the Session Manager Asset IP address, go to the System Manager home page, and click Session Manager > Session Manager Administration. In the Session Manager Instances tab, select a Session Manager instance, and click View. You can see the Session Manager asset IP address in the SIP Entity IP Address field. If you deploy Avaya Aura® Device Services in an environment without Avaya Aura®, this parameter is not required.		
Session Manager management IP address	If you deploy Avaya Aura® Device Services in an environment with Avaya Aura®, you must know the Session Manager management IP address. To view the Session Manager management IP address, go to the System Manager home page, and click Session Manager > Session Manager Administration. In the Session Manager Instances tab, select a Session Manager instance, and click View. You can see the Session Manager management IP address in the Management Access Point Host Name/IP field. If you deploy Avaya Aura® Device Services in an environment without Avaya Aura®, this parameter is not required.		
Keystore password	Set this when running the binary installer to any password of 6 characters or more.		
Avaya Aura® Device Services CLI user name	When running the binary installer, use the same user name that you specify when deploying the Avaya Aura® Device Services OVA.		
Avaya Aura® Device Services CLI password	While running the binary installer, use the same password that you specify while deploying the Avaya Aura® Device Services OVA.		
Number of deployment nodes	Avaya Aura® Device Services supports single node and multiple node deployments. Use the profile chosen during Session Manager deployment and the number of users you need to support to determine how many nodes you require.		
IP addresses and FQDNs	For every N Avaya Aura® Device Services nodes to be deployed, you must have N+1 IP addresses: one address for each node and one virtual IP address.		

Parameter	Notes	Value	✓
	For example, for deploying 3 nodes, you must have 4 IP addresses: one for each node and one IP for the virtual IP address.		
Third-party CA certificates	You must use identity certificates signed by a third-party Certificate Authority if you: • Deploy Avaya Aura® Device Services in an environment without Avaya Aura®. • Do not want to use identity certificates that System Manager issues in an environment Avaya Aura®. Avaya Aura® Device Services requires the following four identity certificates: • REST interface certificate. • OAMP interface certificate. • Node certificate for internode communication. ! Important: • All certificates must contain Subject Alternate Names for the FQDN of the Avaya Aura® Device Services server and the FQDN of the local Avaya Aura® Device Services node. • The Common Name of the Node certificate must contain the FQDN of the local Avaya Aura® Device Services node. In a cluster, every Avaya Aura® Device Services node has a different FQDN. You must also have root and, if used, intermediate third-party CA certificates.		

Virtual machine requirements

Supported hardware for VMware

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see <https://www.vmware.com/guides.html>.

Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)

The only supported hardware for the KVM images is Avaya Solutions Platform 130 Release 6.0.x and Avaya Solutions Platform S8300 Release 6.0.x.

Supported servers

You can deploy the Avaya Aura® Device Services OVA on the following servers:

- HP ProLiant DL360 G9
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G10
- ASP 130 Release 5.x or Dell™ PowerEdge™ R640

*** Note:**

The HP ProLiant DL360 G9, HP ProLiant DL360 G10, Dell™ PowerEdge™ R630 servers are supported on ASP 4200 Release 5.0.

Avaya Aura® Device Services support for Avaya Solutions Platform and Avaya Common Server Release 3

Avaya Aura® Device Services requires 250 GB of disk space. Avaya Common Server Release 3 (CSR3) and below servers might not have the required amount of disk space. If you are planning to deploy Avaya Aura® Device Services on CSR3 or below servers, ensure that these servers have enough disk space by installing additional physical disks to your servers. Alternatively, you can use the updated Avaya Solutions Platform (ASP) 130 Release 5.x server, which has the required amount of disk space by default.

Software requirements

Avaya Aura® supports the following software versions:

- Avaya Solutions Platform 130 (Avaya-supplied KVM on RHEL 8.10): Dell PowerEdge R660xs or R640.
- Avaya Solutions Platform S8300 (Avaya-supplied KVM on RHEL 8.10): S8300E.

*** Note:**

Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs, S8300e) is a single host server with preinstalled KVM on RHEL R8.10 software.

- Customer-provided Virtualized Environment offer supports the following software versions:
 - VMware® vSphere ESXi 7.0 or 8.0
 - VMware® vCenter Server 7.0 or 8.0

To view compatibility with other solution releases, see Broadcom website (formerly VMware) and search for VMware Product Interoperability Matrix.

- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.

*** Note:**

- Avaya Aura® Release 10.2 and later does not support vSphere ESXi 6.7.
- Avaya Aura® Release 10.1 and later does not support vSphere ESXi 6.0 and 6.5.
- Avaya Aura® Release 8.1.x and later supports ASP R6.0.x (KVM on RHEL 8.10) hypervisor.

Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications:

ESXi version	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 5.0	N	N	N	N	N
ESXi 5.1	N	N	N	N	N
ESXi 5.5	Y	N	N	N	N
ESXi 6.0	Y	Y	Y	N	N
ESXi 6.5	Y	Y	Y	N	N
ESXi 6.7	N	Y	Y	Y	N
ESXi 7.0	N	N	Starting from Release 8.1.3: Y	Y	Y
ESXi 8.0	N	N	N	N	Y

*** Note:**

- Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 R6.0 supports Avaya-supplied KVM on RHEL 8.10. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell or RHEL website, this results in an unsupported configuration.
- Avaya Aura® Release 10.2.x supports VMware 8.0, VMware 8.0 Update 2, and VMware 8.0 Update 3.

Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the Broadcom website (formerly VMware).
- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.

For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.
- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only

support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.

- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.
- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0 Update 3.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0, ESXi 8.0 Update 2 (U2) deployments, and ESXi 8.0 Update 3 (U3) deployments.

Supported ASP Server

The following table lists the supported KVM versions of Avaya Aura® applications:

Avaya Solutions Platform	ASP Release Version	Avaya Aura® Release			
		8.1.x	10.1.x	10.2.x	10.3.x
KVM Release 8.10	ASP R6.0.x	Y	Y	Y	Y
KVM Release 9.6	ASP R7.0.x				Y

* Note:

- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x are Avaya-supplied KVM on RHEL 8.10. The Avaya Solutions Platform 130 is Dell R660xs. The Dell R660xs only ships with and supports KVM on RHEL 8.10. The initial Release of Avaya Solutions Platform 130 Release 4.0 supported Avaya-supplied ESXi 6.5 and Avaya Solutions Platform 130/S8300 R5.x supported Avaya-supplied ESXi 7.0.
- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x software is KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R660xs server only supports KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R640 and the ASP S8300 S8300E support both ESXi 7.0 and KVM on RHEL 8.10. Avaya Solutions Platform 130 Dell R640 Release 4.0 supported ESXi 6.5
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R660xs) is a single host server with a preinstalled KVM on RHEL 8.10 software.
Avaya Solutions Platform 130 Release 7.0 (Dell PowerEdge R660xs) is a single host server with a preinstalled KVM on software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) 8.10 for Communication Manager and Branch Session Manager.

- Avaya Solutions Platform130 Release 6.0.x (Dell PowerEdge R660xs, S8300E) is a single host server with preinstalled KVM on RHEL 8.10 software.
- Avaya Solutions Platform130 Release 7.0.x (Dell PowerEdge R660xs, S8300E) is a single host server with preinstalled KVM on RHEL 9.6 software.
- With the introduction of Avaya Solutions Platform R6.0.x there is no longer a specific license key needed as was present with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Avaya Aura® Device Services virtual machine resource requirements

The virtual machine resource requirements apply both to OVA-based and software-only deployment options.

	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
Session Manager Device Footprint ¹	Up to 2000 devices	2000 to 4500 devices	4500 to 7000 devices	7000 to 10,000 devices	10,000 to 23,300 devices
AADS device footprints ²	Up to 2000 devices	2000 to 4500 devices	4500 to 7000 devices	7000 to 10,000 devices	10,000 to 23,300 devices ³
CPU Minimum	2.1 GHz, Hyper-threaded				
vCPUs	6	8	8	10	12
CPU Reservation (MHz)	6900	9200	9200	11,500	13,800
Memory Reservation (MB)	9216	10,240	12,288	13,312	15,360
Disk space (GB)	250				

For information about Session Manager capacities and specifications, see *Avaya Aura® Session Manager Overview and Specification*.

¹ Does not apply if you deploy Avaya Aura® Device Services in an environment without Avaya Aura®.

² If users utilize MDA and login to multiple devices, then the number of users that AADS support will differ. For example, if a user login to two devices, then AADS will support half the capacity of the footprint.

³ AADS Profile 5 Server can process 22-26 requests per second for each AADS node.

Requirements for a host machine for Hyper-V deployments

The following table lists the requirements for a computer that will host a Microsoft Hyper-V virtual machine with Avaya Aura® Device Services:

Resource	Requirement
RAM memory	13 to 19 GB: • 4 GB to operate the Hyper-V host. • 9 to 15 GB depending on the Avaya Aura® Device Services resource profile that you are planning to use.
Hard disk	At least 252 GB of free disk space: • 250 GB for an Avaya Aura® Device Services virtual machine. • 2 GB to operate the Hyper-V host.
CPU	The minimum CPU speed is 2.1 GHz per core. The number of vCPUs that your physical CPU provides must be greater than the number of vCPUs required by the resource profile that you are planning to use. You can find the number of vCPUs that your physical CPU can provide using the following formula: $(\text{Threads} \times \text{Cores}) \times \text{Physical CPU} = \text{Number of vCPU}$ For example, the number of vCPUs for a 4 cores / 8 threads physical CPU is $(8 \text{ threads} \times 4 \text{ cores}) \times 1 \text{ CPU} = 32 \text{ vCPU}$
NICs	Two NIC ports: • One NIC port for Hyper-V access and management. • One NIC port for routing the virtual machine network.
Operating system	The following 64-bit operating systems are supported: • Windows: - Windows 8.1 - Windows 10 • Windows Server: - Windows Server 2008 SP2 or later For more information about the supported operating systems, see Supported Windows guest operating systems for Hyper-V on Windows Server .

Related links

[Avaya Aura Device Services virtual machine resource requirements](#) on page 34

Resource profile specifications for Microsoft Azure virtual machines

The following table lists resource profile specifications for Microsoft Azure virtual machines.

	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
AADS device footprints	Up to 2000 devices	2000 to 4500 devices	4500 to 7000 devices	7000 to 10,000 devices	10,000 to 23,300 devices
Microsoft Azure virtual machine size	D8s_v3				
vCPUs	8				
Memory (GB)	32				
Disk space (GB)	250 (Standard HDD)  Important: Microsoft Azure virtual machines might not have the required amount of disk space by default. Ensure that virtual machines have enough disk space by purchasing additional disk space separately.  Note: Avaya Aura® Device Services uses four disks: • One OS disk. • Three data disks.				
Input/output operations per second for data disks	500				

Resource profile specifications for Google Cloud Platform virtual machines

The following table lists resource profile specifications for Google Cloud Platform virtual machines.

	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
AADS device footprints	Up to 2000 devices	2000 to 4500 devices	4500 to 7000 devices	7000 to 10,000 devices	10,000 to 23,300 devices
Google Cloud Platform virtual machine size	c2-standard-8 (8 vCPUs and 32 GB RAM)			c2-standard-16 (16 vCPU and 64 GB RAM)	
vCPUs	8	8	8	16	16
Memory (GB)	32	32	32	64	64
Disk space (GB)	250  Note: Avaya Aura® Device Services uses four disks: • One OS disk. • Three data disks.				

	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
Input/output operations per second for data disks	500				

Resources profile specifications for Avaya Aura® Device Services on Amazon Web Services

The following table outlines the profiles created by the CloudFormation template generators. You can use the CloudFormation template generation tool to create a template for the required profile. The template contains the computing and networking resources required for the profile.

Profile	Service size	AWS instance type	AWS vCPUs	AWS Memory (GB)
AADS2100	4200 end points	c4.2xlarge	8	15
		c5.2xlarge	8	16
		c5.18xlarge	72	144
		c5a.2xlarge	8	16
		c5a.4xlarge	16	32
		c5n.2xlarge	8	21
		c5n.4xlarge	16	42
AADS5240	13,900 end points	c4.2xlarge	8	15
		c5.2xlarge	8	16
		c5.18xlarge	72	144
		c5a.2xlarge	8	16
		c5a.4xlarge	16	32
		c5n.2xlarge	8	21
		c5n.4xlarge	16	42

Virtual disk volume specifications

The following table shows the file system layout.

Disk Volume	Volume Size (GiB)			
	Disk 1 (sda)	Disk 2 (sdb)	Disk 3 (sdc)	Disk 4 (sdd)
/	17.30			
home	4.00			
/opt/Avaya	14.70			

Disk Volume	Volume Size (GiB)			
	Disk 1 (sda)	Disk 2 (sdb)	Disk 3 (sdc)	Disk 4 (sdd)
/tmp	14.90			
/var	8.5			
/var/log	5.0			
/var/log/audit	6.0			
swap	4.0			
/var/log/Avaya		70.0		
/media/data			40.0	
/media/cassandra				10.0
Reserve	50.1			
Total for disk	124.4	70.0	40.0	10.0
Total disk size	244.4			

After Avaya Aura® Device Services installation, Disk 1 has approximately 50GiB of free space. This space is reserved and can be used to allocate free disk space to a specific disk volume to address unexpected disk engineering issues. For more information about allocating free space to disk volumes, see “Allocating unused disk space to logical volumes” in *Administering Avaya Aura® Device Services*.

Networking considerations for Amazon Web Services

There are some limitations for establishing public internet VPNs and direct connections into AWS. For more information about Amazon VPC Limits, see the AWS documentation at <https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html>.

! Important:

Use a direct connection along with a private WAN connection with Service Level Agreement (SLA) measures to ensure that the network quality is appropriate for signaling and voice traffic.

Avaya is not responsible for network connections between AWS and the customer premises.

When you deploy Avaya Aura® Device Services in an AWS environment, also deploy a local LDAP server in AWS. This LDAP server is a replica server that synchronizes content from a master LDAP server within the enterprise. To reduce latency for authentication and directory lookup operations, this LDAP server must be collocated with Avaya Aura® Device Services in the same AWS region.

Connection types

You can connect applications in a hybrid network on the Amazon VPC in the following ways:

Connection type	Resource
VPN connection	For information about VPN connections, see: https://docs.aws.amazon.com/vpc/
Direct connection	For information about AWS direct connections, see: https://aws.amazon.com/directconnect/ .

Considerations for migrating from a standalone to a cluster environment

If you choose to install a standalone Avaya Aura® Device Services, but later decide to move to a cluster that uses a virtual IP, the original standalone node needs to be reconfigured with the original virtual IP as the front-end FQDN.

To avoid this scenario, you can plan in advance and add a virtual IP for the front-end FQDN of the standalone node. This would make the transition from a standalone node to a cluster easier in the future.

Related links

[Deploying the Avaya Aura Device Services OVA using the Host Client connected directly to the ESXi host](#) on page 83

[Adding an Avaya Aura Device Services instance to System Manager](#) on page 270

[Considerations for large cluster deployments](#) on page 40

[Avaya Aura Device Services cluster installation](#) on page 198

System Manager geographic redundancy

Avaya Aura® Device Services does not support the System Manager geographic redundancy mode. If the primary System Manager fails, Avaya Aura® Device Services does *not* switch to the secondary System Manager automatically. During the System Manager outage period, all operations from Avaya Aura® Device Services to System Manager, such as enrollment, DRS synchronization, or certificate management operations, are unavailable. In certain circumstances, for example, immediately after installation and the first restart, Avaya Aura® Device Services is not available until the primary System Manager is restored.

If you need to use Avaya Aura® Device Services before the primary System Manager is back online, you must enroll Avaya Aura® Device Services against the secondary System Manager. When the primary System Manager is back online, you must manually re-enroll Avaya Aura® Device Services against the primary System Manager.

*** Note:**

Avaya Aura® Device Services does not use System Manager when deployed in an environment without Avaya Aura®. Therefore, this operation is not applicable for deployments without Avaya Aura®.

Related links

[Primary System Manager fails](#) on page 339

Considerations for large cluster deployments

Avaya Aura® Device Services supports a single cluster deployment. A cluster can include up to 14 Avaya Aura® Device Services servers or nodes. All nodes must be in the same network.

By default, Avaya Aura® Device Services uses an on-board nginx load balancer. For IP failover and high-availability purposes, nginx uses the Keepalived service and the Virtual Router Redundancy Protocol (VRRP). This solution requires that the cluster virtual IP address and the two IP addresses for the load balancer nodes must be in the same subnet.

The on-board load balancer only supports small deployments of up to 20,000 devices when Avaya Aura® Device Services is deployed in a single data center.

In larger or geographically distributed deployments, however, you must use an external load balancer instead of the default nginx load balancer.

For these larger cluster deployments, consider the following:

- Configuring a data center topology in System Manager.
- Minimizing the network latency between Avaya Aura® Device Services and other components.

Related links

[External load balancer requirements](#) on page 50

[Port configuration for an external load balancer](#) on page 52

[Deploying the Avaya Aura Device Services OVA using the Host Client connected directly to the ESXi host](#) on page 83

[Adding an Avaya Aura Device Services instance to System Manager](#) on page 270

[Avaya Aura Device Services cluster installation](#) on page 198

[Utility Server deployment considerations](#) on page 42

Data center topology configuration in System Manager

In System Manager, you can create data centers that represent the actual physical data center topology of the Session Manager network. The data center topology is used by the Cassandra database cluster to make routing decisions when reading or writing data to the database. When a Session Manager instance within a particular data center sends a request to the Cassandra cluster, Cassandra performs the request using the Cassandra cluster nodes within that data center whenever possible.

*** Note:**

If you deploy Avaya Aura® Device Services in an environment without Avaya Aura®, you cannot configure the data center topology because Avaya Aura® Device Services does not use System Manager.

Related links

[Adding a data center](#) on page 48

Network latency requirements

Minimize the network latency between Avaya Aura® Device Services and the other elements it interacts with.

Latency between Avaya Aura® Device Services and Session Manager

In addition to its own Cassandra databases, Avaya Aura® Device Services also uses Cassandra databases on Session Manager. Therefore, the network latency between Avaya Aura® Device Services and Session Manager must always be less than 5 milliseconds. To achieve this, co-locate the Avaya Aura® Device Services and paired Session Manager in the same building, if possible.

This requirement is not applicable for deployments without Avaya Aura®.

Latency between Avaya Aura® Device Services and LDAP

The network latency between Avaya Aura® Device Services and the LDAP server must always be less than 75 milliseconds. Higher latency values can result in loss of service. The ideal network latency is less than 5 milliseconds.

Considerations for geographically distributed systems

When you deploy a geographically distributed system, consider the following:

- Users in a specific region resolve the Avaya Aura® Device Services cluster FQDN to a load balancer that is deployed in that region. The region-specific load balancer must be configured to route requests to the Avaya Aura® Device Services cluster FQDN to the Avaya Aura® Device Services nodes within that region only.
- GSLB must route requests to the Avaya Aura® Device Services service port which is by default 443.
- If you use the Utility Server on Avaya Aura® Device Services, you must use an additional external load balancer for the Utility Server virtual IP address.
- On the Avaya Aura® Device Services administration portal, you *must* enable the use of an external load balancer. For details, see *Administering Avaya Aura® Device Services*.

Related links

[Geographically distributed system topology](#) on page 20

[Utility Server deployment considerations](#) on page 42

Utility Server deployment considerations

The Utility Server is an optional component that you can enable when deploying Avaya Aura® Device Services and that offers the file server and firmware management functionality. The Utility Server has its own FQDN and IP address, which is also called the Utility Server virtual IP address (VIP). If you plan to deploy an Avaya Aura® Device Services cluster, consider the following:

- If you deploy a Avaya Aura® Device Services in multiple data centers or in different subnets, you must use a separate external load balancer for the Utility Server VIP in addition to a load balancer for Avaya Aura® Device Services nodes.

 Note:

For non-cloud deployments, if you deploy a Avaya Aura® Device Services in multiple data centers, a load balancer for the Utility Server VIP must be on the same level as the Global Server Load Balancer for Avaya Aura® Device Services nodes.

Related links

[Considerations for large cluster deployments](#) on page 40

[Considerations for geographically distributed systems](#) on page 41

[Geographically distributed system topology](#) on page 20

LDAP authentication domain requirements

If you use a single authentication directory, ensure that all users are in a single authentication domain. This is not required if you use multiple authentication directories.

The first LDAP domain added to Avaya Aura® Device Services is the server that handles user authentication and role assignment. All users that require authentication must be located in this LDAP domain and must be able to authenticate with it.

Third-party CA-signed certificates

If you do not want to use System Manager for certificate management, Avaya Aura® Device Services enables you to use certificates specific to your organization and have the certificates signed by a third-party private or public certificate authority. If you deploy Avaya Aura® Device Services in an environment without Avaya Aura®, you *must* use third-party certificates because Avaya Aura® Device Services cannot use System Manager for certificate management.

You can import third-party CA certificates either during or after Avaya Aura® Device Services installation.

- For more information about certificates required in an Avaya Aura® environment, see [Certificates required for an Avaya Aura environment](#) on page 43.
- For more information about certificates required in an environment without Avaya Aura®, see [Certificates required for an environment without Avaya Aura](#) on page 45.

If you use third-party CA certificates, you must import third-party root and intermediate CA certificates into the trust stores of each server that interact with Avaya Aura® Device Services, including the following:

- System Manager
- Session Manager
- Avaya Aura® Session Border Controller
- Avaya Meetings Server

If you use System Manager for certificate management, Avaya Aura® Device Services does not require any additional third-party certificates.

Related links

[Certificates required for an Avaya Aura environment](#) on page 43

[Certificates required for an environment without Avaya Aura](#) on page 45

[Installing Avaya Aura Device Services](#) on page 179

Certificates required for an Avaya Aura® environment

If you plan to deploy Avaya Aura® Device Services in an Avaya Aura® environment and want to use third-party certificates specific to your organization, obtain the following certificates before installing Avaya Aura® Device Services:

- The System Manager root CA certificate in PEM format in a file with the `smgrca.pem` file name.
- The third-party root CA certificate in the PEM format in a file with the `root.pem` file name.
- One or more intermediate CA certificates in the PEM format concatenated into a single certificate chain in a file with the `intermediate.pem` file name.
- An identity certificate signed by the third-party CA for Avaya Aura® Device Services. The certificate must meet the following requirements:
 - The certificate format is PEM or PKCS12.
 - The Common Name parameter contains the external load balancer FQDN or the Avaya Aura® Device Services virtual IP FQDN.
 - The Subject Alternative Names parameter contains the following entries:
 - FQDNs of all Avaya Aura® Device Services nodes in your deployment.
 - If you want to use the Utility Server: The virtual FQDN of the Utility Server.



Note:

In cloud environments, such as Microsoft Azure, Google Cloud Platform, or AWS, this is the FQDN of the external load balancer.

- If you want to use the onboard Open LDAP: the `localhost.localdomain` record for IPv4 and the `localhost6.localdomain` record for IPv6.

- An identity certificate signed by the third-party CA for System Manager. The certificate must meet the following requirements:
 - The certificate format is PEM or PKCS12.
 - The Common Name parameter contains the virtual FQDN of System Manager.

 Note:

You must use this FQDN when configuring System Manager settings during Avaya Aura® Device Services installation.

You must add this certificate to System Manager before starting to install Avaya Aura® Device Services. Otherwise, Avaya Aura® Device Services installation will fail.

- A third-party CA-signed identity certificate chain to be used for Avaya Aura® Device Services. The certificate chain must be in the PKCS12 format in a file with the `identity.p12` file name. The chain must consist of the identity certificate followed by all intermediate CA certificates in a reverse chain order.

Most third-party CAs use root and intermediate CAs to sign identity certificates. As a result, you must import identity and trust certificate chains to Avaya Aura® Device Services in the PKCS12 format.

Related links

[Third-party CA-signed certificates](#) on page 42

[Configuring third-party identity certificates for System Manager](#) on page 44

Configuring third-party identity certificates for System Manager

About this task

In an Avaya Aura® deployment, you can use identity certificates signed by a third-party CA for Avaya Aura® Device Services. If you use certificates signed by a third-party CA, ensure that System Manager also uses an identity certificate signed by the same third-party CA. If System Manager does not have this certificate, Avaya Aura® Device Services installation will fail.

The third-party CA identity certificate for System Manager must meet the following requirements:

- The certificate format is PKCS12.
- The Common Name attribute is the System Manager virtual FQDN.

For more information about configuring identity certificates on System Manager, see “Managing identity certificates” in *Administering Avaya Aura® System Manager*.

Before you begin

Obtain an identity certificate for System Manager from the third-party CA. For more information about obtaining identity certificates, see the documentation for your third-party CA.

Procedure

1. Log in to the System Manager web console.
2. On the System Manager web console, click **Services > Inventory > Manage Elements**.
3. On the Manage Elements page, select **System Manager** and click **More Actions > Manage Identity Certificates**.

4. On the Manage Identity Certificates page, select **container_tls** and replace the existing certificate with the identity certificate for System Manager you obtained in step 1.
5. To reboot System Manager and apply the changes, do the following:
 - a. On the System Manager web console, click **Services > Shutdown > Shutdown System Manager**.
 - b. In Initiate Reboot, click **Reboot System Manager**.
 - c. In the confirmation window, click **Yes**.

Related links

[Certificates required for an Avaya Aura environment](#) on page 43

Certificates required for an environment without Avaya Aura®

If you plan to deploy Avaya Aura® Device Services in an environment without Avaya Aura®, obtain the following certificates before installing Avaya Aura® Device Services:

- The third-party root CA certificate in the PEM format in a file with the `root.pem` file name.
- One or more intermediate CA certificates in the PEM format concatenated into a single certificate chain in a file with the `intermediate.pem` file name.
- An identity certificate signed by the CA. The Common Name and Subject Alternative Names parameters of the certificate must contain the following values:
 - The certificate format is PEM or PKCS12.
 - Common Name: The external load balancer FQDN or the Avaya Aura® Device Services virtual IP FQDN.
 - Subject Alternative Names:
 - FQDNs of all Avaya Aura® Device Services nodes in your deployment.
 - If you want to use the Utility Server: The virtual FQDN of the Utility Server.

Note:

In cloud environments, such as Microsoft Azure, Google Cloud Platform, or AWS, this is the FQDN of the external load balancer.

- If you want to use the onboard Open LDAP: the `localhost.localdomain` record for IPv4 and the `localhost6.localdomain` record for IPv6.
- A third-party CA-signed identity certificate chain to be used for Avaya Aura® Device Services. The certificate chain must be in the PKCS12 format in a file with the `identity.p12` file name. The chain must consist of the identity certificate followed by all intermediate CA certificates in a reverse chain order.

Most third-party CAs use root and intermediate CAs to sign identity certificates. As a result, you must import identity and trust certificate chains to Avaya Aura® Device Services in the PKCS12 format.

Related links

[Third-party CA-signed certificates](#) on page 42

Cassandra clustering configuration on Avaya Aura® Device Services

In cluster deployments, Cassandra clustering provides redundant storage of SIP device data on Avaya Aura® Device Services nodes. To further improve resiliency, you can assign each node to a specific Cassandra datacenter. A datacenter is a logical grouping of Avaya Aura® Device Services nodes within the cluster. When you use multiple datacenters, the Cassandra database is replicated on the nodes as follows:

- Each Cassandra datacenter configured in your deployment has its own replica of the Cassandra database.
- Within a Cassandra datacenter, the database is replicated on multiple nodes. The exact number of copies depends on the number of nodes in the datacenter.

Avaya Aura® Device Services automatically configures and maintains the replication settings, such as the replication factor, for each datacenter.

By default, all cluster nodes belong to the default Cassandra datacenter, which has the “dc1” name. To assign a node to another datacenter, specify the datacenter name when installing the node or at any time after installation. If you do not select a datacenter during installation, Avaya Aura® Device Services assigns the node to the default datacenter. If required, you can move nodes between datacenters.

Note:

A datacenter is a virtual entity. Therefore, to create a new datacenter, you only need to specify a unique datacenter name when installing or configuring a node. Avaya Aura® Device Services automatically updates the clustering configuration as appropriate.

By default, Avaya Aura® Device Services synchronizes the data between the databases weekly. You can schedule the synchronization on a specific day of the week or disable the synchronization.

Recommendations for configuring Cassandra clustering

Avaya recommends that you:

- Use two Cassandra datacenters in your deployment.
You can configure more than two datacenters, but it might not provide additional redundancy compared to the two datacenters setup.
- Distribute Avaya Aura® Device Services nodes evenly between the Cassandra datacenters to balance the load on each datacenter.
- Configure an additional seed node so that:
 - The primary seed node belongs to one datacenter.
 - The additional seed node belongs to another datacenter.

This approach improves bootstrapping the gossip process for new nodes joining the cluster. When you add a new node to a datacenter, this node communicates with the seed node of the datacenter instead of the main seed node of the cluster.

- In a geographically distributed deployment, assign Avaya Aura® Device Services nodes to Cassandra datacenters based on node location. Thus, you minimize the network latency in internode communications.

Considerations

If you upgrade to Release 10.2.x from a previous release, all nodes in your deployment belong to the default “dc1” datacenter. You can configure datacenters as appropriate on the Clustering configuration page of the configuration utility. For more information about re-assigning nodes to datacenters, see Chapter “Cassandra clustering configuration on Avaya Aura® Device Services” in *Administering Avaya Aura® Device Services*.

Cassandra clustering and data replication configuration on System Manager

Cassandra clustering provides redundant storage of SIP device data on instances of Session Manager. Starting from Avaya Aura® Release 8.0, Cassandra clustering is enabled permanently.

If you use an Avaya Aura® Device Services cluster, you must configure one or more data centers on System Manager. Cassandra data distribution uses the data center settings to identify the Session Manager instances that are within the same data center. Every Session Manager instance that is paired with Avaya Aura® Device Services must be a part of a data center. Session Manager instances that are not paired with Avaya Aura® Device Services can optionally be a part of data center. Session Manager instances should be assigned to data center based on the system topology. The best redundancy is obtained when two or more Session Managers are assigned to each data center.

Checklist for Cassandra clustering configuration on Session Manager

No.	Task	Notes	✓
1	Create data centers.	See Adding a data center on page 48.	
2	Assign co-located Session Managers to the same data center.	See Assigning Session Manager to a data center on System Manager 8.x on page 48 or Assigning Session Manager to a data center on System Manager 10.x or later on page 49, depending on the version you use.	
3	After all Avaya Aura® Device Services nodes are deployed, add the Avaya Aura® Device Services instances to the System Manager inventory.	See Adding an Avaya Aura Device Services instance to System Manager on page 270.	

No.	Task	Notes	✓
4	Pair a Session Manager instance with an Avaya Aura® Device Services node.	See Pairing Session Manager with an Avaya Aura Device Services node on page 272.	

Adding a data center

About this task

Data center is an entity that is used to logically combine Session Managers deployed in the same location. If you use an Avaya Aura® Device Services cluster, then every Session Manager instance that is paired with Avaya Aura® Device Services must be a part of a data center.

In geographically distributed deployments, you usually create a data center for each location in your deployment.

Procedure

1. On the System Manager web console, click **Elements > Session Manager > Session Manager Administration > Groups**.
2. On the **Session Manager Groups** tab, click **New > New Data Center**.
System Manager displays the New Session Manager Group page.
3. In the **Name** field, type the data center name.
4. In the **Description** field, type a description about the data center.
You can assign a Session Manager to the data center while or after creating a data center. For Session Manager assignment, see *Assigning Session Manager to a data center*.
5. Click **Commit**.
System Manager displays the Confirm Data Center assignments page.
6. Verify the data center assignment.
7. Click **Confirm**.

Next steps

Assign Session Manager to the data center.

Related links

[Data center topology configuration in System Manager](#) on page 40

Assigning Session Manager to a data center on System Manager 8.x

About this task

You can assign a Session Manager instance to a data center while adding a Session Manager instance or after adding the Session Manager instance using the **Edit** button.

Before you begin

Add data centers using the System Manager web console.

Procedure

1. On the System Manager web console, click **Elements > Session Manager > System Status > User Data Storage**.
2. On the User Data Storage page, click the **Data Center** tab.
3. Select a data center and click **Edit**.

System Manager displays the Edit Data Center page.

4. To assign Session Manager to data center, under the SMs unassigned or assigned to other Data Center section, from the **Data Center** drop-down list, select the data center name.
 - If you select the same data center name for Session Manager, System Manager refreshes the page and displays the assigned data center under the SMs in Data Center section.
 - If you select the other data center name for Session Manager, System Manager displays the assigned data center under the SMs unassigned or assigned to other Data Center section.
5. Click **Commit**.

System Manager displays the Confirm Data Center assignments page.
6. Verify the data center and Session Manager assignment.
7. Click **Confirm**.

Related links

[Adding a data center](#) on page 48

[Assigning Session Manager to a data center on System Manager 10.x or later](#) on page 49

Assigning Session Manager to a data center on System Manager 10.x or later

About this task

You can assign a Session Manager instance to a data center while adding a Session Manager instance or after adding the Session Manager instance using the **Edit** button.

Before you begin

Add data centers using the System Manager web console.

Procedure

1. On the System Manager web console, click **Elements > Session Manager > Session Manager Administration > Groups**.
2. On the **Session Manager Groups** tab, select a data center and click **Edit**.

System Manager displays the Edit Session Manager Group page.

3. To assign Session Manager to a data center, under the SMs unassigned or assigned to other Data Center section, select the data center name from the **Data Center** list.
 - If you select the same data center name for Session Manager, System Manager refreshes the page and displays the assigned data center under the SMs in Data Center section.
 - If you select another data center name for Session Manager, System Manager displays the assigned data center under the SMs unassigned or assigned to other Data Center section.
4. Click **Commit**.

System Manager displays the Confirm Data Center assignments page.
5. Verify the data center and Session Manager assignment.
6. Click **Confirm**.

Related links

[Assigning Session Manager to a data center on System Manager 8.x](#) on page 48

[Adding a data center](#) on page 48

External load balancer requirements

If you are planning to use an external load balancer, it must comply with the following requirements:

Requirement	Description
If you are deploying a geographically distributed system, the HTTP Global Server Load Balancing (GSLB) must route requests basing on the user's location.	The GSLB functionality can be part of the DNS server and not the load balancer. In this case, however, the DNS server must be able to route requests to different locations based on the location of the browser that initiated the request.
The HTTP Load balancer must support session affinity. Session affinity means that all requests from the client are always routed to the same server.	• Session affinity is based on cookies. • The reverse proxy inserts a cookie to responses for incoming HTTP requests and routes subsequent requests that contain the same cookie to the same Avaya Aura[®] Device Services server. • This feature is also known as sticky sessions. Do not use IP-based sticky sessions because this might affect load balancing.

Requirement	Description
The HTTP load balancer must support web sockets.	- The load balancer must not block web socket requests and must relay the web socket connections between the client and the server. - HTTP request timeout must be configurable. You must be able to configure the timeout value to the maximum duration of the conference to prevent it from timing out the web socket session.
The HTTP load balancer must support URL routing.	This requirement is only needed if you want to reuse a load balancer port. The load balancer must be able to route requests based on the request URL. Requests that start with <code>/acs</code> for Avaya Aura® Device Services services and <code>/auth</code> for keycloak services must be routed to Avaya Aura® Device Services.
The HTTP load balancer must support TLS 1.2 or TLS 1.3.	Avaya Aura® Device Services supports TLS versions 1.2 and 1.3. The load balancer must support the TLS version that you plan to use in your deployment. Some services might not support TLS versions other than 1.2.
The HTTP load balancer must support at least some of the listed ciphers when interacting with back-end services.	The list of ciphers: - ECDHE-RSA-AES128-GCM-SHA256 - ECDHE-ECDSA-AES128-GCM-SHA256 - ECDHE-ECDSA-AES256-GCM-SHA384 - ECDHE-RSA-AES128-SHA256 - ECDHE-ECDSA-AES128-SHA256 - ECDHE-RSA-AES128-SHA - ECDHE-ECDSA-AES128-SHA - AES128-GCM-SHA256 - AES256-GCM-SHA384 - AES128-SHA
The HTTP load balancer must be able to use TCP health checks.	The load balancer must be able to perform health checks of Avaya Aura® Device Services servers using TCP responses. For health checks, the load balancer must use the following URL: <code>http://<AADS_FQDN>:8457/health</code> To avoid leaving multiple TCP sockets opened, you must be able to configure TCP health checks to half-opened connections.
The external HTTP load balancer must relay the client certificates.	This requirement is only needed for authenticating clients using client identity certificates.

Related links

[Geographically distributed system topology](#) on page 20

[Considerations for geographically distributed systems](#) on page 41

Nginx load balancer requirements

If you use Nginx as an external load balancer, ensure the following:

- The network latency between Avaya Aura® Device Services and the associated Session Manager is less than 5 milliseconds.
- The Avaya Aura® Device Services servers, load balancers, and virtual IP addresses are in the same subnet.

Port configuration for an external load balancer

If you are planning to use an external load balancer, you must configure the external load balancer and firewall ports as follows:

- The external load balancer must listen for requests on the Avaya Aura® Device Services service port, which is 443 by default.
- On the Avaya Aura® Device Services administration portal, you *must* enable the use of an external load balancer. For details, see *Administering Avaya Aura® Device Services*.
- The external load balancer must send requests that arrive on the Avaya Aura® Device Services service port to Avaya Aura® Device Services servers in the cluster on the service port. As a result, the service port must be reachable from the load balancer through firewalls.
- The external load balancer must listen to port 8440 for requests from the Apple Push Notification service.

For more information about Avaya Aura® Device Services port usage, see *Port Matrix for Avaya Aura® Device Services*. This document is available on the [Avaya Support website](#). You might need to be logged in to access the document.

Related links

[Considerations for large cluster deployments](#) on page 40

Prerequisites for SSO configuration

Single Sign-On is an authorization flow that enables users to authenticate using a combination of enterprise credentials and other factors that the enterprise has chosen, such as multi-factor authentication. You can configure Avaya Aura® Device Services to support SSO, so that your enterprise users can log in to services, such as Avaya Workspaces, Avaya Workplace Client, Avaya Meeting Scheduler Outlook Add-in, Avaya Meetings Server Unified Portal, Avaya Agent for Desktop, or Avaya Calling for Microsoft Teams, using their enterprise credentials.

Each SSO protocol Avaya Aura® Device Services supports, that is SAML v2.0 and OAuth2 SSO, Device Authorization Flow, and Workspaces SSO, have different set of prerequisites to fulfill. Read the prerequisites corresponding to the SSO flow you are implementing before configuring Avaya Aura® Device Services.

! Important:

You can only enable OAuth when you are installing or upgrading Avaya Aura® Device Services. You cannot enable OAuth at a later point.

Related links

[OAuth configuration](#) on page 257

Prerequisites for SAML v2.0 and OAuth2 SSO configuration

You can configure Avaya Aura® Device Services to support SAML v2.0 and OAuth2 SSO, so that your enterprise users can log in to services, such as, Avaya Workplace Client, Avaya Meeting Scheduler Outlook Add-in, Avaya Meetings Server Unified Portal, Avaya Agent for Desktop, or Avaya Calling for Microsoft Teams, using their enterprise credentials.

Before configuring SSO authentication on Avaya Aura® Device Services, gather the following information and configure an SSO application on the identity provider that you are planning to use:

SAML v2.0

- In a cluster deployment, if Avaya Aura® Device Services nodes are located in multiple data centers, ensure that port 7600 is open in the data centers for subnets where cluster nodes are deployed.
- Determine the attribute names that the identity provider sends in SAML responses for the following:
 - First name
 - Last name
 - Email address
 - Group/Role indicator
- Configure the NameID format. Avaya Aura® Device Services uses the emailAddress format for NameID.
- Ensure that the identity provider supports the Service Provider-initiated (SP-initiated) flow and the SP-initiated flow is enabled and configured on the identity provider.
- Configure an SSO application on the third-party identity provider's side.
- Obtain the SAML v2.0 identity provider's IDPSSODescriptor metadata file.

You can obtain this file from the third-party identity provider.

You must import this metadata file into Keycloak when enabling SSO authentication support on Avaya Aura® Device Services or after Avaya Aura® Device Services is installed.

- Obtain the SPSSODescriptor metadata file.

You can obtain this file from the following URL after the identity provider is added to Keycloak:

```
https://<AADS_FQDN>:<AADS_PORT>/auth/realms/SolutionRealm/broker/
<SAML_V2_PROVIDER_NAME>/endpoint/descriptor
```

For example, if the Avaya Aura® Device Services front-end FQDN is aads.company.com, the AADS front-end port is the default port 443, and you created on SAML v2.0 identity

provider on Keycloak with the name mySAMLProvider, then the URL for retrieving the SPSSODescriptor file is:

```
https://aads.company.com/auth/realms/SolutionRealm/broker/
mySAMLProvider/endpoint/descriptor
```

You can also obtain this file from the Keycloak administration portal.

Important:

If you download the SPSSODescriptor metadata file from the Keycloak administration portal, you must replace port 8445 with the Avaya Aura® Device Services front-end port in the following entries in the metadata file:

- `<AADS_FQDN>:8445/auth/realms/SolutionRealm`
- `<AADS_FQDN>:8445/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`

In these entries, AADS_FQDN is the Avaya Aura® Device Services FQDN and IDP_ALIAS is the identity provider alias.

The default front-end port is 443.

OAuth2

Currently, Avaya Aura® Device Services only supports the Office 365 OAuth2 identity provider.

- Determine the attribute names that the identity provider sends in OAuth2 token responses for the following:
 - First Name
 - Last Name
 - Email Address
 - Client ID
 - Client Secret
- Add and configure an application for SSO purposes on the Microsoft Azure portal.

Prerequisites for Device Authorization Flow configuration

The Device Authorization Flow, which is also called the device flow, enables users to use SSO on phones with limited input capabilities, such as J1xx phones. In this flow, the users provide SSO credentials for their phone on another device, such as a smartphone. The device flow does not use the embedded Keycloak service.

Before configuring SSO authentication on Avaya Aura® Device Services, do the following:

- Obtain the following data from the Avaya IAM identity provider:
 - The Avaya IAM root CA certificate.
 - The Discovery URL address and optionally, proxy server hostnames.

You require proxy server hostnames only if the hostname of the Discovery URL is not accessible from Avaya Aura® Device Services.

- The client secret and client name configured on Avaya IAM for your organization.

 Note:

The client name is mandatory and must start with "aads-" followed by a text or character. Also, configure the same client name in IAM.

Allow any combination of letters, numbers, or other characters after that.

For example:

aads-client

aads-client123

- Obtain the client ID for the phone series, such as J1XX, to configure the Device Authorization Flow.

Phone models of the same phone series have the same client ID. For example, all J1XX phones have client ID aoc-j100-cli.

- Add the Avaya IAM root CA certificate to the Avaya Aura® Device Services truststore.
- Ensure that the Discovery URL or proxy server hostname is accessible from Avaya Aura® Device Services.

To contact Avaya IAM support:

- Submit support request to Avaya IAM (SSO) to integrate with Enterprise IDP.
- Upload your Identity Provider (IdP) metadata file using the following link:

<https://wwwcms.avaya.com/customercare/en/home/?modal=show&function=1397208961931&category=1399860014782&mode=direct>

Prerequisites for Workspaces SSO configuration

The Workspaces SSO Flow enables agents to use their organization credentials to log in to the Avaya Experience Platform™ (On-Prem + Connect) solutions, such as Avaya Workspaces, and use Avaya Aura® Device Services search APIs.

This flow does not use the Keycloak service embedded in Avaya Aura® Device Services. Instead, it leverages Identity and Access Management (IAM) service for authentication and authorization.

Avaya Aura® Device Services requires the following parameters for IAM configuration:

- Client ID, which can be any unique identifier configured for this client.
- Client Name, which is the name of the client configured on the IAM service.

For example, `workspaces`.

- OIDC URL for IAM service, which is the discovery URL of the IAM service.

If the hostname of the OIDC URL is not accessible from Avaya Aura® Device Services, use the proxy server hostnames instead.

Ensure that the OIDC URL or proxy server hostname is accessible from Avaya Aura® Device Services.

! Important:

Workspaces SSO integration does not require IAM client credentials. Therefore, you must type **NA** in the **Client Secret** field when creating a client mapping.

Configuration tools and utilities

To deploy and configure the Avaya Aura® Device Services open virtual application (OVA), you need the following tools and utilities:

- The Avaya Aura® Device Services OVA
- A remote computer running the vSphere client, Solution Deployment Manager Client, or Solution Deployment Manager through System Manager

You can use any of these tools to deploy the Avaya Aura® Device Services OVA: vSphere client, Solution Deployment Manager client, or Solution Deployment Manager through System Manager.

- A physical server
- A browser for accessing the Avaya Aura® Device Services web interface
- PuTTY, WinSCP, and WinZip

Characters supported for Avaya Aura® Device Services passwords

You can use the following characters for Avaya Aura® Device Services passwords:

- Uppercase letters: A to Z
- Lowercase letters: a to z
- Numerics: 0 to 9
- Special characters: !, @, #, %, \$, ^, *, ?, and _

These rules apply to all passwords that you enter manually to access Avaya Aura® Device Services resources and for Keystore passwords.

*** Note:**

The Avaya Aura® Device Services web administration portal supports Active Directory-based authentication. Therefore, you can use other special characters, such as double quotes ("), for web administration portal passwords.

Aliases

Aliases provide an alternate and convenient way to run commonly used commands without specifying long path names. The arguments available for the original commands apply for the command aliases as well.

Alias	Description
app	Provides commands for application-specific tasks such as backup, restore, and view status. If you type <code>app</code> without arguments, Avaya Aura® Device Services displays the available subcommands. For example, to create a backup, run the <code>app backup</code> command.
svc	Provides commands for managing services, such as starting, stopping, and viewing status. If you type <code>svc</code> without arguments, Avaya Aura® Device Services displays the available subcommands. For example, to start the services of Avaya Aura® Device Services, run the <code>svc aads start</code> command.
cdto	Provides an easy way to navigate through directories of the installed application. If you type <code>cdto</code> without arguments, Avaya Aura® Device Services displays the available subcommands. For example, the following commands give the same results: <code>cd /opt/Avaya/DeviceServices/<version>/CAS/<version></code> <code>cdto cas</code>

app commands

The following table displays the available **app** commands.

Command	Description
<code>app install</code>	Runs the staged application installer.
<code>app status</code>	Displays Avaya Aura® Device Services status information.
<code>app configure</code>	Runs the configuration utility.
<code>app listnodes</code>	Displays information about the server nodes.
<code>app collectlogs</code>	Collects logs from an Avaya Aura® Device Services node.
<code>app backup</code>	Creates backup files on all Avaya Aura® Device Services nodes.
<code>app restore</code>	Restores Avaya Aura® Device Services data from a backup file on the current node.
<code>app upgrade</code>	Upgrades Avaya Aura® Device Services on the current node.
<code>app rollback</code>	Aborts the upgrade procedure and rolls back to the previously installed Avaya Aura® Device Services release.
<code>app removeinactive</code>	Removes the inactive Avaya Aura® Device Services version.
<code>app uninstall</code>	Uninstalls Avaya Aura® Device Services.

To receive information about a particular command, run it with the `-h` argument. For example: `app backup -h`

! Important:

If Avaya Aura® Device Services is not installed, then only the `app install` command is available. Other commands become available after Avaya Aura® Device Services is installed.

Related links

[app commands do not work after a failed installation](#) on page 336

cdto commands

The following table lists the available `cdto` commands and directories that become the current directory after running the corresponding command.

Command	Navigation target
<code>cdto base</code>	<code>/opt/Avaya</code>
<code>cdto root</code>	<code>/opt/Avaya/DeviceServices</code>
<code>cdto active</code>	<code>/opt/Avaya/DeviceServices/<version></code>
<code>cdto cas</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version></code>
<code>cdto misc</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc</code>
<code>cdto bin</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin</code>
<code>cdto config</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/config</code>
<code>cdto logs</code>	<code>/opt/Avaya/DeviceServices/<version>/logs</code>
<code>cdto ilogs</code>	<code>/opt/Avaya/DeviceServices/.AADSInstallLogs</code>
<code>cdto tlogs</code>	<code>/opt/Avaya/DeviceServices/<version>/tomcat/<Tomcat version>/logs</code>
<code>cdto cassandra</code>	<code>/opt/Avaya/DeviceServices/<version>/cassandra/<Cassandra version></code>
<code>cdto openldap</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/openldap</code>

System layer commands

The `sys` command line alias facilitates the use and discovery of system layer commands. Typing this command without arguments provides syntax help, and a list of supported system layer commands. The following is an example:

```
[admin@server-dev ~]$ sys
Execute system layer commands.

-h, --help
    Command syntax (this help)
```

```

-hh, --hhhelp
    Verbose help

Available commands:

secconfig          [Manage security settings]
versions           [Query version information]
smcvemgt           [Manage Spectre/Meltdown patches]
ipv6config         [Manage server IPv6 configuration]
extension          [Manage system layer extensions]
passwdrules        [Manage password rules]
encryptionStatus   [Show disk encryption status]
encryptionPassphrase [Manage disk encryption passphrases]
encryptionLocalKey [Manage disk encryption local key]
encryptionRemoteKey [Manage disk encryption remote keys]

Command invocation syntax:
    sys <command> <arguments>

Command syntax:
    sys <command> -h

[admin@server-dev ~]$

```

! Important:

For software-deployments, only the following system layer commands are available:

- **sys versions**
- **sys passwdrules**

Other system layer commands are unavailable.

Verbose help information

-hh is used for verbose help information, which provides a brief description of each available system layer command. The following is an example:

```

[admin@server-dev ~]$ sys -hh

The "sys" command line alias facilitates access to the following commands
related to the system layer of UCAApp appliances. To obtain help with
each of these commands, use the "-h" (or "--help") argument for help
with command line syntax, and "-hh" (or "--hhhelp") for verbose help.

secconfig
    Manages security-related settings.

versions
    Queries the version information of various elements of the system
    layer.

smcvemgt
    Manages the enablement status of Linux kernel patches for the
    Spectre and Meltdown vulnerabilities.

ipv6config
    Manages configuration of server-level IPv6.

extension
    Manages the extensions for the system layer. Supported extensions
    are currently limited to the enablement of JAR files in the
    JRE library's extensions directory to support newer application

```

```

loads.

passwdrules
    Manages the configuration of password rules.

encryptionStatus
    Show the status of disk encryption.

encryptionPassphrase
    Adds, changes, and removes disk encryption passphrases, and
    lists the configuration of disk encryption keys.

encryptionLocalKey
    Enables and disables disk encryption local key.

encryptionRemoteKey
    Adds and removes remote key servers (tang servers), and
    list the configuration of disk encryption keys.

[admin@server-dev ~]$

```

Any arguments provided after the name of the system layer command are passed through to that command.

sys secconfig command

sys secconfig provides access to the **secconfig** command, which existed in previous releases.

This command is only available for OVA-based deployments.

The following is an example of this command:

```

[admin@server4950aads ~]$ sys secconfig --hhelp

This script is used to manage run-time security settings on this appliance.
The following command-line arguments are available:

--help, -h
    Prints terse help (command line syntax).

--hhelp, -hh
    Prints verbose help (this help).

--sshCBC < --enable | --disable | --query >
-cbc      < -e      | -d      | -q >
    Enables, disables, and queries the current state of SSH daemon
    CBC-based ciphers.

--fips < --enable | --disable | --query >
    Enables, disables, and queries the current state of FIPS on the system.

[admin@server4950aads ~]$

```

sys versions command

The **sys versions** command provides a summary of key system layer information, including the type of appliance (OVA), the version number of the system layer, the version of the current partitioning, and the OVA that was originally deployed.

```

[admin@server4889aads ~]$ sys versions

```

```

Appliance type      : AADS
System layer version : 3.4.1.0.3
Partitioning version : 2.0
Original OVA deploy  : aads-7.1.5.0.117

[admin@server4889aads ~]$

```

sys volmgt command

Syntax help: sys volmgt --help

The **sys volmgt** command is used to query and extend disk volumes on the system.

! Important:

- The **sys volmgt** command is only available if data encryption is *disabled* on Avaya Aura® Device Services. If data encryption is enabled, this command is unavailable and you cannot allocate free disk space to disk volumes.
- This command is only available for OVA-based deployments.

The following provides the command line syntax for this command:

```

[admin@server4889aads ~]$ sys volmgt --help

Syntax:
  --help,                -h
  --hhhelp,              -hh
  --version,             -v
  --status,              -st
  --summary,             -s
  --monitor [tail|less], -m [tail|less]
  --logs,                -l
  --scan
  --extend <volume> [ <n>m | <n>g | <n>t --remaining ]
  --extend --all
  --reset

[admin@server4889aads ~]$

```

Verbose help: sys volmgt --hhhelp

The verbose help information for the scripts provides more information about what the tool is used for.

```

[admin@server4889aads ~]$ sys volmgt --hhhelp

```

This script provides for the ability to extend the sizes of volumes on this system. In order for a volume to be extended in size, the disk that hosts the volume must first be increased in size using the tools that are used to manage deployed virtual machines (VMware).

The following example illustrates how to add 20 GiB of storage to the application log volume (/var/log/Avaya). This volume is located on the second disk of the system and so this example assumes that disk 2 has been increased in size by 20 GiB.

```
sys volmgt --extend /var/log/Avaya 20g
```

The above example will do two things:

- 1) It will extend the size of the LVM logical volume by 20 GiB.

- 2) It will then extend the size of the Linux file system that is located inside that volume to the new size of the LVM logical volume.

Step (2) above may take several minutes to complete for larger volumes. If, for some reason, this second operation is interrupted, it can be re-run using the same command, but WITHOUT specifying the size argument. For example, the following command is used to perform step (2) only for the application log volume (/var/log/Avaya).

```
sys volmgt --extend /var/log/Avaya
```

If in doubt as to whether or not all file systems have been fully extended in their respective volumes, step (2) can be executed across all volumes using a single command as follows:

```
sys volmgt --extend --all
```

Performing step (2) on a file system that is already fully extended in its LVM volume is a null operation (does no harm).

Note the following general points regarding this script:

- The extending of a volume cannot be undone. Make sure the correct volume is being extended, and by the correct size. To confirm any extend operation, the user is required to enter the response "confirm" (case insensitive).
- In order to avoid impacting system performance, avoid performing extend operations during periods of high traffic.
- Extend operations are performed by a background process, in order to avoid interference due to loss of an SSH connection. Avoid powering down or rebooting a server while there is a background operation in progress. The presence of a running background operation can be queried as follows:

```
sys volmgt --status
```

- Logical volumes on the system are referenced using their Linux file system mount points, such as /var/log/Avaya and /media/data, with the exception of the volume containing Linux swap, which has no mount point. The Linux swap volume is referenced using "swap".
- Sizes are specified in base 2 units rather than base 10 (SI) units. For example, 1g = 1 GiB = 1024 x 1024 x 1024 bytes.
- Summary information is displayed in GiB, with a resolution of two decimal places. When extending the sizes of LVM volumes, units can be specified in mebibytes (m), gibibytes (g), or tebibytes (t).
- Due to file system overhead allocation by the Linux kernel, the size of a file system will never exactly match the size as reported by the LVM volume that contains that file system. To be certain that a file system is fully extended to the size of the volume that contains it, inspect the log file after issuing the extend operation as follows:

```
sys volmgt --monitor less
```

To perform such a check across all volumes:

```
sys volmgt --extend --all
sys volmgt --monitor less
```

The following arguments are supported by this script:

```

--help, -h
    Terse help.

--hhelp, -hh
    Verbose help (this help).

--version, -v
    Prints the version of this script to stdout.

--status, -st
    Prints the current status of this tool. Use this to determine
    if there is a background operation in progress, or the results
    of the last background operation.

--summary, -s
    Prints a summary of disks, the LVM volumes contained on each disk,
    and the file system contained in each LVM volume. Disk information
    includes the size of the disk and the amount of free space
    available for allocation to volumes on the disk. LVM volume
    information includes the size of the LVM volume. File system
    information includes the size of the Linux file system and the
    current amount of space that is in use on that file system.

    Due to file system overhead allocation by the Linux kernel, the
    size of a file system will never exactly match the size as reported
    by the LVM volume that contains that file system. Refer to the top of
    this help information for more information.

--monitor [tail|less]
-m         [tail|less]
    Browse the log file for the latest extend operation. Specify "tail"
    to use the tail browser. Specify "less" to use the less
    browser, which allows scrolling and searching through the log file.
    If neither is specified, the browser defaults to the tail browser.

--logs
    Generate a zip file in the current working directory that contains
    all logs generated to date by this script.

--scan
    Scan disks for newly available storage. Do this after increasing
    the disk size of one of more disks. Once scanned, the newly
    available space appears in the "Free" column in the "--summary"
    output, and is now available for allocation to volumes on that disk.

    A summary is printed after the scan to show the updated volume
    information.

--extend <volume> [ <n>m | <n>g | <n>t --remaining ]--extend --all
    The first form of the command operates on a single volume. If a size
    is specified, then the LVM volume is extended by that size (step 1),
    and the file system it contains is extended to use the new space
    made available in that volume (step 2). If a size is not specified,
    then the file system contained in that volume is extended (i.e.,
    step 2 only).

    The "--all" form of the command is used to perform step 2 across
    all volumes on the system.

    For more information, see the examples at the top of this help.

    If "--remaining" is specified for the size, then the specified
    volume is extended with all remaining free space on that disk.
    If a specific increment is provided, then the volume is extended
    by that amount, reducing the amount of free space on the disk

```


by that amount. Specific sizes are in the form of a number (e.g., "10", "10.5", or ".5") and a unit. Units are "m" for mebibytes, "g" for gibibytes, and "t" for tebibytes".

The smallest increment that can be specified is 100 MiB.

Example invocations:

```
sys volmgt --extend /var/log/Avaya 10g
sys volmgt --extend /var/log/Avaya 10.5g
sys volmgt --extend /var/log/Avaya 0.5g
sys volmgt --extend /var/log/Avaya .5g
sys volmgt --extend /var/log/Avaya 500m
sys volmgt --extend /var/log/Avaya --remaining
sys volmgt --extend /var/log/Avaya
```

--reset

Resets internal tracking data. Use this if this script is blocked on an invalid background progress indication. This condition can arise if a background operation was prematurely terminated due to, for example, a system reboot. Verify that no background operations are in progress prior to executing this command, through verification of the process id as reported by the "--status" argument.

```
[admin@server4889aads ~]$
```

Partitioning examples: sys volmgt --summary

Avaya Aura® Device Services supports partitioning versions 1.0 and 2.0.

The following example shows a summary of the information provided by this command for a version 1.0 partitioned system:

```
[admin@server4889aads ~]$ sys volmgt --summary
```

Disk and Volume Summary								
Disk				Volume				
Num	Name	Size	Free	Name	LVM Size	File System Size	Usage	
2	sdb	25.00	0.00	/home	4.00	3.94	1.49	
				/opt/Avaya	21.00	20.67	1.27	
3	sdc	10.00	0.00	/media/data	10.00	9.84	0.15	

The following example shows a summary of the information provided by this command for a version 2.0 partitioned system:

```
[admin@server4950aads ~]$ sys volmgt -s
```

Disk and Volume Summary								
Disk				Volume				
Num	Name	Size	Free	Name	LVM Size	File System Size	Usage	
1	sda	124.51	50.10	/	17.30	17.29	1.56	
				/home	4.00	3.99	0.03	
				/opt/Avaya	14.70	14.69	2.04	
				/tmp	14.90	14.89	0.63	
				/var	8.50	8.49	0.09	
				/var/log	5.00	4.99	0.03	
				/var/log/audit	6.00	5.99	0.03	

					swap	4.00	n/a	n/a
2	sdb	70.00	0.00	/var/log/Avaya	70.00	69.98	0.11	
3	sdc	40.00	0.00	/media/data	40.00	39.99	0.55	
4	sdd	10.00	0.00	/media/cassandra	10.00	9.99	0.03	

sys smcvemgt command

The system layer **smcvemgt** command is used to manage the Linux kernel patches related to the following vulnerabilities:

- Variant #2/Spectre (CVE-2017–5715)
- Variant #3/Meltdown (CVE-2017–5754)

* Note:

The kernel patch for the Variant #1/Spectre (CVE-2017–5754) vulnerability is permanently enabled on the system and cannot be disabled.

This command is only available for OVA-based deployments.

The choice to enable or disable these patches is a trade-off between performance and security impact:

- If the patches are enabled, the system might experience noticeable performance losses.
- If the patches are disabled, the system is not protected against the Variant #2/Spectre and Variant #3/Meltdown vulnerabilities.

By default, Linux patches for Variant #2/Spectre and Variant #3/Meltdown are enabled. The Variant #2/Spectre patch is enabled with Linux kernel defaults. In default operation mode, the Variant #2/Spectre Linux patch selects the mitigation method that is best suited for the processor architecture of the host machine.

* Note:

To be fully functional, patches for the Variant #2/Spectre vulnerability require hardware support, which is provided by VMware and hardware vendors through microcode updates.

Changes made by the **smcvemgt** command to the Linux kernel tunables always cause a server reboot. The script does not manage the state of application services. To ensure that the application services are stopped before the reboot, run the `svc aads stop` command before using the **smcvemgt** command. After the reboot, manually start the application services using the `svc aads start` command.

For more information about Spectre and Meltdown kernel tunables that are affected by the **smcvemgt** command, see <https://access.redhat.com/articles/3311301>. For more information about the Spectre and Meltdown vulnerabilities, see <https://access.redhat.com/security/vulnerabilities/speculativeexecution>.

Syntax help: sys smcvemgt --help

```
[admin@server-dev ~]$ sys smcvemgt --help
```

```
Version 1.2
```

```
Syntax:
```

```

--help,      -h
--hhelp,     -hh
--query,     -q
--set,       -s  enabled
--set,       -s  disabled
--set,       -s  [ v2=<v2-mode> ] [ v3=<v3-mode> ]
                (v2-mode: disabled | default | kernel | user | both | user+retp)
                (v3-mode: disabled | enabled)
--history

```

Verbose help: sys smcvemgt --hhelp

```
[admin@srvr-dev ~]$ sys smcvemgt --hhelp
```

Version 1.2

This script manages the enablement status of the Linux kernel patches for the following Spectre and Meltdown vulnerabilities:

```

Variant #2/Spectre (CVE-2017-5715)
Variant #3/Meltdown (CVE-2017-5754)

```

The kernel patch for the following related vulnerability is permanently enabled on the system (cannot be disabled):

```
Variant #1/Spectre (CVE-2017-5753)
```

Note that hardware support is required for Variant #2/Spectre to be fully functional. CPU microcode updates must be applied in order for this hardware support to be provided. The "--query" argument includes an indication as to whether or not hardware support is provided on this server.

For more information on Spectre/Meltdown kernel tunables, refer to:

```
https://access.redhat.com/articles/3311301
```

For additional information on the Spectre/Meltdown vulnerabilities, refer to:

```
https://access.redhat.com/security/vulnerabilities/speculativeexecution
```

Syntax:

```

--help,      -h
                Provide terse help.

--hhelp,     -hh
                Provide verbose help (this text).

--query,     -q
                Query the configuration of the Variant #2/Spectre and Variant #3/
                Meltdown tunables for system reboots, as well as on the running
                system.

--set,       -s  enabled
--set,       -s  disabled
--set,       -s  [ v2=<v2-mode> ] [ v3=<v3-mode> ]
                Enables and disables Variant #2/Spectre ("v2") and/or Variant #3/
                Meltdown ("v3") patches.

                This immediately reboots the server. Applications on the server are
                not managed by this script. Ensure that any applications are
                disabled, as required, prior to changing kernel settings with this
                script.

```

If "enabled" is specified, then both v2 and v3 are enabled, with v2 set to kernel default behavior. If "disabled" is specified, then both v2 and v3 are disabled. Otherwise, kernel patches are enabled or disabled as per the specified "v2" and/or "v3" arguments. If a "v2" or "v3" argument is not specified, the current system value for that item is retained.

v2-mode:

```
disabled
    Variant #2/Spectre is disabled.

default
    The kernel decides how to set tunables for Variant #2/
    Spectre, based on the processor architecture. Note that for
    architectures prior to Skylake, the kernel selects
    retpoline ("return trampoline") over ibrs.

kernel
    Use "ibrs" (i.e., kernel space only).

user
    Use "ibrs_user" (i.e., userland only).

both
    Use "ibrs_always" (i.e., kernel space and userland).

user+retp
    Use "retpoline,ibrs_user".
```

v3-mode:

```
disabled
    Variant #3/Meltdown is disabled.

enabled
    Variant #3/Meltdown is enabled.
The following two commands are equivalent:
```

```
sys smcvemgt enabled
sys smcvemgt v2=default v3=enabled
```

The following two commands are equivalent:

```
sys smcvemgt disabled
sys smcvemgt v2=disabled v3=disabled
```

```
--history
    Show a history of changes made to the enablement status of the
    Spectre and Meltdown patches.
```

sys ipv6config command

The **sys ipv6config** command is used to configure IPv6 at the system level. You can do the following:

- Configure IPv6 interactively or non-interactively. When you configure IPv6 interactively, Avaya Aura® Device Services prompts you to enter the IPv6 address, network prefix, and default gateway. When you configure IPv6 non-interactively, you must provide these settings as command options.
- Review the IPv6 configuration.

- Delete the IPv6 networking configuration.

For more information about the supported options, run this command with the `-h` argument. The following is an example:

```
[admin@aads ~]$ sys ipv6config -h
Usage:
  ipv6config show
    Shows the server's IPv6 networking configuration.

  ipv6config set [options]
    Sets, or updates, the server's IPv6 networking configuration. If no
    options are specified, then data is collected interactively. Existing
    configuration is used for any non-specified IPv6 configuration items.
    A default network prefix of 64 is used if a prefix cannot be resolved.
    Specify "-h" for a list of available options.

  ipv6config delete
    Deletes the server's IPV6 networking.

Options:
  -h, --help          show this help message and exit
  --ip=ADDRESS[/PREFIX]
                      IPv6 interface address.
  --prefix=PREFIX      IPv6 prefix. If a prefix is also specified in the --ip
                      option, then this option takes precedence.
  --gw=GATEWAY_ADDRESS
                      IPv6 default gateway address.
```

This command is only available for OVA-based deployments.

Example: interactive configuration

The following example shows IPv6 configuration in interactive mode:

```
[admin@aads bin]$ sys ipv6config set

Interface IPv6 address ('q' to quit) [] => 2a07:2a42:adc0:112::fa
IPv6 network prefix ('q' to quit) [64] =>
Interface IPv6 default gateway ('q' to quit) [] => 2a07:2a42:adc0:112::1/64

The server IPv6 configuration will be updated to the following and networking
will be restarted:

  Interface address : 2a07:2a42:adc0:112::fa
  Prefix            : 64
  Default gateway   : 2a07:2a42:adc0:112::1
  Network           : 2a07:2a42:adc0:112::/64

Confirm (y/n) => y

Applying configuration:

  Interface address : 2a07:2a42:adc0:112::fa
  Prefix            : 64
  Default gateway   : 2a07:2a42:adc0:112::1
  Network           : 2a07:2a42:adc0:112::/64

Restarting networking.
Done
```

passwdrules command

Description

sys passwdrules allows you to review and edit complexity rules for passwords that you use to log in to the virtual machine with the Avaya Aura® Device Services OVA using an SSH connection.

If data encryption is enabled, these rules also apply to encryption passphrases.

Syntax

```
sys passwdrules [show] [set [options]] [set-default]
```

show Shows the server password rule configuration, including default, minimum, and maximum values.

set Sets server password rules. If you do not specify any options, then Avaya Aura® Device Services prompts you to configure each option separately. If you do not specify a certain option, Avaya Aura® Device Services continues to use the existing rule for this option.

set-default Sets server password rules to their default values.

Syntax help

```
sys passwdrules [-h | --help]
```

Options

Option	Description
--diff= <i>INTEGER</i>	Number of characters in the new password that must not be present in the old password.
--min-len= <i>INTEGER</i>	Minimum length of the password. The default minimum length is 15 characters.
--min-digs= <i>INTEGER</i>	Minimum number of digits in the password.
--min-upper= <i>INTEGER</i>	Minimum number of uppercase characters in the password.
--min-lower= <i>INTEGER</i>	Minimum number of lowercase characters in the password.
--min-other= <i>INTEGER</i>	Minimum number of special characters in the password.  Important: Avaya Aura® Device Services supports the following special characters: !, @, #, %, \$, ^, *, ?, and _.
--min-class= <i>INTEGER</i>	Minimum number of character classes that must be present in the password. The character classes are: • Digits • Uppercase characters • Lowercase characters • Special characters

Option	Description
<code>--max-repeat=INTEGER</code>	Maximum allowed number of consecutively repeated characters. For example, if you set this parameter to 3, then the following password is invalid: paaassword, because a is repeated three times.
<code>--max-class-repeat=INTEGER</code>	Maximum allowed number of consecutively repeated characters of the same class. For example, if you set this parameter to 3, then the pas1sw2or3d password is invalid, because the first three characters, which are p, a, and s, belong to the same character class.
<code>--history=INTEGER</code>	Number of previous passwords that must not match the new password.

Example

The following is an example of a command that sets the following password rules:

- At least 16 characters in total.
- At least two digits.
- At least one special character.
- Other settings are default.

```
sys passwdrules set --min-len=16 --min-digs=2 --min-other=1
```

Data encryption commands

The following sections contains command you can use to manage data encryption. These commands are available if you enabled data encryption during Avaya Aura® Device Services OVA deployment.

You cannot enable or disable data encryption using system layer commands.

! Important:

- In AWS deployments, you enable data encryption on AWS itself. Therefore, you cannot use the system layer commands for disk encryption management in AWS deployments.
- These commands are only available for OVA-based deployments.

encryptionPassphrase command

Description

You can run the `sys encryptionPassphrase` command to manage the encryption passphrase.

Syntax

```
sys encryptionPassphrase [add | change | remove | list]
```

add Enables you to set up an encryption passphrase.

change Enables you to change the existing encryption passphrase.

- remove** Removes the encryption passphrase.
- list** Displays information about passphrases and slot assignments.

encryptionRemoteKey command

Description

You can use the **sys encryptionRemoteKey** command to manage the remote key server. If you run the command without any parameters, Avaya Aura® Device Services displays help information about the command.

Syntax

```
sys encryptionRemoteKey [add <server address> [<port>] | remove <server address> | list]
```

- add** Enables you to add a remote key server.
- remove** Removes the remote key server.
- list** Displays general remote key server information.

encryptionLocalKey command

Description

You can use the **disk encryptionLocalKey** command to manage the local key store. If you run this command without any parameters, Avaya Aura® Device Services displays help information.

Syntax

```
sys encryptionLocalKey [enable | disable]
```

- enable** Enables the local key store.
- disable** Disables the local key store.

encryptionStatus command

Description

The **sys encryptionStatus** command displays information about data encryption on Avaya Aura® Device Services , including the following:

- Whether data encryption is enabled.
- Whether the local key store is enabled.
- Whether the encryption password is used.

Syntax

```
sys encryptionStatus
```

Using the Tmux utility

About this task

Avaya Aura® Device Services resets idle SSH sessions after a certain period of time. This might affect lengthy CLI operations, such as Avaya Aura® Device Services installation or backup. If the connection with the SSH terminal is reset while installation or backup operations are in progress, you must restart these operations. To prevent this issue, you can start a Tmux session before performing a lengthy operation. Commands and processes that you run from a Tmux session continue to run even if the connection with the SSH terminal is reset. Therefore, you can re-connect to the Tmux session and complete the operation.

Procedure

1. To start a Tmux session, run the following command from the Avaya Aura® Device Services CLI:

```
tmux new-session -s <SESSION_NAME>
```

In this command, `SESSION_NAME` is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_session
```

2. To re-connect to the Tmux session, run the following command:

```
tmux attach-session -t <SESSION_NAME>
```

In this command, `SESSION_NAME` is the name of the Tmux session that you created. For example:

```
tmux attach-session -t AADS_session
```

Chapter 4: Initial setup

Deployment methods

You can use the following options to deploy Avaya Aura® Device Services:

- As a software-only application that you can install on your own RHEL 8.4 or RHEL 8.10 physical servers or virtual machines.

For software-only deployments, Avaya Aura® Device Services supports the following virtual environments:

- VMware
 - Amazon Web Services (AWS)
 - Microsoft Hyper-V
 - Microsoft Azure
 - Google Cloud Platform
- As an Avaya-provided, application-specific RHEL 8.4 or RHEL 8.10 OVA that you can install in the VMware virtual environment. This option also includes installing Avaya Aura® Device Services on Avaya Solutions Platform 130 Release 5.

All deployment options support deploying Avaya Aura® Device Services in environments with Avaya Aura® environment or without Avaya Aura®. The initial virtual machine setup procedures are the same for environments with and without Avaya Aura®.

Important:

- Avaya Aura® Device Services is an entitlement, so it does *not* require any licenses.
- For installing Avaya Aura® Device Services as an Avaya-provided OVA, see Chapter “Initial setup for OVA deployments”.
- For installing Avaya Aura® Device Services as a software-only application in VMware virtualization environment, see Chapter “Initial setup for software-only VMware deployments”.
- For installing Avaya Aura® Device Services as a software-only application in AWS environment, see Chapter “Initial setup for software-only deployments on Amazon Web Services”.
- For installing Avaya Aura® Device Services as a software-only application in Microsoft Hyper-V virtualization environment, see Chapter “Initial setup for software-only Hyper-V deployments”.

- For installing Avaya Aura® Device Services as a software-only application in Microsoft Azure virtualization environment, see Chapter “Initial setup for software-only Microsoft Azure deployments”.
- For installing Avaya Aura® Device Services as a software-only application in Google Cloud Platform virtualization environment, see Chapter “Initial setup for software-only Google Cloud Platform deployments”.

Downloading software from PLDS

About this task

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS.

 Note:

Avaya Aura® Device Services is an entitlement, so it does *not* require any licenses.

After downloading an Avaya Aura® Device Services OVA, you must verify that the SHA256 checksum of the OVA file matches the SHA256 checksum value provided on PLDS. To calculate the SHA256 checksum, you can use any SHA256 hash calculation tool, such as sha256sum.

Along with PLDS, you can download the product software from <https://support.avaya.com> using the Downloads and Documents tab at the top of the page.

 Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

Procedure

1. On your web browser, type <https://plds.avaya.com> to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS Home page, select **Assets**.
4. Click **View Downloads**.
5. Click the search icon  for Company Name.
6. In the Search Companies dialog box, do the following:
 - a. In the **%Name** field, type `Avaya` or the Partner company name.
 - b. Click **Search Companies**.
 - c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
 - In **Download Pub ID**, type the download pub ID.

- In the **Application** field, click the application name.
8. Click **Search Downloads**.
 9. In the **Download Manager** box, click the appropriate **Download** link.

 Note:

The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

10. If you use the Download Manager, click **Details** to view the download progress.
11. Select a location to save the file, and click **Save**.
12. **(Optional)** 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.

Changing the administrative user password during the first login

About this task

When you log in to Avaya Aura® Device Services for the first time you must change the password and then log in again.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrative user.

You must use the administrative user defined during OVA or software-only deployment process for logging in to Avaya Aura® Device Services.

Avaya Aura® Device Services prompts you to type the password.

2. Type the password.

Avaya Aura® Device Services displays the following message:

```
You are required to change your password immediately (root
enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user admin.
Changing password for admin.
```

3. Follow the instruction on the screen to change the password.

 Note:

Your new password must include at least 15 characters. If required, you can change the default password complexity rules later using the `sys passwdrules` command.

After you change the password, Avaya Aura® Device Services closes the SSH session.

Related links

[Characters supported for Avaya Aura Device Services passwords](#) on page 56

Chapter 5: Initial setup for OVA deployments

You can deploy Avaya Aura® Device Services as an Avaya-provided, application-specific RHEL 8.4 OVA that you can install in the VMware virtual environment. This option also includes installing Avaya Aura® Device Services on Avaya Solutions Platform 130 Release 5.

Avaya Aura® Device Services does not support Avaya Solutions Platform 120 and Avaya Solutions Platform 130 Release 4 or below.



Note:

Avaya Solutions Platform 120 is synonymous with Avaya Converged Platform 120 and Appliance Virtualization Platform.

Installation checklist for OVA-based deployments

The following checklist describes the high level deployment process on VMware using an Avaya-provided, application-specific RHEL 8.4 OVA:

No.	Task	Notes	✓
1	Download the Avaya Aura® Device Services OVA from PLDS.	For more information, see Downloading software from PLDS on page 74.	
2	Deploy the OVA.	For more information about deploying the OVA, see VMware deployment options on page 78.  Note: The Avaya Aura® Device Services OVA file includes openjdk. Operating system updates for virtual machines include updates for openjdk.	
3	To use IPv6 addresses, enable IPv6 at the system layer.	Before installing the application layer, you must enable IPv6 at the system layer. For more information, see Enabling IPv6 support at the system layer on page 93.	

No.	Task	Notes	✓
4	Enable FIPS mode (optional).	You can only enable FIPS mode before installing the application layer. For more information, see Enabling FIPS mode on page 93.	
5	Enable additional STIG hardening (optional).	You only need to enable additional hardening if your organization policies require full Security Technical Implementation Guide (STIG) compliance. For more information, see Enabling additional STIG hardening on page 95.	

After deploying a virtual machine, install or restore the application layer as described in the “Avaya Aura® Device Services installation” chapter.

VMware deployment options

Use one of the following deployment methods to deploy a virtual machine in a VMware environment using an Avaya-provided Avaya Aura® Device Services OVA. You can use vSphere Client, Host Client connected directly to the ESXi host, or Solution Deployment Manager (SDM) from System Manager. After deploying a virtual machine, install the Avaya Aura® Device Services application as described in “Installing Avaya Aura® Device Services”.

Deploying the Avaya Aura® Device Services OVA using the vSphere Client

About this task

Use this procedure to deploy the Avaya Aura® Device Services OVA on vCenter using the vSphere Client.

This procedure applies to vSphere Client Release 7.0.3. If you use another version of the vSphere Client, the steps might differ from the steps described in this procedure.

FQDNs, where mentioned in the procedure, are mandatory.

* Note:

If you choose to install a standalone Avaya Aura® Device Services at present but in the future decide to move to a cluster that uses a virtual IP, the original standalone node needs to be re-configured with the original virtual IP as the front-end FQDN. Accordingly, the new FQDN addition for Avaya Aura® Device Services must be notified to your clients.

To avoid this scenario, you can plan and add a virtual IP for the front-end FQDN of the standalone node. This planning would make the transition from a standalone node to a cluster easier in the future.

Before you begin

- Obtain the latest OVA from PLDS.
- In an Avaya environment, deploy Session Manager. For more information about deploying Session Manager, see *Deploying Avaya Aura® Session Manager*.

Procedure

1. Log in to the vSphere Client at `https://<VCENTER>/UI`.

In this URL, <VCENTER> is the IP address or FQDN of the vCenter server.

2. Right-click an appropriate cluster or ESXi host where you want to deploy the OVA and select **Deploy OVF Template**.

The vSphere Client displays the Deploy OVF Template window.

3. To download the OVA file, on the Select an OVF template page, do one of the following:

- To download the OVA file from a web location, select **URL** and provide the complete network path to the OVA file.
- To download the OVA file from the local computer, select **Local file** and click **Upload files** and select the OVA file.

4. Click **Next**.

5. On the Select a name and folder page, do the following:

- a. In **Virtual machine name**, type a name for the virtual machine.
- b. In **Select a location for the virtual machine**, select an appropriate location for the virtual machine.

By default, this is the location that you select in step 2 on page 79.

- c. Click **Next**.

6. On the Select a compute resource page, do the following:

- a. In **Select the destination compute resource**, select an appropriate ESXi host for the virtual machine.

By default, this is the location that you select in step 2 on page 79.

- b. Ensure that the Compatibility area displays the `Compatibility check succeeded` message.
- c. Click **Next**.

7. On the Review details page, do the following:

- a. Ensure that the **Publisher** field contains the `Entrust Code Signing CA - OVCS1 (Trusted certificate)` entry.
- b. Verify the OVA template details.
- c. Click **Next**.

8. On the License agreements page, do the following:
 - a. Read the End User License Agreement (EULA).
 - b. To accept the EULA, select the **I accept all license agreements** check box.
 - c. Click **Next**.
9. On the Configuration page, select an Avaya Aura® Device Services profile that matches your deployment requirements.

 Important:

If you deploy the OVA for a non-seed node in a cluster, you must use the same resource profile that you use for the seed node.

For more information about resource profile specifications, see [Avaya Aura Device Services virtual machine resource requirements](#) on page 34. The vSphere Client also displays the basic system requirements for the profile in the Description area.

10. Click **Next**.
11. On the Select storage page, do the following:
 - a. In **Select virtual disk format**, select the appropriate disk format.

If you select **Thick provision**, the entire disk space required for the virtual machine is reserved and unavailable for other virtual machines to use. If you select **Thin provision**, unused space is available for other virtual machines.
 - b. In the Datastore table, select an appropriate data store for the virtual machine.
 - c. Ensure that the Compatibility area displays the **Compatibility check succeeded** message.
 - d. Click **Next**.
12. On the Select networks page, for each source network, select an appropriate destination network.
13. Click **Next**.
14. On the Customize template page, configure the following parameters:
 - a. In **Enhanced Access Security Gateway (EASG)**, configure EASG settings.
 - b. In **Disk Encryption Settings**, configure disk encryption settings.
 - c. In **Management Network Settings**, configure network settings, such as the IP address, FQDN, network mask, and DNS.
 - d. In **Account login Details**, configure credentials for a Linux administrator user, including the user name, password, and group.

For more information about the disk encryption and EASG fields, see the respective sections in [VM Deployment Configuration Parameters, Network Parameters, and Data Encryption field descriptions](#) on page 81.

*** Note:**

- If you do not provide the details in the mandatory fields, you cannot power on the virtual machine even if the deployment is successful. The vSphere Client displays the number of remaining mandatory settings that you must configure at the top of the Customize template page.
- The vSphere Client validates the inputs that you provide. If the inputs are invalid, the system prompts you to provide the inputs again on the virtual machine console.

15. Click **Next**.

16. On the Ready to complete page, review the configuration details and then click **Finish** to complete the virtual machine deployment.

Next steps

Install the Avaya Aura® Device Services application.

VM Deployment Configuration Parameters, Network Parameters, and Data Encryption field descriptions

You must gather and keep ready the configuration data before deploying Avaya Aura® Device Services. An asterisk (*) indicates that inputs for the field are mandatory.

Name	Description
Management Network Settings	
VM IP Address*	Specifies the IP address of the virtual machine.
VM FQDN*	Specifies the FQDN of the virtual machine.
VM Netmask*	Specifies the netmask of the virtual machine.
Default Gateway IP Address*	Specifies the default gateway IP address of the virtual machine.
Default Search List	Specifies the domain name server (DNS) suffix domains for DNS queries. If there are multiple domains, separate each domain with a comma.
DNS Server IP Address*	Specifies the DNS server IP address of the virtual machine. If there are multiple IP addresses, separate each entry with a comma.
NTP Server IP Address or FQDN*	Specifies the NTP server IP address or FQDN. If there are multiple NTP servers, separate each IP address or FQDN with a comma.
Timezone	Specifies the time zone of the virtual machine.

Account login details

Name	Description
Admin user*	Specifies the user name of the administrative user. You must use the administrative user defined during OVA deployment for logging in to Avaya Aura® Device Services.
Admin user password*	Specifies the password of the administrative user.
Confirm Password*	Re-specifies the password of the administrative user.

Name	Description
Admin Group name*	Specifies the group name of the administrative user.

Data encryption

Data encryption is only supported with AVP and the VMware Virtualized Environment.

Name	Description
Data Encryption	Specifies whether data encryption is enabled or disabled on Avaya Aura® Device Services. The options are the following: • 1: To enable data encryption. • 2: To disable data encryption.  Important: You cannot change encrypted Avaya Aura® Device Services to non-encrypted or vice versa without a new OVA installation. • On Solution Deployment Manager: When the Data Encryption field is set to 1, Avaya Aura® Device Services enables the Encryption Pass-Phrase and Re-enter Encryption Pass-Phrase fields to enter the encryption passphrase. • On vCenter or ESXi: When the Data Encryption field is set to 1, enter the encryption passphrase in the Password and Confirm Password fields.
Encryption Pass-Phrase	The passphrase for data encryption. This field is applicable when data encryption is enabled. When you deploy Avaya Aura® Device Services using Solution Deployment Manager, Avaya Aura® Device Services applies the password complexity rules. When you deploy Avaya Aura® Device Services using vCenter or ESXi, Avaya Aura® Device Services does not apply password complexity rules.  Important: While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to a vCenter limitation. Therefore, ensure that you enter the encryption passphrase if data encryption is enabled.
Re-enter Encryption Pass-Phrase	The password for data encryption.
Require Encryption Pass-Phrase at Boot-Time	When this check box is selected, you must type the encryption passphrase whenever Avaya Aura® Device Services reboots. By default, the Require Encryption Pass-Phrase at Boot-Time check box is selected.

Name	Description
	! Important: Remember the data encryption passphrase. If you lose the data encryption password, the only option to access Avaya Aura® Device Services is to reinstall the OVA. If the check box is not selected, Avaya Aura® Device Services creates a local key store, and you do not need to type the encryption passphrase when Avaya Aura® Device Services reboots. However, this makes the system less secure. You can also set up and use a remote key server to store encryption keys. To start using a remote key server, run the sys encryptionRemoteKey command after Avaya Aura® Device Services is installed. The remote key server provides more security than the local key store.

Enhanced Access Security Gateway (EASG)

Name	Description
EASG User Access	Use this option to enable or disable AVAYA remote access to your system. If you select 1, you enable EASG User Access, and AVAYA support engineers can log in to your system and help to resolve issues. For EASG User Access, you must also register Avaya Aura® Device Services and configure remote connectivity and alarming. For more information about EASG User Access, see the Avaya support site. If you select 2, you disable EASG User Access, and AVAYA support engineers cannot log in to your system.

Deploying the Avaya Aura® Device Services OVA using the Host Client connected directly to the ESXi host

About this task

Use this procedure to deploy Avaya Aura® Device Services OVA on vCenter using the Host Client. This procedure also applies to deploying Avaya Aura® Device Services on Avaya Solutions Platform 130 or an equivalent server.

Note:

If you choose to install a standalone Avaya Aura® Device Services at present, but in future decide to move to a cluster that uses a virtual IP, the original standalone node needs to be reconfigured with the original virtual IP as the front-end FQDN. Accordingly, the new FQDN addition for Avaya Aura® Device Services must be notified to your clients.

To avoid this scenario, you can plan in advance and add a virtual IP for the front end FQDN of the standalone node. This would make the transition from a standalone node to a cluster easier in the future.

Before you begin

- Obtain the latest OVA from PLDS.

In an Avaya environment, deploy Session Manager. For more information about deploying Session Manager, see *Deploying Avaya Aura® Session Manager*.

Procedure

1. Log in to the Host Client at `https://<ESXI_HOST>/UI`.
In this URL, `<ESXI_HOST>` is the IP address or FQDN of the ESXi host where you want to deploy your virtual machine.
2. Right-click the ESXi host and select **Create/Register VM**.
The Host Client displays the New Virtual Machine window.
3. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
4. Click **Next**.
5. On the Select OVF and VMDK files page, do the following:
 - a. In **Name for the virtual machine**, type a name for the virtual machine.
 - b. In **Click to select files or drag/drop**, upload the OVA file to the Host Client.
 - c. Click **Next**.
6. On the Select storage page, select an appropriate data storage for your virtual machine and click **Next**.
7. On the License agreements page, do the following:
 - a. Read the End User License Agreement (EULA).
 - b. To accept the EULA, click **I agree**.
 - c. Click **Next**.
8. On the Deployment options page, do the following:
 - a. In **Network mappings**, select an appropriate network.
 - b. In **Deployment type**, select an Avaya Aura® Device Services profile that matches your deployment requirements.



Important:

If you deploy the OVA for a non-seed node in a cluster, you must use the same resource profile that you used for the seed node.

For more information about resource profile specifications, see [Avaya Aura Device Services virtual machine resource requirements](#) on page 34. The Host Client also displays basic system requirements for the profile below the field.

- c. In **Disk provisioning**, select the appropriate disk format.

If you select the **Thick** option, the entire disk space required for the virtual machine is reserved and unavailable for other virtual machines to use. If you select the **Thin** option, unused space is available for other virtual machines.

- d. Clear the **Power on automatically** check box.
- e. Click **Next**.
9. On the Additional Settings page, keep the default values and click **Next**.
10. On the Ready to complete page, review the virtual machine settings and click **Finish**.
11. Wait until the virtual machine is deployed.

 Important:

Do not refresh the browser page while deployment is in progress.

12. To ensure that the virtual machine automatically starts after a hypervisor reboot, right-click your virtual machine and select **Autostart > Enable**.

If you do not enable autostart, you must manually start the virtual machine when the hypervisor reboots.

 Note:

You must enable the autostart functionality on the ESXi host for the virtual machine autostart to function.

13. To start the virtual machine, right-click the virtual machine and select **Power > Power On**.
14. Access the virtual machine console.
15. Follow the system prompts to configure the remaining OVA settings as appropriate.

You must configure data encryption settings, network settings, and Linux administration account settings.

 Note:

When configuring the Default Search List, ensure that the list includes the domains for:

- Avaya Aura® Device Services
- Avaya Meetings Server Management
- System Manager and LDAP

Next steps

- Optionally, enable the Enhanced Access Security Gateway as described in [Enabling the Enhanced Access Security Gateway from the CLI](#) on page 222. The EASG functionality enables Avaya support personnel to access your Avaya Aura® Device Services system and resolve product issues in real-time. Avaya recommends that you enable EASG during installation.
- Install the Avaya Aura® Device Services application.

Related links

[Adding an Avaya Aura Device Services instance to System Manager](#) on page 270

[Considerations for large cluster deployments](#) on page 40

[Avaya Aura Device Services cluster installation](#) on page 198

Deploying the Avaya Aura® Device Services OVA through Solution Deployment Manager from System Manager

About this task

Use the procedure to create a virtual machine on the ESXi host and deploy Avaya Aura® Device Services OVA on the server provided by Avaya.

Before you begin

- Complete the Deployment checklist.

For information about the Deployment checklist, see *Deploying Avaya Aura® applications from System Manager*.

- Add a location.
- Add a required host to the location.
- Download the required OVA file to System Manager.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, click **New**.

Solution Deployment Manager displays the Applications Deployment window.

4. In the Select Location and Platform section, do the following:
 - a. In **Select Location**, select a location.
 - b. In **Select Platform**, select a platform.

The system displays the hostname in the **Platform FQDN** field.

5. In **Data Store**, select a data store, if not displayed upon host selection.

The Capacity Details section displays the capacity details.

6. Click **Next**.

7. In the Deploy OVA section, do the following:

- a. In **Select Software Library**, select the local or remote library where the OVA file is available.
- b. In **Select OVAs**, select the OVA file that you want to deploy.
- c. In **Flexi Footprint**, select the footprint size that the application supports.

8. Click **Next**.

9. On the Enhanced Access Security Gateway page, in **EASG User Access**, do one of the following:

- Select **1** to enable EASG. The EASG functionality enables Avaya support personnel to access your Avaya Aura® Device Services system and resolve product issues in real time. Avaya recommends that you enable EASG during installation.
- Select **2** to disable EASG.

If you select to disable EASG, you can enable it later from the Avaya Aura® Device Services CLI.

10. Click **Next**.

11. On the Properties page, specify the following: management network settings, public network settings, and administrator user details.

Although the system displays the **Out of Band Management** option, it is *not* supported in the current release.

12. Click **Deploy**.

13. Click **Accept the license terms**.

In the Platforms for Selected Location <location name> section, Solution Deployment Manager displays the deployment status in the **Current Action Status** column.

Solution Deployment Manager displays the virtual machine on the Applications for Selected Location <location name> page.

14. To view details, click **Status Details**.

Application Management field descriptions

Locations

Name	Description
Location Name	The location name.
City	The city where the platform is located.
Country	The country where the platform is located.

Button	Description
New	Displays the New Location section where you can provide the details of the location that you want to add.
Edit	Displays the Edit Location section where you can change the details of an existing location.
Delete	Deletes the locations that you select. The system moves the platforms associated with the deleted locations to unknown location.

Platforms

Name	Description
Platform Name	The name of the platform.
Platform IP	The IP address of the platform.
Platform FQDN	The FQDN of the platform.
IPv6	The IPv6 address of the platform. If the IP address of the ESXi platform only supports IPv4, the column does not display any value.
vCenter FQDN	The FQDN of vCenter.
Current Action	The operation that is currently being performed on the platform.
Last Action	The last operation completed on the platform.
License Status	The status of the license.
Platform Version	The platform version.
Offer Type	The platform type. The options are: • ASP: An Avaya Solutions Platform 130 Release 5.1 platform. • Customer VE: A customer-provided VMware ESXi platform • SWONLY: A customer-provided operating system platform • AVP: An Appliance Virtualization Platform platform
SSH Status	The SSH service status. The values are enabled and disabled.
Platform Certificate Status	The certificate status of Appliance Virtualization Platform, Avaya Solutions Platform 130, or standalone ESXi. If the ESXi is managed by vCenter, the system displays the value of this field as NA. The options are: • : The certificate is added in Solution Deployment Manager and is correct. • : The certificate is not accepted or is invalid. You can click View for details of the certificate status.
vCenter Certificate Status	The certificate status of the ESXi host. The options are: • : The certificate is correct. The system enables all the options in More Actions that apply to VMware ESXi host. • : The certificate is not accepted or is invalid. You can click View for details of the certificate status.

Note:

Depending on the Appliance Virtualization Platform, Avaya Solutions Platform 130, standalone ESXi, and vCenter certificate status, the system enables the options in **More Actions**.

Button	Description
Auto Refresh	Automatically refreshes the page with the latest changes. For example, the page updates: • The Application state when an application changes. • The license status or certificate status of the platform when the platform changes. The system refreshes the data every minute.
Add	Displays the Add Platform section where you can provide the details of the platform that you want to add.
Edit	Displays the Platform Information section where you can change the details of an existing platform.
Remove	Removes the platforms that you select only from the Solution Deployment Manager client. The system moves the platforms associated with the deleted locations to an unknown location.
Change Network Params > Change Host IP Settings	Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.
Change Network Params > Change Network Settings	Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.
Refresh Host	Refreshes one or more of the platforms. Solution Deployment Manager displays the following status in the Current Action column. • Refresh Completed: When the refresh platform action completes. • Refresh Failed: When the refresh platform action fails if Solution Deployment Manager is unable to communicate with the platform. • Refresh Queued: When the refresh platform action takes time.
More Actions > AVP Update/ Upgrade Management	Displays the Update host page where you can provide the Appliance Virtualization Platform patch file for updating the Appliance Virtualization Platform host.
More Actions > Change Password	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
More Actions > SSH > Enable SSH	Enables SSH for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts.
More Actions > SSH > Disable SSH	Disables SSH on the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts.
More Actions > Syslog config > Push	Displays the Push Syslog Configuration section where you can push the syslog configuration on the application host. Syslog is only for Appliance Virtualization Platform. You can select multiple platforms and Push syslog configuration on selected platforms.
More Actions > Syslog config > View	Displays the View Syslog Configuration section where you can view syslog profiles of selected Appliance Virtualization Platform platforms.

Button	Description
More Actions > Syslog config > Delete	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.
More Actions > Lifecycle Actions > Host Restart	Restarts the platform and applications that are running on the Appliance Virtualization Platform host.
More Actions > Lifecycle Actions > Host Shutdown	Shuts down the platform and applications that are running on the Appliance Virtualization Platform host.
More Actions > Generate/Accept Certificate	Displays the Certificate dialog box where you can manage certificates for the platform. Depending on the platform type, the options are: • Generate Certificate: To generate a certificate for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts. • Accept Certificate: To accept a valid certificate for the platform or vCenter. • Decline Certificate: To decline the certificate for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts. You must regenerate the certificate and accept if you decline a platform certificate.
More Actions > AVP Cert. Management > Manage Certificate	Displays the Load Certificate dialog box from where you can view/generate certificates for Appliance Virtualization Platform hosts, and download them. You can also upload and push third-party signed certificates to the selected platform.
More Actions > AVP Cert. Management > Generic CSR	Displays the Create/Edit CSR dialog box from where you create or edit the generic CSR data.
More Actions > Snapshot Manager	Displays the Snapshot Manager dialog box from where you can view and delete the application snapshot.
More Actions > WebLM Configuration	Displays the WebLM Configuration dialog box from where you configure WebLM Server for an Appliance Virtualization Platform host.
More Actions > AVP Firewall Rules	Displays the Firewall Settings dialog box from where you can view the firewall rules details for an Appliance Virtualization Platform host.
More Actions > Set Login Banner	Displays the Message of the Day dialog box from where you can push the login banner text to the selected platform.  Note: This feature is only available in System Manager Solution Deployment Manager. Solution Deployment Manager Client does not support Set Login Banner.

Applications

Name	Description
Application Name	The name of the application.
Application IP	The IP address of the application.

Name	Description
Application FQDN	The FQDN of the application.
Application IPv6	The IPv6 address of the application, if any.
App Name	The name of the application. For example, Session Manager.
App Version	The version of the application. For example, 8.1.
Application State	The state of the application. The states are: • Started • Stopped
Current Action Status	The status of the current operation. The options are: • Deploying • Starting • Stopping The Status Details link provides the details of the operation in progress.
Last Action	The last action performed on the application.
Platform Name	The platform name of the operating system, VMware host, or Appliance Virtualization Platform host on which the application resides.
Platform Type	The platform type of the operating system.
Trust Status	The status of the connection between System Manager and the application. The options are: • Success • Failed When the connection between System Manager and the application is established, Trust Status changes to Success. Only when the trust status is Success, you can perform other operations.
Data Store	The data store name.

Button	Description
New	Displays the Application Deployment section where you can provide the platform and deploy an application.
Edit	Displays the Application Deployment section where you can change the details of an application.
Delete	Turns off the applications and deletes the selected application from platform and Solution Deployment Manager Client.
Start	Starts the selected applications.
Stop	Stops the selected applications.
Show Selected	Displays only the selected applications.

Button	Description
VM Console > Open VM Console in New Window	Opens the application VM console in the new browser window.
VM Console > Open VM Console in New Tab	Opens the application VM console in the new tab of the browser.
More Actions > Restart	Starts the selected applications that were stopped earlier.
More Actions > Refresh App	Updates the status of the applications.
More Actions > Re-establish connection	Establishes the connection between System Manager and the application. The Trust Status then changes to Success .
More Actions > Update Static Routing	Displays the VM Update Static Routing section where you can update the IP address of AVP Utilities for static routing.
More Actions > Syslog config > Push	Displays the Push Syslog Configuration section where you can push the syslog configuration on the selected application.
More Actions > Syslog config > View	Displays the View Syslog Configuration section where you can view all configured syslog profiles.
More Actions > Syslog config > Delete	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.

Logging on to the Avaya Aura[®] Device Services console on VMware

About this task

Use this procedure if the Avaya Aura[®] Device Services VM is not already powered on.

Procedure

1. Select the host server, right-click the Avaya Aura[®] Device Services virtual machine.
2. Select **Power**, and click **Power On**.
3. Click the **Console** tab.

The system prompts you to type the login name and password.

4. Log in as the administrative user.

Next steps

All prerequisites for installation are now complete. You can now use the binary installer to complete the installation of the Avaya Aura[®] Device Services server.

Enabling IPv6 support at the system layer

About this task

When IPv6 is enabled, you can use both IPv4 and IPv6 addresses to access Avaya Aura® Device Services. You must enable IPv6 support at the system layer first and then enable it at the application layer. This procedure describes how to enable IPv6 on the system layer.

! Important:

AWS, Microsoft Azure, and GCP software-only deployments *do not* support IPv6.

Procedure

1. Log in to the virtual machine where you plan to deploy the Avaya Aura® Device Services application as an administrator.
2. Run the following command to start an interactive IPv6 configuration:

```
sys ipv6config set
```

+ Tip:

For general information about the `sys ipv6config` command, run the following command:

```
sys ipv6config -h
```

For more information, see [sys ipv6config command](#) on page 67.

3. Follow the system prompts to complete the procedure.

Next steps

Enable IPv6 at the application layer during Avaya Aura® Device Services installation.

Enabling FIPS mode

About this task

FIPS is a cryptographic security standard. Use this procedure if your enterprise requires FIPS-compliant cryptographic algorithms only.

FIPS mode is enabled at the operating system level before starting the Avaya Aura® Device Services installation. If FIPS is enabled in the operating system, then Avaya Aura® Device Services will be installed in FIPS mode. Otherwise, Avaya Aura® Device Services will be installed in non-FIPS mode. FIPS installation is only supported for new installations. You cannot upgrade a non-FIPS system to a FIPS system. If you want to enable FIPS on a non-FIPS system or disable FIPS on a FIPS system, you must uninstall the Avaya Aura® Device Services application first, change FIPS mode, and then install Avaya Aura® Device Services.

! Important:

The following features are unavailable in FIPS mode:

- OAuth / SAML authorization
- Onboard Open LDAP

*** Note:**

- If FIPS mode is enabled, you must use the Secure LDAP (LDAPS) protocol to configure LDAP.
- In cluster deployments, if FIPS mode is enabled, SSL encryption for internode communication between the database servers on the Avaya Aura® Device Services nodes is enabled by default.

Before you begin

If you deploy Avaya Aura® Device Services in Avaya Aura® environment, ensure that FIPS mode is enabled on both System Manager and Session Manager.

- For more information about enabling FIPS on System Manager, see the “Security” chapter in *Administering Avaya Aura® System Manager*.
- For more information about enabling FIPS on Session Manager, see the “Security” chapter in *Administering Avaya Aura® Session Manager*.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to enable FIPS mode:

```
sys seconfig --fips --enable
```

3. **(Optional)** To review the FIPS status, run the following command:

```
sys seconfig --fips --query
```

Disabling FIPS mode

About this task

After Avaya Aura® Device Services is installed with FIPS mode enabled, you *cannot* switch back to non-FIPS mode. You must uninstall Avaya Aura® Device Services first, disable FIPS mode and then reinstall Avaya Aura® Device Services.

Procedure

1. Uninstall Avaya Aura® Device Services.

For more information, see [Uninstalling Avaya Aura Device Services](#) on page 226.

2. Run the following command:

```
sys seconfig --fips --disable
```

Enabling additional STIG hardening

About this task

The Security Technical Implementation Guides (STIGs) are the requirements that, when implemented, enhance application security and monitoring capabilities. By default, Avaya Aura® Device Services enables essential STIG hardening options during the system layer installation or upgrade. These default settings are appropriate for most deployments. If your organization requires stricter STIG compliance, use this procedure to enable additional Linux STIG security hardening options.

! Important:

You *cannot* enable additional STIG hardening in software-only deployments.

* Note:

After you enable additional STIG hardening, ensure that the length of the automatic backup password is at least 15 characters.

Procedure

1. Log in to the virtual machine with the Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to enable additional STIG hardening options:

```
sys seconfig --stig --enable
```

3. When prompted, press **c** to apply new password rules.
4. **(Optional)** To review the STIG hardening status, run the following command:

```
sys seconfig --stig --query
```

Disabling additional STIG hardening

About this task

Use this procedure to disable additional STIG hardening. The default STIG hardening options, which are enabled during the system layer installation or upgrade process, will still be available. Avaya Aura® Device Services also continues to use the password complexity rules that were set up when you enabled additional STIG hardening.

Procedure

1. Log in to the virtual machine with the Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to disable additional STIG hardening:

```
sys seconfig --stig --disable
```

3. **(Optional)** To review the STIG hardening status, run the following command:

```
sys seconfig --stig --query
```

Configuring UEFI Secure Boot for OVA-based virtual machines

About this task

Unified Extensible Firmware Interface (UEFI) is an interface between the operating system and the platform firmware that replaces the legacy BIOS interface. Secure Boot is an UEFI feature that secures the operating system boot-up process by preventing the loading of boot loaders and drivers that are not signed with a trusted digital signature.

By default, Avaya Aura® Device Services Release 10.2.x OVA-based deployments have UEFI and Secure Boot enabled. For security reasons, Avaya recommends that you use Secure Boot whenever possible.

For more information about managing Secure Boot settings on VMware virtual machines, see [UEFI Secure Boot](#) in the VMware product documentation.

Before you begin

Deploy a virtual machine.

Procedure

1. Log in to the vSphere Client.
2. Navigate to a Avaya Aura® Device Services virtual machine.
3. Right-click the virtual machine and select **Edit Settings**.
4. Click the **VM Options** tab.
5. Click **Boot Options**.
6. Ensure that **Firmware** is set to **EFI (recommended)**.
7. Do one of the following:
 - To enable Secure Boot, select the **Secure Boot** check box.
 - To disable Secure Boot, clear the **Secure Boot** check box.
8. Click **OK**.

Checking the UEFI Secure Boot status

About this task

You can check whether the UEFI Secure Boot is enabled on a virtual machine.

Procedure

1. Log in to a virtual machine using an SSH connection.
2. To check the status, run the following command:

```
mokutil --sb-state
```

- If the command output is `SecureBoot enabled`, UEFI Secure Boot is enabled.

- If the command output is `Failed to read SecureBoot`, UEFI Secure Boot is disabled.

Chapter 6: Initial setup for software-only deployments

You can deploy Avaya Aura® Device Services as a software-only application using your own virtual or physical machines and RHEL 8.4 or RHEL 8.10. Avaya Aura® Device Services supports the following deployment options:

- VMware virtualization environment.
Avaya Aura® Device Services supports the following platforms:
 - ESXi: Releases 6.7, 7.0, or later.
 - Avaya Solutions Platform (ASP).
- Amazon Web Services (AWS) virtualization environment.
- Hyper-V virtualization environment.
- Google Cloud Platform (GCP) virtualization environment.
- Microsoft Azure virtualization environment.
- Nutanix 6.5 and later
- Physical servers.

After installing and configuring the operating system, you must install the system layer on virtual machines, and then use the common installation, configuration, and administration tasks to complete the Avaya Aura® Device Services deployment.

Related links

- [Initial setup for software-only VMware deployments](#) on page 98
- [Initial setup for software-only deployments on Amazon Web Services](#) on page 113
- [Initial setup for software-only Hyper-V deployments](#) on page 131
- [Initial setup for software-only Microsoft Azure deployments](#) on page 141
- [Initial setup for software-only Google Cloud Platform deployments](#) on page 157

Initial setup for software-only VMware deployments

The following sections describe how to deploy a virtual machine for the software-only deployment type in an VMware environment.

Software-only installation checklist for VMware-based environment

The following checklist outlines the tasks that you must perform when deploying Avaya Aura® Device Services as a software-only application on your own physical servers or in VMware-based environment.

No.	Task	Notes	✓
1	Ensure that virtual machines that you plan to use to deploy Avaya Aura® Device Services comply with the requirements for software-only installation.	See the requirements in Software requirements on page 31 and Avaya Aura Device Services virtual machine resource requirements on page 34.	
2	Download the Avaya Aura® Device Services software-only installation package from PLDS.	The software-only installation package includes the following files: • Software-only system layer installer. • Avaya Aura® Device Services application installer. The package file name has the <code>aads-swonly-AADS_VERSION.tgz</code> format. For more information about the software downloading process, see Downloading software from PLDS on page 74.	
3	Install RHEL 8.4 or RHEL 8.10.	Avaya Aura® Device Services Release 10.2.x requires RHEL 8.4 or RHEL 8.10. For more information about installation, see Red Hat Enterprise Linux installation on page 101 and the official Red Hat documentation. Avaya also recommends that you install the latest security updates on RHEL.	
4	Create disk partitioning on RHEL.	Avaya Aura® Device Services requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see Creating disk partitioning for VMware-based software-only deployments on page 102 and Disk partitions for software-only deployments on page 101.	
5	Create a non-root Linux user.	The installation and administration of the Avaya Aura® Device Services server is more secure when performed by non-root users with sudo privileges. For more information, see Creating an administrative user on page 103.	

No.	Task	Notes	✓
6	Enable the YUM package manager on RHEL.	The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation.	
7	Install additional packages required by Avaya Aura® Device Services.	By default, RHEL 8.4 or RHEL 8.10 does not contain certain packages that Avaya Aura® Device Services requires. You must install these packages manually. For more information, see Additional packages required by Avaya Aura Device Services on page 104 and Installing additional RHEL 8.4 or RHEL 8.10 packages manually on page 105.	
8	Enable the Haveged service.	See Enabling the Haveged service on page 105.	
9	Enable FIPS mode (optional).	For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information about enabling FIPS, see Enabling FIPS for software-only systems on page 106.	
10	Do one of the following to manage additional RHEL packages: • Register your RHEL instance to the Red Hat subscription. • Create a local repository for RPM installation or updates.	For more information, see RHEL packages management on page 107 and Enabling required RHEL repositories on page 107. Registering your RHEL instance to the Red Hat subscription is the preferred option.	
11	Install the software-only system layer on your RHEL.	The system layer is low-level software that forms the required operational environment for Avaya Aura® Device Services. For more information, see Installing the system layer on page 108.	
12	Ensure that: • The chronyd service is up and running. • System Manager and Session Manager are reachable from your virtual machine. This is only required if you deploy Avaya Aura® Device Services in Avaya Aura® environment.	Perform these checks to ensure that the system layer is installed successfully so you can install the Avaya Aura® Device Services application. For more information, see Checking the Chrony service status on page 111 and Checking the connection to System Manager and Session Manager on page 111.	
13	Enable IPv6 support (optional).	For more information, see Enabling IPv6 support for software-only deployments on page 112.	

After deploying a virtual machine, install the application layer as described in the “Avaya Aura® Device Services installation” chapter.

Red Hat Enterprise Linux installation

When you deploy Avaya Aura® Device Services as a software-only solution, you must use the RHEL 8.4 or RHEL 8.10. For details about obtaining and installing RHEL 8.4 or RHEL 8.10, see the Red Hat website <https://www.redhat.com>.

After obtaining RHEL 8.4 or RHEL 8.10, do the following:

1. Install the RHEL 8.4 or RHEL 8.10 operating system by using the Red Hat installation procedures.

Important:

Avaya Aura® Device Services requires specific disk partitioning. You can create the required data disks and physical volumes for data disks during or after RHEL 8.4 or RHEL 8.10 installation using the values provided in [Disk partitions for software-only deployments](#) on page 101.

2. Install the latest critical security updates.

For update procedures, see Red Hat documentation. You can install security updates by using the YUM package manager.

Disk partitions for software-only deployments

The following table shows Avaya Aura® Device Services disk partitions and their logical volumes with appropriate sizes:

Disk	Disk size (GB)	Mount Point
Disk 1: • /dev/sda for VMware • /dev/xvda for AWS • /dev/sda for Microsoft Azure	125	–
Disk 2: • /dev/sdb for VMware • /dev/xvdb for AWS • /dev/sdc for Microsoft Azure	70	/var/log/Avaya
Disk 3: • /dev/sdc for VMware • /dev/xvdc for AWS • /dev/sdd for Microsoft Azure	40	/media/data

Disk	Disk size (GB)	Mount Point
Disk 4: • /dev/sdd for VMware • /dev/xvdd for AWS • /dev/sde for Microsoft Azure	10	/media/cassandra

Creating disk partitioning for VMware-based software-only deployments

About this task

Avaya Aura® Device Services requires a specific disk layout that includes several disk partitions and logical volumes. Use this procedure to create appropriate disk partitioning.

Before you begin

- Install RHEL.
- Create volumes with the required disk size values. For more information, see “Disk partitions for software-only deployments”.

Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. To create the required directories, run the following commands:

```
mkdir -p /var/log/Avaya
mkdir -p /media/data
mkdir -p /media/cassandra
```

3. To create the required physical volumes and volume groups for these volumes, run the following commands:

```
pvcreate -f /dev/sdb
vgcreate disk2_vg /dev/sdb
pvcreate -f /dev/sdc
vgcreate disk3_vg /dev/sdc
pvcreate -f /dev/sdd
vgcreate disk4_vg /dev/sdd
```

4. To create logical volumes in the volume groups, run the following commands:

```
lvcreate -l100%FREE -n application_log /dev/disk2_vg
lvcreate -l100%FREE -n data /dev/disk3_vg
lvcreate -l100%FREE -n cassandra /dev/disk4_vg
```

5. To create a file system for the /dev/sdb partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk2_vg/application_log
mount /dev/disk2_vg/application_log /var/log/Avaya
echo "/dev/disk2_vg/application_log /var/log/Avaya xfs defaults 0 0" >> /etc/fstab
```

6. To create a file system for the `/dev/sdc` partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk3 vg/data
mount /dev/disk3_vg/data /media/data
echo "/dev/disk3_vg/data /media/data xfs defaults 0 0" >> /etc/fstab
```

7. To create a file system for the `/dev/sdd` partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk4 vg/cassandra
mount /dev/disk4_vg/cassandra /media/cassandra
echo "/dev/disk4_vg/cassandra /media/cassandra xfs defaults 0 0" >> /etc/fstab
```

Creating an administrative user

About this task

You must use a non-root Linux user with sudo privileges to install the Avaya Aura® Device Services application. The User ID (UID) of the Linux user that performs the installation must be the same on all nodes in the cluster.

This procedure describes how to add a user and an administrative group. For a clustered deployment of Avaya Aura® Device Services, perform the steps described in this procedure on every node in the cluster.

! Important:

You must create only one administrative user on each virtual machine.

Before you begin

Deploy RHEL 8.4 or RHEL 8.10 on virtual machines.

Procedure

1. Log in to the virtual machine with deployed RHEL 8.4 or RHEL 8.10 as the root user using an SSH connection.
2. Run the following command to create a group for the administrative user:

```
groupadd -g 4001 <admin_group>
```

In this command, `<admin_group>` is one of the following:

- If you fresh install Release 10.2.x, this is a group name of your choice.
- If you migrate from a previous Avaya Aura® Device Services release, this is the same administrative group that you use in that release.

For example:

```
groupadd -g 4001 admingrp
```

! Important:

For Group ID (GID), you must use 4001.

3. Run the following command to add an administrative user in the new administrative group:

```
usermod -g <admin_group> -u 4001 <admin_name>
```


In this command, `<admin_group>` is the name of the group you created in the previous step, and `<admin_name>` is one of the following:

- If you fresh install Release 10.2.x, this is the name of the administrative user that you created when deploying the virtual machine.
- If you migrate from a previous Avaya Aura® Device Services release, this is the same administrative user that you use in that release.

For example:

```
usermod -g admingrp -u 4001 aadsadmin
```

 Important:

For User ID (UID), you must use 4001.

4. Run the following command to create a password for the new administrative user and then enter the password:

```
passwd <admin_name>
```

In this command, `<admin_name>` is the administrative user name. For example:

```
passwd aadsadmin
```

5. Run the following command to provide sudo privileges for the new administrative user:

```
usermod -aG wheel <admin_name>
```

For example:

```
usermod -aG wheel aadsadmin
```

Next steps

- Enable the YUM package manager on RHEL.
- Install additional packages required by Avaya Aura® Device Services.

Related links

[Characters supported for Avaya Aura Device Services passwords](#) on page 56

Additional packages required by Avaya Aura® Device Services

In software-only deployments, Avaya Aura® Device Services requires certain packages that RHEL 8.4 or RHEL 8.10 does not include by default. You must manually install the following packages:

- `haveged-1.9.14-1.el8.x86_64.rpm` or later.
- `tomcat-native-1.2.23-1.el8.x86_64.rpm` or later. This package is only required if you want to use Avaya Aura® Device Services in FIPS mode.

These packages are available from the Extra Packages for Enterprise Linux (EPEL) Fedora Special Interest Group.

For information about installing packages from the EPEL repository see the [EPEL FAQ](#). You must only install these packages if you deploy Avaya Aura® Device Services as a software-only application.

Installing additional RHEL 8.4 or RHEL 8.10 packages manually

About this task

If you do not have the EPEL repository on your RHEL 8.4 or RHEL 8.10, you can install the additional packages required by Avaya Aura® Device Services manually.

Before you begin

Download the appropriate package or packages on your local machine.

Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. Upload packages to the virtual machine to the `/root` directory.

Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.

3. To install a package, run the following command:

```
rpm -ivh /root/<PACKAGE_NAME>
```

For example, to install Haveged package `haveged-1.9.14-1.el8.x86_64.rpm`, run the following command:

```
rpm -ivh /root/haveged-1.9.14-1.el8.x86_64.rpm
```

4. Repeat the previous step for all packages you need to install.

Next steps

Enable the Haveged service on RHEL.

Enabling the Haveged service

About this task

Haveged is a random number generator based on the HAVEGE algorithm designed for the use on Linux systems.

This procedure applies to software-only deployments and is not required for OVA-based deployments.

Before you begin

Install the Haveged package.

Procedure

1. Log in to the virtual machine as an administrator using an SSH connection.
2. Run the following command to start the Haveged service:


```
systemctl start haveged
```
3. Run the following command to start Haveged automatically after each system restart:


```
systemctl enable haveged
```

Enabling FIPS for software-only systems

About this task

FIPS is a cryptographic security standard. Use this procedure if your enterprise requires FIPS-compliant cryptographic algorithms only.

For software-only installations, FIPS mode is enabled at the operating system level before installing the system layer. If FIPS is enabled in the operating system, Avaya Aura® Device Services are installed in FIPS mode. If not, they are installed in non-FIPS mode. FIPS installation is supported for new installations only. You cannot upgrade a non-FIPS system to a FIPS system. If you want to enable FIPS on a non-FIPS system or disable FIPS on a FIPS system, you must uninstall the Avaya Aura® Device Services application first, change FIPS mode, and then re-install Avaya Aura® Device Services.

! Important:

- You must enable FIPS before installing the system layer.
- The following feature is unavailable in FIPS mode:
 - Onboard Open LDAP

* Note:

- If FIPS mode is enabled, use the Secure LDAP (LDAPS) protocol to configure LDAP.
- If FIPS mode is enabled in cluster deployments, SSL encryption for internode communication between the database servers on the Avaya Aura® Device Services nodes is enabled by default.

Before you begin

Download and install package `tomcat-native-1.2.23-1.el8.x86_64.rpm` or later.

Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. Open the `/etc/ssh/sshd_config` file in a text editor.

For example, to open the file in `vi`, run the `vi /etc/ssh/sshd_config` command.

3. Add the following three entries to the file:

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512,hmac-sha2-256,hmac-sha1
Kexalgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha1
```

4. Save the `/etc/ssh/sshd_config` file.
5. Open the `/etc/ssh/ssh_config` file in a text editor.

For example, to open the file in `vi`, run the `vi /etc/ssh/ssh_config` command.

6. Add the following two entries to the file:

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512,hmac-sha2-256
```

7. Save the `/etc/ssh/ssh_config` file.
8. Open `/usr/share/crypto-policies/back-ends/FIPS/opensshserver.config` file in a text editor.
 - a. Remove the existing line.
 - b. Add the line: `CRYPTO_POLICY='-oCiphers=aes256-ctr,aes192-ctr,aes128-ctr -oMACS=hmac-sha2-512,hmac-sha2-256'`.
9. Save `/usr/share/crypto-policies/back-ends/FIPS/opensshserver.config`.
10. Restart `sshd` service using `systemctl restart sshd`.
11. Complete the steps listed in the [Federal standards and regulations](#) section of the Red Hat documentation.

RHEL packages management

The system layer requires additional RHEL packages, which are not available by default. To obtain these packages, you can do one of the following:

- Subscribe to the Red Hat subscription.

Avaya recommends this option. For more information about the subscription process, see the Red Hat website <https://www.redhat.com>.

Important:

- If you use the Red Hat Network subscription, you must enable additional RPMs from the RHEL CLI as described in [Enabling required RHEL repositories](#) on page 107.
- For AWS software-only deployments, if you use the Red Hat Network subscription, you must assign a public IP address to each of your AWS instances using the AWS Elastic IP service.
- For Microsoft Azure software-only deployments, if you use the Red Hat Network subscription, you must assign a public IP address to each of your Microsoft Azure instances using the Microsoft Azure Static IP service.
- For Google Cloud Platform software-only deployments, if you use the Red Hat Network subscription, you must assign a public IP address to each of your Microsoft Azure instances. You can assign either static or dynamic public IP addresses.
- Create a local repository for RPM installation or updates.

Enabling required RHEL repositories

About this task

If you subscribe to the Red Hat subscription, you must enable the following RHEL repositories before installing the system layer:

- `rhel-8-for-x86_64-baseos-rpms`

- rhel-8-for-x86_64-appstream-rpms

These repositories contain RPMs that are required for system layer installation.

Before you begin

Subscribe to the Red Hat subscription.

Procedure

1. Log in to the RHEL virtual machine as the root user using an SSH connection.
2. Run the following command to view the enabled repositories:

```
yum repolist
```

3. Ensure that the command output contains the following entries in the “repo id” column:

- rhel-8-for-x86_64-baseos-rpms for rhel-8-for-x86_64-baseos-rpms.
- rhel-8-for-x86_64-appstream-rpms for rhel-8-for-x86_64-appstream-rpms

4. If the command output does not contain the required entries, do the following:

- To enable the rhel-8-for-x86_64-baseos-rpms repository, run the following command:

```
subscription-manager repos --enable=rhel-8-for-x86_64-baseos-rpms
```

- To enable the rhel-8-for-x86_64-appstream-rpms repository, run the following command:

```
subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms
```

Installing the system layer

About this task

The system layer is a low-level software that provides the required operational environment for the Avaya Aura® Device Services application.

During installation, the system downloads the required packages from the remote repository. The package installation might take up to 10 minutes depending on your network bandwidth.

Before you begin

- Install RHEL 8.4 or RHEL 8.10 on virtual machines.
- Create disk partitioning for the virtual machine.
- Enable the YUM package management on RHEL. For more information, see Red Hat documentation on the <https://www.redhat.com> website.
- Create at least one non-root administrative user as described in [Creating an administrative user](#) on page 103.
- Download the `aads-swonly-<AADS_VERSION>.tgz` software-only installation package from PLDS.
- Obtain the FQDN of the IP address of a Network Time Protocol (NTP) server.

The system will be in **Permissive** mode by default. When you install SELinux in the system, **Enforcing** mode is enabled in RHEL. You must change SELinux to enforcing mode to update the system layer.

- Verify if SELinux is enforcing.

```
# getenforce
```

- Open the file `/etc/selinux/config` in a text editor of your choice.

For example: `# vi /etc/selinux/config`

- Configure the **SELINUX=enforcing** option:

This file controls the state of SELinux on the system.

SELINUX= accepts one of the following values:

- # enforcing - SELinux security policy is enforced.
- # permissive - SELinux prints warnings instead of enforcing.
- # disabled - No SELinux policy is loaded.

- SELINUX=enforcing

- # SELINUXTYPE= can take one of these two values:
- # targeted - Targeted processes are protected
- # mls - Multi Level Security protection
- SELINUXTYPE=targeted

- Save the change, and restart the system:

```
# reboot
```

Note:

Avaya recommends using the NTP servers of your organization instead of public NTP servers.

- If you are planning to use FIPS, enable it as described in [Enabling FIPS for software-only systems](#) on page 106. You cannot enable FIPS mode during or after Avaya Aura® Device Services installation.

Procedure

1. Upload the software-only installation package on the virtual machine to the `/root` directory.

Use a file transfer program of your choice, such as SFTP, SCP or WinSCP.

2. Log in to the virtual machine as the root user.
3. To extract the content of the installation package, run the following command:

```
tar -xzf aads-swnonly-<AADS_VERSION>.tgz
```

For example: `tar -xzf aads-swnonly-8.1.3.0.x.tgz`

The `/root/aads-swonly-AADS_RELEASE/` directory contains the following files:

- The system layer package in TGZ archive `ucapp-swonly-system-<VERSION>.tgz`.
- The Avaya Aura® Device Services application binary `aads-<AADS_RELEASE>.bin`.

4. Go to the directory with the extracted installation package:

```
cd aads-swonly-<AADS_VERSION>
```

5. To extract the content of the archive with the system layer installation files, run the following command:

```
tar -xzf ucapp-swonly-system-<SYSTEM_LAYER_VERSION>.tgz
```

For example: `tar - xzf ucapp-swonly-system-1.0.0.0.1.tgz`

6. Go to the directory with the extracted system layer package:

```
cd ucapp-swonly-system-<SYSTEM_LAYER_VERSION>
```

7. Run the following command to install the system layer:

```
./swOnlyUpdate.sh --install
```

8. When the system prompts you to enable the Enhanced Access Security Gateway (EASG) functionality, do one of the following:

- Enter `yes` to enable EASG.

The EASG functionality enables Avaya support personnel to access your Avaya Aura® Device Services system and resolve product issues in real time. Avaya recommends that you enable EASG during installation.

- Enter `no` if you do not want to enable the EASG functionality.

If you select `no`, you can enable it later if required.

9. When the system prompts you, provide the IP address or FQDN of the NTP server.
10. After the system reboots, run one of the following commands to ensure that system layer is installed:

- `sys versions`

- `/root/aads-swonly-<AADS_RELEASE>/ucapp-swonly-system-<SYSTEM_LAYER_VERSION>/swOnlyUpdate.sh --status`

Next steps

- Ensure that:
 - The Chrony service is running.
 - System Manager and Session Manager are reachable.
- If you deploy Avaya Aura® Device Services in an AWS environment, create target groups to forward traffic from the load balancer to nodes.
- Install the Avaya Aura® Device Services application.

Checking the Chrony service status

About this task

For the optimal functioning of the Avaya Aura® Device Services server, the local system clock must have an accuracy of 100 milliseconds or less. You must ensure that the Chrony service is running on the virtual machine before installing the Avaya Aura® Device Services application.

Procedure

1. Log in to the virtual machine CLI as the root user using an SSH connection.
2. To verify that the Chrony service is running, run the following command:

```
systemctl status chronyd
```

Ensure that the system displays `active (running)`.

3. If the Chrony service is not running, run the following command:

```
systemctl start chronyd
```

4. To verify that the system clock is synchronized, run the following command:

```
ntpstat
```

5. Ensure that the system displays `synchronized to NTP server`.

Checking the connection to System Manager and Session Manager

About this task

You must ensure that System Manager and Session Manager are reachable before installing the Avaya Aura® Device Services application.

This procedure is only required if you deploy Avaya Aura® Device Services in Avaya Aura® environment.

Procedure

1. Log in to the virtual machine CLI as an administrator using an SSH connection.
2. Run the following commands:

```
ping -c 10 <SMGR_ADDRESS>
ping -c 10 <SM_ADDRESS>
```

In these commands, `<SMGR_ADDRESS>` is the FQDN of System Manager and `<SM_ADDRESS>` is the FQDN of Session Manager.

If System Manager and Session Manager are reachable, the system displays the following output for each command:

```
10 packets transmitted, 10 received, 0% packet loss
```

Next steps

Install the application layer as described in the “Avaya Aura® Device Services installation” chapter.

Enabling IPv6 support for software-only deployments

About this task

When IPv6 is enabled, you can use both IPv4 and IPv6 addresses to access Avaya Aura® Device Services. You must enable IPv6 support at the system layer first and then enable it at the application layer. This procedure describes how to enable IPv6 on the system layer for software-only deployments.

Procedure

1. Log in to the virtual machine where you plan to deploy the Avaya Aura® Device Services application as the root user.
2. Open the `/etc/sysconfig/network-scripts/ifcfg-eth0` file in a text editor of your choice.

For example: `vi /etc/sysconfig/network-scripts/ifcfg-eth0`.

3. Add the following entries to the file:

```
IPV6INIT=yes
IPV6ADDR=<IPV6_ADDRESS>
IPV6_DEFAULTGW=<IPV6_DEFAULT_GATEWAY_ADDRESS>
```

In these entries:

- `<IPV6_ADDRESS>` is an IPv6 address that you want to use for Avaya Aura® Device Services. This IPv6 address can optionally contain the IPv6 prefix.
- `<IPV6_DEFAULT_GATEWAY_ADDRESS>` is the IPv6 default gateway address.

Do *not* enclose the `IPV6ADDR` and `IPV6_DEFAULTGW` parameter values with quotation marks.

The following is an example of the configured IPv6 settings:

```
IPV6INIT=yes
IPV6ADDR=2001:0DB8:A001::0123/64
IPV6_DEFAULTGW=2001:0DB8:A001::1
```

4. Save the file.
5. To restart the RHEL networking service, run the following commands:

```
nmcli connection reload
nmcli networking off && nmcli networking on
```

Next steps

Enable IPv6 at the application layer when installing the Avaya Aura® Device Services application.

Initial setup for software-only deployments on Amazon Web Services

The following sections describe how to deploy a virtual machine in an Amazon Web Services environment.

Software-only installation checklist for Amazon Web Services

The following checklist outlines the tasks that you must perform when deploying Avaya Aura® Device Services as a software-only application in an AWS environment.

No.	Task	Notes	✓
1	Ensure that the virtual machines that you plan to use to deploy Avaya Aura® Device Services comply with the requirements for software-only installation.	Avaya Aura® Device Services supports the c4.2xlarge AWS instance type. For more information, see Resources profile specifications for Avaya Aura Device Services on Amazon Web Services on page 37.	
2	Download the Avaya Aura® Device Services software-only installation package from PLDS.	The software-only installation package includes the following files: • Software-only system layer installer. • Avaya Aura® Device Services application installer. The package file name has the <code>aads-swonly-AADS_VERSION.tgz</code> format. For more information about the software downloading process, see Downloading software from PLDS on page 74.	
3	Prepare your AWS instance for software-only installation.	See Prerequisites for software-only deployment on AWS on page 115.	
4	Create security groups on AWS.	See Creating security groups on page 118.	
5	Install RHEL 8.4 or RHEL 8.10 on AWS.	Avaya Aura® Device Services Release 10.2.x requires RHEL 8.4 or RHEL 8.10. For more information about installation, see Installing RHEL 8.4 or RHEL 8.10 on AWS on page 121.	
6	Configure security groups for the eth1 secondary network interface.	See Configuring security groups for the secondary eth1 interface on page 123.	
7	Enable root access to RHEL.	RHEL deployed on AWS does not have the root user enabled by default. For more information, see Enabling root access on page 124.	

No.	Task	Notes	✓
8	Create disk partitioning on RHEL.	Avaya Aura® Device Services requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see Creating disk partitioning for software-only deployments on AWS on page 124 and Disk partitions for software-only deployments on page 101.	
9	Create a non-root Linux user.	The installation and administration of the Avaya Aura® Device Services server is more secure when performed by non-root users with sudo privileges. For more information, see Creating an administrative user on page 103.	
10	Enable the YUM package manager on RHEL.	The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation.	
11	Install additional packages required by Avaya Aura® Device Services.	By default, RHEL 8.4 or RHEL 8.10 does not contain certain packages that Avaya Aura® Device Services requires. You must install these packages manually. For more information, see Additional packages required by Avaya Aura Device Services on page 104 and Installing additional RHEL 8.4 or RHEL 8.10 packages manually on page 105.	
12	Enable the Haveged service.	See Enabling the Haveged service on page 105.	
13	Enable FIPS mode (optional).	For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information about enabling FIPS, see Enabling FIPS for software-only systems on page 106.	
14	Do one of the following to manage additional RHEL packages: • Register your RHEL instance to the Red Hat subscription. • Create a local repository for RPM installation or updates.	For more information, see RHEL packages management on page 107 and Enabling required RHEL repositories on page 107. Registering your RHEL instance to the Red Hat subscription is the preferred option.	
15	Prepare you RHEL system for installing the software-only system layer.	See Prerequisites for installing the system layer on AWS on page 126.	

No.	Task	Notes	✓
16	Install the software-only system layer on your RHEL.	The system layer is low-level software that forms the required operational environment for Avaya Aura® Device Services. For more information, see Installing the system layer on page 108.	
17	In cluster deployments, create target groups for the load balancer.	See Creating target groups on page 127.	
18	In cluster deployments, configure Elastic load balancers.	See Creating and configuring Elastic load balancers on page 128.	
19	Ensure that: • The chronyd service is up and running. • System Manager and Session Manager are reachable from your virtual machine. This is only required if you deploy Avaya Aura® Device Services in Avaya Aura® environment.	Perform these checks to ensure that the system layer is installed successfully so you can install the Avaya Aura® Device Services application. For more information, see Checking the Chrony service status on page 111 and Checking the connection to System Manager and Session Manager on page 111.	

After deploying a virtual machine, install the application layer as described in the “Avaya Aura® Device Services installation” chapter.

Prerequisites for software-only deployment on AWS

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud and subnet settings.
- Add records with the following FQDNs to your DNS or AWS Route 53 hosted zone:
 - Avaya Aura® Device Services front-end FQDN.
 - Avaya Aura® Device Services Utility Server FQDN.
- Ensure that you have an NTP server. You can deploy your own NTP server or use the NTP server provided by AWS.
- Create key pairs. For more information, see [Creating a key pair](#) on page 118.
- If you are deploying an Avaya Aura® Device Services cluster, create load balancer certificates for the following FQDNs:
 - Avaya Aura® Device Services virtual FQDN.
 - Avaya Aura® Device Services Utility Server virtual FQDN.

For more information, see [Creating and applying load balancer certificates](#) on page 116.

Creating and applying load balancer certificates

About this task

Load balancers only appear in the private DNS within AWS. Therefore, certificates generated by external certificate authorities might not work. Use this procedure to obtain a certificate from System Manager within AWS.

Important:

Avaya recommends that you perform this procedure on the System Manager that you later connect to Avaya Aura® Device Services when installing the Avaya Aura® Device Services application. If you perform this procedure on another System Manager, you must import that System Manager CA to Avaya Aura® Device Services as described in “Managing truststore certificates” in *Administering Avaya Aura® Device Services*.

Procedure

1. On the System Manager web console, navigate to **Home > Services > Security > Certificates > Authority**.
2. Click **Add End Entity** and complete the settings in the following fields:
 - a. **End Entity Profile:** Type `<INBOUND_OUTBOUND_TLS>`.
 - b. **Username:** Type `<FQDN of the load balancer>`.

The FQDN of the load balancer is the service FQDN of the cluster. This domain name portion of the FQDN represents the domain name that clients use to access service. The FQDN must be the combination of the stack name followed by the domain. For example, if the stack name is `yourStack` and the domain is `your.domain.com`, then the FQDN is `yourStack.your.domain.com`.

Note:

The stack name must start with a letter and must contain only letters, numbers, or dashes. This stack name must be used during multi-node CloudFormation.

- c. **Password:** Type your password.
- d. **Confirm Password:** Retype your password.
- e. **CN, Common name:** Type `<FQDN of the load balancer>`.
- f. Subject Alternative Name section: In **DNS Name**, type the following FQDNs:
 - FQDN of the load balancer.
 - FQDNs of all Avaya Aura® Device Services nodes in the cluster.
 - FQDNs of all Utility Server nodes in the cluster, if you plan to use the Utility Server.
 - `localhost.localdomain`
- g. **Token:** Select the `PEM` file.

 Note:

The remaining fields are optional. For more information, see *Administering Avaya Aura® System Manager*.

3. Click **Add**.
4. Navigate to **Home > Services > Security > Certificates > Authority > Public Web**.

The system displays the EJBCA public page.

5. Click **Create Keystore**.
6. In **Username**, type the FQDN of the load balancer.
7. In **Password**, type the End Entity password that you created earlier.
8. Click **OK**.

The system displays the EJBCA Token Certificate Enrollment page.

9. In **Key length**, select the required key length.
A length of 2048 bits is recommended.
10. Click **Enroll** and select a text editor to view the certificate.
11. Save the PEM file to your computer.

12. Sign in to the AWS console and navigate to **Services > Security, Identity & Compliance > Certificate Manager**.

13. Click **Import a certificate**.

The system displays a form with three fields: **Certificate Body**, **Certificate private key**, and **Certificate chain**.

14. Open the PEM file you saved earlier with a text editor and do the following:

 Note:

You must include the BEGIN and END labels for each section that you paste into the form.

- a. In the Private Key section, copy the string from -----BEGIN PRIVATE KEY----- to -----END PRIVATE KEY----- and paste it into the **Certificate private key** field.
- b. In the Certificate section, copy the first certificate string from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE----- and paste it into the **Certificate body** field.
- c. In the Certificate section, copy the second certificate string from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE----- and paste it into the **Certificate chain** field.

15. Click **Review and import**.

16. Click **Import**.

The system imports the certificate and displays the status and details of the certificate.

17. Copy and save the ARN value in the Details section.

The ARN is required for the **Load balancer certificate ARN** field during the multi-node CloudFormation deployment.

Creating a key pair

About this task

A key pair is a set of public and private keys. The public key is used to encrypt data, such as the login password. The private key is used to decrypt the encrypted data. You provide this key pair when you create a CloudFormation stack, and use it for SSH access to the Amazon Machine Instances.

For more information, see the following website:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

Procedure

1. Sign in to the Amazon Web Services Management console.
2. In the left navigation pane, go to **NETWORK & SECURITY**, and click **Key Pairs**.
3. Click **Create Key Pair**.
4. In the Create Key Pair dialog box, in the **Key pair name** field, type a name for the key pair.
5. Click **Create**.

The system generates a *.pem file and prompts you to save the file on your computer. You can also view the created key pair name in the Key pair name column.

6. Save the *.pem file.

 Important:

When you create a key pair, save it. If you lose the key, you cannot retrieve it and you will not be able to access the instance.

Creating security groups

About this task

AWS uses security groups to control inbound and outbound traffic. For software-only installation, you must create the following security groups:

- Avaya Aura® Device Services security group.

This security group uses the primary eth0 interface.

- Utility Server security group.

This security group uses the secondary eth1 interface.

- Avaya Aura® Device Services load balance security group.
- Utility Server load balance security group.

Procedure

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2** > **Security group**.
2. Click **Create Security Group**.
3. In **Security group name**, type a name of your choice.
For example: `AADS security group eth0`
4. **(Optional)** In **Description**, type a description for the group.
5. From **VPC**, select the Virtual Private Cloud that you plan to use for Avaya Aura® Device Services.
6. Configure the inbound and outbound traffic rules for the group.
For more information, see the “Traffic rules” section for the appropriate group.
7. Repeat steps [2](#) on page 119 to [6](#) on page 119 to create the additional required security groups.
8. Make a note of the security group ID of the Utility Server security group.

You require this ID when configuring security groups for the secondary network interface.

Traffic rules for the Avaya Aura® Device Services security group

Inbound rules

Type	Protocol	Port range	Source
Custom TCP	TCP	31415	0.0.0.0/0
Custom TCP	TCP	8447	0.0.0.0/0
Custom TCP	TCP	7001	0.0.0.0/0
Custom TCP	TCP	8468	0.0.0.0/0
Custom TCP	TCP	8543	0.0.0.0/0
Custom TCP	TCP	7000	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
Custom TCP	TCP	8457	0.0.0.0/0
Custom TCP	TCP	3268	0.0.0.0/0
Custom TCP	TCP	21000	0.0.0.0/0
Custom TCP	TCP	9999	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0
Custom TCP	TCP	8440	0.0.0.0/0
Custom TCP	TCP	2009	0.0.0.0/0
Custom TCP	TCP	8458	0.0.0.0/0

Type	Protocol	Port range	Source
Custom TCP	TCP	3269	0.0.0.0/0
Custom TCP	TCP	8445	0.0.0.0/0
Custom TCP	UDP	161	0.0.0.0/0
Custom TCP	TCP	8442	0.0.0.0/0

Outbound rules

Type	Protocol	Port range	Source
All traffic	All	All	0.0.0.0/0
All traffic	All	All	::/0

Traffic rules for the Utility Server security group

Inbound rules

Type	Protocol	Port range	Source
Custom TCP	TCP	8468	0.0.0.0/0
Custom TCP	TCP	8543	0.0.0.0/0
Custom TCP	TCP	8458	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
Custom TCP	TCP	8457	0.0.0.0/0

Outbound rules

Type	Protocol	Port range	Source
All traffic	All	All	0.0.0.0/0
All traffic	All	All	::/0

Traffic rules for the Avaya Aura[®] Device Services load balancer security group

Inbound rules

Type	Protocol	Port range	Source
Custom TCP	TCP	8440	0.0.0.0/0
Custom TCP	TCP	8442	0.0.0.0/0
Custom TCP	TCP	8443	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
Custom TCP	TCP	8445	0.0.0.0/0
Custom TCP	TCP	9443	0.0.0.0/0

Outbound rules

Type	Protocol	Port range	Source
All traffic	All	All	0.0.0.0/0
All traffic	All	All	::/0

Traffic rules for the Utility Server load balancer security group**Inbound rules**

Type	Protocol	Port range	Source
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

Outbound rules

Type	Protocol	Port range	Source
All traffic	All	All	0.0.0.0/0
All traffic	All	All	::/0

Installing RHEL 8.4 or RHEL 8.10 on AWS**About this task**

Use this procedure to deploy the Red Hat Enterprise Linux (RHEL) 8.4 or RHEL 8.10 operating system on your AWS instance. If you are deploying a cluster, repeat this procedure for each Avaya Aura® Device Services node.

Before you begin

Create security groups.

Procedure

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2**.
2. Click **Launch instance**.
3. On the Choose an Amazon Machine Image page, in the left pane, click **Community AMIs** and then click the **Red Hat** check box.
4. From the list of operating systems, select the RHEL 8.4 or RHEL 8.10 and then click **Select**.

The following is an example of the RHEL 8.4 or RHEL 8.10 name: **RHEL-8.4_HVM-GA-20181017-X86_64-0-hOURLY2-gp2**

5. On the Choose an Instance Type page, select an appropriate instance type and then click **Next**.

For more information about the supported instance types, see [Resources profile specifications for Avaya Aura Device Services on Amazon Web Services](#) on page 37.

6. On the Configure Instance Details page, configure the settings as follows:
 - a. In **Network**, select the VPC that you configured for your deployment.
 - b. In **Subnet**, select the subnet that you configured for your deployment.
 - c. In **Domain join directory**, select one of the following:
 - If you plan to use your own DNS server, select **No directory**.
 - If you plan to use the AWS Route 53 for DNS, select an appropriate domain from Route 53.
 - d. In the Network interfaces area, create two ethernet network interfaces as follows:
 - `eth0` with the IP address of the Avaya Aura® Device Services node.
 - `eth1` with the IP address of the Utility Server.
 - e. For other parameters, keep the default values.
7. On the Add Storage page, create four EBS volumes using the values provided in [Disk partitions for software-only deployments](#) on page 101.

For **Volume type**, use **General Purpose SSD (gp2)** for all volumes.

The following image shows the configured volumes:

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ
Root	/dev/sda1	snap-0f9a46653a138be40	125	General Purpose SSD (gp2)	375 / 3000	N/A	☒
EBS	/dev/sdb	Search (case-insensit	70	General Purpose SSD (gp2)	210 / 3000	N/A	☒
EBS	/dev/sdc	Search (case-insensit	40	General Purpose SSD (gp2)	120 / 3000	N/A	☒
EBS	/dev/sdd	Search (case-insensit	10	General Purpose SSD (gp2)	100 / 3000	N/A	☒

Add New Volume

8. **(Optional)** On the Add Tags page, add tags for the management instance and volumes.
9. On the Configure Security Group page, do the following:
 - a. In **Assign a security group**, select **Select an existing security group**.
 - b. Select the Avaya Aura® Device Services security group that you created when configuring security groups.
10. On the Review Instance Launch page, verify the instance settings and then click **Launch**.

Next steps

- If you are using your own DNS server or a public DNS server, configure DNS settings as described in [Configuring DNS settings on RHEL](#) on page 123.
- Configure security groups for the secondary `eth1` interface.

Configuring DNS settings on RHEL

About this task

If you do not use the Route 53 DNS service, you must provide the IP address of a DNS server that you plan to use on RHEL.

Before you begin

Install RHEL on AWS.

Procedure

1. Log in to the RHEL as the root user using an SSH connection.
2. Open the `/etc/resolv.conf` file in a text editor.

For example: `vi /etc/resolv.conf`

3. Add the following entry to the file:

```
nameserver <DNS_ADDRESS>
```

In this entry, `<DNS_ADDRESS>` is the IP address of the DNS server that you plan to use in your deployment.

4. **(Optional)** Do one of the following:

- If the file does not contain the `search` entry, add the following entry:

```
search <DOMAIN_NAME>
```

In this entry, `<DOMAIN_NAME>` is your domain name. For example: `search mycompany.com`

- If the file contains the `search` entry, enter your domain name at the end of the entry.

Domain names must be separated with space characters. For example: `search example.com mydomain.com`

5. Save the file.

Configuring security groups for the secondary eth1 interface

About this task

When you configure the RHEL 8.4 or RHEL 8.10 instance, AWS assigns the same security group to all network interfaces. After launching the RHEL 8.4 or RHEL 8.10 instance, you must assign the appropriate security group to the secondary eth1 interface.

Before you begin

Launch the RHEL 8.4 or RHEL 8.10 instance.

Procedure

1. On the Amazon Web Services Management console, navigate to **Services > EC2 > Instances**.

2. Right-click the RHEL 8.4 or RHEL 8.10 instance that you created and then navigate to **Security > Change security groups**.
3. In the Instance details area, in **Network interface ID**, select the network ID of the secondary eth1 network interface.
4. In the Associated security groups area, click **Remove** for the security group assigned to the secondary network interface by default.
5. In the Associated security groups area, select the Utility Server security group that you created from the security group list and then click **Add security group**.
6. Click **Save**.

Enabling root access

About this task

You must use the root user to install the system layer. On RHEL installed on AWS, the root user is disabled by default, therefore you must enable it.

Procedure

1. Log in to your AWS instance using the AWS CLI as the ec2-user.
This is the default administration user, which does not require a login password.
2. Run the following command to edit the `/etc/ssh/sshd_config` file:

```
sudo vi /etc/ssh/sshd_config
```
3. Add the following line to the file:

```
PermitRootLogin yes
```
4. Save the file.
5. Run the following command to apply the changes:

```
sudo service sshd restart
```
6. Set a password for the root user using the following command:

```
sudo passwd root
```

Creating disk partitioning for software-only deployments on AWS

About this task

Avaya Aura® Device Services requires a specific disk layout that includes several disk partitions and logical volumes. Use this procedure to create appropriate disk partitioning.

Before you begin

- Install RHEL.
- Create volumes with the required disk size values. For more information, see “Disk partitions for software-only deployments”.

Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. To create the required directories, run the following commands:

```
mkdir -p /var/log/Avaya
mkdir -p /media/data
mkdir -p /media/cassandra
```

3. If you use either c5, c5a or c5n AWS instances, run the following command to determine the name and size of each volume in your deployment:

```
lsblk
```

The following is an example of the command output:

```
[aadsadmin ~]$ lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme3n1              259:0    0   40G  0 disk
nvme2n1              259:1    0   70G  0 disk
nvme1n1              259:2    0   10G  0 disk
nvme0n1              259:3    0  125G  0 disk
-nvme0n1p1           259:4    0  125G  0 part /
-nvme0n1p128         259:5    0    1M  0 part
```

In this example, the RHEL volumes have the following names and sizes:

- /dev/nvme0n1: 125 Gb
- /dev/nvme1n1: 10 Gb
- /dev/nvme2n1: 70 Gb
- /dev/nvme3n1: 40 Gb

This step is not required if you use c4 instances.

4. To create the required physical volumes and volume groups for these volumes, run the following commands:
 - If you use c4 AWS instances, run the following commands:

```
pvccreate -f /dev/xvdb
vgcreate disk2_vg /dev/xvdb
pvccreate -f /dev/xvdc
vgcreate disk3_vg /dev/xvdc
pvccreate -f /dev/xvdd
vgcreate disk4_vg /dev/xvdd
```

- If you use either c5, c5a, or c5n AWS instances, run the following commands:

```
pvccreate -f <name of 70 Gb volume>
vgcreate disk2_vg <name of 70 Gb volume>
pvccreate -f <name of 40 Gb volume>
vgcreate disk3_vg <name of 40 Gb volume>
pvccreate -f <name of 10 Gb volume>
vgcreate disk4_vg <name of 10 Gb volume>
```

For example:

```
pvccreate -f /dev/nvme2n1
vgcreate disk2_vg /dev/nvme2n1
pvccreate -f /dev/nvme3n1
```

```
vgcreate disk3_vg /dev/nvme3n1
pvccreate -f /dev/nvme1n1
vgcreate disk4_vg /dev/nvme1n1
```

5. To create logical volumes in the volume groups, run the following commands:

```
lvcreate -l100%FREE -n application_log /dev/disk2_vg
lvcreate -l100%FREE -n data /dev/disk3_vg
lvcreate -l100%FREE -n cassandra /dev/disk4_vg
```

6. To create a file system for the /dev/sdb partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk2_vg/application_log
mount /dev/disk2_vg/application_log /var/log/Avaya
echo "/dev/disk2_vg/application_log /var/log/Avaya xfs defaults 0 0" >> /etc/fstab
```

7. To create a file system for the /dev/sdc partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk3_vg/data
mount /dev/disk3_vg/data /media/data
echo "/dev/disk3_vg/data /media/data xfs defaults 0 0" >> /etc/fstab
```

8. To create a file system for the /dev/sdd partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk4_vg/cassandra
mount /dev/disk4_vg/cassandra /media/cassandra
echo "/dev/disk4_vg/cassandra /media/cassandra xfs defaults 0 0" >> /etc/fstab
```

Prerequisites for installing the system layer on AWS

In addition to the prerequisites for the software-only system layer installation that are common for all deployment types, AWS has the following specific prerequisites:

- Ensure that you configured the following FQDNs in the AWS Route 53 service or the DNS service that you use:
 - Avaya Aura® Device Services front-end FQDN.
 - Avaya Aura® Device Services Utility Server FQDN.
- On all Avaya Aura® Device Services nodes in your deployment, add information about each Avaya Aura® Device Services node to the `/etc/hosts` file in the following format:

`<IP_Address> <Corresponding_FQDN> <hostname>`

For example:

```
195.51.100.5 aads1.mycompany.com aads1
195.51.100.6 aads2.mycompany.com aads2
```

- Enable root access to RHEL. For more information, see [Enabling root access](#) on page 124.
- Create a non-root user on RHEL. For more information, see [Creating an administrative user](#) on page 103.
- If you are using a Red Hat subscription for RHEL package management, you must configure a public IP address on each of your AWS instances using the AWS Elastic IP service. For more information about setting up public IP addresses, see [Elastic IP addresses](#).

Creating target groups

About this task

In cluster deployments, target groups forward traffic from the load balancer to a specific node of the Avaya Aura® Device Services cluster when certain conditions are met.

You must configure two target groups for Avaya Aura® Device Services node IP addresses and two target groups for Utility Server IP addresses with the following parameters:

Group	Protocol	Port	IP to register
Target group for Avaya Aura® Device Services nodes #1	HTTPS	443	IP addresses of all Avaya Aura® Device Services nodes in the cluster. These are the IP addresses of the primary eth0 interface of cluster nodes. On the Avaya Aura® Device Services administration portal, you <i>must</i> enable the use of an external load balancer. For details, see <i>Administering Avaya Aura® Device Services</i> .
Target group for Avaya Aura® Device Services nodes #2	HTTPS	8445	IP addresses of all Avaya Aura® Device Services nodes in the cluster. These are the IP addresses of the primary eth0 interface of cluster nodes.
Target group for Utility Server nodes #1	HTTP	8468	IP addresses of the Utility Server on each node in the cluster. This is the IP addresses of the secondary eth1 interface of cluster nodes.
Target group for Utility Server nodes #2	HTTPS	8458	IP addresses of the Utility Server on each node in the cluster. This is the IP addresses of the secondary eth1 interface of cluster nodes.

Only perform this procedure if you have an Avaya Aura® Device Services cluster.

Procedure

Repeat the following steps for each target group:

1. On the Amazon Web Services Management console, navigate to **Services > EC2 > Target Groups**.
2. Click **Create target group**.

The Amazon Web Services Management displays the Specify group details page.

3. In the Basic configuration area, configure settings as follows:
 - a. In **Choose a target type**, select **IP addresses**.
 - b. In **Target group name**, type a name of your choice for the group.

- c. In **Protocol**, select the protocol specified for the group in the “Protocol” column of the table.
 - d. In **Port**, type the port number specified for the group in the “Port” column of the table.
 - e. In **VPC**, select the Virtual Private Cloud that you are using for your deployment.
 - f. In **Protocol version**, select **HTTP1**.
4. In the Health checks area, configure the settings as follows:
 - a. In **Health check protocol**, select **HTTP**.
 - b. In **Health check path**, type `/health`.
5. Click **Next**.
6. On the Register targets page, configure IP addresses for the group as follows:
 - a. In **IP**, type the IP address of a node as specified in the “IP to register” column of the table for the group you are configuring.
 - b. In **Port**, type the port number specified for the group in the “Port” column of the table.
 - c. Click **Include as pending below**.
 - d. Repeat substeps a to c for all remaining IP addresses that you must include in the group.
7. Click **Create target group**.
8. After creating all target groups, do the following:
 - a. Navigate to **Services > EC2 > Target Groups** and select the target group that you have created.
 - b. Select the target group for port 8445 that you have just created.
 - c. In the Attributes area, click **Edit**.
 - d. On the Edit attributes page, select the **Stickiness** check box.
 - e. Click **Save changes**.

Creating and configuring Elastic load balancers

About this task

The Elastic load balancer distributes incoming traffic between Avaya Aura[®] Device Services nodes. In cluster deployments, you must create the following two Elastic load balancers:

- For Avaya Aura[®] Device Services nodes.
- For the Utility Server.

Before you begin

- Create four target groups as described in [Creating target groups](#) on page 127.

- Ensure that you have the load balancer certificates for the following FQDNs:
 - Avaya Aura® Device Services front-end FQDN.
 - Avaya Aura® Device Services Utility Server FQDN.

For more information about creating certificates, see [Creating and applying load balancer certificates](#) on page 116.

Procedure

Repeat the following steps to create an Elastic load balancer for Avaya Aura® Device Services nodes and an Elastic load balancer for Utility Server nodes.

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2** > **Load Balancers**.
2. Click **Create Application Load Balancer**.
3. On the Configure Load Balancer page, configure the settings as follows:
 - a. In **Name**, type a name of your choice.
 - b. In **Scheme**, select **Internal**.
 - c. In **IP address type**, select **ipv4**.
 - d. In **Listener**, add listeners for each load balancer as follows:

Load balancer	Protocol	Port
Avaya Aura® Device Services load balancer	HTTPS	443
	HTTPS	8440
	HTTPS	8442
	HTTPS	8443
	HTTPS	8445
Utility Server load balancer	HTTP	80
	HTTPS	443

- e. In **VPC**, select the Virtual Private Cloud that you are using for your deployment.
 - f. In **Availability Zones**, select the subnet that you configured for all nodes in the cluster.
4. On the Configure Security Settings page, do the following:
 - a. In **Certificate Type**, select **Choose a certificate from ACM** and then select the certificates that you prepared for the Avaya Aura® Device Services and Utility Server FQDNs.
 - b. In **Security Policy**, select **ELBSecurityPolicy-TLS-1-2-2017-01**.
 5. On the Configure Security Groups page, in **Assign a security group**, select **Select an existing security group** and then select a security group as follows:
 - For the Avaya Aura® Device Services load balancer, select the Avaya Aura® Device Services load balancer security group that you created.

- For the Utility Server load balancer, select the Utility Server load balancer security group that you created.

For more information, see [Creating security groups](#) on page 118.

6. On the Configure Routing page, configure routing as follows:

a. In **Target**, select **Existing target group**.

b. In **Name**, select the target groups that you created as follows:

- For the Avaya Aura[®] Device Services load balancer, select the target group for Avaya Aura[®] Device Services nodes for port 443.

In [Creating target groups](#) on page 127, this is the “Target group for Avaya Aura[®] Device Services nodes #1” group.

- For the Utility Server load balancer, select the target group for Utility Server nodes for port 8468.

In [Creating target groups](#) on page 127, this is the “Target group for Utility Server nodes #1” group.

For more information about the target groups, see [Creating target groups](#) on page 127.

7. On the **Register Targets** page, click **Next: Review**.

8. Click **Create**.

9. Repeat the previous steps to create all required load balancers.

10. On the Load Balancers page, select the load balancer for Avaya Aura[®] Device Services nodes that you have just created and then do the following:

a. In the Listeners table, select a listener with the “HTTPS : 8445” listener ID and then click **Edit**.

Amazon Web Services displays the Settings page for the listener.

b. In Default Actions, click the **Edit** icon for the “Forward to” action.

c. In **Select a target group**, select the target group for Avaya Aura[®] Device Services nodes for port 8445.

In [Creating target groups](#) on page 127, this is the “Target group for Avaya Aura[®] Device Services nodes #2” group.

d. Click **Update**.

11. On the Load Balancers page, select the load balancer for Utility Server nodes that you have just created and then do the following:

a. In the Listeners table, select a listener with the “HTTPS : 443” listener ID and then click **Edit**.

Amazon Web Services displays the Settings page for the listener.

b. In Default Actions, click the **Edit** icon for the “Forward to” action.

- c. In **Select a target group**, select the target group for Utility Server nodes for port 443.
In [Creating target groups](#) on page 127, this is the “Target group for Utility Server nodes #2” group.
- d. Click **Update**.

Configuring idle timeout

About this task

By default, the AWS environment sets the idle timeout for the Elastic load balancer to 60 seconds. Set this value to 150 seconds to provide Avaya Aura® Device Services enough time for cluster wide operations like generating certificates, collecting logs, and restarting services.

Procedure

1. On the Amazon Web Services Management console, navigate to **Services > EC2 > Load Balancers**.
2. Select the created load balancer.
3. On the **Destination** tab, click **Edit idle timeout**.
4. In **Idle timeout**, enter 150.
5. Click **Save**.

Initial setup for software-only Hyper-V deployments

The following sections describe how to deploy a virtual machine in an Hyper-V environment.

Software-only installation checklist for a Hyper-V virtualized environment

The following checklist outlines the tasks that you must perform when deploying Avaya Aura® Device Services as a software-only application in a Microsoft Hyper-V virtualized environment.

No.	Task	Notes	✓
1	Ensure that virtual machines that you plan to use to deploy Avaya Aura® Device Services comply with the requirements for software-only installation.	See the requirements in Requirements for a host machine for Hyper-V deployments on page 35 and Avaya Aura Device Services virtual machine resource requirements on page 34.	

No.	Task	Notes	✓
2	Download the Avaya Aura® Device Services software-only installation package from PLDS.	The software-only installation package includes the following files: • Software-only system layer installer. • Avaya Aura® Device Services application installer. The package file name has the <code>aads-swonly-AADS_VERSION.tgz</code> format. For more information about the software downloading process, see Downloading software from PLDS on page 74.	
3	Enable the Hyper-V service.	On certain Windows operating systems, the Hyper-V service is disabled by default. For information about enabling Hyper-V, see Enabling the Hyper-V service on page 134.	
4	Create a virtual switch on Hyper-V.	Hyper-V virtual machines require a virtual switch to interact with networks. For information about creating a virtual switch, see Creating a virtual switch on page 135.	
5	Configure network settings for the virtual switch.	For information, see Configuring network settings for the virtual switch on page 135.	
6	Create a virtual machine on Hyper-V.	Create a virtual machine that meets the requirements for the selected Avaya Aura® Device Services resource profile. For information, see Creating a new virtual machine on Hyper-V on page 136.	
7	Create additional virtual hard disks for the virtual machine.	Avaya Aura® Device Services requires four virtual hard disks. For information about creating additional virtual hard disks, see Creating required virtual hard disks for the virtual machine on page 138.	
8	Configure CPU settings for the virtual machine.	See Configuring CPU settings for a Hyper-V virtual machine on page 139.	
9	Configure Windows Defender Firewall rules for Avaya Aura® Device Services ports.	See Configuring Windows Defender firewall rules for ports on page 140.	
10	Install RHEL 8.4 or RHEL 8.10	Avaya Aura® Device Services Release 10.2.x requires RHEL 8.4 or RHEL 8.10. For more information about installation, see the official Red Hat documentation. Avaya also recommends that you install the latest security updates on RHEL.	

No.	Task	Notes	✓
11	Create disk partitioning on RHEL.	Avaya Aura® Device Services requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see Creating disk partitioning for software-only deployments on Hyper-V on page 140 and Disk partitions for software-only deployments on page 101.	
12	Create a non-root Linux user.	The installation and administration of the Avaya Aura® Device Services server is more secure when performed by non-root users with sudo privileges. For more information, see Creating an administrative user on page 103.	
13	Enable the YUM package manager on RHEL.	The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation.	
14	Install additional packages required by Avaya Aura® Device Services.	By default, RHEL 8.4 or RHEL 8.10 does not contain certain packages that Avaya Aura® Device Services requires. You must install these packages manually. For more information, see Additional packages required by Avaya Aura Device Services on page 104 and Installing additional RHEL 8.4 or RHEL 8.10 packages manually on page 105.	
15	Enable the Haveged service.	See Enabling the Haveged service on page 105.	
16	Enable FIPS mode (optional).	For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information about enabling FIPS, see Enabling FIPS for software-only systems on page 106.	
17	Do one of the following to manage additional RHEL packages: • Register your RHEL instance to the Red Hat subscription. • Create a local repository for RPM installation or updates.	For more information, see RHEL packages management on page 107 and Enabling required RHEL repositories on page 107. Registering your RHEL instance to the Red Hat subscription is the preferred option.	
18	Install the software-only system layer on your RHEL.	The system layer is low-level software that forms the required operational environment for Avaya Aura® Device Services. For more information, see Installing the system layer on page 108.	

No.	Task	Notes	✓
19	Ensure that: • The chronyd service is up and running. • System Manager and Session Manager are reachable from your virtual machine. This is only required if you deploy Avaya Aura® Device Services in Avaya Aura® environment.	Perform these checks to ensure that the system layer is installed successfully so you can install the Avaya Aura® Device Services application. For more information, see Checking the Chrony service status on page 111 and Checking the connection to System Manager and Session Manager on page 111.	
20	Enable IPv6 support (optional).	For more information, see Enabling IPv6 support for software-only deployments on page 112.	

After deploying a virtual machine, install the application layer as described in the “Avaya Aura® Device Services installation” chapter.

Enabling the Hyper-V service

About this task

The Hyper-V service is not enabled by default on Windows 8.1 and Windows 10 operating systems. You must enable Hyper-V manually.

The following procedure is for Windows 10.

Procedure

1. From the Windows **Start** menu, navigate to **Programs > Programs and Features**.
2. Click **Turn Windows features on or off**.
3. In the Windows Features window, select the **Hyper-V** check box.
4. Ensure that all the check boxes under the **Hyper-V** check box are selected.
5. Click **OK**.
6. Restart your computer to apply changes.

After the restart, you can run the Hyper-V Manager to manage virtual machines.

Starting Hyper-V Manager

About this task

Hyper-V Manager is the application that you use to create and manage Hyper-V virtual machines.

Before you begin

Enable the Hyper-V service on your operating system.

Procedure

1. Press **WIN+S** to display the Start Menu search.
2. In **Search**, type **Hyper-V Manager**.
3. Click the **Hyper-V Manager** icon.

Creating a virtual switch

About this task

Hyper-V virtual machines require virtual switches to connect to physical and virtual networks.

Procedure

1. Start the Hyper-V Manager.
2. On the Menu bar, click **Action**, and then click **Virtual Switch Manager**.
3. In the Virtual Switch Manager window, select **New virtual network switch**.
4. For the switch type, select **External**.
5. Click **Create Virtual Switch**.

Windows displays the Virtual Switch Properties window.

6. In **Name**, type a name of your choice for the switch.
7. In the Connection type area, select **External network** and then select the Network Interface that you want to use for the virtual switch.
8. Click **Apply** and then click **OK**.

Configuring network settings for the virtual switch

About this task

After creating a virtual switch, you must set up network settings of your company.

Before you begin

Configure a virtual switch.

Procedure

1. From the Windows **Start** menu, navigate to **Network and Internet > Network and Sharing Center**.
2. On the Network and Sharing Center page, click the Hyper-V virtual switch that you created.
For example: **vEthernet (Hyper-V External Virtual Switch)**.
3. In the Status window, click **Properties**.
4. In the Properties window, select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.

5. Do one of the following:

- If your organization uses DHCP to assign network addresses, select **Obtain an IP address automatically**.

 Important:

Use this option if you are planning to use the Utility Server.

- If your organization uses static network settings, select **Use the following IP address** and then configure the IP address, subnet mask, and default gateway as appropriate for your organization.

6. Click **OK**

7. If you are planning to use IPv6 in your deployment, in the Properties window, select **Internet Protocol Version 6 (TCP/IPv6)** and then click **Properties**.

If you do not require IPv6 in your deployment, continue from step [10](#) on page 136.

8. Do one of the following to configure IPv6 settings:

- If your organization uses DHCP to assign network addresses, select **Obtain an IP address automatically**.

 Important:

Use this option if you are planning to use the Utility Server.

- If your organization uses static network settings, select **Use the following IP address** and then configure the IP address, subnet mask, and default gateway as appropriate for your organization.

9. Click **OK**.

10. Click **Close** twice.

Creating a new virtual machine on Hyper-V

About this task

Create a Hyper-V virtual machine for RHEL and the Avaya Aura® Device Services application.

The virtual machine specifications must meet the requirements for the Avaya Aura® Device Services profile that you are planning to use. For more information, see [Avaya Aura Device Services virtual machine resource requirements](#) on page 34.

Before you begin

- Obtain an ISO image of the RHEL 8.4 or RHEL 8.10 operating system.
- Create a Hyper-V virtual switch.

Procedure

1. Start the Hyper-V Manager.
2. On the Menu bar, click **Action**, and then click **New > Virtual Machine**.

The Hyper-V Manager displays the New Virtual Machine Wizard window.

3. In the Specify Name and Location window, in **Name**, type a name of your choice for the virtual machine.
4. **(Optional)** If you do not want to use the default location for the virtual machine, then select the **Store the virtual machine in a different location** check box and in **Location**, choose the appropriate location.
5. Click **Next**.
6. In the Specify Generation window, select a generation version for the virtual machine as appropriate.

For information about Hyper-V virtual machine generations, see [Should I create a generation 1 or 2 virtual machine in Hyper-V](#).

 Important:

You cannot change the generation type of the virtual machine after creating it.

7. Click **Next**.
8. In the Assign Memory window, do the following:
 - a. In **Startup Memory**, select the amount of RAM memory to allocate to your virtual machine.

The amount of memory must be equal or greater than the amount of memory required for the Avaya Aura® Device Services profile that you want to use.
 - b. Select the **Use Dynamic Memory for this virtual machine** check box.
9. Click **Next**.
10. In the Configure Networking window, in **Connection**, select the virtual switch that you created in [Creating a virtual switch](#) on page 135.
11. Click **Next**.
12. In the Connect Virtual Hard Disk, do the following to create a primary virtual disk with the size of 125 Gb:
 - a. Select **Create a virtual hard disk**.
 - b. In **Size**, type 125.

This virtual hard disk corresponds to the `/dev/sda` disk on Avaya Aura® Device Services.
13. Click **Next**.
14. In Installation Options, select **Install an operating system from a bootable CD/DVD-ROM**.
15. Select **Image file** and then specify the path to the RHEL 8.4 or RHEL 8.10 ISO image.
16. Click **Next**.
17. In the Summary window, verify the virtual machine data and then click **Finish** to create the virtual machine.

Result

Hyper-V creates a new virtual machine and displays it in the list of virtual machines in the Hyper-V Manager.

Disabling time synchronization

About this task

For Avaya Aura® Device Services proper functioning on a Hyper-V virtual machine, you must disable the Hyper-V time synchronization feature.

Procedure

1. In the Hyper-V Manager, click the created virtual machine.
2. On the Virtual Machines tab, right-click the name of the machine and select **Settings....**
3. In the Management section, click **Integration Services**.
4. Clear the **Time Synchronization** check box.
5. Click **Apply**.

Creating required virtual hard disks for the virtual machine

About this task

By default, Hyper-V creates a virtual machine with a single virtual hard disk. Avaya Aura® Device Services requires four virtual hard disks. You must add the required virtual hard disks manually.

You must create three additional virtual disks with the following disk sizes:

- First additional disk (Disk 2): 70 Gb
- Second additional disk (Disk 3): 40 Gb
- Third additional disk (Disk 4): 10 Gb

Before you begin

Create a virtual machine.

Procedure

1. Start the Hyper-V Manager.
2. In Virtual Machines, right-click your virtual machine and then select **Settings**.
Hyper-V Manager displays the Settings window for the virtual machine.
3. In the Hardware area, select **SCSI Controller**.
4. In the right area of the Settings window, select **Hard Drive** and then click **Add**.
5. In the Media area, select **Virtual hard disk** and then click **New**.
Hyper-V Manager displays the New Virtual Hard Disk Wizard.
6. Click **Next**.

7. In the Choose Disk Format window, select **VHDX** and then click **Next**.
8. In the Choose Disk Type window, select either **Fixed size** or **Dynamically expanding** and then click **Next**.

*** Note:**

The **Fixed size** disk type provides better performance for Avaya Aura® Device Services.

9. In the Specify Name and Location window, in **Name**, type a disk name of your choice.
For example, for the first additional disk, type `Disk2` and so on.
10. Click **Next**.
11. In the Configure Disk window, do the following:
 - a. Select **Create a new blank virtual hard disk**.
 - b. In **Size**, type the disk size according to the following table:

Disk	Size (Gb)
First additional disk (Disk 2)	70
Second additional disk, (Disk 3)	40
Third additional disk (Disk 4)	10

12. Click **Next**.
13. Verify the virtual disk settings and then click **Finish**.
Hyper-V Manager creates an additional virtual hard disk for your virtual machine.
14. Repeat steps [3](#) on page 138 to [13](#) on page 139 to create the additional required virtual hard disks.

Configuring CPU settings for a Hyper-V virtual machine

About this task

The new virtual machine configuration wizard does not allow you to configure CPU settings for your virtual machine. You must configure CPU settings after you create the virtual machine.

Before you begin Procedure

1. Start Hyper-V Manager.
2. In the Virtual Machines area, right-click your virtual machine and then select **Settings**.
Hyper-V Manager displays the Settings window for the virtual machine.
3. In the Hardware area, select **Processor**.
4. In **Number of virtual processors**, select the number of virtual processors for your virtual machine that are required for the Avaya Aura® Device Services profile that you want to use.

5. For other settings, keep the default values.
6. Click **Apply** and then click **OK**.

Configuring Windows Defender firewall rules for ports

About this task

If you need to use certain Avaya Aura® Device Services ports, such as 8442 or 8440, you must configure firewall rules for these ports on the computer that hosts the Hyper-V virtual machine.

For information about Avaya Aura® Device Services ports, see *Port Matrix for Avaya Aura® Device Services*. This document is available on the [Avaya Support website](#).

Procedure

1. Press **WIN+S** to display the Start Menu search.
2. In **Search**, type **Windows Defender** and then click the **Windows Defender Firewall with Advanced Security** icon.
3. Click **Inbound Rules**.
4. Do the following to configure a new rule:
 - a. In the Actions area, click **New Rule**.

Windows Defender Firewall displays the New Rule Wizard window.
 - b. In the Rule Type window, select **Port** and then click **Next**.
 - c. In the Protocol and Ports window, select **TCP**.
 - d. In **Specific local ports**, type the port number and then click **Next**.
 - e. In the Action window, select **Allow the connection** and then click **Next**.
 - f. In the Profile window, keep the default settings and then click **Next**.
 - g. In the Name window, type a name and description of your choice for the new rule.
 - h. Click **Finish**.
5. Repeat the previous step to add more inbound rules as appropriate.
6. To configure outbound rules, click **Outbound Rules** and then repeat step 4 on page 140 to add more outbound rules as appropriate.

Creating disk partitioning for software-only deployments on Hyper-V

About this task

Avaya Aura® Device Services requires a specific disk layout that includes several disk partitions and logical volumes. Use this procedure to create appropriate disk partitioning.

Before you begin

- Install RHEL.

- Create volumes with the required disk size values. For more information, see “Disk partitions for software-only deployments”.

Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. To create the required directories, run the following commands:

```
mkdir -p /var/log/Avaya
mkdir -p /media/data
mkdir -p /media/cassandra
```

3. To create the required physical volumes and volume groups for these volumes, run the following commands:

```
pvcreate -f /dev/sdb
vgcreate disk2_vg /dev/sdb
pvcreate -f /dev/sdc
vgcreate disk3_vg /dev/sdc
pvcreate -f /dev/sdd
vgcreate disk4_vg /dev/sdd
```

4. To create logical volumes in the volume groups, run the following commands:

```
lvcreate -l100%FREE -n application_log /dev/disk2_vg
lvcreate -l100%FREE -n data /dev/disk3_vg
lvcreate -l100%FREE -n cassandra /dev/disk4_vg
```

5. To create a file system for the /dev/sdb partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk2_vg/application_log
mount /dev/disk2_vg/application_log /var/log/Avaya
echo "/dev/disk2_vg/application_log /var/log/Avaya xfs defaults 0 0" >> /etc/fstab
```

6. To create a file system for the /dev/sdc partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk3_vg/data
mount /dev/disk3_vg/data /media/data
echo "/dev/disk3_vg/data /media/data xfs defaults 0 0" >> /etc/fstab
```

7. To create a file system for the /dev/sdd partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk4_vg/cassandra
mount /dev/disk4_vg/cassandra /media/cassandra
echo "/dev/disk4_vg/cassandra /media/cassandra xfs defaults 0 0" >> /etc/fstab
```

Initial setup for software-only Microsoft Azure deployments

The following sections describe how to deploy a virtual machine in an Microsoft Azure environment.

Software-only installation checklist for Microsoft Azure

The following checklist outlines the tasks that you must perform when deploying Avaya Aura® Device Services as a software-only application in a Microsoft Azure environment.

No.	Task	Notes	✓
1	Ensure that the virtual machines that you plan to use to deploy Avaya Aura® Device Services comply with the requirements for software-only installation.	For information about the Microsoft Azure virtual machine size that is required for each Avaya Aura® Device Services profile, see Resource profile specifications for Microsoft Azure virtual machines on page 35.	
2	Download the Avaya Aura® Device Services software-only installation package from PLDS.	The software-only installation package includes the following files: • Software-only system layer installer. • Avaya Aura® Device Services application installer. The package file name has the <code>aads-swonly-AADS_VERSION.tgz</code> format. For more information about the software downloading process, see Downloading software from PLDS on page 74.	
3	Prepare your Microsoft Azure instance for software-only installation.	See Prerequisites for software-only deployment on Microsoft Azure on page 145.	

No.	Task	Notes	✓
4	Deploy a virtual machine and install RHEL 8.4 or RHEL 8.10 on Microsoft Azure.	Avaya Aura® Device Services requires the RHEL 8.4 or RHEL 8.10 operating system. For information about installing Linux operating systems on Microsoft Azure virtual machines, see the official documentation at Create a Linux virtual machine in Azure. For the settings, specific for Avaya Aura® Device Services, see Red Hat Enterprise Linux virtual machine deployment in Microsoft Azure on page 146. By default, the size of the primary disk of your virtual machine is not equal to 125 Gb. You must resize the disk to 125 Gb during or after virtual machine deployment. Avaya also recommends that you install the latest security updates on RHEL. * Note: During the RHEL installation process, you create primary network interface eth0. Do <i>not</i> modify the <code>ifcfg-eth0</code> configuration file before installing the system layer. Avaya Aura® Device Services deployment might fail if you modify this file before installing the system layer. You can freely modify this file after you install the system layer.	
5	If you are planning to use the Utility Server, configure the eth1 secondary network interface.	See Configuring the secondary network interface on a Microsoft Azure virtual machine on page 146. * Note: Do <i>not</i> modify secondary network interface configuration file <code>ifcfg-eth1</code> configuration file before installing the system layer. Avaya Aura® Device Services deployment might fail if you modify this file before installing the system layer. You can freely modify this file after you install the system layer.	
6	Add the required virtual hard disks to your virtual machine.	See Creating required virtual hard disks for a virtual machine on page 147.	
7	Enable root access to RHEL.	RHEL deployed on Microsoft Azure does not have the root user enabled by default. For more information, see Enabling root access on page 148.	

No.	Task	Notes	✓
8	Create disk partitioning on RHEL.	Avaya Aura® Device Services requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see Creating disk partitioning for a Microsoft Azure virtual machine on page 149 and Disk partitions for software-only deployments on page 101.	
9	Configure security groups on Microsoft Azure.	See Configuring security groups on page 150 and Assigning security groups to network interfaces on page 152.	
10	Create a non-root Linux user.	The installation and administration of the Avaya Aura® Device Services server is more secure when performed by non-root users with sudo privileges. For more information, see Creating an administrative user on page 103.	
11	Enable the YUM package manager on RHEL.	The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation.	
12	Install additional packages required by Avaya Aura® Device Services.	By default, RHEL 8.4 or RHEL 8.10 does not contain certain packages that Avaya Aura® Device Services requires. You must install these packages manually. For more information, see Additional packages required by Avaya Aura Device Services on page 104 and Installing additional RHEL 8.4 or RHEL 8.10 packages manually on page 105.	
13	Enable the Haveged service.	See Enabling the Haveged service on page 105.	
14	Enable FIPS mode (optional).	For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information about enabling FIPS, see Enabling FIPS for software-only systems on page 106.	
15	Do one of the following to manage additional RHEL packages: • Register your RHEL instance to the Red Hat subscription. • Create a local repository for RPM installation or updates.	For more information, see RHEL packages management on page 107 and Enabling required RHEL repositories on page 107. Registering your RHEL instance to the Red Hat subscription is the preferred option.	

No.	Task	Notes	✓
16	Prepare your RHEL system for installing the software-only system layer.	See Prerequisites for installing the system layer on Microsoft Azure on page 153.	
17	Install the software-only system layer on your RHEL.	The system layer is low-level software that forms the required operational environment for Avaya Aura® Device Services. For more information, see Installing the system layer on page 108.	
18	Ensure that: - The chronyd service is up and running. - System Manager and Session Manager are reachable from your virtual machine. This is only required if you deploy Avaya Aura® Device Services in Avaya Aura® environment.	Perform these checks to ensure that the system layer is installed successfully so you can install the Avaya Aura® Device Services application. For more information, see Checking the Chrony service status on page 111 and Checking the connection to System Manager and Session Manager on page 111.	
22	In cluster deployments, configure the Microsoft Azure load balancer.	See Creating a Microsoft Azure load balancer on page 154 and Configuring a Microsoft Azure load balancer on page 155.	

After deploying a virtual machine, do the following:

- Install the application layer as described in the “Avaya Aura® Device Services installation” chapter.
- If you deploy a cluster, after installing the application layer, configure the Microsoft Azure load balancer as described in [Creating a Microsoft Azure load balancer](#) on page 154 and [Configuring a Microsoft Azure load balancer](#) on page 155.

Prerequisites for software-only deployment on Microsoft Azure

There are a number of prerequisites for a software-only deployment on Microsoft Azure:

- Use standard Microsoft Azure procedures to create the required network setup, including Virtual Private Cloud and subnet settings.
- Ensure that you have an NTP server. You can deploy your own NTP server or use the NTP server provided by Microsoft Azure.
- Add records with the following FQDNs to your own DNS server or to the Microsoft Azure DNS service:
 - Avaya Aura® Device Services front-end FQDN.
 - Avaya Aura® Device Services Utility Server FQDN.

Red Hat Enterprise Linux virtual machine deployment in Microsoft Azure

When you deploy Avaya Aura® Device Services as a software-only solution, you must use the Red Hat Enterprise Linux (RHEL) 8.4 or RHEL 8.10 (LVM) GEN1 or GEN2, which is available in Microsoft Azure Marketplace.

After obtaining RHEL 8.4 or RHEL 8.10, do the following:

1. Deploy a RHEL 8.4 or RHEL 8.10-based virtual machine in Microsoft Azure. For more information, see [Create a Linux virtual machine in Azure](#).

When creating a virtual machine, use the virtual machine size that is appropriate for the Avaya Aura® Device Services resource profile that you selected. For information about virtual machine sizes, see [Resource profile specifications for Microsoft Azure virtual machines](#) on page 35.

For cluster deployments, you can deploy virtual machines in different subnets and in different Availability Zones as appropriate.

Important:

- Avaya Aura® Device Services requires 250 Gb of free disk space in total. Microsoft Azure virtual machines might not have the required amount of disk space by default. Before deploying RHEL, ensure that virtual machines have enough disk space and purchase additional disk space if required.

By default, the size of the primary hard disk of a virtual machine does not equal to the required size of 125 Gb. You must resize the disk during or after virtual machine deployment.

Avaya Aura® Device Services requires specific disk partitioning. After installing RHEL, you must create the required data disks and physical volumes for data disks as described in [Creating required virtual hard disks for a virtual machine](#) on page 147 and [Creating disk partitioning for a Microsoft Azure virtual machine](#) on page 149.

- During the RHEL installation process, you create primary network interface eth0. Do *not* modify the `ifcfg-eth0` configuration file before installing the system layer. Avaya Aura® Device Services deployment might fail if you modify this file before installing the system layer. You can freely modify this file after you install the system layer.

2. Install the latest critical security updates.

For update procedures, see Red Hat documentation. You can install security updates by using the YUM package manager.

Configuring the secondary network interface on a Microsoft Azure virtual machine

About this task

If you plan to use the Utility Server in your deployment, configure the secondary network interface on your Microsoft Azure virtual machine.

For more information about creating network interfaces on Microsoft Azure, see [Create a network interface](#).

! Important:

Do *not* modify secondary network interface configuration file `ifcfg-eth1` before installing the system layer. Avaya Aura® Device Services deployment might fail if you modify this file before installing the system layer. You can freely modify this file after you install the system layer.

Procedure

1. Log in to the Microsoft Azure administration portal.
2. On the Virtual Machines page, select your virtual machine.
Microsoft Azure displays the Settings window for the virtual machine.
3. Click **Stop** to stop the virtual machine.
You cannot attach a new network interface to a running virtual machine.
4. In the Settings area, click **Networking**.
5. Click **Attach Network Interface**.
6. Click **Create and attach network interface**.
7. In the Create network interface window, configure the following settings:
 - a. In **Name**, type a name of your choice for the network interface.
 - b. In **Subnet**, select an appropriate subnet configured for your deployment.
 - c. For other parameters, keep the default values.
8. Click **Create**.
9. Click **Start** to start the virtual machine.

Creating required virtual hard disks for a virtual machine

About this task

By default, Microsoft Azure creates a virtual machine with a single virtual hard disk. Avaya Aura® Device Services requires four virtual hard disks. You must add the required virtual hard disks manually.

You must create three additional virtual disks with the following disk sizes:

- First additional disk (Disk 2): 70 Gb
- Second additional disk (Disk 3): 40 Gb
- Third additional disk (Disk 4): 10 Gb

Before you begin

- Ensure that your virtual machine has 250 Gb of free disk space.
- Ensure that the size of the primary hard disk where RHEL is installed equals to 125 Gb. If the disk size is not equal to 125 Gb, resize the disk.

Procedure

1. On the Microsoft Azure administration portal, on the Virtual Machines page, select your virtual machine.

Microsoft Azure displays the Settings window for the virtual machine.

2. Stop the Microsoft Azure virtual machine.
3. In the Settings area, click **Disks**.
4. Click **Add data disk**.
5. In the **Name** field, click the arrow icon and then click **Create disk**.

Microsoft Azure displays the Create managed disk window.

6. In the Create managed disk window, do the following:
 - a. In **Disk name**, type a disk name of your choice.
For example, for the first additional disk, type `Disk2`.
 - b. In **Size**, click **Change size** and type the disk size according to the following table:

Disk	Size (Gb)
First additional disk (Disk 2)	70
Second additional disk (Disk 3)	40
Third additional disk (Disk 4)	10

- c. For other parameters, keep the default values.
7. Click **Create**.
 8. Click **Save**.
 9. Repeat steps [4](#) on page 148 to [8](#) on page 148 to create the additional required virtual hard disks.

Enabling root access

About this task

You must use the root user to install the system layer. On RHEL installed on Microsoft Azure, the root user is disabled by default, therefore you must enable it.

Procedure

1. Log in to your virtual machine as the default administration user that you created when deploying RHEL.
2. Run the following command to edit the `/etc/ssh/sshd_config` file:

```
sudo vi /etc/ssh/sshd_config
```

3. Add the following line to the file:

```
PermitRootLogin yes
```

4. Save the file.
5. Run the following command to apply the changes:
6. Set a password for the root user using the following command:

```
sudo service sshd restart
```

```
sudo passwd root
```

Creating disk partitioning for a Microsoft Azure virtual machine

About this task

Avaya Aura® Device Services requires a specific disk layout that includes several disk partitions and logical volumes. Use this procedure to create appropriate disk partitioning.

Before you begin

- Create volumes with the required disk size values as described in [Creating required virtual hard disks for a virtual machine](#) on page 147.

Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. To extend the file system, run the following commands:

```
lvextend -L +8G /dev/rootvg/rootlv
xfs_growfs /dev/rootvg/rootlv

lvextend -L +7G /dev/rootvg/homelv
xfs_growfs /dev/rootvg/homelv

lvextend -L +7G /dev/rootvg/tmplv
xfs_growfs /dev/rootvg/tmplv
```

3. To create the required directories, run the following commands:

```
mkdir -p /var/log/Avaya
mkdir -p /media/data
mkdir -p /media/cassandra
```

4. To create the required physical volumes and volume groups for these volumes, run the following commands:

```
pvccreate -f /dev/sdc
vgcreate disk2_vg /dev/sdc
pvccreate -f /dev/sdd
vgcreate disk3_vg /dev/sdd
pvccreate -f /dev/sde
vgcreate disk4_vg /dev/sde
```

5. To create logical volumes in the volume groups, run the following commands:

```
lvcreate -l100%FREE -n application_log /dev/disk2_vg
lvcreate -l100%FREE -n data /dev/disk3_vg
lvcreate -l100%FREE -n cassandra /dev/disk4_vg
```

6. To create a logical volume for the /opt directory, run the following command:

```
lvcreate -L 8G -n optlv /dev/rootvg
```

7. To create a file system for the `/dev/sda3` partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/rootvg/optlv
mount /dev/rootvg/optlv /opt
echo "/dev/rootvg/optlv /opt xfs defaults 0 0" >> /etc/fstab
```

8. To create a file system for the `/dev/sdc` partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk2_vg/application_log
mount /dev/disk2_vg/application_log /var/log/Avaya
echo "/dev/disk2_vg/application_log /var/log/Avaya xfs defaults 0 0" >> /etc/fstab
```

9. To create a file system for the `/dev/sdd` partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk3_vg/data
mount /dev/disk3_vg/data /media/data
echo "/dev/disk3_vg/data /media/data xfs defaults 0 0" >> /etc/fstab
```

10. To create a file system for the `/dev/sde` partition and mount the file system, run the following commands:

```
mkfs.xfs /dev/disk4_vg/cassandra
mount /dev/disk4_vg/cassandra /media/cassandra
echo "/dev/disk4_vg/cassandra /media/cassandra xfs defaults 0 0" >> /etc/fstab
```

Configuring security groups

About this task

Microsoft Azure uses security groups to control inbound and outbound traffic. For the software-only installation, you must create and configure the following security groups:

- Avaya Aura® Device Services security group.

This security group uses the primary `eth0` network interface.

- Optionally, the Utility Server security group. Only create this security group if you plan to use the Utility Server in your deployment.

This security group uses the secondary `eth1` network interface.

For more information about managing security groups on Microsoft Azure, see [Create, change, or delete a network security group](#).

Before you begin

If you plan to use the Utility Server in your deployment, configure the secondary network interface as described in [Configuring the secondary network interface on a Microsoft Azure virtual machine](#) on page 146.

Procedure

1. On the Microsoft Azure administration portal, in the search field, type `network security groups` and then click **Network security groups**.

! Important:

Do *not* click **Network security groups (classic)**.

2. In the Network security groups window, click **Add**.
3. In **Resource group**, click **Create new** and create a new resource group.
4. In **Name**, type a name of your choice.
5. In **Region**, select an appropriate region for your deployment.
6. Click **Review and Create**.
7. From the list of the network security groups, select the group that you created.
8. Do the following to configure inbound security rules for the group:
 - a. In the left navigation pane, select **Inbound security rules**.
 - b. Click **Add**.
 - c. In the Add inbound security rule window, configure the security rule as described in the “Inbound traffic rules” section for the appropriate group.
 - d. Click **Add**.

Microsoft Azure displays the new security rule in the list of inbound security rules.

 - e. Repeat substeps a to d to add the required inbound security rules to the security group.
9. If you plan to use the Utility Server, on the Networking page, repeat steps 1 to 8 to create a security group for the Utility Server.

Next steps

Assign the created security groups to network interfaces.

Inbound traffic rules for the Avaya Aura® Device Services security group

The following tables list the traffic rules for the security group that controls inbound Avaya Aura® Device Services traffic.

Inbound rules

Source	Source port ranges	Destination	Service	Destination port range	Protocol
Any	*	Any	Custom	161	UDP
Any	*	Any	Custom	31415	TCP
Any	*	Any	Custom	8447	TCP
Any	*	Any	Custom	7001	TCP
Any	*	Any	Custom	8468	TCP
Any	*	Any	Custom	8543	TCP
Any	*	Any	Custom	7000	TCP

Source	Source port ranges	Destination	Service	Destination port range	Protocol
Any	*	Any	HTTPS	443	TCP
Any	*	Any	Custom	8457	TCP
Any	*	Any	Custom	3268	TCP
Any	*	Any	Custom	8448	TCP
Any	*	Any	Custom	21000	TCP
Any	*	Any	Custom	9999	TCP
Any	*	Any	SSH	22	TCP
Any	*	Any	Custom	8440	TCP
Any	*	Any	Custom	2009	TCP
Any	*	Any	Custom	8458	TCP
Any	*	Any	Custom	3269	TCP
Any	*	Any	Custom	8445	TCP
Any	*	Any	Custom	8442	Any
Any	*	Any	HTTP	80	TCP
Any	*	Any	Custom	9443	TCP*

Inbound traffic rules for the Utility Server security group

The following tables list the traffic rules for the security group that controls inbound traffic of the Utility Server.

Source	Source port range	Destination	Service	Port range	Protocol
Any	*	Any	Custom	8468	TCP
Any	*	Any	Custom	8543	TCP
Any	*	Any	Custom	8458	TCP
Any	*	Any	HTTPS	443	TCP
Any	*	Any	Custom	8457	TCP
Any	*	Any	HTTP	80	TCP

Assigning security groups to network interfaces

About this task

When you configure a virtual machine instance, Microsoft Azure assigns the same default security rules to all network interfaces. You must assign an appropriate security group to the primary and, if configured, to the secondary network interface of each Avaya Aura® Device Services virtual machine.

*** Note:**

If you are planning to use the Utility Server, you have two network interfaces on Avaya Aura[®] Device Services virtual machines and two security groups. If you are not using the Utility Server, you only have the primary network interface on each virtual machine and a single security group.

Before you begin

Create the required security groups as described in [Configuring security groups](#) on page 150.

Procedure

1. On the Microsoft Azure administration portal, in the search field, type `network interfaces` and then click **Network Interfaces**.
Microsoft Azure displays the list of network interfaces.
2. Select a network interface that belongs to an Avaya Aura[®] Device Services node.
3. Click **Network security group**.
4. In the **Network security group** field, select an appropriate security group as follows:
 - If you selected the primary `eth0` network interface of a node, select the Avaya Aura[®] Device Services security group that you created when configuring security groups.
 - If you selected the secondary `eth1` network interface of a node, select the Utility Server security group that you created when configuring security groups.
5. Repeat steps [2](#) on page 153 to [4](#) on page 153 for all remaining Avaya Aura[®] Device Services nodes and network interfaces assigned to these nodes.

Prerequisites for installing the system layer on Microsoft Azure

In addition to the prerequisites for the software-only system layer installation that are common for all deployment types, Microsoft Azure has the following specific prerequisites:

- On all Avaya Aura[®] Device Services nodes in your deployment, add information about each Avaya Aura[®] Device Services node to the `/etc/hosts` file in the following format:

```
<IP_Address> <Corresponding_FQDN> <hostname>
```

For example:

```
195.51.100.5 aads1.mycompany.com aads1
195.51.100.6 aads2.mycompany.com aads2
```

- Enable root access to RHEL. For more information, see [Enabling root access](#) on page 148.
- Create a non-root user on RHEL. For more information, see [Creating an administrative user](#) on page 103.

Creating a Microsoft Azure load balancer

About this task

In a cluster deployment, a load balancer distributes incoming traffic between Avaya Aura® Device Services nodes. In Microsoft Azure cluster deployments, you must create and configure an internal Microsoft Azure load balancer.

Before you begin

- Deploy all required nodes for your Avaya Aura® Device Services cluster.
- On each node, add information about the Avaya Aura® Device Services front-end FQDN to the `/etc/hosts` file in the following format:

```
<Node_IP_Address> <Front-end_FQDN>
```

- Ensure that you configured security rules as described in [Configuring security groups](#) on page 150.
- Log in to the Avaya Aura® Device Services CLI as an administrator and run the following commands to ensure that the HTTP services are running:

```
cdto misc  
./us-http-port.sh --enable
```

Procedure

1. On the Microsoft Azure administration portal, navigate to **Networking > Load Balancers**.
2. Click **Add**.
Microsoft Azure displays the Create Load Balancer page.
3. In **Name**, type a name of your choice for the load balancer.
4. In **Region**, select an appropriate region for your load balancer.
5. In **Resource group**, click **Create new** and create a new resource group for the load balancer.
6. In **Type**, select **Internal**.
7. In **SKU**, select **Standard**.
8. In **Virtual Network**, select an appropriate network.
9. In **Availability Zone**, select **Zone-redundant**.
10. Click **Review and Create**.
11. Click **Create**.

Microsoft Azure creates a new load balancer and displays it in the list of load balancers.

Next steps

Configure the load balancer settings.

Configuring a Microsoft Azure load balancer

About this task

You must do the following to configure a load balancer for your Avaya Aura® Device Services cluster:

- Configure a front-end IP address for the load balancer.
If you use the Utility Server in your deployment, you also need another front-end IP address for the Utility Server.
- Connect all network interfaces of all nodes to the load balancer.
- Configure health monitoring probes.
- Configure load balancing rules.

Procedure

1. On the Microsoft Azure administration portal, navigate to **Networking > Load Balancers**.
2. Select your load balancer.
3. Do the following to create a new front-end IP address for Avaya Aura® Device Services nodes:
 - a. In the Settings area, click **Frontend IP configuration**.
 - b. Click **Add**.
 - c. In **Name**, type a name of your choice.
 - d. In **Subnet**, select an appropriate subnet of your network.
 - e. In **Assignment**, select **Dynamic**.
 - f. Click **Add**.

Microsoft Azure displays the new front-end IP address.

4. If you have the Utility Server in your deployment, repeat step [3](#) on page 155 to create an additional front-end IP address for the Utility Server.
5. In the Network area, click **Backend pools**.
6. Do the following to connect the nodes of your cluster to the load balancer:
 - a. In the Settings area, click **Backend pools**.
 - b. Click **Add**.
 - c. In **Name**, type a name of your choice.
 - d. In **Backend pool configuration**, select **NIC**.
 - e. In **IP version**, select **IPv4**.
 - f. In the Virtual machines area, click **Add**.

- g. In the Add virtual machines to backend pool window, select IP addresses as follows:
 - For the Avaya Aura® Device Services back-end pool, select IP addresses of all Avaya Aura® Device Services nodes in the cluster. These are the IP addresses of the primary eth0 interface of cluster nodes.
 - For the Utility Server back-end pool, select IP addresses of all Utility Server nodes in the cluster. These are the IP addresses of the secondary eth1 interface of cluster nodes.
 - h. Click **Add**.
 - i. Click **Add** again.
7. If you are using the Utility Server in your deployment, repeat step 6 on page 155 to connect the IP addresses of all Utility Server nodes to the load balancer.
 8. In the Settings area, click **Health probes** and then configure two health probes with the following settings:

Setting	First health probe	Second health probe
Name	Any name of your choice	Any name of your choice
Protocol	TCP	HTTPS
Path	Not applicable	/
Port	80	443
Interval	5 seconds	5 seconds
Unhealthy threshold	2 consecutive failures	2 consecutive failures

9. Do the following to create six load balancing rules for the Avaya Aura® Device Services nodes and three load balancing rules for the Utility Server nodes:
 - a. In the Settings area, click **Load balancing rules**.
 - b. Click **Add**.
 - c. In **Name**, type a name of your choice.
 - d. In **IP Version**, select **IPv4**.
 - e. In **Protocol**, select **TCP**.
 - f. In **Health Probe**, select the health probe that you created that uses the TCP protocol.
 - g. In **Idle timeout (minutes)**, type 15.
 - h. In **Floating IP**, select **Disabled**.
 - i. In **TCP reset**, select **Enabled**.
 - j. Configure the remaining settings as follows:

Table 1: Load balancing rules for Avaya Aura® Device Services nodes

Setting	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6
Frontend IP address	The front-end IP address for the Avaya Aura® Device Services nodes.					
Port	80	443	8440	8442	8443	8445
Backend port	80	443	8440	8442	8443	8445
Session Persistence	None	None	None	None	None	Client IP and protocol
Backend pool	The back-end pool for the Avaya Aura® Device Services nodes.					

Table 2: Load balancing rules for Utility Server nodes

Setting	Rule 1	Rule 2	Rule 3
Frontend IP address	The front-end IP address for the Utility Server nodes.		
Port	80	443	8443
Backend port	80	443	8443
Session Persistence	None	None	None
Backend pool	The back-end pool for the Utility Server nodes.		

Initial setup for software-only Google Cloud Platform deployments

The following sections describe how to deploy a virtual machine in an Google Cloud Platform environment.

Software-only installation checklist for Google Cloud Platform

The following checklist outlines the tasks you must perform when deploying Avaya Aura® Device Services as a software-only application in a Google Cloud Platform environment:

No.	Task	Notes	✓
1	Ensure that the virtual machines you plan to use to deploy Avaya Aura® Device Services comply with the requirements for software-only installation.	For information about the Google Cloud Platform virtual machine size that is required for each Avaya Aura® Device Services profile, see Resource profile specifications for Google Cloud Platform virtual machines on page 36.	
2	Download the Avaya Aura® Device Services software-only installation package from PLDS.	The software-only installation package includes the following files: • Software-only system layer installer. • Avaya Aura® Device Services application installer. The package file name has the <code>aads-swonly-AADS_VERSION.tgz</code> format. For more information about the software downloading process, see Downloading software from PLDS on page 74.	
3	Prepare your Google Cloud Platform environment for software-only installation.	See Prerequisites for software-only deployment on Google Cloud Platform on page 160.	
4	Create VPC network peering.	See Creating VPC peering on page 161.	
5	Configure firewall rules for the VPC networks.	See Configuring firewall rules on page 161.	
6	Assign the firewall rules to virtual machines.	See Assigning firewall rules to virtual machines on page 164.	
7	Deploy a virtual machine with Red Hat Enterprise Linux on Google Cloud Platform.	Avaya Aura® Device Services requires the RHEL 8.4 or RHEL 8.10 operating system. For information about deploying a Linux virtual machine in Google Cloud Platform, see steps in Virtual machine deployment checklist on page 164.	
8	If you deploy a cluster, create an instance group.	See Creating an instance group for load balancers on page 169.	
9	If you deploy a cluster, create and configure load balancers.	See Creating load balancers on page 170.	
10	Add the required virtual hard disks to your virtual machines.	See Creating required virtual hard disks for a virtual machine on page 172.	
11	Enable root access to RHEL.	RHEL deployed on Google Cloud Platform does not have the root user enabled by default. For more information, see Enabling root access on page 168.	
12	Enable LVM on RHEL.	See Enabling LVM on RHEL on page 173.	

No.	Task	Notes	✓
13	Create disk partitioning on RHEL.	Avaya Aura® Device Services requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see Creating disk partitioning for a Google Cloud Platform virtual machine on page 173 and Disk partitions for software-only deployments on page 101.	
14	Make entries in the <code>/etc/hosts/</code> file permanent.	See Enabling editing of the /etc/hosts file on page 174.	
15	Create a non-root Linux user.	The installation and administration of the Avaya Aura® Device Services server are more secure when performed by non-root users with sudo privileges. For more information about creating non-root Linux users, see Creating an administrative user on page 103.	
16	Install additional packages required by Avaya Aura® Device Services.	By default, RHEL 8.4 or RHEL 8.10 does not contain certain packages that Avaya Aura® Device Services requires. You must install these packages manually. For more information, see Additional packages required by Avaya Aura Device Services on page 104 and Installing additional RHEL 8.4 or RHEL 8.10 packages manually on page 105.	
17	Enable the Haveged service.	See Enabling the Haveged service on page 105.	
18	Enable FIPS mode (optional).	For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information about enabling FIPS, see Enabling FIPS for software-only systems on page 106.	
19	Do one of the following to manage additional RHEL packages: • Register your RHEL instance to the Red Hat subscription. • Create a local repository for RPM installation or updates.	For more information, see RHEL packages management on page 107 and Enabling required RHEL repositories on page 107. Registering your RHEL instance to the Red Hat subscription is the preferred option.	
20	Prepare your RHEL system for installing the software-only system layer.	See Prerequisites for installing the system layer on Google Cloud Platform on page 174.	

No.	Task	Notes	✓
21	Install the software-only system layer on your RHEL.	The system layer is low-level software that forms the required operational environment for Avaya Aura® Device Services. For more information, see Installing the system layer on page 108.	
22	Ensure that: • The chronyd service is up and running. • System Manager and Session Manager are reachable from your virtual machine. This is only required if you deploy Avaya Aura® Device Services in Avaya Aura® environment.	Perform these checks to ensure that the system layer is installed so you can install the Avaya Aura® Device Services application. For more information, see Checking the Chrony service status on page 111 and Checking the connection to System Manager and Session Manager on page 111.	

After deploying a virtual machine, do the following:

- Install the application layer as described in the “Avaya Aura® Device Services installation” chapter.
- If you deploy a cluster, after installing the application layer, create redirection rules for port 443 as described in [Configuring redirection rules for port 443](#) on page 175.

Prerequisites for software-only deployment on Google Cloud Platform

There are several prerequisites for a software-only deployment on the Google Cloud Platform:

- Use standard Google Cloud Platform procedures to create the required network setup, including Virtual Private Cloud (VPC) network and subnet settings. For information about creating VPC networks, see [VPC network overview](#) and [Using VPC networks](#).

! Important:

You can deploy a VPC network in auto or custom mode. Auto mode VPC networks are easier to set up than custom mode VPC networks. Custom mode VPC networks, however, provide more control over the network configuration. For example, you can use your IP addresses in custom mode VPC networks. Therefore, Google recommends that you use custom mode VPC network in the production environment. For more information about considerations and limitations of automatic VPC networks, see [Considerations for auto mode VPC networks](#).

- If you plan to use the Utility Server, you must create a separate VPC for network interfaces used by Utility Server nodes.

The Utility Server is installed as part of the Avaya Aura® Device Services application but requires a separate network interface to operate. However, in the Google Cloud Platform each network interface of a virtual machine must be located in a separate VPC network. Therefore, you require two VPC networks to deploy Avaya Aura® Device Services.

- Ensure that you have an NTP server. You can deploy your NTP server or use the NTP server provided by Google Cloud Platform.
- Add records with the following FQDNs to your DNS server or the Google Cloud Platform DNS service:
 - Avaya Aura® Device Services front-end FQDN.
 - Avaya Aura® Device Services Utility Server FQDN.

Creating VPC peering

About this task

In Google Cloud Platform, network interfaces of Avaya Aura® Device Services nodes and Utility Server nodes are located in different VPC networks. Therefore, to enable connectivity between these networks, you must configure VPC network peering.

You must repeat this procedure for each VPC network in your deployment. For example, if you have VPC networks aadsvpc and aadsvpcus, you must create the following peerings:

- aadsvpc to aadsvpcus
- aadsvpcus to aadsvpc

Before you begin

Create the required network setup, including Virtual Private Cloud and subnet settings.

Procedure

1. In the Google Cloud Console, navigate to **VPC Network > VPC Network Peering**.
2. Click **Create Connection**.
3. In **Name**, type a name for the VPC peering.
4. In **Your VPC network**, enter the name of the network you want to peer.
5. Select **In project <NAME_OF_YOUR_PROJECT>**.
6. In **VPC network name**, select the VPC network you want to peer with.
7. Select **Import custom routes** and **Export custom routes** check boxes.
8. Click **Create**.
9. Repeat the previous steps for another network in your deployment.
10. On the VPC network peering page, ensure that the status of the peering that you created is **Active**.

Configuring firewall rules

About this task

Firewall rules are used to control inbound and outbound traffic in a VPC network. Depending on your deployment type, you must configure firewall rules for the following VPC networks:

- The VPC network that contains network interfaces for Avaya Aura® Device Services nodes.

- The VPC network that contains network interfaces for Utility Server nodes. You must only configure firewall rules for this network if you plan to use the Utility Server.

By default, firewall rules apply to the whole VPC network and to all network interfaces configured in that network. However, you can configure a rule to apply only to specific virtual machines in the network.

Procedure

1. On the Google Cloud Console, navigate to **VPC network > VPC networks**.
2. Select a VPC network.
3. Do the following to create a firewall rule for the selected VPC network:
 - a. Click **Create firewall rule**.
 - b. Configure firewall rule settings as described in the “Firewall rules for VPC network” section for the appropriate rule.
 - c. If you selected **Specific target tags** for a rule in the previous step, in **Target tags**, type a unique tag of your choice for the rule.

You will use this tag later to apply the rule to your virtual machines.
 - d. In **Name**, type a name of your choice for the firewall rule.
 - e. In **Network**, select the VPC network for which you want to configure the firewall rule.
 - f. In **Direction**, select **Ingress**.
 - g. In **Action on match**, select **Allow**.
 - h. For other parameters, keep the default values.
 - i. Click **Create**.
4. Repeat step 3 on page 162 to create the remaining firewall rules for the selected VPC network.
5. Repeat the previous steps to create firewall rules for the remaining VPC network.

Next steps

Assign firewall rules to virtual machines.

Firewall rules for Avaya Aura® Device Services application network interfaces

The following table lists the traffic rules for a VPC network that contains network interfaces for the Avaya Aura® Device Services application. On a virtual machine, this is the NIC0 network interface.

Rule	Targets	Source filter	Source IP ranges	Protocols and ports	Protocol	Port range
Rule specific to Avaya Aura® Device Services (Firewall rule #1)	Specified target tags	IP ranges	0.0.0.0/0	Specified protocols and ports	TCP	31415, 8447, 7001, 8468, 8543, 7000, 8457, 3268, 8448, 21000, 9999, 8440, 2009, 8458, 3269, 8445, 8442, 9443
Rule specific to Avaya Aura® Device Services (Firewall rule #2)	Specified target tags	IP ranges	0.0.0.0/0	Specified protocols and ports	UDP	161
Rule common to Avaya Aura® (Firewall rule #3)	All instances in the network	IP ranges	0.0.0.0/0	Specified protocols and ports	TCP	22, 80, 443
Rule for health checks (Firewall rule #4)	Specified target tags	IP ranges	35.191.0.0/16, 130.211.0.0/22	Specified protocols and ports	TCP	80, 443
Rule specific to System ManagerSession Manager (Firewall rule #5) ⁴	Specified target tags	IP ranges	One or more subnets where your Avaya Aura® Device Services virtual machines are deployed.	Specified protocol and ports	ALL	ALL

Firewall rules for Utility Server network interfaces

The following table lists the traffic rules for a VPC network that contains Utility Server network interfaces. On a virtual machine, this is the NIC1 network interface.

You do not need to configure these rules if you do not use the Utility Server in your deployment.

⁴ This rule is not required if you deploy Avaya Aura® Device Services in an environment without Avaya Aura®.

Rule	Targets	Source filter	Source IP ranges	Protocols and ports	Protocol	Port range
Rule specific to Avaya Aura® Device Services (Firewall rule #1)	Specified target tags	IP ranges	0.0.0.0/0	Specified protocols and ports	TCP	8468, 8543, 8458, 8457
Rule common to Avaya Aura® (Firewall rule #2)	All instances in the network	IP ranges	0.0.0.0/0	Specified protocols and ports	TCP	80, 443
Rule for health checks (Firewall rule #3)	Specified target tags	IP ranges	35.191.0.0/16, 130.211.0.0/22	Specified protocols and ports	TCP	80, 443

Assigning firewall rules to virtual machines

About this task

You must manually assign a firewall rule to your virtual machines if the Target parameter of the rule is set to Specific target tags. In Google Cloud Platform, you use a tag associated with a rule to assign firewall rules to virtual machines indirectly.

Before you begin

Configure firewall rules for Avaya Aura® Device Services application network interfaces and for Utility Server network interfaces, and remember the tags that you assigned to the firewall rules.

Procedure

1. In Google Cloud Console, navigate to **Compute Engine > VM instances**.
2. In **Instances**, click the name of your Avaya Aura® Device Services virtual machine.
Google Cloud Console displays the VM instance details page.
3. Click **Edit**.
4. In **Network tags**, type the tags that you assigned to the firewall rules.
5. Click **Save**.
6. In a cluster deployment, repeat the previous steps for all virtual machines.

Virtual machine deployment checklist

Avaya Aura® Device Services requires the RHEL operating system. However, you cannot install Avaya Aura® Device Services on a virtual machine deployed using the “default” RHEL image provided by Google Cloud Platform. By default, Google Cloud Platform virtual machines only

support /32 netmasks. Therefore, you must create a custom RHEL image based on the RHEL image provided by Google Cloud Platform and then use it to deploy virtual machines.

*** Note:**

If you are deploying a cluster, you only need to create the custom RHEL image once. Then, you can use it to deploy Avaya Aura® Device Services virtual machines.

The following checklist outlines the tasks you must perform to deploy a virtual machine with RHEL 8.4 or RHEL 8.10 in a Google Cloud Platform environment:

No.	Task	Notes	✓
1	Deploy a virtual machine using an RHEL image provided by Google Cloud Platform.	See Deploying virtual machines in Google Cloud Platform on page 165. For more information about deploying virtual machines in Google Cloud Platform, see Creating instances . ! Important: If you plan to use the Utility Server, configure the second network interface when deploying a virtual machine. You cannot add network interfaces to an existing virtual machine.	
2	Enable the YUM package manager on RHEL.	The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation.	
3	Reimage the RHEL operating system disk.	You must manually create an operating system disk image that supports netmasks other than /32. After reimagining the operating system disk, you can use this image to deploy virtual machines. See Reimagining the operating system disk on page 167.	
4	Deploy a virtual machine using the custom RHEL image.	This process is similar to deploying a virtual machine using an RHEL image provided by Google Cloud Platform. For information about deploying a virtual machine, see Deploying virtual machines in Google Cloud Platform on page 165.	

Deploying virtual machines in Google Cloud Platform

About this task

To install Avaya Aura® Device Services, you must deploy a virtual machine with two network interfaces. The virtual machine specifications must meet the requirements for the Avaya Aura® Device Services profile you are planning to use.

For cluster deployments, you must deploy all virtual machines in the same subnet.

! Important:

You can only create additional network interfaces when deploying a virtual machine. You *cannot* add network interfaces to an existing virtual machine.

For more information about deploying virtual machines on Google Cloud Platform, see [Creating instances with multiple network interfaces](#).

Before you begin

- Configure VPC networks for your deployment as appropriate.
- Configure VPC peering.

Procedure

1. Log in to the Google Cloud Console as an administrator.
2. Navigate to the **Compute Engine > VM instances** page.
3. Click **Create**.

Google Cloud Platform displays the New VM instance page with the new virtual machine settings.

4. In **Name**, provide a name of your choice for the virtual machine.
5. In **Region**, select an appropriate region.
6. In **Zone**, select an appropriate availability zone.
7. In the Machine configuration area, configure the following settings:
 - a. In **Machine family**, select **Compute-optimized**
 - b. In **Machine type**, select a machine type appropriate for the Avaya Aura® Device Services profile you plan to use.
8. In the Boot disk area, click **Change**.
9. If you created a custom image of the operating system disk, do the following:
 - a. On the Boot disk page, click **Custom images**.
 - b. In **Show images from**, select your project.
 - c. Select the custom RHEL image that you created.
 - d. In **Boot disk type**, select **SSD persistent disk**.
 - e. In **Size**, type 125.
 - f. Click **Select**.
10. If you did not create a custom image of the operating system disk, do the following:
 - a. On the Boot disk page, click **Public images**.
 - b. In **Operating system**, select **Red Hat Enterprise Linux**.
 - c. In **Version**, select **Red Hat Enterprise Linux 7.9**.

- d. In **Boot disk type**, select **SSD persistent disk**.
 - e. In **Size**, type 125.
 - f. Click **Select**.
11. For the parameters in the Identity and API access and Firewall sections, keep the default values.
 12. Click **Networking**.
 13. In the Network interfaces section, click the default network interface and configure the following settings:
 - a. In **Network**, select the VPC network for the Avaya Aura® Device Services nodes.
 - b. In **Subnetwork**, select an appropriate subnet for your virtual machine.
 - c. In **Internal IP address**, select **Custom**.
 - d. In **Custom ephemeral IP address**, select **Reverse static internal IP**.
 - e. In **External IP**, select **Ephemeral**.
 - f. In **Network Service Tier**, select **Premium**.
 - g. Click **Done**.
 14. Do the following to create a network interface for Utility Server:
 - a. Click **Add network interface**.
 - b. In **Network**, select the VPC network for Utility Server nodes.
 - c. In **Subnetwork**, select an appropriate subnet for your virtual machine.
 - d. In **Custom ephemeral IP address**, select **Reverse static internal IP**.
 - e. In **External IP**, select **Ephemeral**.
 - f. In **Network Service Tier**, select **Premium**.
 - g. Click **Done**.
 15. Click **Create**.

Result

Google Cloud Platform creates a new virtual machine and displays it on the VM instances page.

Next steps

If you used a public image to deploy the virtual machine, reimage the RHEL operating system disk as described in [Reimaging the operating system disk](#) on page 167.

Reimaging the operating system disk

About this task

By default, network interfaces configured in Google Private Cloud instances support /32 subnets only. To enable support for subnets other than /32, you must create a custom image of the RHEL operating system disk and then use it to deploy your virtual machines.

In a cluster deployment, you can perform this procedure once and then use the image to deploy all virtual machines.

For more information about creating custom images, see [Google Private Cloud documentation](#).

Before you begin

Stop the virtual machine instance.

Procedure

In the gcloud command-line tool, run the following command:

```
gcloud compute images create <REIMAGED_DISK_NAME> \
  --source-disk <DISK_NAME> \
  --source-disk-zone <ZONE> \
  --guest-os-features MULTI_IP_SUBNET
```

In this command:

- `REIMAGED_DISK_NAME` is a name of your choice for the reimaged operating system disk.
- `DISK_NAME` is the name of the disk where you deployed the RHEL operating system.
- `ZONE` is the network zone where the disk is located.

For example:

```
gcloud compute images create aads-vm-multi-ip-subnet \
  --source-disk RHEL-7.9-disk \
  --source-disk-zone us-central1-a \
  --guest-os-features MULTI_IP_SUBNET
```

Result

You created a custom image of the operating system disk.

Next steps

Re-deploy the virtual machine that you used to create a custom image using the custom image that you have just created.

Enabling root access

About this task

You must use the root user to install the system layer. On RHEL installed on Google Cloud Platform, the root user is disabled by default, therefore you must enable it.

Procedure

1. Log in to your virtual machine as the default administration user that you created when deploying RHEL.
2. Run the following command to edit the `/etc/ssh/sshd_config` file:

```
sudo vi /etc/ssh/sshd_config
```

3. Add the following line to the file:

```
PermitRootLogin yes
```

4. Save the file.
5. Run the following command to apply the changes:
6. Set a password for the root user using the following command:

```
sudo service sshd restart
```

```
sudo passwd root
```

Creating an instance group for load balancers

About this task

An instance group is a collection of virtual machines that you can manage as a single entity. In a cluster deployment, you require an instance group to configure load balancers. You do not need an instance group in a standalone deployment.

If virtual machines in your deployment are located in multiple zones or regions, you must create a separate instance group for each specific zone or region.

For more information about instance groups, see [Instance groups](#).

Before you begin

Deploy virtual machines as described in [Virtual machine deployment checklist](#) on page 164.

Important:

Do *not* install the Avaya Aura® Device Services application on the virtual machines until you configure instance groups and load balancers. If you install Avaya Aura® Device Services before configuring load balancers, then Avaya Aura® Device Services firewall rules might be configured incorrectly.

Procedure

1. In the Google Cloud Console, navigate to **Compute Engine > Instance groups**.
2. Click **Create instance group**.
3. In the left area of the page, click **New unmanaged instance group**.
4. In **Name**, type a name of your choice.
5. In **Location** and **Zone**, select the location and zone where your virtual machines are located.
6. In **Network**, select the VPC network that contains the primary nic0 network interfaces of your virtual machines.
7. In **Subnetwork**, select the subnetwork where your virtual machines are deployed.
8. In **VM instances**, click **Add an instance** and then select a virtual machine that you deployed.

Note:

The list only contains virtual machines deployed in the region and zone that you selected in step [5](#) on page 169.

9. Repeat the previous step to add other virtual machines in your deployment to the instance group.
10. Click **Create**.
11. If you have virtual machines located in other zones or regions, repeat the procedure for all these zones or regions.

Next steps

Configure load balancers.

Creating load balancers

About this task

In a cluster deployment, a load balancer distributes incoming traffic between Avaya Aura® Device Services nodes. In Google Cloud Platform cluster deployments, you must create and configure a separate load balancer for each VPC network:

- A load balancer for a VPC network that contains application network interfaces of the Avaya Aura® Device Services application. These network interfaces are the NIC0 interfaces of virtual machines.
- A load balancer for a VPC network that contains network interfaces of the Utility Server nodes. These network interfaces are the NIC1 interfaces of virtual machines.

Before you begin

Configure instance groups for your deployment as described in [Creating an instance group for load balancers](#) on page 169.

Procedure

Repeat the following steps to create a load balancer for Avaya Aura® Device Services nodes and for Utility Server nodes.

1. In Google Cloud Console, navigate to **Network services > Load Balancing**.
2. Click **Create load balancer**.
3. Select **TCP Load Balancing**.
4. In **Internet facing or internal only**, select **Only between my VMs** and then click **Continue**.
5. In **Name**, type a name of your choice for the load balancer.
6. Click **Backend configuration** and configure the following settings:
7. In **Region**, select a region where you want to create the load balancer.
8. In **Network**, select a VPC network depending on the load balancer that you are configuring:
 - For the load balancer for the VPC network that contains Avaya Aura® Device Services application network interfaces, select the VPC network that contains NIC0 network interfaces of the virtual machines.

- For the load balancer for the VPC network that contains Utility Server network interfaces, select the VPC network that contains NIC1 network interfaces of the virtual machines.
9. In **Instance group**, select the instance group that you created previously.
 10. In **Health check**, in the drop-down list, click **Create another health check** and configure the following settings:
 - a. In **Name**, type a name of your choice for the health check.
 - b. In **Protocol**, select **TCP**.
 - c. In **Port**, type 443.
 - d. For other settings, keep the default values.
 - e. Click **Save and continue**.
 11. In **Health check**, select the health check that you just created.
 12. In **Session affinity**, select **Client IP and protocol**.
 13. Click **Frontend configuration**
Google Cloud Platform displays the Frontend configuration page.
 14. In **Name**, type a name of your choice for the frontend configuration.
 15. In **Subnetwork**, select the subnetwork where you deployed virtual machines.
 16. In the Internal IP section, in **Purpose**, select **Non-shared**.
 17. In the Internal IP section, in **IP address**, select **Reserve static internal IP address** and configure the following settings:
 - a. In **Name**, type a name of your choice.
 - b. In **Static IP address**, select **Assign automatically**.
 - c. Click **Reserve**.
 18. In **Ports**, select **Multiple**.
 19. In **Port number**, type the following comma-separated port numbers:
 - For the load balancer for Avaya Aura® Device Services nodes, type 443, 8440, 8442, 8443, 8445.
 - For the load balancer for Utility Server nodes, type 80, 8443, 443.
 20. For other frontend settings, keep the default values.
 21. Click **Done**.
 22. **(Optional)** To verify the load balancer settings, click **Review and finalize**.
 23. Click **Create**.
 24. Repeat the procedure to create a load balancer for the Utility Server nodes.

Creating required virtual hard disks for a virtual machine

About this task

By default, Google Cloud Platform creates a virtual machine with a single virtual hard disk. Avaya Aura® Device Services requires four virtual hard disks. You must add the required virtual hard disks manually.

You must create three additional virtual disks with the following disk sizes:

- First additional disk (Disk 2): 70 Gb
- Second additional disk (Disk 3): 40 Gb
- Third additional disk (Disk 4): 10 Gb

Before you begin

- Ensure that your virtual machine has 250 Gb of free disk space.
- Ensure that the size of the primary hard disk where RHEL is installed equals to 125 Gb. If the disk size is not equal to 125 Gb, resize the disk.

Procedure

1. In the Google Cloud Console, navigate to the **VM instances** page and select your virtual machine.

Google Cloud Platform displays the Settings window for the virtual machine.

2. If the virtual machine is running, click **Stop** to stop it.
3. Click **Edit**.
4. In the Additional disks area, click **Add new disk**.

Google Cloud Platform displays the New Disk window.

5. In the New Disk window, do the following:

- a. In **Name**, type a disk name of your choice.

For example, for the first additional disk, type `Disk2`.

- b. In **Type**, select **SSD persistent disk**.

- c. In **Size**, type the disk size according to the following table:

Disk	Size (Gb)
First additional disk (Disk 2)	70
Second additional disk (Disk 3)	40
Third additional disk (Disk 4)	10

- d. For other parameters, keep the default values.

6. Click **Create** and then click **Done**.

7. Repeat steps [4](#) on page 172 to [6](#) on page 172 to create the additional required virtual hard disks.

8. Click **Save**.

Enabling LVM on RHEL

About this task

Logical Volume Management (LVM) is a tool that enables you to manage Linux logical and physical volumes. You require this tool to create the required disk layout for Avaya Aura® Device Services. On the Google Cloud Platform RHEL, LVM is disabled by default. You must enable LVM manually.

Before you begin

Enable the YUM package manager on RHEL. For information about enabling YUM, see the Red Hat YUM documentation.

Procedure

1. Log in to the virtual machine as the root user using the SSH connection.
2. Run the following command:

```
yum install lvm2*
```

Creating disk partitioning for a Google Cloud Platform virtual machine

About this task

Avaya Aura® Device Services requires a specific disk layout that includes several disk partitions and logical volumes. Use this procedure to create appropriate disk partitioning.

Before you begin

- Create volumes with the required disk size values as described in [Creating required virtual hard disks for a virtual machine](#) on page 147.

Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. Run the following commands to create the required directories:

```
mkdir -p /var/log/Avaya
mkdir -p /media/data
mkdir -p /media/cassandra
```

3. Run the following commands to create the required physical volumes and volume groups for these volumes:

```
pvccreate -f /dev/sdb
vgcreate disk2_vg /dev/sdb
pvccreate -f /dev/sdc
vgcreate disk3_vg /dev/sdc
pvccreate -f /dev/sdd
vgcreate disk4_vg /dev/sdd
```

4. Run the following commands to create logical volumes in the volume groups:

```
lvcreate -l100%FREE -n application_log /dev/disk2_vg
lvcreate -l100%FREE -n data /dev/disk3_vg
lvcreate -l100%FREE -n cassandra /dev/disk4_vg
```

5. Run the following commands to create a file system for the `/dev/sdb` partition and mount the file system:

```
mkfs.xfs /dev/disk2_vg/application_log
mount /dev/disk2_vg/application_log /var/log/Avaya
echo "/dev/disk2_vg/application_log /var/log/Avaya xfs defaults 0 0" >> /etc/fstab
```

6. Run the following commands to create file systems for the `/dev/sdc` partition and mount the file system:

```
mkfs.xfs /dev/disk3_vg/data
mount /dev/disk3_vg/data /media/data
echo "/dev/disk3_vg/data /media/data xfs defaults 0 0" >> /etc/fstab
```

7. Run the following commands to create file systems for the `/dev/sdd` partition and mount the file system:

```
mkfs.xfs /dev/disk4_vg/cassandra
mount /dev/disk4_vg/cassandra /media/cassandra
echo "/dev/disk4_vg/cassandra /media/cassandra xfs defaults 0 0" >> /etc/fstab
```

Enabling editing of the `/etc/hosts` file

About this task

You use the `/etc/hosts` file to manually map the IP addresses of System Manager and Avaya Aura® Device Services and Utility Server nodes to their hostnames. By default, every time when Avaya Aura® Device Services restarts, Google Cloud Platform automatically changes the content of the `/etc/hosts/` file to its “default” state. Use this procedure to make your entries in the file permanent.

Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. Run the following command to delete the `google_hostname.sh` file:

```
rm -rf /etc/dhcp/dhclient.d/google_hostname.sh
```

Prerequisites for installing the system layer on Google Cloud Platform

In addition to the prerequisites for the software-only system layer installation that are common for all deployment types, Google Cloud Platform has the following specific prerequisites:

- On all Avaya Aura® Device Services nodes in your deployment, add information about each Avaya Aura® Device Services node to the `/etc/hosts` file in the following format:

```
<IP_Address> <Corresponding_FQDN> <hostname>
```

For example:

```
195.51.100.5 aads1.mycompany.com aads1
195.51.100.6 aads2.mycompany.com aads2
```

- Enable root access to RHEL. For more information, see [Enabling root access](#) on page 168.
- Create a non-root user on RHEL. For more information, see [Creating an administrative user](#) on page 103.

Configuring redirection rules for port 443

About this task

In a cluster deployment, if you use the public Google Cloud Platform load balancer, you must manually add a redirection rule for port 443 to Avaya Aura® Device Services. If you use the Utility Server in your deployment, you must also configure an additional redirection rule for the Utility Server load balancer.

Before you begin

Install Avaya Aura® Device Services.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as the root user.
2. Open the `/etc/nftables/aads-rules.nft` file in a text editor.

For example:

```
vi /etc/nftables/aads-rules.nft
```

3. In the `table inet nat` section, in the `chain PREROUTING_direct` text block, and the following entries:

- For Avaya Aura® Device Services:

```
ip daddr <AADS_PUBLIC_LB_IP> tcp dport 443 counter packets 0
bytes 0 redirect to :8443
```

- For the Utility Server:

```
ip daddr <US_PUBLIC_LB_IP> tcp dport 443 counter packets 0 bytes
0 redirect to :1543
```

In these entries, `AADS_PUBLIC_LB_IP` is the IP address of the public Google Cloud Platform load balancer that is used for Avaya Aura® Device Services, and `US_PUBLIC_LB_IP` is the IP address of the public Google Cloud Platform that is used for the Utility Server. The rule for the Utility Server is only required if you use the Utility Server in your deployment.

Important:

Do not delete entries from the `/etc/nftables/aads-rules.nft` file.

4. Save the file.

5. Run the following command:

```
systemctl restart nftables
```

6. Repeat the procedure for all remaining cluster nodes.

Example

The following is an example of the configured `/etc/nftables/aads-rules.nft` file, where the IP address of the Avaya Aura® Device Services load balancer is 190.0.2.10 and the IP address of the Utility Server load balancer is 190.0.2.20:

```
table inet nat {
    chain PREROUTING_direct {
        tcp dport 80 counter packets 0 bytes 0 redirect to :8082
        ip daddr 190.0.2.10 tcp dport 443 counter packets 0 bytes 0 redirect to :8443
        ip daddr 190.0.2.20 tcp dport 443 counter packets 0 bytes 0 redirect to :1543
    }
}
```

Chapter 7: Avaya Aura® Device Services installation

Avaya Aura® Device Services installation checklist

The following checklist describes the high-level deployment steps you must perform to install the Avaya Aura® Device Services application on virtual machines:

No.	Task	Notes	✓
1	Install or restore a standalone Avaya Aura® Device Services application or the initial node for an Avaya Aura® Device Services cluster.	• If you deploy Avaya Aura® Device Services in an Avaya Aura® environment, see Installing Avaya Aura Device Services on page 179. • If you deploy Avaya Aura® Device Services in an environment without Avaya Aura®, see Installing Avaya Aura Device Services in an environment without Avaya Aura on page 189. Optionally, you can perform a silent installation as described in Performing a silent installation on page 217. These procedures apply to standalone and cluster deployment types.	
2	If you deploy a cluster, install additional Avaya Aura® Device Services nodes.	• If you deploy Avaya Aura® Device Services in an Avaya Aura® environment, see Installing additional non-seed nodes on page 199. • If you deploy Avaya Aura® Device Services in an environment without Avaya Aura®, see Installing additional non-seed nodes in an environment without Avaya Aura on page 206. Optionally, you to install additional nodes, you can perform a silent installation as described in Performing a silent installation on page 217.	

No.	Task	Notes	✓
3	If you deploy a cluster, configure RSA keys for SSH connections after all additional nodes are installed.	See Configuring RSA public and private keys for SSH connections in a cluster on page 213.	
4	Run the post-installation script.	See Running the post-installation script on page 223.	
5	In an Avaya Aura® environment, check for DRS synchronization.	See Checking for DRS synchronization on page 224.	
6	If you deploy Avaya Aura® Device Services in a Google Cloud Platform or Microsoft Azure virtual environment, perform additional post-installation procedures.	If you deploy a cluster on Google Cloud Platform or Microsoft Azure, you can complete the virtual environment configuration only after installing the Avaya Aura® Device Services application layer. Perform the following procedures: • For Microsoft Azure: Configure the Microsoft Azure load balancer as described in Creating a Microsoft Azure load balancer on page 154 and Configuring a Microsoft Azure load balancer on page 155. • For Google Cloud Platform: Create redirection rules for port 443 as described in Configuring redirection rules for port 443 on page 175.	
7	Change the default Cassandra database password.	See Changing the Cassandra user name and password on page 248.	
8	Change the default password for automatic backups.	See Changing the default password for automatic backups on page 226.	
9	If you deploy a cluster and enable OAuth, enable OAuth database replication.	See Enabling OAuth database replication in a cluster environment on page 264.	
10	If you deploy a cluster and enable Open LDAP, enable Open LDAP replication.	See Enabling Open LDAP replication on page 255.	
11	In you deploy a cluster, configure an additional seed node.	See Configuring an additional seed node on page 217.	
12	Optionally, enable the Enhanced Access Security Gateway.	See Enabling the Enhanced Access Security Gateway from the CLI on page 222.	
13	Optionally, create an Advanced Intrusion Detection Environment baseline database.	See Creating an AIDE baseline database on page 225.	

Installing Avaya Aura® Device Services

About this task

Use this procedure to install Avaya Aura® Device Services in an Avaya Aura® environment as a standalone instance or as a seed node in a cluster deployment.

You can enable the following features only when installing or upgrading Avaya Aura® Device Services:

- IPv6

 Note:

AWS, Microsoft Azure, and GCP software-only deployments do not support IPv6.

- Utility Server
- Onboard Open LDAP
- SSO/OAuth2

You cannot enable these features using the Avaya Aura® Device Services administration portal or configuration utility.

 Note:

Avaya recommends that you install Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the installation operation is in progress, you can re-connect to the Tmux session and complete the installation operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 72.

Before you begin

- If you are planning to use certificates specific to your organization and signed by a private or public certificate authority instead of System Manager certificates:
 - Ensure that you have all required certificates. For more information, see [Third-party CA-signed certificates](#) on page 42.
 - Import the third-party root and intermediate CA certificates into the trust stores of each server that interacts with Avaya Aura® Device Services to ensure that all these servers trust the third-party CAs.
 - Ensure that you have access to the deployed Avaya Aura® Device Services virtual machine using SSH or to a computer with a recent version of the OpenSSL library.
 - Ensure that System Manager uses an identity certificate signed by the same CA that signs the Avaya Aura® Device Services identity certificates. For more information, see [Configuring third-party identity certificates for System Manager](#) on page 44.
- If you are planning to use FIPS, enable it as described in [Enabling FIPS mode](#) on page 93. You cannot enable FIPS mode during or after Avaya Aura® Device Services installation. You cannot use OAuth and Onboard Open LDAP features when FIPS mode is enabled.
- To use IPv6, enable IPv6 support at the system layer as described in [Enabling IPv6 support at the system layer](#) on page 93.

Procedure

1. Log in to the Avaya Aura® Device Services virtual machine as the administrative user.
You must use the administrative user defined during OVA deployment for logging in to Avaya Aura® Device Services.

2. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_INSTALLATION
```

3. If you are planning to use certificates specific to your organization, do the following:

- a. Transfer the following files to the Avaya Aura® Device Services virtual machine:

- smgrca.pem
- root.pem
- intermediate.pem
- identity.pl2

- b. Concatenate the `intermediate.pem`, `root.pem` and `smgrca.pem` files into a single file with the `cert-chain.pem` name to create a trust chain.

For example, you can run the following command to concatenate files:

```
cat intermediate.pem root.pem smgrca.pem > cert-chain.pem
```

4. Do one of the following:

- If you install Avaya Aura® Device Services using the Avaya-provided OVA, go to the `/opt/Avaya/` directory and run the following command:

```
app install
```

- If you install Avaya Aura® Device Services as a software-only application, run the following command:

```
app install <PATH>/<INSTALLER>
```

In this command, <PATH> is the full path to the directory where you extracted the application binary when installing the system layer, and <INSTALLER> is the Avaya Aura® Device Services application binary. For example:

```
app install /root/aads-swonly-10.2.0.0.70/aads-10.2.0.0.70.bin
```

The system displays the Avaya Aura® Device Services Installer dialog box.

Important:

Do *not* resize the SSH console while installing and configuring Avaya Aura® Device Services.

5. When prompted, type the password for the administrative user.

6. In the Initial Installation Configuration, select **Aura Support**.
7. Select **Enable Aura**, and press `Enter`.
8. In the Enable Aura screen, select **Yes** and then press `Enter`.
9. Select **Return to Main Menu** and press `Enter`.
10. **(Optional)** If you want to enable the Utility Server, do the following:
 - a. In the Initial Installation Configuration screen, select **Utility Server**.
 - b. In the Utility Server menu, select **Utility Server** again and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

 Important:

- If you install a cluster, you must either enable the Utility Server on all nodes or leave it disabled on all nodes. You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.
- If you do not enable the Utility Server, you cannot generate configuration files for endpoints using the Dynamic Configuration service. For more information, see “Administration of the Dynamic Configuration service” in *Administering Avaya Aura® Device Services*.

11. **(Optional)** If you want to enable OAuth, do the following:
 - a. In the Initial Installation Configuration screen, select **OAuth**.
 - b. In the OAuth menu, select **OAuth** again and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

OAuth is unavailable if you enabled FIPS mode.

12. **(Optional)** If you want to enable IPv6 support, do the following:
 - a. In the Initial Installation Configuration screen, select **Enable IPv6**.
 - b. In the Enable IPv6 menu, select **IPv6 support** and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

 Important:

AWS, Microsoft Azure, and GCP software-only deployments *do not* support IPv6.

13. In the Initial Installation Configuration screen, select **Cluster Configuration** and press `Enter`.
14. In the Clustering screen, ensure that the value of the **Initial cluster node** field is `y`.
15. For cluster deployments, ensure that the **Local Node IP address** option is set to the IP address of the node.

16. For cluster deployments, In **Cassandra Datacenter name**, configure a Cassandra datacenter for the node as follows:
 - To add the node to a new datacenter, provide a name of your choice for that datacenter.
 - To add the node to the default “dc1” datacenter, leave the field blank.

Avaya Aura® Device Services logically groups nodes with the same Cassandra datacenter name and configures specific Cassandra replication policies for the members of the datacenter.

17. Select **Return to Main Menu** and press `Enter`.
18. **(Optional)** For cluster deployments, in the **Cassandra Encryption** menu, enable or disable SSL encryption for internode communication between the database servers on the Avaya Aura® Device Services nodes.

If you enabled FIPS mode, SSL encryption for internode communication is enabled by default and the **Cassandra Encryption** menu is unavailable.

19. In the Initial Installation Configuration screen, select **Front-end host, System Manager and Certificate Configuration** and press `Enter`.
20. In the Front-end host, System Manager and Certificate Configuration screen, set values for the following parameters:
 - Front-end FQDN of the Avaya Aura® Device Services server
 - System Manager FQDN
 - System Manager version
 - System Manager HTTPS port
 - System Manager Enrollment Password
 - Local Front-end host
 - Keystore password

Ensure that the keystore password is at least 8 characters long.

 Important:

- For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If you are planning to use an external load balancer, set this value to the FQDN of the load balancer.
 - If Cassandra internode encryption is enabled, you must complete the configuration settings from this menu during the initial installation phase and not at a later time.
21. Do one of the following:
 - If you are planning to use System Manager for certificates, in **Use System Manager for certificates**, select **Yes** and then proceed to step [23](#) on page 183.
 - If you are planning to use certificates that are specific for your organization and signed by a third-party CA, in **Use System Manager for certificates**, select **No** and proceed to step [22](#) on page 183.

22. If you are planning to use certificates that are specific for your organization, do the following:
 - a. For each of the REST, OAM, and NODE interface certificate configuration options, in **Is the interface certificate in PKCS12 format?**, select one of the following:
 - **Yes**, if your interface certificate has the PKCS12 format.
 - **No**, if your interface certificate has the PEM format.
 - b. If you use identity certificates in the PKCS12 format, configure the following settings:
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS12 file**, enter the path to the `identity.pl2` file.
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS file password**, enter the password for the `identity.pl2` file.

If you provide an incorrect password, Avaya Aura® Device Services displays a warning message. You cannot continue installing Avaya Aura® Device Services until you enter the correct password.
 - c. If you use identity certificates in the PEM format, configure the following settings:
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PEM certificate file**, enter the path to the identity certificate file.
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PEM key file**, enter the path to the key file for the identity certificate.
 - d. Select **Signing authority certificate configuration**.
 - e. In **Is the Signing Authority certificate in PKCS12 format?**, select **No**.
 - f. In **Signing Authority PEM certificate file**, enter the path to the `cert-chain.pem` file that you created in step 3.
23. Select **Return to Main Menu** and press `Enter`.
24. In the Initial Installation Configuration screen, select **Session Manager Configuration** and press `Enter`.
25. In the Session Manager Configuration screen, set values for the following parameters:
 - Session Manager Management IP or FQDN
 - Session Manager Asset IP or FQDN

Avaya Aura® Device Services compares the configured Session Manager IP addresses with the ones obtained from System Manager. If they differ, Avaya Aura® Device Services will use the IP addresses obtained from System Manager.
26. Select **Return to Main Menu** and press `Enter`.
27. **(Optional)** If you want to use onboard Open LDAP, do the following:
 - a. In the Initial Installation Configuration screen, select **Onboard Open LDAP**.
 - b. Select **Onboard Open LDAP** again and then select **Yes**.

- c. In **Directory Manager**, enter a name for the Open LDAP administrator.
- d. In **Domain Name**, provide the domain name of your company.

The domain name must include two components. For example: `example.com`. If you provide a domain name that contain three or more domain components, then Avaya Aura® Device Services will use only two rightmost domain components. For example, if you enter `subdomain.example.com`, Avaya Aura® Device Services will use `example.com`.
- e. In **Administrator's password**, provide a password for the Open LDAP administrator.
- f. Select **Return to Main Menu** and press `Enter`.

 Important:

You cannot install onboard Open LDAP if you enabled FIPS mode.

28. In the Initial Installation Configuration screen, select **Continue** and press `Enter`.
29. In the Configuration Summary screen, select **Accept and continue** and press `Enter`.
30. In the Results of Configuration Checks screen, select **Continue** and press `Enter`.

Avaya Aura® Device Services displays the End User License Agreement.
31. Select **Accept** and press `Enter`.

Avaya Aura® Device Services installs the required RPMs, downloads certificates from System Manager, creates database schema, and performs the required initial configuration. After successful installation, Avaya Aura® Device Services displays the Results of Installation Script screen.

32. In the Results of Installation Script screen, select **Continue** and press `Enter`.
33. In the Main Menu screen, select **LDAP Configuration** and press `Enter`.

 Note:

- The LDAP configuration for the cluster is performed during the installation of the initial node. Additional configuration on each of the additional nodes is not required.
 - You can configure LDAP settings after installing the Avaya Aura® Device Services application using the Avaya Aura® Device Services web administration portal.
34. In the LDAP Configuration screen, set values for the following parameters:
 - Use LDAP for authentication

This option is only available when OAuth is enabled.

If you use OpenLDAP, Avaya Aura® Device Services sets values for other LDAP parameters automatically.
 - Use for Contact Search

If you use onboard Open LDAP, this option is enabled by default.

- Use DNS

This option determines how Avaya Aura® Device Services discovers the LDAP server:

- If you select this option, Avaya Aura® Device Services discovers available LDAP server instances using DNS SRV records.
- If you do not select this option, Avaya Aura® Device Services discovers the LDAP server using its IP address or FQDN.

- Directory Type

- URL for LDAP server

- If FIPS is enabled, use the Secure LDAP (LDAPS) protocol to access the LDAP server.
- If you are using global catalog ports 3268 or 3269, you must also configure attribute replication to the global catalog. For more information, see [LDAP attributes replication to the global catalog](#) on page 280.
- If you are using the LDAPS protocol, you cannot use IP addresses in the server URL. LDAPS only supports FQDNs.

This parameter is unavailable if you selected the Use DNS option.

- Bind DN

- Bind Credential

- UID Attribute ID

- Base Context DN

- Administrator Role

- Security Administrator Role

- Auditor Role

- User Role

- Services Administrator Role

- Services Maintenance & Support Role

- Integrated Windows Authentication Configuration

- testUser

The testUser parameter is optional. If you do not specify a value, Avaya Aura® Device Services skips validation and directly saves the configuration in the database. For more information, see [testUser validations](#) on page 188.

For more information about LDAP parameters, see [LDAP configuration](#) on page 234.

35. Select **Advanced LDAP Parameters** and press `Enter`.

36. In the Advanced LDAP Parameters screen, verify the default values for the parameters and update them if required.

For more information about advanced LDAP parameters, see the *Advanced LDAP attributes* table in [LDAP configuration](#) on page 234.

37. Select **Return to previous menu** and press `Enter`.
38. In the LDAP Configuration screen, select **Apply** and press `Enter`.
39. In the LDAP Configuration screen, select **Yes** and press `Enter`.
40. In the Results of LDAP Parameter Configuration screen, select **Continue** and press `Enter`.
41. Select **Return to previous menu** and press `Enter`.

If you are deploying a standalone system, continue from step [47](#) on page 187. The steps [42](#) on page 186 to [46](#) on page 187 are for cluster deployments.

42. In the Main Menu screen, select **Clustering Configuration** and press `Enter`.
43. In the Clustering Configuration screen, select **Virtual IP Configuration** and press `Enter`.

 Important:

The virtual IP address is used for redundancy management, which is supported for two or more Avaya Aura® Device Services nodes.

If you use an external load balancer, you do not need to configure a virtual IP address, but you must configure the Avaya Aura® Device Services front-end host as the FQDN of the load balancer.

This option is unavailable if you are deploying Avaya Aura® Device Services on AWS.

44. In the Virtual IP Configuration screen, set values for the following parameters:
 - a. Set **Enable virtual IP** to `y`.
 - b. Set **Virtual IP address** to the virtual IPv4 address that you want to use.
 - c. If you enabled IPv6, set **Virtual IPv6 address** to the virtual IPv6 address you want to use.
 - d. Set **Virtual IP interface** to the required value.
 - e. Set **Virtual IP master node** to `y`.
 - f. Set **Virtual IP router ID** to the required value.
 - g. Set **Virtual IP authentication password**.

Ensure that you use the same password for subsequent Avaya Aura® Device Services nodes in the cluster.

 Important:

Write down the virtual IP authentication password. You need this password for configuring the virtual IP backup node.

45. Select **Apply** and press `Enter`.

46. Select **Return to previous menu** and press `Enter`.
47. If you chose to enable the Utility Server, in the Main menu screen, select **Utility Server Configuration** and press `Enter`.

If you do not need the Utility Server, continue from step [51](#) on page 187. Steps from [48](#) on page 187 to [50](#) on page 187 are for the Utility Server configuration.

 Important:

If you are deploying a cluster, you must configure cluster settings in **Clustering Configuration** before configuring Utility Server settings. The cluster configuration steps are described earlier in this procedure.

48. In the Utility Server Configuration screen, update the following parameters:
 - a. Set **Utility Server VIP** to a virtual IPv4 address that you want to use for the Utility Server.

 Note:

- You cannot use the Avaya Aura® Device Services cluster virtual IP address as the Utility Server virtual IP address.
- The Utility Server virtual IP address must be in the same subnet as the IP addresses of the Avaya Aura® Device Services cluster nodes.

- b. If you enabled IPv6, set **Utility Server ipv6 VIP** to a virtual IPv6 address that you want to use for the Utility Server.
 - c. Set **Utility Server FQDN** to a FQDN that you want to use for the Utility Server.

In AWS cluster deployments, you must use the following scheme for the seed node Utility Server FQDN:

```
<Utility Server Host Name>0.<Domain Name>
```

For example, if the Utility Server host name is “aads716-us” and the domain name is “avaya.in”, then the Utility Server FQDN is “aads716-us0.avaya.in”.

For more information about Utility Server VIP and FQDNs in AWS deployments, see [Utility Server VIP and FQDN in AWS cluster deployments](#) on page 189.

- d. Set **System Manager Enrollment Password** to the System Manager enrollment password.

The System Manager enrollment password is configured in the System Manager console under **Home > Services > Security > Certificates > Enrollment Password**.

49. Select **Apply** and press `Enter`.
50. Select **Continue** and press `Enter`.
51. In the Main menu screen, select **Continue** and press `Enter`.
52. **(Optional)** To manually start Avaya Aura® Device Services, run the `svc aads start` command.

Next steps

- If you are installing a cluster, install additional cluster nodes and then configure the SSH/RSA Public/Private keys on the seed node.
- Change the default password for automatic backups. For more information, see [Changing the default password for automatic backups](#) on page 226.
- If you enabled OAuth, configure Keycloak settings. You must install all additional cluster nodes before configuring Keycloak settings. For more information, see [OAuth configuration](#) on page 257.
- In a cluster deployment, if you enabled OAuth, enable OAuth database replication after all additional nodes are installed. For more information, see [Enabling OAuth database replication in a cluster environment](#) on page 264.
- If you installed Open LDAP, after all additional nodes are installed and configured, enable Open LDAP replication. For more information, see [Enabling Open LDAP replication](#) on page 255.
- Pair an Avaya Aura® Device Services instance with Session Manager as described in [Adding an Avaya Aura Device Services instance to System Manager](#) on page 270 and [Pairing Session Manager with an Avaya Aura Device Services node](#) on page 272.

Timeout values for Cassandra and Keycloak operations

Avaya Aura® Device Services displays the progress bar during installation or upgrade to indicate that the process is in progress. Certain operations, such as Cassandra database creation and Keycloak initialization, might take some time to install. When performing these operations, Avaya Aura® Device Services does not update the progress bar. To ensure that installation is still in progress, Avaya Aura® Device Services uses the following timeout values for these operations:

- Cassandra database creation: 122 seconds.
- Keycloak initial start-up during installation: 180 seconds.
- Keycloak export and import operations during upgrade: 180 seconds.

In the absence of a response within the specified timeout interval, Avaya Aura® Device Services cancels the installation or upgrade process and displays an error message.

testUser validations

You can optionally specify a value for the testUser parameter. The testUser must be a valid user on LDAP and in the given base context DN.

When you specify a value for testUser and then select **Apply**, Avaya Aura® Device Services validates the following in the LDAP:

- That the user is searchable with a given base DN and search filter.
- The group to which the user belongs — user, administrator, or auditor.
- The values for Role Attribute ID and Role Name Attribute.
- The Last Updated Time attribute, role filter syntax, and active users search filter syntax.

Utility Server VIP and FQDN in AWS cluster deployments

In AWS cluster deployments, the Utility Server VIP is assigned to the `eth1` interface. To find this VIP address, in the AWS Management Console, navigate to **EC2 > Instances > <node name> > Network interfaces > eth1**.

Unlike VMware and ASP deployments, where the Utility Server VIP and FQDN remain the same across the cluster nodes, AWS deployments have a dedicated set of Utility Server VIPs and FQDNs. That is why AWS deployments use a separate `eth1` network interface.

In AWS deployments, the Utility Server FQDNs uses the following pattern:

```
<Utility Server Host Name><node number reduced by one>.<Domain Name>
```

For example, in a cluster with two nodes, where the Utility Server with the “aads716–us” host name is added to the “avaya.in” domain, the Utility Server FQDNs will be the following:

- “aads716–us0.avaya.in” for the first, that is, the seed node in the cluster.
- “aads716–us1.avaya.in” for the second node in the cluster.

Installing Avaya Aura® Device Services in an environment without Avaya Aura®

About this task

Use this procedure to install Avaya Aura® Device Services in an environment without Avaya Aura® as a standalone instance or as a seed node in a cluster deployment.

You can enable the following features only when installing or upgrading Avaya Aura® Device Services:

- IPv6

 Note:

AWS, Microsoft Azure, and GCP software-only deployments do not support IPv6.

- Utility Server
- Onboard Open LDAP
- SSO/OAuth2

You cannot enable these features using the Avaya Aura® Device Services administration portal or configuration utility.

 Note:

Avaya recommends that you install Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the installation operation is in progress, you can re-connect to the Tmux session and complete the installation operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 72.

Before you begin

- Ensure that you have all required certificates signed by a third-party private or public certificate authority. For more information about the required certificates, see [Certificates required for an environment without Avaya Aura](#) on page 45.
- Import the third-party root and intermediate CA certificates into the trust stores of each server that interacts with Avaya Aura® Device Services to ensure that all these servers trust the third-party CAs.
- Ensure that you have access to the deployed Avaya Aura® Device Services virtual machine using SSH or to a computer with a recent version of the OpenSSL library.
- Ensure that System Manager uses an identity certificate signed by the same CA that signs the Avaya Aura® Device Services identity certificates. For more information, see [Configuring third-party identity certificates for System Manager](#) on page 44.

Procedure

1. Log in to the Avaya Aura® Device Services virtual machine as the administrative user.
You must use the administrative user defined during OVA deployment for logging in to Avaya Aura® Device Services.

2. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_INSTALLATION
```

3. To create a certificate chain that you will use when configuring certificate settings, do the following:

- a. Transfer the following files to the Avaya Aura® Device Services virtual machine:

- root.pem
- intermediate.pem
- identity.pl2

- b. Concatenate the intermediate.pem and root.pem files into a single file with the cert-chain.pem name to create a trust chain.

For example, you can run the following command to concatenate files:

```
cat intermediate.pem root.pem > cert-chain.pem
```

4. Do one of the following:

- If you install Avaya Aura® Device Services using the Avaya-provided OVA, go to the /opt/Avaya/ directory and run the following command:

```
app install
```

- If you install Avaya Aura® Device Services as a software-only application, run the following command:

```
app install <PATH>/<INSTALLER>
```

In this command, <PATH> is the full path to the directory where you extracted the application binary when installing the system layer, and <INSTALLER> is the Avaya Aura® Device Services application binary. For example:

```
app install /root/aads-swonly-10.2.0.0.70/aads-10.2.0.0.70.bin
```

The system displays the Avaya Aura® Device Services Installer dialog box.

 Important:

Do *not* resize the SSH console while installing and configuring Avaya Aura® Device Services.

5. When prompted, type the password for the administrative user.
6. To disable the use of Avaya Aura® components, do the following:
 - a. In the Initial Installation Configuration, select **Aura Support**.
 - b. Select **Enable Aura**, and press `Enter`.
 - c. In the Enable Aura screen, select **No** and then press `Enter`.
 - d. Select **Return to Main Menu** and press `Enter`.
7. **(Optional)** If you want to enable the Utility Server, do the following:
 - a. In the Initial Installation Configuration screen, select **Utility Server**.
 - b. In the Utility Server menu, select **Utility Server** again and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

 Important:

- If you install a cluster, you must either enable the Utility Server on all nodes or leave it disabled on all nodes. You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.
- If you do not enable the Utility Server, you cannot generate configuration files for endpoints using the Dynamic Configuration service. For more information, see “Administration of the Dynamic Configuration service” in *Administering Avaya Aura® Device Services*.

8. **(Optional)** If you want to enable OAuth, do the following:
 - a. In the Initial Installation Configuration screen, select **OAuth**.
 - b. In the OAuth menu, select **OAuth** again and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

OAuth is unavailable if you enabled FIPS mode.

9. **(Optional)** If you want to enable IPv6 support, do the following:
 - a. In the Initial Installation Configuration screen, select **Enable IPv6**.
 - b. In the Enable IPv6 menu, select **IPv6 support** and then select **Yes**.

- c. Select **Return to Main Menu** and press `Enter`.

 Important:

AWS, Microsoft Azure, and GCP software-only deployments *do not* support IPv6.

10. In the Initial Installation Configuration screen, select **Cluster Configuration** and press `Enter`.
11. In the Clustering screen, ensure that the value of the **Initial cluster node** field is `y`.
12. For cluster deployments, ensure that the **Local Node IP address** option is set to the IP address of the node.
13. For cluster deployments, In **Cassandra Datacenter name**, configure a Cassandra datacenter for the node as follows:
 - To add the node to a new datacenter, provide a name of your choice for that datacenter.
 - To add the node to the default “dc1” datacenter, leave the field blank.

Avaya Aura® Device Services logically groups nodes with the same Cassandra datacenter name and configures specific Cassandra replication policies for the members of the datacenter.

14. Select **Return to Main Menu** and press `Enter`.
15. **(Optional)** For cluster deployments, in the **Cassandra Encryption** menu, enable or disable SSL encryption for internode communication between the database servers on the Avaya Aura® Device Services nodes.

If you enabled FIPS mode, SSL encryption for internode communication is enabled by default and the **Cassandra Encryption** menu is unavailable.

16. In the Initial Installation Configuration screen, select **Front-end host and Certificate Configuration** and press `Enter`.
17. In the Front-end host and Certificate Configuration screen, set values for the following parameters:
 - Front-end FQDN of the Avaya Aura® Device Services server
 - Local Front-end host
 - Keystore password

Ensure that the keystore password is at least 8 characters long.

 Important:

- For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If you are planning to use an external load balancer, set this value to the FQDN of the load balancer.
- If you enabled Cassandra internode encryption, you must complete the configuration settings from this menu during the initial installation phase and not at a later time.

18. To configure certificates, do the following:

- a. For each of the REST, OAM, and NODE interface certificate configuration options, in **Is the interface certificate in PKCS12 format?**, select one of the following:
 - **Yes**, if your interface certificate has the PKCS12 format.
 - **No**, if your interface certificate has the PEM format.
- b. If you use identity certificates in the PKCS12 format, configure the following settings:
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS12 file**, enter the path to the `identity.p12` file.
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS file password**, enter the password for the `identity.p12` file.

If you provide an incorrect password, Avaya Aura® Device Services displays a warning message. You cannot continue installing Avaya Aura® Device Services until you enter the correct password.
- c. If you use identity certificates in the PEM format, configure the following settings:
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PEM certificate file**, enter the path to the identity certificate file.
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PEM key file**, enter the path to the key file for the identity certificate.
- d. Select **Signing authority certificate configuration**.
- e. In **Is the Signing Authority certificate in PKCS12 format?**, select **No**.
- f. In **Signing Authority PEM certificate file**, enter the path to the `cert-chain.pem` file that you created in step 3.

19. Select **Return to Main Menu** and press `Enter`.

20. **(Optional)** If you want to use onboard Open LDAP, do the following:

- a. In the Initial Installation Configuration screen, select **Onboard Open LDAP**.
- b. Select **Onboard Open LDAP** again and then select **Yes**.
- c. In **Directory Manager**, enter a name for the Open LDAP administrator.
- d. In **Domain Name**, provide the domain name of your company.

The domain name must include two components. For example: `example.com`. If you provide a domain name that contain three or more domain components, then Avaya Aura® Device Services will use only two rightmost domain components. For example, if you enter `subdomain.example.com`, Avaya Aura® Device Services will use `example.com`.

- e. In **Administrator's password**, provide a password for the Open LDAP administrator.
- f. Select **Return to Main Menu** and press `Enter`.

 Important:

You cannot install onboard Open LDAP if you enabled FIPS mode.

21. In the Initial Installation Configuration screen, select **Continue** and press `Enter`.
22. In the Configuration Summary screen, select **Accept and continue** and press `Enter`.
23. In the Results of Configuration Checks screen, select **Continue** and press `Enter`.

Avaya Aura® Device Services displays the End User License Agreement.

24. Select **Accept** and press `Enter`.

Avaya Aura® Device Services installs the required RPMs, creates database schema, and performs the required initial configuration. After successful installation, Avaya Aura® Device Services displays the Results of Installation Script screen.

25. In the Results of Installation Script screen, select **Continue** and press `Enter`.
26. In the Main Menu screen, select **LDAP Configuration** and press `Enter`.

 Note:

- The LDAP configuration for the cluster is performed during the installation of the initial node. Additional configuration on each of the additional nodes is not required.
- You can configure LDAP settings after installing the Avaya Aura® Device Services application using the Avaya Aura® Device Services web administration portal.

27. In the LDAP Configuration screen, set values for the following parameters:

- Use LDAP for authentication

This option is only available when OAuth is enabled.

If you use OpenLDAP, Avaya Aura® Device Services sets values for other LDAP parameters automatically.

- Use for Contact Search

If you use onboard Open LDAP, this option is enabled by default.

- Use DNS

This option determines how Avaya Aura® Device Services discovers the LDAP server:

- If you select this option, Avaya Aura® Device Services discovers available LDAP server instances using DNS SRV records.
- If you do not select this option, Avaya Aura® Device Services discovers the LDAP server using its IP address or FQDN.

- Directory Type

- URL for LDAP server

- If FIPS is enabled, use the Secure LDAP (LDAPS) protocol to access the LDAP server.

- If you are using global catalog ports 3268 or 3269, you must also configure attribute replication to the global catalog. For more information, see [LDAP attributes replication to the global catalog](#) on page 280.
- If you are using the LDAPS protocol, you cannot use IP addresses in the server URL. LDAPS only supports FQDNs.

This parameter is unavailable if you selected the Use DNS option.

- Bind DN
- Bind Credential
- UID Attribute ID
- Base Context DN
- Administrator Role
- Security Administrator Role
- Auditor Role
- User Role
- Services Administrator Role
- Services Maintenance & Support Role
- Integrated Windows Authentication Configuration
- testUser

The testUser parameter is optional. If you do not specify a value, Avaya Aura® Device Services skips validation and directly saves the configuration in the database. For more information, see [testUser validations](#) on page 188.

For more information about LDAP parameters, see [LDAP configuration](#) on page 234.

28. Select **Advanced LDAP Parameters** and press `Enter`.
29. In the Advanced LDAP Parameters screen, verify the default values for the parameters and update them if required.

For more information about advanced LDAP parameters, see the *Advanced LDAP attributes* table in [LDAP configuration](#) on page 234.

30. Select **Return to previous menu** and press `Enter`.
31. In the LDAP Configuration screen, select **Apply** and press `Enter`.
32. In the LDAP Configuration screen, select **Yes** and press `Enter`.
33. In the Results of LDAP Parameter Configuration screen, select **Continue** and press `Enter`.
34. Select **Return to previous menu** and press `Enter`.

If you are deploying a standalone system, continue from step [40](#) on page 196. The steps 33 to 37 are for cluster deployments.

35. In the Main Menu screen, select **Clustering Configuration** and press `Enter`.
36. In the Clustering Configuration screen, select **Virtual IP Configuration** and press `Enter`.

 Important:

The virtual IP address is used for redundancy management, which is supported for two or more Avaya Aura® Device Services nodes.

If you use an external load balancer, you do not need to configure a virtual IP address, but you must configure the Avaya Aura® Device Services front-end host as the FQDN of the load balancer.

This option is unavailable if you are deploying Avaya Aura® Device Services on AWS.

37. In the Virtual IP Configuration screen, set values for the following parameters:
 - a. Set **Enable virtual IP** to `y`.
 - b. Set **Virtual IP address** to the virtual IPv4 address that you want to use.
 - c. If you enabled IPv6, set **Virtual IPv6 address** to the virtual IPv6 address you want to use.
 - d. Set **Virtual IP interface** to the required value.
 - e. Set **Virtual IP master node** to `y`.
 - f. Set **Virtual IP router ID** to the required value.
 - g. Set **Virtual IP authentication password**.

Ensure that you use the same password for subsequent Avaya Aura® Device Services nodes in the cluster.

 Important:

Write down the virtual IP authentication password. You need this password for configuring the virtual IP backup node.

38. Select **Apply** and press `Enter`.
39. Select **Return to previous menu** and press `Enter`.
40. If you chose to enable the Utility Server, in the Main menu screen, select **Utility Server Configuration** and press `Enter`.

If you do not need the Utility Server, continue from step 42. Steps from 39 to 41 are for the Utility Server configuration.

 Important:

If you are deploying a cluster, you must configure cluster settings in **Clustering Configuration** before configuring Utility Server settings. The cluster configuration steps are described earlier in this procedure.

41. In the Utility Server Configuration screen, update the following parameters:

- a. Set **Utility Server VIP** to a virtual IPv4 address that you want to use for the Utility Server.

 Note:

- You cannot use the Avaya Aura® Device Services cluster virtual IP address as the Utility Server virtual IP address.
- The Utility Server virtual IP address must be in the same subnet as the IP addresses of the Avaya Aura® Device Services cluster nodes.

- b. If you enabled IPv6, set **Utility Server Ipv6 VIP** to a virtual IPv6 address that you want to use for the Utility Server.

- c. Set **Utility Server FQDN** to a FQDN that you want to use for the Utility Server.

In AWS cluster deployments, you must use the following scheme for the seed node Utility Server FQDN:

```
<Utility Server Host Name>0.<Domain Name>
```

For example, if the Utility Server host name is “aads716-us” and the domain name is “avaya.in”, then the Utility Server FQDN is “aads716-us0.avaya.in”.

For more information about Utility Server VIP and FQDNs in AWS deployments, see [Utility Server VIP and FQDN in AWS cluster deployments](#) on page 189.

42. Select **Apply** and press `Enter`.

43. Select **Continue** and press `Enter`.

44. In the Main menu screen, select **Continue** and press `Enter`.

45. **(Optional)** To manually start Avaya Aura® Device Services, run the `svc aads start` command.

Next steps

- If you are installing a cluster, install additional cluster nodes and then configure the SSH/RSA Public/Private keys on the seed node.
- Change the default password for automatic backups. For more information, see [Changing the default password for automatic backups](#) on page 226.
- If you enabled OAuth, configure Keycloak settings. You must install all additional cluster nodes before configuring Keycloak settings. For more information, see [OAuth configuration](#) on page 257.
- In a cluster deployment, if you enabled OAuth, enable OAuth database replication after all additional nodes are installed. For more information, see [Enabling OAuth database replication in a cluster environment](#) on page 264.
- If you installed Open LDAP, after all additional nodes are installed and configured, enable Open LDAP replication. For more information, see [Enabling Open LDAP replication](#) on page 255.

Avaya Aura® Device Services cluster installation

An Avaya Aura® Device Services cluster requires Avaya Aura® Device Services servers that belong to the same network, with one seed node and up to 27 additional nodes.

The installation of a cluster consists of installing the Avaya Aura® Device Services server on all the nodes, by following a process similar to the single-server installation, while also configuring cluster-specific details.

Resource profiles

You must use the same profile for each Avaya Aura® Device Services server in a cluster. Mixed profile clusters are not supported. For example, your cluster cannot consist of one Profile 1 server and three Profile 5 servers. All servers in the cluster must use either Profile 1 only or Profile 5 only.

Redundancy

For redundancy, you require multiple nodes and a virtual IP address or an external load balancer. The client applications use the FQDN that resolves to the virtual IP address or the FQDN of the load balancer to gain access to Avaya Aura® Device Services.

Load balancer

If you use the embedded Avaya Aura® Device Services load balancing mechanism, you must configure a virtual IP master node and a virtual IP backup node. The virtual IP address must be in the same subnet as the Avaya Aura® Device Services nodes.

- The virtual IP master node is the initial node and handles the Avaya Aura® Device Services requests by default.
- The virtual IP backup node is an additional node that handles the load balancing functions when the master node is not functioning.

Warning:

To be able to handle all the HTTP requests, at least two virtual IP nodes, the Virtual IP master node and Virtual IP backup node, must function correctly at all times.

Related links

[External load balancer requirements](#) on page 50

[Considerations for large cluster deployments](#) on page 40

[Deploying the Avaya Aura Device Services OVA using the Host Client connected directly to the ESXi host](#) on page 83

[Adding an Avaya Aura Device Services instance to System Manager](#) on page 270

[Considerations for large cluster deployments](#) on page 40

Installing an Avaya Aura® Device Services cluster

About this task

Use this procedure to install an Avaya Aura® Device Services cluster.

Before you begin

Ensure that you understand the Avaya Aura® Device Services prerequisites. The prerequisites for installing an Avaya Aura® Device Services cluster are the same as for installing an individual Avaya Aura® Device Services server.

Note:

The Avaya Aura® Device Services cluster must be installed by a Linux user with sudo privileges, created during the pre-configuration setup. The User ID (UID) of the Linux user that performs the installation must be the same on all the Avaya Aura® Device Services nodes. After a user is configured, run the following command to display the ID of the user:

```
id -u <user_name>
```

For example:

```
id -u Avaya
```

Procedure

1. Install the initial node.

For more information, see [Installing Avaya Aura Device Services](#) on page 179.

2. Install one or more additional nodes.

Important:

Proceed with the next steps only after installing all the Avaya Aura® Device Services nodes.

3. After all the required cluster nodes are installed, configure the SSH/RSA Public/Private keys on the seed node.

For more information, see [Configuring RSA public and private keys for SSH connections in a cluster](#) on page 213.

4. **(Optional)** Start every node in the cluster individually.

Using a Linux shell for each Avaya Aura® Device Services server in the cluster, run the following command:

```
svc aads start
```

Initial cluster node installation

Install the initial or seed node by following the same procedure as for single server deployment, while also configuring cluster-specific details. For more information, see [Installing Avaya Aura Device Services](#) on page 179.

Installing additional non-seed nodes

About this task

Use this procedure to install a second node or any subsequent node in the cluster.

You can enable the following features only when installing or upgrading Avaya Aura® Device Services:

- IPv6

*** Note:**

AWS, Microsoft Azure, and GCP software-only deployments do not support IPv6.

- Utility Server
- Onboard Open LDAP
- SSO/OAuth2

You cannot enable these features using the Avaya Aura® Device Services administration portal or configuration utility.

*** Note:**

Avaya recommends that you install Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the installation operation is in progress, you can re-connect to the Tmux session and complete the installation operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 72.

Before you begin

If you are planning to use certificates specific to your organization instead of System Manager certificates, ensure that you have the `cert-chain.pem` certificate chain file created during the seed node installation. For more information, see step 3 of [Installing Avaya Aura Device Services](#) on page 179.

Procedure

1. Log in to Avaya Aura® Device Services as the administrative user.

You must use the administrative user defined during OVA deployment for logging in to Avaya Aura® Device Services.

2. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_INSTALLATION
```

3. Do one of the following:

- If you install Avaya Aura® Device Services using the Avaya-provided OVA, go to the `/opt/Avaya/` directory and run the following command:

```
app install
```

- If you install Avaya Aura® Device Services as a software-only application, run the following command:

```
app install <PATH>/<INSTALLER>
```

In this command, <PATH> is the full path to the directory where you extracted the application binary when installing the system layer, and <INSTALLER> is the Avaya Aura® Device Services application binary. For example:

```
app install /root/aads-swonly-10.2.0.0.70/aads-10.2.0.0.70.bin
```

The system displays the Avaya Aura® Device Services Installer dialog box.

! Important:

Do *not* resize the SSH console while installing and configuring Avaya Aura® Device Services.

4. When prompted, type the administrative user password.
5. **(Optional)** If you want to enable the Utility Server, do the following:
 - a. In the Initial Installation Configuration screen, select **Utility Server**.
 - b. In the Utility Server menu, select **Utility Server** again and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

! Important:

- If you install a cluster, you must either enable the Utility Server on all nodes or leave it disabled on all nodes. You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.
- If you do not enable the Utility Server, you cannot generate configuration files for endpoints using the Dynamic Configuration service. For more information, see “Administration of the Dynamic Configuration service” in *Administering Avaya Aura® Device Services*.

6. **(Optional)** If you want to enable OAuth, do the following:
 - a. In the Initial Installation Configuration screen, select **OAuth**.
 - b. In the OAuth menu, select **OAuth** again and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

OAuth is unavailable if you enabled FIPS mode.

7. **(Optional)** If you want to enable IPv6 support, do the following:
 - a. In the Initial Installation Configuration screen, select **Enable IPv6**.
 - b. In the Enable IPv6 menu, select **IPv6 support** and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

! Important:

AWS, Microsoft Azure, and GCP software-only deployments *do not* support IPv6.

8. In the Initial Installation Configuration screen, select **Cluster Configuration** and press `Enter`.
9. In the Clustering screen, set **Initial cluster node** to `n`.
10. In the Clustering screen, set **Local node IP address** to the IP address of the new Avaya Aura® Device Services node and then press `Enter`.

11. In the Clustering screen, set **Cluster seed node** to the IP address of the seed node or the first cluster node and then press `Enter`.
12. In **Cassandra Datacenter name**, configure a Cassandra datacenter for the node as follows:
 - To add the node to an existing datacenter, provide the name of one of the already existing datacenters on Avaya Aura® Device Services.
 - To add the node to a new datacenter, provide a name of your choice for that datacenter.
 - To add the node to the default “dc1” datacenter, leave the field blank.

Avaya Aura® Device Services logically groups nodes with the same Cassandra datacenter name and configures specific Cassandra replication policies for the members of the datacenter.

13. In the Clustering screen, set **User ID of product user on seed node**, type the UID of the seed node, and then click `Enter`.
14. Select **Return to Main Menu** and then press `Enter`.
15. In the Initial Installation Configuration screen, select **Front-end host, System Manager and Certificate Configuration** and press `Enter`.
16. In the Front-end host, System Manager and Certificate Configuration screen, set values for the following:
 - System Manger FQDN
 - System Manager version
 - System Manager HTTPS port
 - System Manager Enrollment Password
 - Local Front-end host
 - Keystore password

Ensure that the keystore password is at least 8 characters long.

 Important:

The values that you specify on this screen must match the values provided for the seed node *except for* the local front-end host.

17. Do one of the following:
 - If you are planning to use System Manager for certificates, in **Use System Manager for certificates**, select **Yes** and proceed to step 17.
 - If you are planning to use certificates that are specific for your organization and signed by a third-party CA, in **Use System Manager for certificates**, select **No** and perform step 16.

18. If you use certificates that are specific for your organization, do the following:
 - a. For each of the REST, OAM, and NODE interface certificate configuration options, in **Is the interface certificate in PKCS12 format?**, select one of the following:
 - **Yes**, if your interface certificate has the PKCS12 format.
 - **No**, if your interface certificate has the PEM format.
 - b. If you use identity certificates in the PKCS12 format, configure the following settings:
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS12 file**, enter the path to the `identity.p12` file.
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS file password**, enter the password for the `identity.p12` file.

If you provide an incorrect password, Avaya Aura® Device Services displays a warning message. You cannot continue installing Avaya Aura® Device Services until you enter the correct password.
 - c. If you use identity certificates in the PEM format, configure the following settings:
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PEM certificate file**, enter the path to the identity certificate file.
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PEM key file**, enter the path to the key file for the identity certificate.
 - d. Select **Signing authority certificate configuration**.
 - e. In **Is the Signing Authority certificate in PKCS12 format?**, select **No**.
 - f. In **Signing Authority PEM certificate file**, enter the path to the `cert-chain.pem` certificate chain file.
19. Select **Return to Main Menu** and then press `Enter`.
20. In the Initial Installation Configuration screen, select **Session Manager Configuration** and press `Enter`.
21. In the Session Manager Configuration screen, set values for the following parameters:
 - Session Manager Management IP
 - Session Manager Asset IP
22. Select **Return to Main Menu** and then press `Enter`.
23. **(Optional)** If your cluster uses Open LDAP, do the following:
 - a. In the Initial Installation Configuration screen, select **Onboard Open LDAP**.
 - b. Select **Onboard Open LDAP** again and then select **Yes**.

 Important:

For Open LDAP parameters values, you must use the same values that you used while deploying the seed node. Otherwise, data replication between nodes might not work as expected.

- c. In **Directory Manager**, enter a name for the Open LDAP administrator.
 - d. In **Domain Name**, provide the domain name of your company.
 - e. In **Administrator's password**, provide a password for the Open LDAP administrator.
 - f. Select **Return to Main Menu** and press `Enter`.
24. Select **Continue** and then press `Enter`.
25. In the Configuration Summary screen, verify the values, select **Accept and Continue** and then press `Enter`.
- The installer performs pre-install checks.
26. In the Results of configuration checks screen, select **Continue** and then press `Enter`.
- Avaya Aura® Device Services displays the End User License Agreement.
27. Select **Accept** and then press `Enter`.
- Avaya Aura® Device Services displays the progress of the tasks in the Running Installer Script window. Avaya Aura® Device Services installs the required RPMs, downloads certificates from System Manager, creates database schema, and performs the required initial configuration. After successful installation, Avaya Aura® Device Services displays the Results of Installation Script screen.
28. Select **Continue** and then press `Enter`.
29. In the Main Menu screen, select **Clustering Configuration** and then press `Enter`.
30. In the Clustering Configuration screen, select **Virtual IP Configuration** and then press `Enter`.

 Important:

If you are using an external load balancer, do not configure a virtual IP address.

31. In the Virtual IP Configuration screen, set values for the following parameters:
- a. Set **Enable virtual IP** to `y`.
 - b. Set **Virtual IP address** to the virtual IPv4 address that you want to use.
 - c. If you enabled IPv6, set **Virtual IPv6 address** to the virtual IPv6 address you want to use.
 - d. Set **Virtual IP interface** to the required value.
 - e. Set **Virtual IP master node** to `n`.
 - f. Set **Virtual IP router ID** to the required value.

- g. Set **Virtual IP authentication password** to the password you set on the seed node.
- 32. Select **Apply** and then press `Enter`.
- 33. In the Clustering Configuration screen, select **Return to Main Menu** and then press `Enter`.
- 34. If you chose to enable the Utility Server, in the Main menu screen, select **Utility Server Configuration** and press `Enter`.

If you do not need the Utility Server, continue from step 36. Steps from 32 to 35 are for the Utility Server configuration.

 Important:

If you are deploying a cluster, you must configure cluster settings in **Clustering Configuration** before configuring Utility Server settings. The cluster configuration steps are described earlier in this procedure.

- 35. In the Utility Server Configuration screen, update the following parameters:
 - a. Set **Utility Server VIP** to a virtual IPv4 address that you want to use for the Utility Server.

You cannot use the Avaya Aura® Device Services cluster virtual IP address as the Utility Server virtual IP address.

- b. If you enabled IPv6, set **Utility Server Ipv6 VIP** to a virtual IPv6 address that you want to use for the Utility Server.
 - c. Set **Utility Server FQDN** to a FQDN that you want to use for the Utility Server.

In AWS cluster deployments, you must use the following scheme for a non-seed node Utility Server FQDN:

```
<Utility Server Host Name><number>.<Domain Name>
```

In this scheme, `<number>` is the number of a node reduced by one. For example, if the cluster has three nodes, the Utility Server host name is “aads716-us”, and the domain name is “avaya.in”, then the Utility Server FQDN is “aads716-us1.avaya.in” for the second node, or the first non-seed node, and “aads716-us2.avaya.in” for the third node, or the second non-seed node in the cluster. The Utility Server FQDN of the seed node is “aads716-us0.avaya.in”.

For more information about Utility Server VIP and FQDNs in AWS deployments, see [Utility Server VIP and FQDN in AWS cluster deployments](#) on page 189.

- d. Set **System Manager Enrollment Password** to the System Manager enrollment password.

The System Manager enrollment password is configured in the System Manager console under **Home > Services > Security > Certificates > Enrollment Password**.

When a Utility Server FQDN or VIP is updated on a node, the changes are propagated to all other nodes in the cluster. However, you still must configure Utility Server settings on

each node in order to set the firewall redirection rules and certificate configuration on each node.

36. Select **Apply** and press `Enter`.

37. Select **Continue** and press `Enter`.

38. **(Optional)** In the Main Menu screen, select **Add a Certificate to the TrustStore** and then press `Enter`.

This step is optional if you use a certificate different from the System Manager certificate.

39. Select **Continue** and then press `Enter`.

Avaya Aura® Device Services prompts you to restart services.

40. Select **Yes** and then press `Enter`.

41. In the Results of service AADS restart screen, select **Continue** and then press `Enter`.

Avaya Aura® Device Services service installation is completed.

Next steps

- After all additional nodes are installed, configure the SSH/RSA Public and Private keys on the seed node.
- If you enabled OAuth, do the following after all additional nodes are installed:
 - Configure Keycloak settings. For more information, see [OAuth configuration](#) on page 257 .
 - Enable OAuth database replication. For more information, see [Enabling OAuth database replication in a cluster environment](#) on page 264 .
- If you installed Open LDAP, after all additional nodes are installed and configured, enable Open LDAP replication. For more information, see [Enabling Open LDAP replication](#) on page 255.

Installing additional non-seed nodes in an environment without Avaya Aura®

About this task

Use this procedure to install a second node or any subsequent node in the cluster in an environment without Avaya Aura®.

You can enable the following features only when installing or upgrading Avaya Aura® Device Services:

- IPv6

Note:

AWS, Microsoft Azure, and GCP software-only deployments do not support IPv6.

- Utility Server
- Onboard Open LDAP

- OAuth2

You cannot enable these features using the Avaya Aura® Device Services administration portal or configuration utility.

*** Note:**

Avaya recommends that you install Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the installation operation is in progress, you can re-connect to the Tmux session and complete the installation operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 72.

Before you begin

- Ensure that you have all required certificates signed by a third-party private or public certificate authority. For more information about the required certificates, see [Certificates required for an environment without Avaya Aura](#) on page 45.
- Ensure that you have the `cert-chain.pem` certificate chain file created during the seed node installation. For more information, see step 3 of [Installing Avaya Aura Device Services in an environment without Avaya Aura](#) on page 189.

Procedure

1. Log in to the Avaya Aura® Device Services virtual machine as the administrative user.

You must use the administrative user defined during OVA deployment for logging in to Avaya Aura® Device Services.

2. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_INSTALLATION
```

3. Do one of the following:

- If you install Avaya Aura® Device Services using the Avaya-provided OVA, go to the `/opt/Avaya/` directory and run the following command:

```
app install
```

- If you install Avaya Aura® Device Services as a software-only application, run the following command:

```
app install <PATH>/<INSTALLER>
```

In this command, <PATH> is the full path to the directory where you extracted the application binary when installing the system layer, and <INSTALLER> is the Avaya Aura® Device Services application binary. For example:

```
app install /root/aads-swonly-10.2.0.0.70/aads-10.2.0.0.70.bin
```

The system displays the Avaya Aura® Device Services Installer dialog box.

 Important:

Do *not* resize the SSH console while installing and configuring Avaya Aura® Device Services.

4. When prompted, type the password for the administrative user.
5. To disable the use of Avaya Aura® components, do the following:
 - a. In the Initial Installation Configuration, select **Aura Support**.
 - b. Select **Enable Aura**, and press `Enter`.
 - c. In the Enable Aura screen, select **No** and then press `Enter`.
 - d. Select **Return to Main Menu** and press `Enter`.
6. **(Optional)** If you want to enable the Utility Server, do the following:
 - a. In the Initial Installation Configuration screen, select **Utility Server**.
 - b. In the Utility Server menu, select **Utility Server** again and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

 Important:

- If you install a cluster, you must either enable the Utility Server on all nodes or leave it disabled on all nodes. You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.
- If you do not enable the Utility Server, you cannot generate configuration files for endpoints using the Dynamic Configuration service. For more information, see “Administration of the Dynamic Configuration service” in *Administering Avaya Aura® Device Services*.

7. **(Optional)** If you want to enable OAuth, do the following:
 - a. In the Initial Installation Configuration screen, select **OAuth**.
 - b. In the OAuth menu, select **OAuth** again and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

OAuth is unavailable if you enabled FIPS mode.

8. **(Optional)** If you want to enable IPv6 support, do the following:
 - a. In the Initial Installation Configuration screen, select **Enable IPv6**.
 - b. In the Enable IPv6 menu, select **IPv6 support** and then select **Yes**.
 - c. Select **Return to Main Menu** and press `Enter`.

 Important:

AWS, Microsoft Azure, and GCP software-only deployments *do not* support IPv6.

9. In the Initial Installation Configuration screen, select **Cluster Configuration** and press `Enter`.

10. In the Clustering screen, set **Initial cluster node** to `n`.
11. In the Clustering screen, set **Local node IP address** to the IP address of the new Avaya Aura® Device Services node and then press `Enter`.
12. In the Clustering screen, set **Cluster seed node** to the IP address of the seed node or the first cluster node and then press `Enter`.
13. In **Cassandra Datacenter name**, configure a Cassandra datacenter for the node as follows:
 - To add the node to an existing datacenter, provide the name of one of the already existing datacenters on Avaya Aura® Device Services.
 - To add the node to a new datacenter, provide a name of your choice for that datacenter.
 - To add the node to the default “dc1” datacenter, leave the field blank.

Avaya Aura® Device Services logically groups nodes with the same Cassandra datacenter name and configures specific Cassandra replication policies for the members of the datacenter.

14. In the Clustering screen, set **User ID of product user on seed node**, type the UID of the seed node, and then click `Enter`.
15. Select **Return to Main Menu** and then press `Enter`.
16. In the Initial Installation Configuration screen, select **Front-end host, System Manager and Certificate Configuration** and press `Enter`.
17. In the Front-end host and Certificate Configuration screen, set values for the following parameters:
 - Local Front-end host
 - Keystore password

Ensure that the keystore password is at least 8 characters long.

 Important:

The values that you specify on this screen must match the values provided for the seed node *except for* the local front-end host.

18. To configure certificates, do the following:
 - a. For each of the REST, OAM, and NODE interface certificate configuration options, in **Is the interface certificate in PKCS12 format?**, select one of the following:
 - **Yes**, if your interface certificate has the PKCS12 format.
 - **No**, if your interface certificate has the PEM format.
 - b. If you use identity certificates in the PKCS12 format, configure the following settings:
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS12 file**, enter the path to the `identity.p12` file.

- For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS file password**, enter the password for the `identity.p12` file.

If you provide an incorrect password, Avaya Aura® Device Services displays a warning message. You cannot continue installing Avaya Aura® Device Services until you enter the correct password.

- c. If you use identity certificates in the PEM format, configure the following settings:
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PEM certificate file**, enter the path to the identity certificate file.
 - For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PEM key file**, enter the path to the key file for the identity certificate.
 - d. Select **Signing authority certificate configuration**.
 - e. In **Is the Signing Authority certificate in PKCS12 format?**, select **No**.
 - f. In **Signing Authority PEM certificate file**, enter the path to the `cert-chain.pem` certificate chain file.
19. Select **Return to Main Menu** and then press `Enter`.
 20. **(Optional)** If your cluster uses Open LDAP, do the following:
 - a. In the Initial Installation Configuration screen, select **Onboard Open LDAP**.
 - b. Select **Onboard Open LDAP** again and then select **Yes**.
-  **Important:**

For Open LDAP parameters values, you must use the same values that you used while deploying the seed node. Otherwise, data replication between nodes might not work as expected.
- c. In **Directory Manager**, enter a name for the Open LDAP administrator.
 - d. In **Domain Name**, provide the domain name of your company.
 - e. In **Administrator's password**, provide a password for the Open LDAP administrator.
 - f. Select **Return to Main Menu** and press `Enter`.
21. Select **Continue** and then press `Enter`.
 22. In the Configuration Summary screen, verify the values, select **Accept and Continue**, and press `Enter`.
 23. In the Results of Configuration Checks screen, select **Continue** and press `Enter`.
- Avaya Aura® Device Services displays the End User License Agreement.
24. Select **Accept** and press `Enter`.

Avaya Aura® Device Services displays the progress of the tasks in the Running Installer Script window. Avaya Aura® Device Services installs the required RPMs, downloads certificates from System Manager, creates database schema, and performs the required

initial configuration. After successful installation, Avaya Aura® Device Services displays the Results of Installation Script screen.

25. Select **Continue** and then press `Enter`.
26. In the Main Menu screen, select **Clustering Configuration** and then press `Enter`.
27. In the Clustering Configuration screen, select **Virtual IP Configuration** and then press `Enter`.

 Important:

If you are using an external load balancer, do not configure a virtual IP address.

28. In the Virtual IP Configuration screen, set values for the following parameters:
 - a. Set **Enable virtual IP** to `y`.
 - b. Set **Virtual IP address** to the virtual IPv4 address that you want to use.
 - c. If you enabled IPv6, set **Virtual IPv6 address** to the virtual IPv6 address you want to use.
 - d. Set **Virtual IP interface** to the required value.
 - e. Set **Virtual IP master node** to `n`.
 - f. Set **Virtual IP router ID** to the required value.
 - g. Set **Virtual IP authentication password** to the password that you set on the seed node.
29. Select **Apply** and then press `Enter`.
30. In the Clustering Configuration screen, select **Return to Main Menu** and then press `Enter`.
31. If you chose to enable the Utility Server, in the Main menu screen, select **Utility Server Configuration** and press `Enter`.

If you do not need the Utility Server, continue from step [35](#) on page 212. Steps from [31](#) on page 211 to [34](#) on page 212 are for the Utility Server configuration.

 Important:

If you are deploying a cluster, you must configure cluster settings in **Clustering Configuration** before configuring Utility Server settings. The cluster configuration steps are described earlier in this procedure.

32. In the Utility Server Configuration screen, update the following parameters:
 - a. Set **Utility Server VIP** to a virtual IPv4 address that you want to use for the Utility Server.

You cannot use the Avaya Aura® Device Services cluster virtual IP address as the Utility Server virtual IP address.
 - b. If you enabled IPv6, set **Utility Server ipv6 VIP** to a virtual IPv6 address that you want to use for the Utility Server.

- c. Set **Utility Server FQDN** to a FQDN that you want to use for the Utility Server.

In AWS cluster deployments, you must use the following scheme for a non-seed node Utility Server FQDN:

```
<Utility Server Host Name><number>.<Domain Name>
```

In this scheme, <number> is the number of a node reduced by one. For example, if the cluster has three nodes, the Utility Server host name is “aads716-us”, and the domain name is “avaya.in”, then the Utility Server FQDN is “aads716-us1.avaya.in” for the second node, or the first non-seed node, and “aads716-us2.avaya.in” for the third node, or the second non-seed node in the cluster. The Utility Server FQDN of the seed node is “aads716-us0.avaya.in”.

For more information about Utility Server VIP and FQDNs in AWS deployments, see [Utility Server VIP and FQDN in AWS cluster deployments](#) on page 189.

When a Utility Server FQDN or VIP is updated on a node, the changes are propagated to all other nodes in the cluster. However, you still must configure Utility Server settings on each node in order to set the firewall redirection rules and certificate configuration on each node.

33. Select **Apply** and press `Enter`.
34. Select **Continue** and press `Enter`.
35. **(Optional)** In the Main Menu screen, select **Add a Certificate to the TrustStore** and then press `Enter`.

This step is optional if you use a certificate different from the System Manager certificate.

36. Select **Continue** and then press `Enter`.

Avaya Aura® Device Services prompts you to restart services.

37. Select **Yes** and then press `Enter`.
38. In the Results of service AADS restart screen, select **Continue** and then press `Enter`.

Avaya Aura® Device Services service installation is completed.

Next steps

- After all additional nodes are installed, configure the SSH/RSA Public and Private keys on the seed node.
- If you enabled OAuth, do the following after all additional nodes are installed:
 - Configure Keycloak settings. For more information, see [OAuth configuration](#) on page 257 .
 - Enable OAuth database replication. For more information, see [Enabling OAuth database replication in a cluster environment](#) on page 264 .
- If you installed Open LDAP, after all additional nodes are installed and configured, enable Open LDAP replication. For more information, see [Enabling Open LDAP replication](#) on page 255.

Configuring RSA public and private keys for SSH connections in a cluster

About this task

After nodes are added to a cluster, you must configure the RSA public and private keys to enable internode SSH communications.

Use this procedure to configure the RSA public and private keys on the initial node for the entire cluster.

Before you begin

Install all of the required nodes for the cluster.

Procedure

1. Log in to the Linux shell on the initial Avaya Aura® Device Services node as an administrator.
2. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
3. Navigate to **Clustering Configuration > Cluster Utilities > Configure SSH RSA Public/Private Keys**.

Avaya Aura® Device Services displays the RSA Public and Private key configuration tool.
4. When the system displays the `Add additional hosts to the list? (y/n)` prompt, enter `y` (yes) if you are generating keys for the first time or if you need to generate keys for a new node in the cluster.

Otherwise, enter `n` (no).
5. If you chose to update the node list in the previous step, when Avaya Aura® Device Services prompts you, enter the IP address of the non-seed node in the cluster you want to generate keys for and then press `Enter`.
6. Repeat the previous step for all remaining non-seed nodes.
7. When Avaya Aura® Device Services prompts you to enter a user name for a node, enter the username for the Linux administrator account that you used to perform the Avaya Aura® Device Services installation.
8. If Avaya Aura® Device Services prompts you to replace the existing keys, enter `y` (yes).
9. When Avaya Aura® Device Services prompts you to enter a password, enter the password for the Linux administrator account that you used to perform the installation.
10. When the configuration is complete, press `Enter`.
11. Return to the main menu.
12. From the main menu, select **Continue** and then select **Yes** to apply the changes.

Changing the LDAP parameters after installing an Avaya Aura® Device Services cluster

About this task

You can change the LDAP configuration by running the Avaya Aura® Device Services configuration utility or by using the Avaya Aura® Device Services administration portal.

The LDAP reconfiguration is performed locally on one Avaya Aura® Device Services node by running a script that synchronizes the LDAP configuration through all the cluster nodes.

The following procedure describes how to change the LDAP parameters after an Avaya Aura® Device Services cluster is installed.

Procedure

1. Change the LDAP configuration by performing one of the following actions on one of the Avaya Aura® Device Services cluster nodes:
 - Run the Avaya Aura® Device Services configuration utility using the `app configure` command and select **LDAP Configuration**.
 - Log in to the administration portal and select **Server Connections > LDAP Configuration > Enterprise Directory**.
2. Restart each node in the Avaya Aura® Device Services cluster.

Changing the seed node of a cluster

About this task

Use this procedure to change the seed node only if you need to decommission the seed node. If you are not installing a new node but assigning the seed node function to an existing node, follow the procedure starting with Step 2.

Note:

Before running the `setSeedNode` script, disable the virtual IP on the node so that the new seed node can be set as the virtual IP master afterwards.

Procedure

1. Install the new node as an additional cluster node.
2. Log on to the new node and run the `setSeedNode.sh` script.
For example:

```
sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/setSeedNode.sh
```
3. Log on to each of the other cluster nodes and run the `setSeedNode.sh` script with the IP address of the new seed node as a parameter.
4. Restart the Avaya Aura® Device Services service on the new seed node.

```
svc aads restart
```

- Restart the Avaya Aura® Device Services service on the other cluster nodes.

```
svc aads restart
```

Next steps

- Disable the virtual IP on the old seed node.
- Configure the new node to be the virtual IP Master node. The initial node of the cluster is usually designated as the virtual IP master node.

Configuring the virtual IP address for Avaya Aura® Device Services clusters

About this task

In cluster environments, Avaya Aura® Device Services uses a virtual IP address to interact with clients. You must configure a virtual IP for the cluster seed node before installing other cluster nodes. Then configure a virtual IP for a non-seed node that will be used as a backup node for the seed node.

You only need to configure the virtual IP if you use the on-board Nginx load balancer in the cluster. If you are using an external load balancer, you must disable the virtual IP and set the front-end FQDN to the FQDN of the external load balancer.

* Note:

If you use a virtual IP address, you must use it or the front-end FQDN to access Avaya Aura® Device Services the following resources over port 443:

- `https://<AADS_IP>:443/acs/resources/<RESOURCE_NAME>`
- `https://<AADS_IP>/acs/resources/<RESOURCE_NAME>`

When a virtual IP is enabled, Avaya Aura® Device Services blocks access to these resources over port 443 for node IP addresses and node FQDNs.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the `app configure` command.
3. In the Avaya Aura Device Services Configuration Utility dialog box, click **Front-end host, System manager and Certificate Configuration** and click **Select**.
4. Click **Front-end FQDN** and then click **Select**.
5. Type the FQDN of the virtual IP and then click **OK**.
6. Click **Local frontend host** and then click **Select**.
7. Type the FQDN of the node to which you have logged in and then click **OK**.
8. Click **Apply**.
9. Click **Clustering Configuration** and then click **Select**.
10. Click **Virtual IP Configuration** and then click **Select**.

11. Click **Enable Virtual IP**.

Avaya Aura® Device Services enables the virtual IP address that forms the interface for client requests in the clustered environment. Avaya Aura® Device Services displays **Enable or disable Virtual IP handling on this node**.

12. Click **Yes** to enable the virtual IP address.

13. Click **Virtual IP Address** and then click **Select**.

14. Type the IP address that forms the front end to the clients and then click **OK**.

15. Click **Virtual IP Interface** and then click **Select**.

16. Type the Ethernet interface over which the virtual IP must be configured.

For example, in **Virtual IP Interface**, type `eth0`.

17. Click **Virtual IP master node** and then click **Select**.

18. Do one of the following:

- For the initial or seed node, click **Yes**.
- For the backup in the cluster, click **No**.

19. Click **Virtual IP router ID** and then click **Select**.

20. Type a value between 1 and 255 and then click **OK**.

The Virtual IP router ID in the master and backup Avaya Aura® Device Services instances must match. The default value for this field is 61. When an Avaya Multimedia Messaging cluster and an Avaya Aura® Device Services cluster are configured on the same subnet, the Virtual IP router ID differentiates between the clusters. The Virtual IP router ID must be unique for each cluster.

21. Click **Virtual IP authentication password** and click **Select**.

22. Type the password for the virtual IP address and click **OK**.

23. Click **Apply** to continue.

Avaya Aura® Device Services displays the results of the virtual IP configuration.

24. Click **Continue**.

25. Click **Return to Main Menu**.

26. Click **Continue** to continue with the virtual IP configuration.

Avaya Aura® Device Services restarts services.

27. Run the `app configure` command for another node in the cluster and repeat the previous steps to configure a virtual IP.

This node is designated as the backup node when you set **Virtual IP Master Node** to `n`. Virtual IP configuration is required only for the master and backup nodes in the cluster, and not for subsequent nodes in the cluster.

28. On the Avaya Aura® Device Services administration portal, go to **Cluster Configuration > Cluster Nodes** to confirm whether Avaya Aura® Device Services are running.

Configuring an additional seed node

About this task

For internode communication, Cassandra uses a protocol called gossip. To improve bootstrapping the gossip process for new nodes joining the cluster, you can configure an additional seed node so that each Cassandra datacenter in your cluster has one seed node. With this approach, when you add a node to a Cassandra datacenter, this node communicates with the seed node of the datacenter instead of the main seed node.

Note:

You do not need to configure an additional seed node if you use a single Cassandra datacenter in your cluster.

If you configure an additional seed node, you must repeat this procedure on all nodes in the cluster. You must also ensure that you use the same list of additional seed nodes on all nodes in the cluster.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. To start the configuration utility, run the following command:

```
app configure
```
3. Select **Cassandra configuration** and press `Enter`.
4. Select **Additional Seed node IP** and press `Enter`.
5. Type the IP address of the non-seed node in the cluster that you want to make the additional seed node.
6. Select **Save** and press `Enter`.
7. Select **Apply** and press `Enter`.
8. Repeat the steps above on all remaining cluster nodes.

Performing a silent installation

About this task

Use this procedure to perform a silent installation of the Avaya Aura® Device Services server.

The silent installation consists of configuring most of the settings in a properties file, instead of using the installation and the configuration menu for every item.

The properties file is called `installation.properties`. It contains the same settings that you configure during the interactive installation. The settings are grouped, and the file contains comments that describe the settings.

*** Note:**

The properties file does not contain settings for the following elements:

- The Avaya Aura® Device Services cluster
- The SSH RSA configuration
- IPv6 configuration

You must configure these settings using the configuration utility after the silent installation is complete.

If you want to enable IPv6, then you must perform a standard, interactive installation. You cannot enable IPv6 using the Avaya Aura® Device Services web administration portal or configuration utility.

If errors occur after the installation, you can use the configuration utility to re-configure some of the settings.

Before you begin

- If you want to configure a third-party identity provider during installation, obtain the identity provider configuration file in XML format from the provider and upload it to the seed node using a file transfer program, such as SFTP or SCP.
- If you plan to use third-party identity certificates, obtain and upload on Avaya Aura® Device Services the required certificates. For more information about the required certificates, see [Third-party CA-signed certificates](#) on page 42.

Procedure

1. From the Avaya Aura® Device Services binary file, extract the template file.

```
./aads-<version>.bin --tar xf -- ./installation.properties
```

2. Edit the `installation.properties` file and configure the settings as described in the chapter [Initial configuration with the Avaya Aura Device Services configuration utility](#) on page 228.

You can leave some of the settings blank and then configure them manually after the installation is complete.

3. Select whether you want to install Avaya Aura® Device Services in an Avaya Aura® environment as follows:

- To install Avaya Aura® Device Services in an Avaya Aura® environment, set `INCLUDE_AURA` to `y`.

In an Avaya Aura® environment, Avaya Aura® Device Services requires Avaya Aura® components, such as System Manager to operate.

- To install Avaya Aura® Device Services in an environment without Avaya Aura®, set `INCLUDE_AURA` to `n`.

In an environment without Avaya Aura®, Avaya Aura® Device Services does not require Avaya Aura® components to operate, but the features related to these components are not available.

4. If you install Avaya Aura® Device Services in an Avaya Aura® environment, configure the following Avaya Aura®-related parameters:
 - `SYSTEM_MGR_IP`: The System Manager IP address.
 - `SYSTEM_MGR_HTTPS_PORT`: The HTTPS port for contacting System Manager. The default value is 443.
 - `SYSTEM_MGR_PW`: The System Manager enrollment password.
 - `KEYSTORE_PW`: A keystore password for Avaya Aura® Device Services certificates. The minimum length is 6 characters.
 - `SESSION_MANAGER_IP`: The Session Manager Management IP address.
 - `ASSET_HOST_IP`: The Session Manager Asset IP address.
5. For cluster deployments, in `DC_NAME`, configure a Cassandra datacenter name for the node as follows:
 - To add the node to a new datacenter, provide a name of your choice for that datacenter.
 - To add the node to an existing datacenter, provide the name of one of existing datacenters on Avaya Aura® Device Services.
 - To add the node to the default “dc1” datacenter, leave the field blank.

Avaya Aura® Device Services logically groups nodes with the same Cassandra datacenter name and configures specific Cassandra replication policies for the members of the datacenter.
6. If you deploy Avaya Aura® Device Services in an environment without Avaya Aura® or if you want to use third-party identity certificates in an Avaya Aura® environment, configure the following parameters:
 - `USE_SMGR`: Set this parameter to `n`.
 - If you use identity certificates in PEM format, configure the following parameters:
 - `REST_CERT_FILE`: The full path to the third-party identity certificate for the REST interface.
 - `REST_KEY_FILE`: The full path to the key file for the REST interface certificate.
 - `OAM_CERT_FILE`: The full path to the third-party identity certificate for the OAMP interface.
 - `OAM_KEY_FILE`: The full path to the key file for the OAMP interface certificate.
 - `NODE_CERT_FILE`: The full path to the third-party identity certificate for the Avaya Aura® Device Services node.
 - `NODE_KEY_FILE`: The full path to the key file for the node interface certificate.

- CA_CERT_FILE: The third-party CA certificate chain that contains all intermediate CA certificates followed by the root CA certificate.
- If you use identity certificates in PKCS12 format, configure the following parameters:
 - REST_PKCS12_FILE: The full path to the third-party identity certificate for the REST interface.
 - REST_PKCS12_PWD: The password for the REST interface certificate.
 - OAM_PKCS12_FILE: The full path to the third-party identity certificate for the OAMP interface.
 - OAM_PKCS12_PWD: The password for the OAMP interface certificate.
 - NODE_PKCS12_FILE: The full path to the third-party identity certificate for the Avaya Aura® Device Services node.
 - NODE_PKCS12_PWD: The password for the node interface certificate.
 - CA_PKCS12_FILE: The third-party CA certificate chain that contains all intermediate CA certificates followed by the root CA certificate.
 - CA_PKCS12_PWD: The password for the third-party CA certificate chain.

 Note:

You can use the same third-party identity certificate for REST, OAM, and NODE interfaces.

7. **(Optional)** To enable OAuth, set INCLUDE_OAUTH to `y` and configure the following parameters:

- KEYCLOAK_ADMIN: A user name of your choice for the initial Keycloak administrative account.
- KEYCLOAK_ADMIN_PASSWD: A password of your choice for the Keycloak administrative account.
- IMPORT_IDENTITY_PROVIDER: If you want to configure a third-party identity provider during installation, set this parameter to `y`. Otherwise set to `n`.

If IMPORT_IDENTITY_PROVIDER is set to `y`, you must configure the following parameters:

- FILE4_IDP_XML: The absolute path to the third-party identity provider configuration file in XML format.
- LASTNAME_ATTR: The Last Name attribute to map the account on Keycloak using the identity provider SAML. For example: `sn`.
- FIRSTNAME_ATTR: The First Name attribute to map the account on Keycloak using the identity provider SAML. For example: `givenName`.
- ROLE_ATTR: The Membership attribute. For example: `memberOf`.

- **ROLE_USER_VALUE**: The User Role value from the Membership attribute. It must be a full LDAP Distinguished Name (DN). For example:
`cn=users,dc=avaya,dc=com.`
- **ROLE_ADMIN_VALUE**: The Admin Role value from the Membership attribute. It must be a full LDAP DN. For example: `cn=admins,dc=avaya,dc=com.`
- **OAUTH_CLUSTER_ENABLED**: OAuth database replication. If you are installing a cluster, set this parameter to `y`. Otherwise, set it to `n`.
- **USE_LDAP_FOR_AUTH**: If you want to use LDAP for authentication, set this parameter to `y`.

When **INCLUDE_OAUTH** is set to `y`, **USE_LDAP_FOR_AUTH** is set to `n` by default. You can also enable LDAP for authentication after installation using the Avaya Aura® Device Services web administration portal.

8. **(Optional)** To enable the Utility Server, set **INCLUDE_UTILITY_SERVER** to `y`.
9. **(Optional)** To install onboard Open LDAP, set **INCLUDE_OPENLDAP** to `y` and configure the following parameters:
 - **DIRECTORY_MANAGER**: The name of the Open LDAP administrator.
 - **OPENLDAP_DOMAIN**: The domain name of your company.

Avaya Aura® Device Services uses the two right-most dot-separated parts of the domain name. For example, if you enter `division.company.com`, Avaya Aura® Device Services converts this entry to “`cn=<Administrator password>,dc=company,dc=com`”.
 - **OPENLDAP_ADMIN_PASSWD**: The Open LDAP administrator password.
10. **(Optional)** If you configure a LDAP server and do not want to use it for contact search, set **LDAP_CONTACT_SEARCH** to `n`.

This also applies to onboard Open LDAP.

11. Run the Avaya Aura® Device Services binary with a parameter that represents the full path to the properties file.

For example:

```
app install /home/avaya/installation.properties
```

12. **(Optional)** To start the Avaya Aura® Device Services service, run the following command:

```
svc aads start
```

13. Manually configure the remaining items.

When possible, use the web administration portal to modify configuration settings instead of the configuration utility. For more information about using the web administration portal, see *Administering Avaya Aura® Device Services*.

Related links

[Characters supported for Avaya Aura Device Services passwords](#) on page 56

Enabling the Enhanced Access Security Gateway from the CLI

About this task

Use this procedure to enable Enhanced Access Security Gateway (EASG) functionality in Avaya Aura® Device Services. Avaya support engineers can use this functionality to access your computer and resolve product issues in real time.

Procedure

1. Open the SSH console as an administrator.
2. Run the following command to check the EASG status:

```
EASGStatus
```

By default, the EASG status is disabled.

3. Run the following command to enable EASG:

```
sudo /usr/sbin/EASGManage --enableEASG
```

4. Run the following command to verify the product certificate:

```
sudo EASGProductCert --certInfo
```

Avaya Aura® Device Services displays the product certificate details.

For example:

```
[admin@amm-ova-test ~]$ EASGStatus
EASG is disabled
[admin@amm-ova-test ~]$ sudo /usr/sbin/EASGManage --enableEASG

By enabling Avaya Services Logins you are granting Avaya access to
your system. This is required to maximize the performance and value
of your Avaya support entitlements, allowing Avaya to resolve product
issues in a timely manner.

The product must be registered using the Avaya Global Registration
Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote
connectivity. Please see the Avaya support site (https://support.avaya.com/
registration) for additional information for registering products and
establishing remote access and alarming.

Do you want to continue [yes/no]? yes

EASG Access is enabled. Performed by user ID: 'admin', on Oct 19 2016 - 12:28
[admin@amm-ova-test ~]$ EASGProductCert --certInfo
Subject:          CN=
                  , OU=EASG, O=Avaya Inc.
Serial Number:    10005
Expiration:       Aug  6 04:00:00 2031 GMT
Trust Chain:
  1. O=Avaya, OU=IT, CN=AvayaITrootCA2
  2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
  3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
  4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
  5. CN=
                  .0, OU=EASG, O=Avaya Inc.
[admin@amm-ova-test ~]$
```

If the certificate expires within 360, 180, 30, or 0 days, Avaya Aura® Device Services writes a certificate expiry notification to the `/var/log/messages` log file.

Running the post-installation script

About this task

Avaya Aura® Device Services are available only after DRS and LDAP synchronization is completed. The time required for synchronization varies based on the number of contacts administered.

Note:

When a contact is added to Associated Contact in System Manager, the contact will be synchronized to the client. Any contact that is not added to Associated Contact will not be synchronized. For information about adding a contact to Associated Contact, see *Administering Avaya Aura® System Manager*.

For information about installing patches and upgrades, see Avaya Aura® Device Services release notes.

The post-installation script determines the status of the system after a fresh Avaya Aura® Device Services installation or upgrade.

Procedure

1. Log in to the Avaya Aura® Device Services server.
2. Run the following command to navigate to the directory containing the script:

```
cdto misc
```

3. Run the following command:

```
sudo ./clitool-acs.sh postInstallSystemVerification
```

4. Run the following command:

```
sudo ./clitool-acs.sh postInstallSystemVerification -u <user_ID> -p <password> -e <email_address>
```

Here, <user_ID> is the Avaya Aura® Device Services user ID, <password> is the password, and <email_address> is the user's email address.

This command checks whether REST API services such as web deployment, resource discovery, contact service, search directory, and auto-configuration are available. In addition, it checks whether Avaya Aura® Device Services PPM connectivity is established.

Checking for DRS synchronization

About this task

The DRS process synchronizes data between System Manager and Avaya Aura® Device Services. The synchronization time varies depending on the network and number of users in the system. Services might fail if DRS is not in sync. Therefore, ensure that DRS is synchronized after installation.

This procedure is not required if you deploy Avaya Aura® Device Services in an environment without Avaya Aura®.

Procedure

1. In System Manager, go to **Services > Replication**.
2. Select the replication group.
3. Search for the Avaya Aura® Device Services nodes and check whether they are listed as Synchronized.

The following is an example of a synchronized Avaya Aura® Device Services system.

Replica Nodes			
View Details Repair Remove Remove From Queue Show All Replica Groups			
1 Item 			
☐	Replica Node Host Name	Product	Synchronization Status
☐	aads164.apac.avaya.com	AADS	Synchronized
Select : All, None			
Last Synchronization Time			
			December 27, 2019 2:28:10 PM +05:30

Creating an AIDE baseline database

About this task

Advanced Intrusion Detection Environment (AIDE) is a tool for monitoring file system changes. AIDE creates a baseline database of operational system and Avaya Aura® Device Services files and then verifies the integrity of the files by comparing the database to the actual state of the system files. On Avaya Aura® Device Services, you can manage AIDE using the `fsit.sh` system layer script.

Use this procedure to create a baseline database. The database creation process can take up to 50 minutes depending on the system data.

After the database is created, you can start running AIDE scans periodically. For more information, see AIDE tool management procedures in *Administering Avaya Aura® Device Services*.

Before you begin

Install Avaya Aura® Device Services.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the `fsit.sh` script location:

```
cd /opt/Avaya/bin
```

3. Run the following command to create an AIDE database in the background:

```
sudo ./fsit.sh -updateDB &
```

Creating the database as a background process enables you to perform other tasks at the same time.

Result

AIDE creates the baseline database and records the results in the `/var/log/aide/aide_update_status.log` file. You can view the status using the `sudo /opt/Avaya/bin/fsit.sh -status` command.

Changing the default password for automatic backups

About this task

Change the default password that Avaya Aura® Device Services uses for automatic backups.

Important:

If STIG hardening is enabled, you must configure a password of 15 characters or more.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal at `https://<AADS FQDN or IP>:8445/admin/`.

For more information about the login procedure, see “Logging in to the Avaya Aura® Device Services web administration portal” in *Administering Avaya Aura® Device Services*.
2. Go to **Backup Settings > Automatic Backup Configuration**.
3. Select the **Change Password** check box.
4. In **Backup File Password**, type a new password.

The password must comply with the password complexity rules. To view the rules, point the cursor to the **Backup File Password** field.
5. In **Re-Enter Password**, type the password again.
6. Click **Save**.

Related links

[Characters supported for Avaya Aura Device Services passwords](#) on page 56
[passwdrules command](#) on page 69

Uninstalling Avaya Aura® Device Services

About this task

When you uninstall the Avaya Aura® Device Services application, the virtual machine is restored to the point before deploying Avaya Aura® Device Services. The Avaya Aura® Device Services OVA is still deployed on the virtual machine.

In cluster deployments, if you need to uninstall several non-seed nodes and the seed node, decommission the additional nodes first, and the seed nodes last.

Procedure

1. Log in to Avaya Aura® Device Services CLI.
2. Run the `app uninstall` command.
3. Type `uninstall` and then press `Enter`.

Next steps

In cluster deployments, if you are using onboard Open LDAP, you must re-enable Open LDAP replication. For more information, see [Re-enabling Open LDAP replication after removing a node from a cluster](#) on page 256.

Related links

[app commands do not work after a failed installation](#) on page 336

Uninstalling the system layer

About this task

Use this procedure to uninstall the software-only system layer from RHEL.

This procedure does not apply to OVA-based deployments.

Before you begin

Uninstall the Avaya Aura® Device Services application.

Procedure

1. Log in to the RHEL as the root user using an SSH connection.
2. Go to the `/root/aads-swonly-AADS_RELEASE/ucapp-swonly-system-<SYSTEM_LAYER_VERSION>` directory.

For example: `cd /root/aads-swonly-8.1.3.0.0/ucapp-swonly-system-1.0.0.0.4`

3. Run the following command:
`./swOnlyUpdate.sh --uninstall`

Chapter 8: Initial configuration with the Avaya Aura® Device Services configuration utility

The following table summarizes the server configuration tasks that you must perform during or after the installation of the Avaya Aura® Device Services server for each of the deployment models presented.

Table 3: Summary of server configuration tasks

Task	OVA deployment on a virtual machine	
	Single server	Cluster
Configure Front-end host, System Manager and certificate configuration Certificates can be: • Managed by System Manager • Local certificates • Intermediate CA certificates Perform the task that corresponds to the certificate type that you use.	If not configured during the initial installation phase.	If not configured during the initial installation phase. Repeat for every node in the cluster.
LDAP configuration Cassandra database username and password	Yes	Yes — once, on the seed node
Clustering configuration	No	Yes Perform tasks as indicated in the Cluster installation section.
Open LDAP replication	No	Yes Perform the task if you are using onboard Open LDAP.

Task	OVA deployment on a virtual machine	
	Single server	Cluster
OAuth configuration: • Keycloak configuration • OAuth database replication	Yes Configure Keycloak if you enabled OAuth during the initial installation phase. OAuth database replication is not required.	Yes If you enabled OAuth during the initial installation phase, configure Keycloak on the seed node and enable OAuth database replication on every node in the cluster.

Configuring Avaya Aura® Device Services using the configuration utility

Before you begin

Finish installing Avaya Aura® Device Services. Otherwise, the `app configure` command will not work.

Procedure

1. **(Optional)** Run the Avaya Aura® Device Services configuration utility using the `app configure` command.

```
app configure
```

Important:

Perform this step only if you run the configuration utility at a later time after the installation.

During the installation, the configuration menu is displayed after you accept the EULA.

The script checks the current configuration of Avaya Aura® Device Services and opens the configuration menu.

2. Provide the required configuration settings.
3. Select **Continue** and press **Enter**.

Next steps

The following settings are mandatory for an Avaya Aura® Device Services installation:

- Front-end host, System Manager and certificate configuration, if not configured during the initial installation phase.
- LDAP authentication parameters.
- Cassandra username and password.
- Cluster configuration, mandatory if you are deploying an Avaya Aura® Device Services cluster.

- Utility Server virtual IP and FQDN, if you enabled the Utility Server during the initial installation phase.
- Leave **CORS Configuration** and **Serviceability Agent Configuration** unchanged.
- Onboard Open LDAP replication, which is mandatory if you enabled Open LDAP in a cluster deployment.

 Important:

Configure Open LDAP replication after configuring all cluster nodes.

- OAuth configuration, including Keycloak configuration and OAuth database replication. These steps are mandatory if you enabled OAuth.

In a cluster environment, configure OAuth settings only after configuring all cluster nodes.

To configure advanced settings, such as certificate warning period, security banner, or re-run the firewall configuration script, select the **Advanced Configuration** menu option.

 Important:

After you configure the mandatory settings, you must restart the Avaya Aura® Device Services service:

```
svc aads restart
```

If there are other settings that you must configure after restarting the Avaya Aura® Device Services server, you can run the configuration utility as described in *Step 1* and gain access to the required configuration settings.

Front-end host, System Manager, and certificate configuration

Use the following table as an aid for configuring the front-end host, System Manager, and certificate related settings.

In an Avaya Aura® environment, if you do not select the **Front-end host, System Manager and Certificate Configuration** option during the installation, then the self-signed certificates are automatically generated. Self-signed certificates are also generated when:

- The **System Manager FQDN** option is not set.
- The **Use System Manager for certificates** option is set to `n`.
- Certificates were not provided for one of the interfaces: REST, OAMP, or NODE.

 Note:

In an environment without Avaya Aura®, Avaya Aura® Device Services uses identity certificates signed by a third-party CA. You must configure the certificate settings when installing the Avaya Aura® Device Services application.

You can modify certificate configuration settings from the administration portal anytime. This is useful if you do not complete the certificate configuration as part of the initial setup process or if you generate certificates at a later time. For information about managing certificates through the administration portal, see *Administering Avaya Aura® Device Services*.

 Warning:

Changing the System Manager Server FQDN after the installation will invalidate existing users data in the system, if the FQDN points to a System Manager server that contains a different set of users. You must change the FQDN only when switching to another replicated instance of the current System Manager. For any other situation, you must reinstall the Avaya Aura® Device Services system.

In an environment without Avaya Aura®, this menu has the **Front-end host and Certificate Configuration** name and does not contain settings related to System Manager.

Table 4: Front-end host, System Manager and Certificate Configuration settings

Item name	Description	Equivalent properties file parameter
Front-end FQDN	The front-end FQDN of the Avaya Aura® Device Services server. For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If an external load balancer is used, set this value to the FQDN of the load balancer. The front-end FQDN is the address that end-user clients use to access the services provided by Avaya Aura® Device Services. The default value depends on the configuration present in the <code>/etc/hosts</code> file of the Avaya Aura® Device Services server.  Important: Use split-horizon DNS and the same FQDN for Session Border Controller and Avaya Aura® Device Services if you want to prevent users from re-configuring their clients when working outside of the enterprise network. The same front-end FQDN resolves to one IP for Session Border Controller external to the enterprise, and a different IP inside the enterprise directly to Avaya Aura® Device Services.	REST_FRONTEND_HOST
System Manager FQDN	The FQDN of the System Manager that signs the Avaya Aura® Device Services certificates. This field is not available in an environment without Avaya Aura®.	SYSTEM_MGR_IP

Item name	Description	Equivalent properties file parameter
System Manager web admin username	The System Manager web administration portal user name. This field is optional. This field is not available in an environment without Avaya Aura®.	SMGR_USER_NAME
System Manager web admin password	The System Manager web administration portal password. This field is optional. This field is not available in an environment without Avaya Aura®.	SMGR_USER_PASSWORD
System Manager web version	The version number of Avaya Aura® System Manager. This field is not available in an environment without Avaya Aura®.	SYSTEM_MGR_VERSION
System Manager HTTPS Port	The HTTPS port used for the Alarm Agent for the current Avaya Aura® Device Services server. The default value for this setting is 443. This field is not available in an environment without Avaya Aura®.	SYSTEM_MGR_HTTPS_PORT
System Manager Enrollment Password	The System Manager enrollment password. This field is not available in an environment without Avaya Aura®.	SYSTEM_MGR_PW
Override port for reverse proxy	Specifies if you use an external reverse proxy server. Enable this setting only if clients will not be connecting directly to the Avaya Aura® Device Services server, but rather using a proxy server as part of a remote access solution that is configured to receive connections on a port other than default port 443. Select y (yes) to configure the port for the reverse proxy server or n (no) to keep the default configuration that remains disabled. If you select y (yes), the menu displays a new setting for the reverse proxy port: Front-end port for reverse proxy .	OVERRIDE_FRONTEND_PORT For the Front-end port for reverse proxy setting, the equivalent parameter is REST_FRONTEND_PORT.

Item name	Description	Equivalent properties file parameter
	 Note: If this parameter is changed after the installation, all of the nodes in a cluster must be restarted using the <code>svc aads restart</code> command to apply the change. For more information about overriding ports in a clustered environment, see Overriding port configuration in a cluster on page 319.	
Current Listen Port	Specifies the port Avaya Aura® Device Services uses to receive connections. This is the read-only field.	—
Use System Manager for certificates	Specifies if the certificates are retrieved from System Manager or from imported files. Select <code>y</code> (yes) to retrieve certificates from System Manager or <code>n</code> (no) to retrieve certificates from imported files. If you select <code>n</code> (no), the menu displays new settings for configuring the certificate files. To configure the certificate settings, you must provide the complete file path name to the: • REST interface key file • REST interface certificate file • OAM interface key file • OAM interface certificate file • node key file • node certificate file • signing authority certificate file In an environment without Avaya Aura®, the Use System Manager for certificates field is not available, and the menu displays the settings for configuring the certificate files by default.	USE_SMGR If the USE_SMGR option is set to <code>n</code> (no), you must configure the following parameters for importing the certificate files: • REST_KEY_FILE • REST_CERT_FILE • OAM_KEY_FILE • OAM_CERT_FILE • NODE_KEY_FILE • NODE_CERT_FILE • CA_CERT_FILE
Local frontend host	The local FQDN of the node. This FQDN is not used for a client to access services, but is used to access the server within the enterprise, and is bound to the same Ethernet port as the front-end FQDN.	LOCAL_FRONTEND_HOST

Item name	Description	Equivalent properties file parameter
	The Avaya Aura® Device Services configuration utility uses this value to generate certificates for the node. ! Important: In a clustered configuration, the local front-end host is different from one node to the other and is also different from the front-end FQDN. In a non-clustered environment, the local front-end host is usually different from the front-end FQDN to create a clustered configuration from a non-clustered configuration.	
Keystore password	The keystore password for the MSS and Tomcat Avaya Aura® Device Services certificates. The minimum length for this password is 6 characters. The characters supported for the keystore password are: • a to z • A to Z • 0 to 9 • Special characters: !, @, #, %, \$, ^, *, ?, and _	KEYSTORE_PW

LDAP configuration

If you do not complete LDAP configuration during the initial Avaya Aura® Device Services setup, then you can complete it later using the Avaya Aura® Device Services administration portal. Some administration options, such as configuring multiple LDAP directories, are only available on the administration portal. For more information, see the “LDAP server management” section in *Administering Avaya Aura® Device Services*.

Warning:

Changing the LDAP configuration parameters, other than Bind DN and Bind Credential, when they are configured, might invalidate the existing user data. For example, changing how user roles are found can remove one or more roles from the existing user, which will block the user from accessing the Avaya Aura® Device Services system. In addition, do not change the server URL unless you need to switch the configuration to another replicated instance of the current LDAP directory. In all the other cases, you must reinstall the Avaya Aura® Device Services system.

The following image shows the LDAP Configuration screen in the Avaya Aura® Device Services configuration utility:

[illegible]

Item name	Description	Equivalent properties file parameter
Use LDAP for Authentication	Specifies whether this LDAP server is used for authentication. This check box is only available when OAuth is enabled.	—
Use for Contact Search	Specifies whether this LDAP server is used for the contact search. The following options are available: • y (yes): To enable the contact search functionality. • n (no): To disable the contact search functionality. If you use the Onboard Open LDAP server, this option is enabled by default.	LDAP_CONTACT_SEARCH
Use DNS	Specifies whether Avaya Aura® Device Services uses DNS SRV records to discover the LDAP server. • If the check box is selected, Avaya Aura® Device Services uses the domain name specified in the URL for LDAP server field to discover all LDAP	

Item name	Description	Equivalent properties file parameter
	servers associated with this domain name in DNS SRV records. If the check box is not selected, Avaya Aura® Device Services uses the IP address or FQDN specified in the URL for LDAP server field to discover the LDAP server.	
Load LDAP properties from file	The Load LDAP properties from file menu contains an item called Path to properties file. You can create a Java properties file that contains the LDAP properties instead of entering the LDAP configuration settings manually. The Path to properties file option is for configuring the absolute path to this file. The LDAP properties file must contain the <i>equivalent properties file parameters</i> specified in this table. The default value for this setting is <code><install_dir>/config/ldap.properties</code>, where <code><install_dir></code> is the Avaya Aura® Device Services installation directory.	pathToLdapPropertiesFile
Import Secure LDAP trusted certificate	The Import Secure LDAP trusted certificate menu contains the following items: Certificate file: The path and filename for the LDAP trusted certificate. The certificate file must be in the .PEM format. If you want to configure secure LDAP for onboard Open LDAP, use the nginx certificate located at <code>/etc/openldap/certs/nginx.crt</code>. You cannot import a certificate if: - The certificate contains an unsupported critical extension. - The certificate expired. - The start date of the certificate is in the future.	LDAP_TRUSTSTORE_CERTFILE LDAP_TRUSTSTORE_PASSWORD

Item name	Description	Equivalent properties file parameter
	 Important: Only configure these settings if you need a Secure LDAP connection.	
Directory Type	The LDAP directory type of the enterprise. The supported directory types are the following: • Azure Active Directory • IBM Domino Server 7.0 and 8.5.3  Note: The Domino server must be patched to support TLS, so Avaya Aura® Device Services can connect to the Domino server through secure LDAP (LDAPS). For a list of supported patch fixes, see https://www-10.lotus.com/ldd/dominowiki.nsf/dx/IBM_Domino_TLS_1.0. • Microsoft Active Directory 2012, 2016, and 2019 • Microsoft Active Directory Lightweight Directory Services (LDS) 2012 • Novell e-Directory 8.8 • OpenLDAP 2.4.44 and 2.4.46 • Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1.7.0) For detailed information about supported product releases, see the Avaya Compatibility Matrix.	ldapType
URL for LDAP server	The URL for gaining access to the LDAP server. This is the mandatory setting. The URL for LDAP server parameter is unavailable if you selected the Use DNS check box. The URL must have one of the following formats: <pre>ldap://<LDAP server FQDN or IP address>:<port> ldaps://<LDAP server FQDN>:<port></pre>	ldapUrl

Item name	Description	Equivalent properties file parameter
	For example: <pre>ldap://myserver.mycompany.com:3268 ldaps:// myserver.mycompany.com:3269</pre> The protocol can be LDAP or LDAPS, depending on the LDAP server type. If you are using LDAPS, you cannot use IP addresses in the URL. ! Important: If FIPS is enabled, use the LDAPS protocol to access the LDAP server. If the LDAP server uses IPv6, use the server FQDN in the URL. If you are configuring LDAPS for onboard Open LDAP, use the local domain name as follows: <pre>ldaps://localhost.localdomain:3269</pre> For Microsoft Active Directory, use the catalog LDAP ports. The default global catalog LDAP port values are 3268 for LDAP and 3269 for LDAPS. The default domain LDAP ports values are 389 for LDAP and 636 for LDAPS. * Note: If an FQDN is used to specify the LDAP server, the enterprise might map the FQDN to multiple, replicated LDAP servers using the DNS round-robin mechanism as an attempt for load-balance and for redundancy purpose. Sporadic authentication failures can occur if one of the LDAP servers is offline and the DNS round-robin mechanism resolves the FQDN to the IP of the LDAP server that is offline. If this outcome cannot be tolerated, a more reliable load-balancing mechanism, such as a dedicated load-balancer in front of the LDAP servers, will be needed.	

Item name	Description	Equivalent properties file parameter
	For Active Directory, use the Global Catalog service port instead of the default LDAP/LDAPS ports. ! Important: If you are using the global catalog ports, you must configure attribute replication to the global catalog. For more information, see LDAP attributes replication to the global catalog on page 280.	
Bind DN	The Distinguished Name (DN) of the user that has read and search permissions for the LDAP server users and roles. This is the mandatory setting. The format of the Bind DN depends on the configuration of the LDAP server. * Note: Even though the parameter name is Bind DN, the format of its value is not limited to the DN format. The format can be any format that the LDAP server can support for LDAP bind. For example: for Active Directory, you can use <code>domain\user</code>, <code>user@domain</code>, as well as the actual DN of the user object.	bindDN
Bind Credential	Specifies the password of the administrative user. The maximum password length depends on the LDAP server type that you use in your deployment. The supported characters are: • Lowercase letters: a to z • Uppercase letters: A to Z • Numerics: 0 to 9 • Special characters are supported.	! Important: If you configure the LDAP settings using the properties file, you must enter the Bind Credential manually by running the configureAADS.sh script.
UID Attribute ID	The User ID attribute name, as determined by the LDAP server configuration. This is the mandatory setting.	uidAttrID

Item name	Description	Equivalent properties file parameter
	This parameter is used for searching users in the LDAP server. For example: <code>sAMAccountName</code>  Note: When the UID attribute is set to <code>mail</code> on onboard Open LDAP, use Apache Directory Studio to set the email value for the Open LDAP administrative user. This enables the administrative user to log in to the Avaya Aura® Device Services web administration portal using their email.	
Base Context DN	The DN of the context used for LDAP authentication. For example: <code>ou=aadsusers,dc=example,dc=com</code>	<code>baseCtxDN</code>
Administrator Role	The list of LDAP roles that match the Avaya Aura® Device Services Administrator role. For example: If the role is configured as <code>AADSAdmin</code>, <code>AADSxyz</code>, any user whose list of roles contains <code>AADSAdmin</code> or <code>AADSxyz</code> is mapped to the Avaya Aura® Device Services Administrator role.  Note: The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Device Services application roles to succeed.  Important: To avoid situations when potential loss of credentials could impact the administration tasks, Avaya recommends creating more than one user account with administrator privileges.	<code>adminRole</code>

Item name	Description	Equivalent properties file parameter
Auditor Role	The list of LDAP roles that match the Avaya Aura® Device Services Auditor role. For example: If the Auditor role is configured as <code>AADSAuditor</code>, <code>AADSxyz</code>, any user whose list of roles contains the <code>AADSAuditor</code> or <code>AADSxyz</code> role is mapped to the Avaya Aura® Device Services AUDITOR role.  Note: The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Device Services application roles to succeed.	auditorRole
User Role	The list of LDAP roles that match the Avaya Aura® Device Services User role. For example: If the User role is configured as <code>AADSUser</code>, <code>AADSxyz</code>, any user whose list of roles contains the <code>AADSUser</code> or <code>AADSxyz</code> role is mapped to the Avaya Aura® Device Services USER role.  Note: The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Device Services application roles to succeed.	usersRole
Services Administrator Role	The list of LDAP roles that match the Services Administrator role. For example: If the User role is configured as <code>AADSUser</code>, <code>AADSxyz</code>, any user whose list of roles contains the <code>AADSUser</code> or <code>AADSxyz</code> role is mapped to the	serviceAdminRole

Item name	Description	Equivalent properties file parameter
	Avaya Aura® Device Services Services Administrator role.  Note: The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Device Services application roles to succeed.	
Services Maintenance and Support Role	The list of LDAP roles that match the Maintenance and Support role. For example: If the User role is configured as <code>AADSUser</code>, <code>AADSxyz</code>, any user whose list of roles contains the <code>AADSUser</code> or <code>AADSxyz</code> role is mapped to the Avaya Aura® Device Services Maintenance and Support role.  Note: The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Device Services application roles to succeed.	<code>serviceMaintenanceRole</code>
Security Administrator Role	The list of LDAP roles that match the Avaya Aura® Device Services Security Administrator role. For example: If the role is configured as <code>AADSSecurityAdmin</code>, <code>AADSxyz</code>, any user whose list of roles contains <code>AADSSecurityAdmin</code> or <code>AADSxyz</code> is mapped to the Avaya Aura® Device Services Security Administrator role.  Note: The values of the roles are case-sensitive when they are mapped to the application roles. So they	<code>securityAdminRole</code>

Item name	Description	Equivalent properties file parameter
	must match exactly to the role name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Device Services application roles to succeed.	
Advanced LDAP parameters	The menu that contains advanced LDAP parameters to configure depending on the structure of the LDAP server.	
Test User	If you select testUser and select Apply, this option is used to validate the following LDAP settings: • Verifies that the user is searchable with a given base DN and search filter. • Lists the group to which the user belongs — user, administrator, or auditor. • Validates the values for Role Attribute ID and Role Name Attribute. • Verifies the Last Updated Time attribute, role filter syntax, and active users search filter syntax. The configuration is not saved if any of these validations fail. The testUser parameter is optional. If you do not specify a value, the system skips validation and directly saves the configuration in the database.	testUser

Supported characters for LDAP attributes

For LDAP attributes, you can use the majority of special characters as is. The following are the exceptions:

- The userid attribute does *not* support the following characters:
 - Colon (:)
 - Slash (/)
 - Left brace ({)
 - Right brace (})
- The basectxdn, rolesctxdn, and role attributes do *not* support the comma (,).

If you want to use quotation marks (") or a backslash (\) in LDAP attributes, you must prepend these characters with a single backslash (\) character. For example, if you want to use the `backslash\` value for the `sAMAccountName` attribute, you need to enter it as `backslash\\`.

Item name	Description	Equivalent properties file parameter
	The roles search in LDAP is performed by using the Roles Context DN in combination with the Role Filter. For example: <code>ou=aadsusers,dc=example,dc=com</code>	
Role Name Attribute	This parameter has a different meaning, depending on the value of Role Attribute Is DN: • If Role Attribute Is DN is set to true, the value of the attribute set in Role Attribute ID is used to find the object that contains the role and this parameter stores the name of the attribute that contains the role name. • If Role Attribute Is DN is set to false, this parameter is ignored. For example: <code>cn</code>	<code>roleNameAttrID</code>
Role Attribute is DN (true/false)	The setting to determine if the role attribute is stored in the DN or in another object. If you set this parameter to <code>true</code>, the role is stored in the attribute defined by the Role Name Attribute parameter. If you set this parameter to <code>false</code>, the role attribute of the user contains the name of the role.	<code>roleAttrIsDN</code>
Role Recursion	The setting to enable or disable role recursion. For example: the user jsmith can be in the Sales group, which can be in the AADS users group. In this case, Role Recursion must be set to true to permit role recursion.	<code>roleRecursion</code>
Allow Empty Passwords (true/false)	The setting to determine if empty passwords are allowed in the LDAP directory.	<code>allowEmptyPasswords</code>

Item name	Description	Equivalent properties file parameter
Search Scope (0 - 2)	The setting to determine the scope of the role search. The role search starts from the <i>Role Context DN</i> and uses the <i>Role Filter</i>. The search scope determines the depth of the search as follows: • Level 0, also named OBJECT_SCOPE, indicates that the search is performed only on the named role context. • Level 1, also named ONELEVEL_SCOPE, indicates that the search is performed directly under the named role context. • Level 2, also named SUBTREE_SCOPE, indicates that the search is performed at the named role context and in the sub-tree rooted at the named role context.	searchScope
Language used in Directory	The language used in the LDAP directory. The following languages are supported: • Russian • German • Spanish • English • Korean • French • Portuguese • Simplified Chinese • Japanese • Italian	language
Active users search filter	The search filter string used to identify active users. This field must only contain a filter to determine whether a user is	activeUsersFilter

Item name	Description	Equivalent properties file parameter
	active in LDAP. Do not use any other filters in this field. If this setting is not configured, the Avaya Aura® Device Services User Management component handles all the users as active users. For example: (! (userAccountControl:1.2.840.113556.1.4.803:=2)).	
Users search additional filter	The search filter that provides extended search options in addition to Active users search filter. If you want to search for users using additional criteria other than whether a user is active, provide that criteria in this field. This field has no default value. For example, if you want to search for users in the object class “user” and the object category “Person”, use the following filter: (&(objectClass=user)(objectCategory=Person)).	—
Last updated time attribute	The attribute indicating the last time an LDAP object was modified, in the ASN.1 Generalized Time Notation. The Avaya Aura® Device Services User Management component uses this attribute to identify updated users when synchronizing the user data with the LDAP server. Avaya recommends that you use the following values: • For Active Directory: whenChanged. • For OpenLDAP: modifyTimestamp. If this parameter is not configured, the User	lastUpdatedTimeAttr

Item name	Description	Equivalent properties file parameter
	Management component compares the data of every user to the data that exists in the LDAP server.  Note: Configuring this parameter improves the efficiency of the user synchronization process and reduces the traffic between the Avaya Aura® Device Services server and the LDAP server during user synchronization.	
Load parameter defaults	The script to load the default values for the parameters.	—

Related links

[Supported characters for LDAP attributes](#) on page 243

Cassandra DB user and password

When you configure Avaya Aura® Device Services, you must change the default Cassandra database credentials to ensure a secure connection to the Cassandra database server.

Item name	Description	Equivalent properties file parameter
New Cassandra Database User Name	The new user name for gaining access to the Cassandra database server.	NEW_CASSANDRA_USER
New Cassandra Database Password	The new password for gaining access to the Cassandra database server.	NEW_CASSANDRA_PW

Related links

[Characters supported for Avaya Aura Device Services passwords](#) on page 56

Changing the Cassandra user name and password**About this task**

This procedure describes how to change the Cassandra database user name and password after installing of an Avaya Aura® Device Services cluster.

Procedure

1. On the seed node, do the following:

a. Run the Avaya Aura® Device Services configuration utility.

```
app configure
```

b. Select **Cassandra DB User and Password**.

c. Select **New Cassandra Database User Name** and enter the new user name.

d. Select **New Cassandra Database User Password** and enter the new password.

e. Select **Apply**.

2. On every non-seed node, do the following:

a. Run the `cassandraSetPassword` command and specify the new database user name and password as parameters.

```
sudo /opt/Avaya/DeviceServices/<verion>/CAS/<version>/cassandra/  
cassandraSetPassword.sh <new user name> <new password>
```

b. Restart Avaya Aura® Device Services.

```
svc aads restart
```

Clustering configuration

The Cluster Configuration menu contains the tools and settings that you must use for configuring the Avaya Aura® Device Services nodes in a clustered environment.

The Cluster Configuration menu contains the following submenus:

- Cluster Utilities
- Virtual IP Configuration Settings

The following table describes the Cluster Utilities settings in the configuration utility:

Item name	Description	Equivalent properties file parameter
Configure SSH RSA Public/Private Keys	This utility configures the SSH RSA keys for SSH login configuration. You must run this utility from the seed node after installing the other nodes in the cluster.	This setting does not have an equivalent parameter in the <code>installation.properties</code> file. You must configure the cluster using the configuration tool after the silent installation is complete.

Item name	Description	Equivalent properties file parameter
Propagate REST and OAMP certificates to cluster	The Propagate REST and OAMP certificates to cluster utility provides REST and OAMP certificates for each node in a cluster. You must run this utility after re-configuring certificates for any node in the cluster. You can run this utility from any node in the cluster. You do not need to use this utility if you use certificates signed by the System Manager CA.	This setting does not have an equivalent parameter in the <code>installation.properties</code> file.

The virtual IP address is necessary in a clustered environment, so that all the nodes in the cluster can be accessed using the same IP address.

The following table describes the Virtual IP Configuration settings in the configuration utility.

Item name	Description	Equivalent properties file parameter
Enable virtual IP	The setting to enable the usage of a virtual IP address. If you select <code>n</code> (no), the configuration script does not configure the virtual IP address. If you select <code>y</code> (yes), new configuration settings for the virtual IP address are displayed in the configuration menu: - Virtual IP address: The virtual IPv4 address to be shared by the current node. - Virtual IPv6 address: The virtual IPv6 address to be shared by the current node. This option is only available if IPv6 is enabled. - Virtual IP interface: The network interface to use for the virtual IP. The form of this interface must be <code>eth0</code>. - Virtual IP master node: The setting to determine if the current node is the master node in the cluster. - Virtual IP router ID: An integer with a value from 1 to 255. The value must be the same for both virtual IP master and backup. The default value is 61. This value must be unique across Virtual Router Redundancy Protocol	<code>KA_ENABLED</code> If you set this parameter to <code>y</code> (yes), you must also configure the following parameters: <code>KA_VIRTUAL_IP</code> <code>KA_INTERFACE</code> <code>KA_MASTER_YN</code> <code>KA_AUTHENTICATION_PASSWORD</code> <code>KA_ROUTER_ID</code>

Item name	Description	Equivalent properties file parameter
	(VRRP) installations and it is limited to cluster deployments. Virtual IP authentication password: The password to use for virtual IP authentication.	

Utility Server configuration

Configure the following settings in the Utility Server Configuration menu if your deployment uses the Utility Server.

Item name	Description	Equivalent properties file parameter
Utility Server VIP	A virtual IPv4 address of your choice for the Utility Server. You must configure this setting on every Avaya Aura® Device Services node in the cluster. You cannot use the Avaya Aura® Device Services cluster virtual IP address as the Utility Server virtual IP address.	UTILITY_SERVER_VIP
Utility Server Ipv6 VIP	A virtual IPv6 address of your choice for the Utility Server. You must configure this setting on every Avaya Aura® Device Services node in the cluster. You cannot use the Avaya Aura® Device Services cluster virtual IP address as the Utility Server virtual IP address. This option is only available if IPv6 is enabled on Avaya Aura® Device Services.	—
Utility Server FQDN	An FQDN of your choice for the Utility Server. You must configure this setting on every Avaya Aura® Device Services node in the cluster.	UTILITY_SERVER_FQDN

Item name	Description	Equivalent properties file parameter
System Manager Enrollment Password	The Avaya Aura® System Manager enrollment password. The System Manager enrollment password is configured in the System Manager console under Home > Services > Security > Certificates > Enrollment Password. This setting is not available in an environment without Avaya Aura®.	SYSTEM_MANAGER_PW

Advanced configuration

Item name	Description	Equivalent properties file parameter
Certificate Warning Period	The number of days before the expiry date of a certificate causes the system to raise an alarm.	CERT_WARNING_PERIOD
OS Security Utility	The menu for configuring the firewall automatically on the current node. Select Run the firewall configuration script and press Enter to run the firewall configuration script. Avaya recommends that you run this script to configure the firewall automatically and not perform a manual configuration.  Warning: The firewall configuration script replaces the current configuration of the firewall on the server where you are performing the installation, so you must open any other ports required for your server manually after you run this script.	RUN_FIREWALL_CONFIG If you set this parameter to y (yes), the firewall configuration script is run during the silent installation.

Item name	Description	Equivalent properties file parameter
Long Poll Timeout	The menu that contains the Recommended Long Poll Timeout configuration option. Use this option for setting the value to use in the Avaya-Request-Timeout HTTP header for long-poll requests.  Important: The long poll timeout value can be from 30 to 120. Lowering this value results in increased traffic on the server, but network configuration may require that you set a lower value. If you do not configure this parameter, the default database initialization setting is used.	AVAYA_REQUEST_TIMEOUT
Configure Host IP for SNMP management	The menu that contains the IP address for managing this server setting for configuring the IP address of the Network Interface to use for SNMP.	SNMP_IP_ADDR
Security Banner File	The menu for configuring security banner settings. The Security Banner File setting must contain the path to the security banner file. The security banner file is a text file that contains the security warnings displayed when a user or administrator logs in to the administration portal or using an SSH console.	SECURITY_BANNER_PATH
Change Application JAVA_HOME setting	The menu for configuring a path to a directory containing the Java Runtime Environment. The default value is <code>/etc/alternatives/jre</code>.	—

Configuring the Avaya Aura® Device Services server firewall

About this task

You can reset the firewall settings back to the defaults, or allow additional ports through the server firewall.

Important:

This procedure applies to AADS 8.x releases. If you are using AADS 10.x releases, see [Configuring additional ports in Avaya Aura® Device Services server firewall in 10.x releases](#).

Procedure

1. **(Optional)** Add the required ports to the firewall configuration file `/opt/Avaya/DeviceServices/<version>/CAS/<version>/os/security/firewall.config`.
2. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
3. Select **Advanced Configuration > OS Security Utility > Run the firewall configuration script**.

The firewall is configured automatically.

Configuring additional ports in Avaya Aura® Device Services server firewall in 10.x releases

About this task

You can allow additional ports through the server firewall in Avaya Aura® Device Services 10.x releases.

Before you begin

In OVA-based deployments, contact Avaya support personnel to configure the root password. Avaya Aura® Device Services does not have root access by default in OVA-based deployments.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as follows:
 - In OVA-based deployments, log in as an administrator and then switch to the root user using the following command:

```
su root
```
 - In software-only deployments, log in as the root user.
2. Open the `/etc/nftables/aads-rules.nft` file in a text editor.

For example, to open the file in vi, run the following command:

```
vi /etc/nftables/aads-rules.nft
```

3. In the inet filter section, in the chain INPUT_direct text block, add the following entry for each port:

```
tcp dport <port_no> counter packets 0 bytes 0 accept
```

In this command, <port_no> is the allowed port.

For example, to open port 3268, add the following entry:

```
tcp dport 3268 counter packets 0 bytes 0 accept
```

4. Save the /etc/nftables/aads-rules.nft file.
5. Run the following command:

```
systemctl restart nftables
```

Enabling Open LDAP replication

About this task

Enable Open LDAP database replication in a cluster deployment. This procedure is not applicable for standalone installations.

Before you begin

- Ensure that an FQDN is assigned to each node in the cluster.
- Ensure that each node is accessible from all other nodes in the cluster.
- From a node CLI, run the `app listnodes` command and ensure that all cluster nodes have the “live” status.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **Enable Open LDAP Replication**.
3. Select **Enable Open LDAP Replication** again.
4. Select **Yes**.
5. Select **Open LDAP Password**. and enter the Open LDAP administrator password.
6. Select **OK**.

The data replication process might take several minutes to complete.

7. After the data replication is complete, select **Continue**.
8. To ensure that data replication is enabled, view the `/var/log/Avaya/openldap/openldap.log` file.

The following is an example of a `/var/log/Avaya/openldap/openldap.log` file entry indicating that data replication is enabled:

```
Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 fd=17 ACCEPT from IP=1.2.3.5:63930 (IP=1.2.3.4:3268)
Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 BIND
dn="cn=administrator,dc=company,dc=com" method=12
Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 BIND
dn="cn=administrator,dc=company,dc=com" mech=SIMPLE ssf=0
Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 RESULT tag=97 err=0 text=
```

If `/var/log/Avaya/openldap/openldap.log` contains error messages, such as `ldap_sasl_bind_s failed rc -1`, then some nodes are not accessible. In this case, you must make these nodes accessible from other nodes and then repeat the data replication procedure.

9. Repeat steps 1 to 8 on all remaining nodes on the cluster.

Related links

[Open LDAP replication fails](#) on page 340

Re-enabling Open LDAP replication after removing a node from a cluster

About this task

Removing a node from a cluster affects Open LDAP replication. After a node is removed from the cluster, you must re-enable Open LDAP replication manually.

Important:

When you perform this procedure, *all* LDAP user data will be erased. After the procedure is complete, you must re-upload the user data using the Avaya Aura® Device Services web administration portal.

Before you begin

Ensure that you have a copy of the user data currently stored in Open LDAP.

Procedure

1. Log in to an Avaya Aura® Device Services node as an administrator.
2. Run the following commands:

```
cdto openldap
sudo ./recover_openldap.sh
```

Important:

This script erases *all* user data stored in Open LDAP.

3. Repeat steps 1 to 2 on all remaining nodes in the cluster.
4. On each cluster node, perform the Open LDAP replication procedure.

Next steps

Re-upload user data using the Avaya Aura® Device Services web administration portal. For more information, see *Administering Avaya Aura® Device Services*.

OAuth configuration

For single sign-on authentication purposes, Avaya Aura® Device Services uses Keycloak. When OAuth is enabled on Avaya Aura® Device Services, you must also configure the Keycloak service. The following sections describe the mandatory Keycloak configuration. Additional management tasks that you can perform using the Keycloak web administration portal are described in *Administering Avaya Aura® Device Services*.

For more information about Keycloak, see [Keycloak online documentation](#).

Authorization realm configuration on UC servers and Avaya Workplace Client

When SSO/OAuth is enabled on Avaya Aura® Device Services, you must provision the following parameters for all Avaya Workplace Client softphones configured to use the Avaya Authorization service (OAuth2):

- **AVAYA_AUTHORIZATION_REALM:** Set the value to the Keycloak realm configured on Avaya Aura® Device Services, which is “SolutionRealm” by default.

Important:

If other UC servers, such as Avaya Aura® Web Gateway or Presence and Multimedia Messaging, are configured to use SSO/OAuth, ensure that they use the same Keycloak realm.

- **ACSSSO:** Set the value to 3, so that Avaya Workplace Client uses Avaya Authorization for Avaya Aura® Device Services.
- **ESMSSO:** Set the value to 3, so that Avaya Workplace Client uses Avaya Authorization for Presence and Multimedia Messaging.
- **AUTOCONFIG_USESSO:** Set the value to 3 so that Avaya Workplace Client uses Avaya Authorization for automatic configuration.
- **SETTINGS_FILE_URL:** Set the value to the Avaya Aura® Device Services dynamic configuration URL with the additional `preferredAuth=bearer` query parameter. For example: `https://<AADS_FRONT_END_FQDN>:<AADS_PORT>/acs/resources/configurations?preferredAuth=bearer`

Note:

In a cluster environment, if you use front-end port 443, you must use the Avaya Aura® Device Services front-end FQDN or virtual IP address when configuring this parameter.

Configuring Keycloak settings

About this task

Use this procedure to set up a Keycloak administrator account. Avaya Aura® Device Services configures Keycloak automatically. After the configuration process is complete, you can view and update the default configuration using the Keycloak web administration portal.

If you use the Shibboleth identity provider, you can also upload an identity provider entity descriptor file in XML format.

! Important:

You can upload an entity descriptor file using the Avaya Aura® Device Services configuration utility for the Shibboleth identity provider only. For other identity providers, you must upload an entity descriptor file using the Keycloak web administration portal. If you do not upload an entity descriptor file to Keycloak, OAuth will not work.

Before you begin

- Install Avaya Aura® Device Services.
- Ensure that you gather all information and configured an SSO application on the third-party identity provider. For information about the prerequisites, see [Prerequisites for SSO configuration](#) on page 52.
- If you configure integration with Office 365, you must configure an SSO application on Microsoft Azure. For more information, see the “Avaya Aura® Device Services OAuth2 management” chapter in *Administering Avaya Aura® Device Services*.
- If you configure the Shibboleth identity provider, obtain the IDPSSODescriptor configuration file in the XML format. You can download the file from `https://<shibboleth site address>:<port>/idp/shibboleth`.

Procedure

1. On the seed node, run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **Keycloak Configuration**.
3. In the **Keycloak Admin** and **Keycloak Admin user's password** fields, provide a user name and password of your choice for the initial Keycloak administrative account.

These credentials are used to log in to the Keycloak web administration portal. Your password must comply with the password complexity rules.
4. **(Optional)** If you are configuring the Shibboleth identity provider, do the following to upload the identity provider configuration file:
 - a. Upload the identity provider configuration file to the seed node using a file transfer program, such as SFTP or SCP.
 - b. In the **IDP XML** field, enter `y`.
 - c. In the **Custom IDP xml file** field, select the IDPSSODescriptor configuration file that you uploaded to Avaya Aura® Device Services.

If you do not provide the Shibboleth configuration file using CLI, you must upload this file later using the Keycloak administration portal.

5. If you want to configure the mapping between attributes used by the identity provider and attributes used by Keycloak, do the following:
 - a. In **Last Name attribute**, provide the Last Name attribute that is used by the identity provider. For example, `sn`.
 - b. In **First Name attribute**, provide the First Name attribute that is used by the identity provider. For example, `givenName`.
 - c. In **Membership attribute**, provide the Membership attribute containing role information that is used by the identity provider. For example, `memberOf`.
 - d. In **User Role value**, provide the User Role value, which comes from the Membership attribute. It must be a full LDAP distinguished name (DN). For example, `cn=users,dc=avaya,dc=com`.
 - e. In **Administrator Role value**, provide the Administrator Role value, which comes from the Membership attribute. It must be a full LDAP DN. For example, `cn=admins,dc=avaya,dc=com`.

You can configure the mapping later using the Keycloak administration portal.

6. Select **Apply**.
7. After the configuration process is complete, select **Continue**.

Next steps

In a cluster environment, configure OAuth database replication as described in [Enabling OAuth database replication in a cluster environment](#) on page 264.

If required, view and configure additional Keycloak settings using the Keycloak web administration portal. For more information, see “Logging in to the Keycloak web administration portal” in *Administering Avaya Aura® Device Services*.

Starting and stopping the Keycloak service

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run one of the following commands:
 - `svc keycloak start` to start the Keycloak service.
 - `svc keycloak stop` to stop the Keycloak service.
 - `svc keycloak restart` to restart the Keycloak service.

Logging in to the Keycloak web administration portal

About this task

Use this procedure to log in to the Keycloak web administration portal. The portal becomes available after you configure Keycloak settings during the initial Avaya Aura® Device Services configuration.

Procedure

1. Open a web browser.
2. Enter the following URL:

```
https://<AADS IP or FQDN>:8445/auth/admin
```

In this URL, <AADS IP or FQDN> is either the Avaya Aura® Device Services front-end FQDN or IP address.

3. Enter the user name and the password that you created when configuring the Keycloak settings.

Obtaining the client secret

About this task

The client secret is required to establish communication between Keycloak and Avaya Aura® Device Services. The client secret is generated automatically during Keycloak configuration.

Procedure

1. On the Keycloak web administration portal, navigate to your realm and then click **Clients**.
By default, the realm is SolutionRealm.
2. From the Clients table, select **aads**.
3. Click the **Credentials** tab.
4. Copy the text in **Secret** field.

Next steps

Create a client mapping as described in [Creating client mapping](#) on page 260.

Creating client mapping

About this task

In the authorization flow, Avaya Aura® Device Services interacts with Keycloak on behalf of a client, such as Avaya Workplace Client, Avaya Meeting Scheduler Outlook Add-in, Avaya Meetings Server Unified Portal, Avaya Agent for Desktop, or Avaya Calling for Microsoft Teams. To enable Avaya Aura® Device Services to communicate with Keycloak, you must provision Avaya Aura® Device Services with the Keycloak client secret and the URL to discover Keycloak resources. You must create a client mapping for each client that your deployment supports.

! Important:

If you have multiple client mappings in your deployment, the value of Access token email address attribute must be the same for each client mapping.

To configure the device flow for phones, such as J1XX, see “Creating client mapping for the device flow” in *Administering Avaya Aura® Device Services*.

Before you begin

Obtain the client secret as described in [Obtaining the client secret](#) on page 260.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Client ID Mapping**.
3. Click **Add**.
4. In the Create new client mapping window, complete the fields as follows:

- a. In **Client ID**:

- For Avaya Workplace Client, type `Equinox`.
- For Avaya Meeting Scheduler Outlook Add-in, type `MeetingScheduler`.
- For Avaya Meetings Server Unified Portal, type `UnifiedPortal`.
- For Avaya Agent for Desktop, type `aafd`.
- For Avaya Calling for Microsoft Teams, type `CallAssist`.

This value is case sensitive.

- b. In **OIDC Discovery URL**, type `https://<AADS_FQDN>:<PORT>/auth/realms/<REALM>/ .well-known/openid-configuration`

In this string:

- `<AADS_FQDN>` is the Avaya Aura® Device Services front-end FQDN.
- `<PORT>` is the Avaya Aura® Device Services front-end FQDN service port.
- `<REALM>` is the Keycloak realm, which is `SolutionRealm` by default.

- c. In **Client Secret**, enter the string copied from the Keycloak web administration interface.
 - d. Leave the **Client Name** and **Proxy Address** fields blank.
 - e. Clear the **Enable device Auth** check box.
 - f. For other fields, keep the default values.
5. Click **OK**.

Avaya Aura® Device Services displays the new client mapping on the page.

6. If you already have another client mapping in your deployment, do the following:
 - a. On the Client ID Mapping page, click **Edit** for the client mapping that you have just created.
 - b. Ensure that the value of **Access token email address attribute** matches the value that you recorded.
 - c. If the values are different, update **Access token email address attribute** with the value that you recorded.
 - d. Click **OK**.
7. **(Optional)** Create a client mapping for any additional clients that your deployment supports.

Modifying the attribute mapping between the third-party identity provider and Keycloak

About this task

To authenticate a user, a third-party identity provider sends to Keycloak an authentication response that contains various user attributes, such as first name, last name, phone number, and email address. Keycloak then maps this user information to the attributes of the access token that is generated and sent back to clients.

The Avaya Aura® Device Services configuration utility provides a default attribute mapping. The identity provider you are using, however, might use attribute names that differ from the attribute names provided in the default mapping. In this case, you must update the default mapping. Use this procedure to modify the default attribute mapping.

Each identity provider uses its own attribute mapping. For information about the mappers for your identity provider, see the “Attribute mapping parameters” section for your identity provider in *Administering Avaya Aura® Device Services*.

Before you begin

Configure a third-party identity provider on Keycloak.

Procedure

1. On the Keycloak web administration portal, navigate to your realm and then click **Identity Providers**.
2. Select the identity provider.
3. Click **Mappers**.
4. From the table, select an appropriate attribute.

Avaya Aura® Device Services displays the attribute mapping for the selected attribute.

- The **Friendly Name** field contains the attribute name that the identity provider passes to Keycloak.

If the identity provider does not provide a value for the **Friendly Name** field, use the **Attribute Name** field instead.

- The **User Attribute Name** field contains the attribute name that Keycloak passes to clients in access tokens.

For a person's given name, last name, and email address, use the following **User Attribute Name** values:

- Given name: `givenName`.
- Last name: `lastName`.
- Email address: `email`

These values are case sensitive.

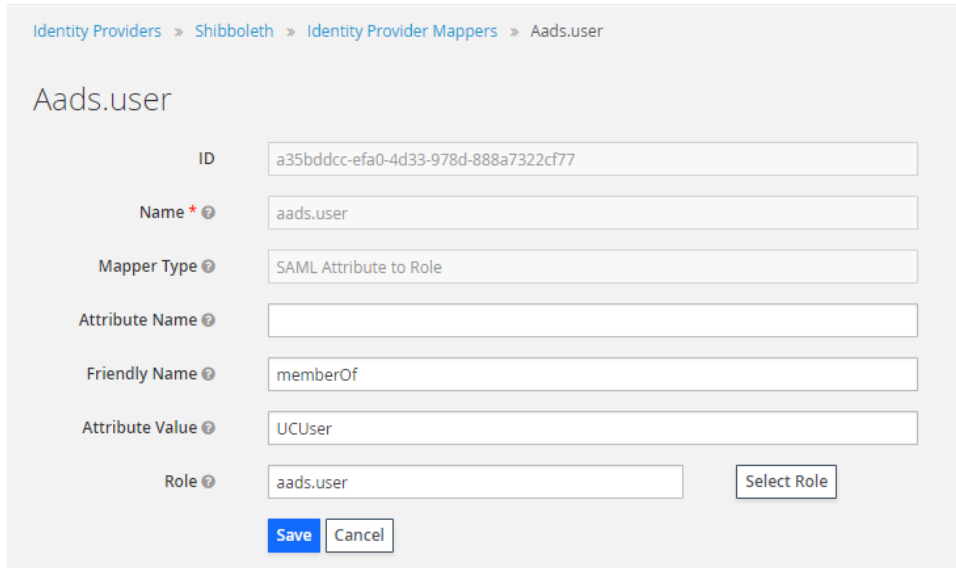
The following image shows the `givenName` attribute.

The screenshot shows the configuration page for an Identity Provider Mapper named 'GivenName'. The breadcrumb trail at the top is 'Identity Providers > saml > Identity Provider Mappers > GivenName'. The form contains the following fields:

- ID**: 1cb82654-acb7-449b-8e35-2d82d5b07cd7
- Name**: givenName
- Mapper Type**: Attribute Importer
- Attribute Name**: (empty field)
- Friendly Name**: givenName
- User Attribute Name**: firstName

At the bottom of the form are 'Save' and 'Cancel' buttons.

5. Modify the **Friendly Name** value according to the attribute name that is used by the identity provider you are using.
6. If **Mapper type** is set to **SAML Attribute to Role**, do the following to map a role:
 - a. Click **Select Role**.
 - b. In the Role Selector window, in the **Client Roles** drop-down list, select **aads**.
 - c. Select the required role and then click **Select client role**.



7. Click **Save**.
8. Repeat the above steps for any other attributes you need to map.

Enabling OAuth database replication in a cluster environment

About this task

In a cluster environment, you must have a copy of the OAuth database on each cluster node. Use this procedure to enable OAuth database replication. If your deployment includes OAuth, you must perform this procedure in the following cases:

- After installing Avaya Aura® Device Services
- After performing a migration
- After rolling back Avaya Aura® Device Services
- Before restoring Avaya Aura® Device Services

Note:

You do not need to perform this procedure after upgrading Avaya Aura® Device Services. After upgrading, Avaya Aura® Device Services enables OAuth database replication automatically.

Before you begin

- Enable OAuth during Avaya Aura® Device Services installation.
- Install all cluster nodes.
- Configure Keycloak settings. For more information, see [Configuring Keycloak settings](#) on page 258.

Procedure

Perform steps 1 to 6 on the seed node first and then on all non-seed nodes.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the configuration utility using the `app configure` command.
3. Select **Enable OAuth Cluster**.
4. Select **Enable OAuth Cluster** again and then enter `y`.
5. Select **Exit**.
6. Select **Yes** and then select **Apply**.
7. On the seed node, run the `svc aads restart` command to restart Avaya Aura® Device Services and then wait until the restart process is completed.
8. On all non-seed nodes, run the `svc aads restart` command to restart Avaya Aura® Device Services.

Checklist to Configure Keycloak using a secure LDAP

Configuration Checklist

The following checklist outlines the configuration tasks that you must perform:

No.	Task	Notes	✓
1	Obtain LDAP server certificate	Obtaining LDAP Server Certificate on page 265	
2	Import the certificate to a keycloak Truststore	Importing the Certificate into the Keycloak Truststore on page 266	
3	Configure LDAPS in Keycloak	Configuring LDAPS in Keycloak on page 267	

Obtaining LDAP Server Certificate

About this task

Use this procedure to obtain LDAP server certificate and configure Keycloak using a secure LDAP.

Before you begin

Use `openssl` to export the LDAP server's certificate, by running the following commands:

```
echo | openssl s_client -connect <LDAP FQDN>:636 -showcerts
```

```
echo | openssl s_client -connect ldap.example.com:636 -showcerts
```

Example:

The following command displays the LDAP servers certificate:

```
echo | openssl s_client -connect  
asewinsrvdc.aseteam.ch:636 -showcerts
```

- When the certificate is displayed, copy the certificate along with the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines to a file. For example: ldap-server.crt.

Next steps

Importing the Certificate into the Keycloak Truststore

Importing the Certificate into the Keycloak Truststore

About this task

If your Keycloak installation uses a Java keystore, you must first convert the certificate to the JKS format and then import it into a Java Keystore (JKS) file. To import the certificate into a Keycloak truststore, you must use the truststore used by the Java runtime Keycloak.

Procedure

1. Run the following command to import the certificate into a Java Keystore (JKS) file:

```
keytool -import -alias ldap-server -file ldap-server.crt -keystore  
truststore.jks -storepass changeit
```

Example:

```
keytool -import -alias ldap-server -file /home/admin/ldap-  
server.crt -keystore truststore.jks -storepass changeit
```

2. Run the following command to import the certificate into the Keycloak Truststore:

```
keytool -importcert -file ldap-server.crt -alias ldap-server  
-keystore /path/to/keycloak/conf/cacerts -storepass changeit
```

Example:

```
keytool -importcert -file /home/admin/ldap-server.crt -alias  
ldap-server -keystore /etc/alternatives/jre_17/lib/security/cacerts  
-storepass changeit
```

Following is the location for Keycloak certificate: /etc/alternatives/jre_17/lib/security/

Next steps

Configuring LDAPS in Keycloak

Configuring LDAPS in Keycloak

Procedure

1. Login to Keycloak Admin Console.
2. In the left navigation pane, go to the realm where you want to configure LDAP.
3. If you are using the default realm, select **Master** or the custom realm you want to configure.
4. Click **User Federation** under **Realm Settings**.
5. Click **LDAP** to configure LDAP.
6. Click **Add provider** and select **ldap**.

 Note:

For LDAPS, ensure the connection URL starts with *ldaps://*.

7. Enter the required LDAP connection details.
8. In the **Use Truststore SPI** field, select **ldapsOnly** if you have configured a custom truststore.
9. Disable the **Enable StartTLS** option.
10. Click **Test authentication** to connect Keycloak to your LDAP server.
11. Save the configuration.

Example

Following are the configuration examples:

```
plaintext
Copy code
Vendor: Other
Connection URL: ldaps://ldap.example.com:636
Bind Type: simple
Bind DN: cn=admin,dc=example,dc=com
Bind Credential: <your password>
```

Chapter 9: Configuring Session Manager for cluster environments

If you use an Avaya Aura® Device Services cluster in Avaya Aura® environment, you can pair Avaya Aura® Device Services nodes with Session Manager instances to provide a redundant storage for SIP data.

The procedures in this chapter are not applicable for Avaya Aura® Device Services deployments in an environment without Avaya Aura®.

Related links

[Managing an incoming call](#) on page 268

[Adding an Avaya Aura Device Services instance to System Manager](#) on page 270

[Pairing Session Manager with an Avaya Aura Device Services node](#) on page 272

[Enabling PPM rate limiting for Session Manager](#) on page 273

[Effect of Session Manager on Avaya Aura Device Services](#) on page 274

[Session Manager operations that impact Avaya Aura Device Services](#) on page 274

Managing an incoming call

About this task

When you receive an incoming call, a number of options becomes available. You can accept a call, forward it to another user, reply to a call with a message, ignore a call or send it to Voicemail.

Procedure



1. To accept the call, click **Answer** ().
2. To accept the call, click **Answer** ().
3. To accept the call, click **Answer** ().
4. To accept the call, click **Answer** ().



5. To accept the call, click **Answer** ().
6. To accept the call, click **Answer** ().
7. To accept the call, click **Answer** ().
8. To accept the call, click **Answer** ().
9. To accept the call, click **Answer** ().

10. To forward the call to a different destination, click **Forward** (📞), enter the phone number, and click **Forward**.
11. To reply to a call with a message, click **Reply** (📞), select one of the default replies or create a custom message, and click **Send**.
The caller receives your reply as a voice message.
12. To ignore a call, click **Ignore** (📞).
13. To send a call to Voicemail, click **To Voicemail** (📞).
14. To listen to the voicemail while being left and decide whether to pick up the call, click the arrow under the **To Voicemail** button and click **Screen Voicemail**.

Related links

[Configuring Session Manager for cluster environments](#) on page 268

Adding an Avaya Aura® Device Services instance to System Manager

Repeat these steps for all Avaya Aura® Device Services nodes in the cluster.

Before you begin

Deploy the Avaya Aura® Device Services OVA.

* Note:

Avaya Aura® Device Services is available only with Avaya Workplace Client 3.0.

Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
The system displays the New Elements page.
4. In the **General** section, from the **Type** field, select **Avaya Aura Device Services**.
The system refreshes the page and displays the New Avaya Aura Device Services page.
5. On the **General** tab, perform the following:
 - a. In the **Name** field, type the name of the Avaya Aura® Device Services server.
 - b. In the **Description** field, type the description of the Avaya Aura® Device Services server.
 - c. In the **Node** field, type the IP of the Avaya Aura® Device Services server.

6. On the **Attributes** tab, perform the following:

- a. In the **Login** field, type the administrator login name to access the Avaya Aura® Device Services server.
- b. In the **Password** field, type the administrator password to access the Avaya Aura® Device Services server.
- c. In the **Confirm Password** field, retype the administrator password to access the Avaya Aura® Device Services server.
- d. In the **Version** field, type the version of the Avaya Aura® Device Services server.
- e. In the **Location** field, type the location name of the Avaya Aura® Device Services server.

7. Go back to the General tab.

 Important:

Access profiles of type GRCommunication and TrustManagement are available by default.

8. Select the TrustManagement access profile, and click **Edit**.
9. In the Access Profile Details section, in the **Name** field, type a name for the access profile.
10. In the **Access Profile Type** field, click **Trust Management**.
11. In the **Protocol** field, click **https**.
12. In the **Host** field, type the FQDN or IP address of the Avaya Aura® Device Services server.

 Important:

If you provide an IP address, you must use the IPv4 address of the Avaya Aura® Device Services server even if IPv6 is enabled on Avaya Aura® Device Services.

13. Leave the **Container Type** field blank.
14. Leave the other fields unchanged at default values.
15. Click **Save**.

To enable SSO login, you must add an access profile of type EMURL. Steps 16a to 16k show how to add an access profile of type EMURL.

16. To add an EMURL access profile, on the **General** tab, in the Access Profile section, perform the following:
 - a. Click **New**.
 - b. In the Application System Supported Protocol section, in the **Protocol** field, click **URI**.
 - c. In the Access Profile Details section, in the **Name** field, type a name for the access profile.
 - d. In the **Access Profile Type** field, click **EMURL**.

- e. In the **Protocol** field, click **https**.
- f. In the **Host** field, type the Avaya Aura® Device Services server FQDN.
- g. In the **Port** field, type 8445.
- h. In the **Path** field, type /admin.
- i. In the **Order** field, retain the default value.
- j. In the **Description** field, type a description of the access profile.
- k. Click **Save**.

17. Click **Commit**.

Next steps

Go to the System Manager home page and click **Device Services** in the Elements section.

The Device Services page displays the Avaya Aura® Device Services element you added. After Avaya Aura® Device Services installation is complete, you can click the name of the Avaya Aura® Device Services element to open the Avaya Aura® Device Services home page.

Related links

[Configuring Session Manager for cluster environments](#) on page 268

[Deploying the Avaya Aura Device Services OVA using the Host Client connected directly to the ESXi host](#) on page 83

[Considerations for large cluster deployments](#) on page 40

[Avaya Aura Device Services cluster installation](#) on page 198

Pairing Session Manager with an Avaya Aura® Device Services node

About this task

You can pair a Session Manager instance to an Avaya Aura® Device Services (AADS) node when adding or after adding a Session Manager instance.

Do this procedure for all AADS nodes in the cluster.

For example, for a Session Manager cluster with two nodes, SM01 and SM02, to deploy an AADS cluster with two nodes, AADS01 and AADS02, you must pair:

- SM01 with AADS01
- SM02 with AADS02

Before you begin

Assign the Session Manager instance to a data center.

Procedure

1. On the System Manager web console, click **Elements > Session Manager > Session Manager Administration**.
2. On the Session Manager Administration page, click the **Session Manager** tab.
3. In the **Session Manager Instances** section, select a Session Manager instance and click **Edit**.

System Manager displays the Edit Session Manager page.

4. From the **Avaya Aura Device Services Server Pairing** list, select an AADS server.

When an AADS server is already paired with a Session Manager instance, System Manager does not display that server in the **Avaya Aura Device Services Server Pairing** list.

5. Click **Commit**.

Related links

[Configuring Session Manager for cluster environments](#) on page 268

[Assigning Session Manager to a data center on System Manager 8.x](#) on page 48

[Assigning Session Manager to a data center on System Manager 10.x or later](#) on page 49

Enabling PPM rate limiting for Session Manager

Before you begin

Ensure that the Session Manager instance is associated with Avaya Aura® Device Services.

Procedure

1. Log in to the System Manager web console.
2. Click **Inventory > Manage Elements**.
3. Select the Session Manager instance that is associated with Avaya Aura® Device Services, and click **Edit**.
4. In the Personal Profile Manager (PPM) - Connection Settings section, select the **Limited PPM Client Connection** check box.
5. In the **Maximum Connections per PPM Client** field, type 3.
6. Select the **PPM Packet Rate Limiting** check box.
7. In the **PPM Packet Rate Limiting Threshold** field, type 200.
8. Click **Commit**.

Related links

[Configuring Session Manager for cluster environments](#) on page 268

Effect of Session Manager on Avaya Aura® Device Services

Session Manager can have one of the following Service States:

- **Accept New Service:** In this state, Session Manager accepts incoming calls.

When Session Manager is in Accept New Service state, Avaya Aura® Device Services contact services works uninterrupted.

- **Deny New Service:** In this state, Session Manager denies any new call attempts and service requests.

When Session Manager is in Deny New Service state, Avaya Aura® Device Services Contact Services do not work. Avaya Aura® Device Services is also placed in Deny New Service state and sends an HTTP/503 error for all add, update, and delete requests for contact service.

- **Maintenance Mode:** In this state, Session Manager is placed in a dormant state for maintenance.

When Session Manager is in Maintenance state, Avaya Aura® Device Services Contact Services do not work. Avaya Aura® Device Services is also placed in Maintenance state and sends an HTTP/503 error for all add, update, and delete requests for contact service.

Related links

[Configuring Session Manager for cluster environments](#) on page 268

Session Manager operations that impact Avaya Aura® Device Services

Various operations performed on Session Manager can impact associated Avaya Aura® Device Services servers. These operations include, but are not limited to the following operations:

- Adding or deleting Session Manager.
- Modifying the IP address of Session Manager.
- Setting the Session Manager in the JITC compliant mode.

For more information, see *Administering Avaya Aura® Session Manager*.

Related links

[Configuring Session Manager for cluster environments](#) on page 268

Chapter 10: Deploying AADS on ASP R6.0.x (KVM on RHEL 8.10)

Deploying Avaya Aura® Device Services on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit

Before you begin

- Install ASP R6.0.x (KVM on RHEL 8.10).

For more information, see *Installing the Avaya Solutions Platform 130 Series* at <https://support.avaya.com/css/public/documents/101091802>.

- Download the Avaya Aura® Device Services KVM image `aads-kvm-10.2.0.0.70.ova` from PLDS to your computer.
- Login to the ASP R6.0.x CLI with `custadm` credentials.
- Ensure that the staging folder exists: `/var/lib/libvirt/staging`.

```
sudo ls -ld /var/lib/libvirt/images
```

Ensure to remove the older images from the staging folder.

Ensure sufficient space is available in the staging folder to copy the KVM image.

If the staging folder does not exist, create it using the following commands:

```
sudo mkdir /var/lib/libvirt/staging
```

```
sudo chown custadm:wheel /var/lib/libvirt/staging
```

- Copy the Avaya Aura® Device Services KVM image `aads-kvm-10.2.0.0.70.ova` to the ASP R6.0.x host in `/var/lib/libvirt/staging` using the `winscp` tool and `custadm` credentials.
- If not still in the CLI, login again to the ASP R6.0.x CLI with `custadm` credentials.

* Note:

All the following commands *must* be prefaced with “`sudo`”:

- Run the following command to verify the Avaya Aura® Device Services KVM image available in the staging folder: `sudo ls -lr /var/lib/libvirt/staging`
- Go to `/var/lib/libvirt/staging` folder, and run the following command to extract the ova file: `sudo tar -xvf aads-kvm-10.2.0.0.70.ova`

KVM OVA file extracts the following files:

- aads-10.2.0.0.70_OVF10.mf
- aads-10.2.0.0.70_OVF10.ova
- aads-10.2.0.0.70_OVF10.ovf
- aads-10.2.0.0.70_OVF10.cert
- disk1.qcow2
- disk2.qcow2
- disk3.qcow3
- disk4.qcow2

The extracted qcow2 images are in thin provision format. The qcow2 images MUST be converted to thick provision. Ensure you are in the `/var/lib/libvirt/staging` directory before proceeding. When running the commands to convert to thick provision, a unique identifier can be added to the new qcow2 image. Avaya recommends to use VM name as a unique identifier. Convert disk1.qcow2(thin) to AADS10.2[unique identifier]-disk1.qcow2 (thick). For example:

- `sudo qemu-img convert -O qcow2 -o preallocation=full disk1.qcow2 AADS10.2[unique identifier]-disk1.qcow2`
- `sudo qemu-img convert -O qcow2 -o preallocation=full disk2.qcow2 AADS10.2[unique identifier]-disk2.qcow2`
- `sudo qemu-img convert -O qcow2 -o preallocation=full disk3.qcow2 AADS10.2[unique identifier]-disk3.qcow2`
- `sudo qemu-img convert -O qcow2 -o preallocation=full disk4.qcow2 AADS10.2[unique identifier]-disk4.qcow2`

To verify that the conversion is successful and verify the disk size, run the following commands:

- `sudo qemu-img info disk1.qcow2`
Disk size must display as 2.4GB
- `sudo qemu-img info AADS10.2[unique identifier]-disk1.qcow2`
Disk size must display as 125GB

Copy the AADS10.2[unique identifier]-disk1.qcow2, AADS10.2[unique identifier]-disk2.qcow2, AADS10.2[unique identifier]-disk3.qcow2 and AADS10.2[unique identifier]-disk4.qcow2 qcow2 to the `/var/lib/libvirt/images` directory. Ensure you are in the `/var/lib/libvirt/staging` directory before performing these steps.

- `sudo cp /var/lib/libvirt/staging/ AADS10.2[unique identifier]-disk*.qcow2 /var/lib/libvirt/images/`
- `cd /var/lib/libvirt/images/`
- `sudo ls -lr`

From the `/var/lib/libvirt/images` directory, run the following command to change the owner and permissions to 640 on the files:

- `sudo chown qemu:qemu AADS10.2[unique identifier]-disk*`
`chmod 640 AADS10.2[unique identifier]-disk*`

Go to `/var/lib/libvirt/staging` directory and remove all the extracted images and converted images. This is important to ensure that there is sufficient space for future deployments of KVM images. Do NOT remove files from the “images” directory.

- `cd /var/lib/libvirt/staging`
- `sudo ls -lr`
- `sudo rm *AADS*`

Ensure that the network bridge is configured during the KVM deployment.

Procedure

1. Log in to the KVM Cockpit web console as **custadm** in the following format: `https://<IP address or FQDN of KVM host>:9090`.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

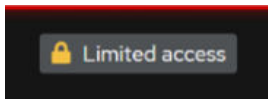


Figure 1: Limited access button

* Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **custadm**.

Figure 2: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

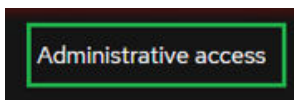


Figure 3: Administrative access button

4. Navigate to **System > Virtual Machines > Import VM**.
5. In the Import a virtual machine window, do the following:
 - a. In the **Name** field, enter a name for the Avaya Aura® Device Services virtual machine.

- b. In the **Disk Image** field, select the AADS10.2[unique identifier]-disk1.qcow2 image of the Avaya Aura® Device Services on the KVM Cockpit host under /var/lib/libvirt/images/ directory.
- c. In the **Operating System** field, select **RHEL 8.6** version.
- d. In the **Memory** field, select the required memory in MiB format.

 Note:

Based on the required footprint, enter a value in the **Memory** field.

For more information on footprints, see [Avaya Aura Device Services virtual machine resource requirements](#) on page 34

- e. Click **Import and edit**.

Virtual Machine details page appears.

Under the Disks section, verify the AADS10.2[unique identifier]-disk1.qcow2 image disk image size is correctly displayed in the Capacity field. By default, **virtio** is selected under the **Bus** field, and this needs to be modified.

6. Under the Disks section, click **Edit**.

7. In the Edit <attributes name> window, do the following:

- a. in the **Bus** field, select **scsi**.
- b. In the **Cache** field, select **directsync**.
- c. click **Save**.

In the Disks section, ensure that **scsi** appears under the **Bus** field and **directsync** appears under the **Additional Cache** field.

8. Click **Add disk** to add AADS10.2[unique identifier]-disk2.qcow2 , AADS10.2[unique identifier]-disk3.qcow2, AADS10.2[unique identifier]-disk4.qcow2 disk image, and do the following:
 - a. In the **Source** field, select **Custom path**.
 - b. In the **Custom path** field, select AADS10.2[unique identifier]-disk1.qcow2 image on the KVM host location path /var/lib/libvirt/images
 - c. In the **Device** field, select **Disk image file**.
 - d. Expand the **Show additional options** field.
 - e. In the **Cache** field, select **directsync**.
 - f. In the **Bus** field, select **SCSI** bus type.
 - g. Click **Add**.

In the Disks section, verify that the four disk images are assigned correctly.

The newly added disk must have the 125 GiB AADS10.2[unique identifier]-disk1.qcow2, 70 GiB for AADS10.2[unique identifier]-disk2.qcow2, 40 GiB for AADS10.2[unique identifier]-disk3.qcow2 and 10 GiB for

AADS10.2[unique identifier]-disk4.qcow2 assigned under the **Capacity** and field, **scsi** assigned under the **Bus** field, and **directsync** under the **Cache** field.

9. In the Overview section, in the **Firmware** field, select **UEFI** and click **Save**.
10. In the Overview section, in the **CPU** field, click **edit**.
CPU Details window opens.
11. In the CPU details window, based on the required footprint, enter a value in the **vCPU Maximum** and **vCPU Count** fields.
For more information on footprints, see [Avaya Aura Device Services virtual machine resource requirements](#) on page 34.
12. Click **Apply**.
13. In the Network interfaces section, click **Edit** and select the Network Bridge, and click **Save**.
14. On the virtual machine, click **Run** to start the Avaya Aura® Device Services virtual machine.

Next steps

On first boot of the Avaya Aura® Device Services configure the AADS virtual machine, network properties and follow the Avaya Aura® Device Services deployment guide.

Existing instructions for installation of these artifacts using the CLI and UI are applicable. Note that the “snapshot” functionality present in ASP R5.1.x and earlier is replaced with an equivalent feature, titled Virtual Machine Backup (clone).

For more information about the Virtual Machine Backup (clone), see Appendix of the Avaya Aura® Device Services deployment guide.

Chapter 11: LDAP settings configuration

Avaya Aura® Device Services uses the LDAP servers for user authentication, user authorization, and retrieving user details.

The LDAP settings configuration is performed during the Avaya Aura® Device Services installation and there are no additional actions required after the installation is complete.

Avaya Aura® Device Services will follow referrals in LDAP in case the returned host is known. It will work if the bind credentials are valid in the referred to server.

LDAP authentication domain requirements

If you use a single authentication directory, ensure that all users are in a single authentication domain. This is not required if you use multiple authentication directories.

The first LDAP domain added to Avaya Aura® Device Services is the server that handles user authentication and role assignment. All users that require authentication must be located in this LDAP domain and must be able to authenticate with it.

LDAP attributes replication to the global catalog

If you are using global catalog ports 3268 or 3269 to connect to LDAP, then LDAP queries can only return attributes marked for replication to the global catalog. For example, a user's department cannot be returned because this attribute is not replicated to the global catalog. You must manually add all required attributes in the global catalog attributes list.

Installing LDAP schema snap-in

About this task

The Active Directory schema snap-in is used to manage the Active Directory schema. For example, to modify the existing schema attributes and classes. By default, the Active Directory schema snap-in is disabled in Microsoft Management Console (MMC). Use this procedure to enable the Active Directory schema snap-in.

This procedure is applicable for Active Directory only.

Procedure

1. Log in to the machine where Active Directory is deployed as an administrator.
2. Open the command prompt.
3. Run the `regsvr32 schmmgmt.dll` command to register `schmmgmt.dll` on your system.
4. Click **Start**.
5. Click **Run**.
6. Run the `mmc /a` command.
7. In the Console window, click **File** > **Add or Remove Snap-in**
8. In the Add or Remove Snap-in window, under **Available snap-ins**, select the **Active Directory Schema** and click **Add**.
9. Click **OK** to add the schema to your console.
10. In the Console window, click **File** > **Save** to save this console.

Requirements for LDAP attribute values

LDAP attributes	Requirements
• <code>phoneNumber</code> • <code>otherTelephone</code> • <code>facsimileTelephoneNumber</code> • <code>homePhone</code> • <code>otherHomePhone</code> • <code>mobile</code> • <code>otherMobile</code> • <code>pager</code> • <code>otherPager</code> • <code>postalCode</code>	Only the following characters are supported: • Numbers: 0 to 9 • Parentheses: () • Plus sign: +

Indexing an attribute

About this task

Avaya Aura® Device Services does unified search on LDAP. Use this procedure to improve Avaya Aura® Device Services unified search performance and ensure LDAP indexing to speed up searches.

Before you begin

Install the LDAP schema snap-in.

Procedure

1. Open the command prompt on the machine where Active Directory is deployed.
2. Run the `mmc /a` command.

The system displays the Console window.

3. In the navigation pane, click **Active Directory Schema > Attributes**.

The system displays a list of attributes.

4. Select the attribute you want to index.
5. Right click the selected attribute and then click **Properties**.

The system displays properties window for the selected attribute.

6. On the **General** tab, select the **Index this attribute** and **Index this attribute for containerized searches** check boxes.

Ensure that the attributes mapped against the labels in the Avaya Aura® Device Services interface of the Enterprise Directory Mappings window are indexed on Active Directory.

7. Click **Apply** and then click **OK** to save changes for the selected attribute.

List of attributes to index

Ensure that the attributes mapped against the labels below in the Avaya Aura® Device Services interface of Enterprise Directory Mappings window are indexed on Active Directory.

- Alias
- ASCII DisplayName
- ASCII Givenname
- ASCII Surname
- BusinessPhone
- BusinessPhone-1
- City
- Department
- DisplayName

- * EmailAddress
- EmailAddress-1
- Fax
- Fax-1
- Givenname
- HomePhone
- HomePhone-1
- IMHandle
- IMHandle-1
- LyncAddress
- MobilePhone
- MobilePhone-1
- * NativeGivenname
- * NativeSurname
- Pager
- Pager-1
- Surname

Saving existing LDAP settings

About this task

Before configuring Avaya Aura® Device Services, you can use the following steps to save the current LDAP settings.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as the administrative user.
2. Run the following command:

```
cdto misc
```

3. Run the following command:

```
clitool-aes.sh ldapConfiguration >> ~/ldap_settings.txt
```

Avaya Aura® Device Services copies the existing LDAP configuration to the `ldap_settings.txt` file in your home directory.

Do *not* cut and paste to a file directly from a terminal. Pasting from a terminal might introduce some unwanted white spaces in the file.

Setting up user synchronization with LDAP after deployment

About this task

Before using Avaya Aura® Device Services, you must synchronize the user with the LDAP server.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal.
2. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.

Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

3. In the User Synchronization Update Instructions section, do the following:

- a. Click **Force LDAP Sync**.

Avaya Aura® Device Services displays the following message:

```
WARNING!Force LDAP Sync will re-synchronize all the LDAP
user data. This action will impact on-going Device Services
operations and must be performed during a maintenance window.
```

- b. Click **OK**.

Avaya Aura® Device Services displays the following message:

Starting update.

- c. Click **OK**.

- d. Ensure that Avaya Aura® Device Services displays the following message:

Last Sync Status : Successful as on : <date and time of the synchronization>.

For example: Last Sync Status : Successful as on : Tue, Sep 06, 2016 13:54:36 (UTC+5:30) .

- e. Specify a date and time to schedule the synchronization of Avaya Aura® Device Services users with the Enterprise LDAP Server users.
- f. Select the **Repeat** check box and click the day to set up a recurring event for synchronization.
- g. Click **Save**.

LDAP configuration for Microsoft Active Directory

The following sections describe how to configure the LDAP server for Microsoft Active Directory (AD).

The following sections use the example below to provide a comprehensive view of how to perform the LDAP configuration.

LDAP secure configuration

By default, Avaya Aura® Device Services uses an unsecured LDAP connection. For secured connectivity, you must import an LDAP certificate to the Tomcat trust store.

! Important:

The FQDN that is configured as the address of the LDAP source must be defined in the LDAP certificate in one of the following places:

- The Common Name in the Subject field.
- Subject Alternative Name.

For more information about enabling a secure connection, see <https://support.microsoft.com/en-us/help/931351/how-to-add-a-subject-alternative-name-to-a-secure-ldap-certificate>.

For more information about installing LDAP certificates on Avaya Aura® Device Services, see [LDAP certificates](#) on page 359.

LDAP configuration example

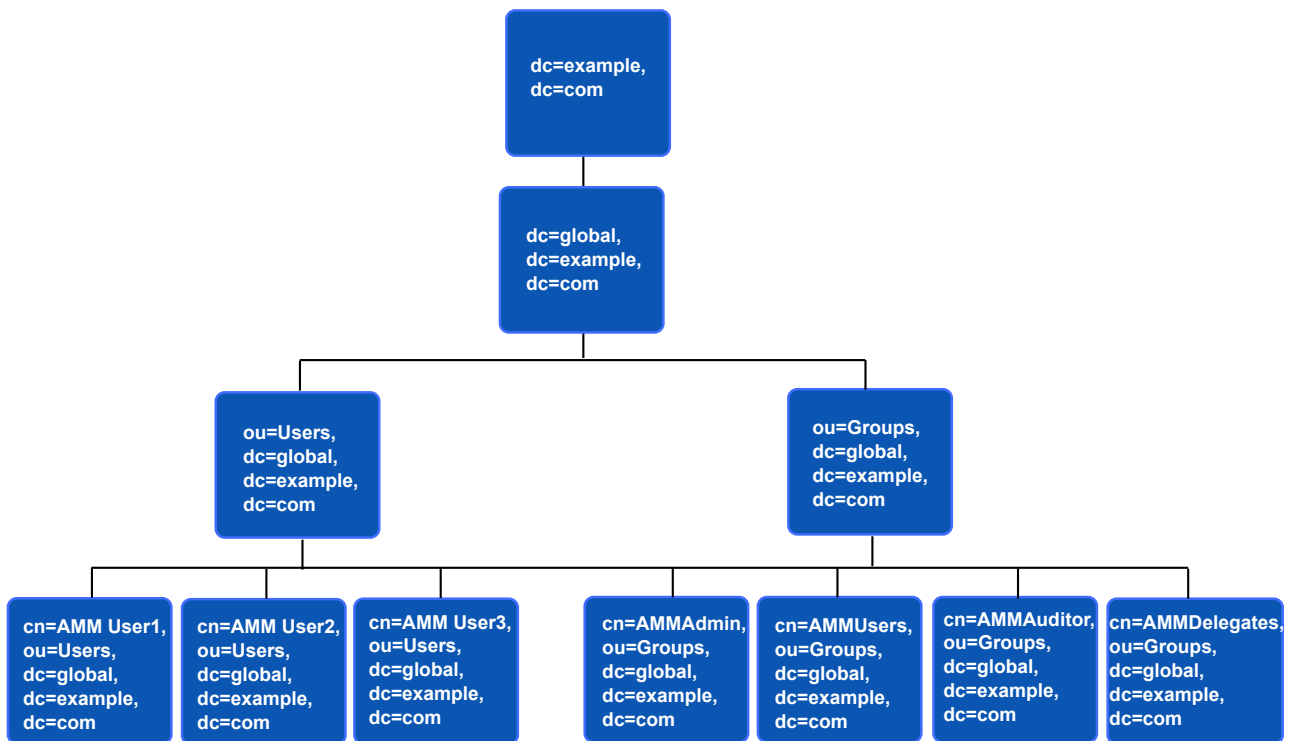


Figure 4: LDAP configuration example

- Company DNS domain: example.com
- Domain: GLOBAL
- Active Directory FQDN: gdc.global.example.com. This FQDN could be mapped to more than one replicated AD servers with different IPs.

- The Active Directory provides both LDAP and LDAPS (LDAP over TLS) accesses to the Active Directory Global Catalog (see [http://technet.microsoft.com/en-us/library/cc728188\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx) for details on what is Global Catalog) through ports 3268 and 3269, respectively.
- The user that has privileges to read and search the Active Directory (User: AADSAssistant, Password: admin123).
- Domain users.

 Note:

The LDAP attribute “mail” must be set because its value is used as the unique identifier for an AADS User.

- AADS User 1, which has the following attributes:
 - sAMAccountName=aadsuser1
 - userPrincipalName=aadsuser1@global.example.com
 - mail=aadsuser1@example.com
 - givenName=User1
 - sn=AADS
- AADS User 2, which has the following attributes:
 - sAMAccountName=aadsuser2
 - userPrincipalName=aadsuser2@global.example.com
 - mail=aadsuser2@example.com
 - givenName=User2
 - sn=AADS
- AADS Admin, which has the following attributes:
 - sAMAccountName=aadsadmin
 - userPrincipalName=aadsadmin@global.example.com
 - mail=aadsadmin@example.com
 - givenName=Admin
 - sn=AADS
- Groups:
 - “AADSAdmin” contains the users that can access the AADS OAMP GUI. In this example, this group contains the DN (Distinguished Name) of the user “AADS Admin” as the value of its “member” attributes.
 - “AADSUsers” contains the users that can access the AADS REST interface. In this example, this group contains the DN of the user “AADS User1” and the group “AADSDelegates” as the value of its “member” attributes.
 - “AADSAuditor” contains the users that have read-only access to the OAMP GUI. In this example, this group contains the DN of the users “AADS User1” and “AADS User2” as the values of its “member” attribute.

- “AADSDelegates” is a subgroup of “AADSUsers”. So the users in this group should also have access to AADS REST interface. In this example, this group contains the DN of the user “AADS User 2” as the value of its “member” attributes.

Configuring the binding parameters

About this task

This procedure describes how to configure the LDAP binding parameters when Microsoft Active Directory (AD) is used.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **LDAP Configuration**.
3. Configure the following settings:

Parameter	Description	Example
URL for LDAP Server	The URL used to locate the Active Directory server. Avaya Aura® Device Services uses the AD Global Catalog instead of the Avaya Aura® Device Services LDAP interface. The Global Catalog contains the replicated copies of data in all of the enterprise domains. This avoids the need for delegated searches by following references in the LDAP to other AD domain controllers.  Note: • You must configure attribute replication for the Global Catalog. For more information, see LDAP attributes replication to the global catalog on page 280. • Microsoft Active Directory uses a Secure LDAP connection. For the LDAPS connection, a CA (Certificate Authority) certificate for the CA that signed the AD server certificate needs to be imported into the Avaya Aura® Device Services trust store before the LDAP configuration can be made. LDAPS does not support the use of IP addresses in URLs. • If FIPS is enabled, you must use the LDAPS protocol to connect to the LDAP server.	ldaps://gdc.global.example.com:3269
Bind User	The user that has read and search access to Active Directory.	global\AADSAssistant
Bind Credential	The password for the Bind User.	admin123

Configuring the authentication parameters

About this task

This procedure describes how to configure the LDAP authentication parameters when Microsoft Active Directory (AD) is used.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **LDAP Configuration** and configure the following settings:

Parameter	Description	Example
UID Attribute ID	The LDAP attribute that contains the user ID used for authentication. For AD, there are usually two types of userID: Domain user ID or User Principal Names. Avaya Aura® Device Services also supports authentication using the email address of a user. • For Domain user ID authentication, the “UID Attribute ID” must be set to “sAMAccountName”. See <code>MultipleActiveDirectorydomains</code> for how to set this up in an AD forest • For authentication using User Principal Name, “UID Attribute ID” must be set to “userPrincipalName”.  Note: For Microsoft Active Directory, “userPrincipalName” is an optional attribute. So if authentication using User Principal Name (or UPN) is used, ensure that each user has the “userPrincipalName” attribute set.	sAMAccountName userPrincipalName
Base Context DN	The base DN where the search for the user must start. Usually, the base DN is the root DN for the AD domain.	dc=global,dc=example,dc=com

3. Select **LDAP Configuration > Advanced LDAP parameters** and configure the following settings:

Parameter	Description	Example
Allow Empty Passwords	The setting to enable user authentication without a password. Microsoft Active Directory does not allow users to authenticate without a password, so you must set the <i>Allow Empty Passwords</i> setting to false.	false

Configuring the role search parameters

About this task

This procedure describes how to configure the LDAP role search parameters when Microsoft Active Directory (AD) is used.

Role search for Avaya Aura® Device Services users are really about finding the associated “role” strings for a user in LDAP. For AD, this is about the user group names that a user belongs to.

In Microsoft Active Directory, the DN's of the groups that a user belongs to are stored in the “memberOf” attribute of a user. The “memberOf” attribute also stores the Exchange mailing lists that a user belongs to. Conversely, the group objects that the user belongs to contain a “member” attribute that stores the DN's of all of the users and sub-groups that are members of this group.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **LDAP Configuration > Advanced LDAP parameters**.
3. Configure the parameter settings as described in [Parameter settings](#) on page 296.
4. Configure the attributes as described in [Role configuration](#) on page 298.

Configuring the internationalization parameters

About this task

The internationalization parameters specify how a user's given name and surname are stored in Microsoft Active Directory (AD), and which language is used to store these names. Optionally, for non-Latin script languages, two of the parameters also specify how the ASCII transliteration of these names is stored.

The following procedure describes configuring the LDAP internationalization parameters when AD is used.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.

Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. Configure the language setting:

Parameter	Description	Default value
Language used in Directory	The language code of one of the languages supported by Avaya Aura® Device Services.	English (en)

3. Click **Save**.
4. Click **Modify Attribute Mappings**.
5. Configure the following settings:

Parameter	Description	Default value
NativeFirstName	The attribute that stores the “given name” of the user in the language of the LDAP server.	givenName
NativeSurName	The attribute that stores the “surname” of the user in the language of the LDAP server.	sn
GivenName	This is only applicable if the language in AD is one of the non-Latin script based ones.	
SurName	This is only applicable if the language in AD is one of the non-Latin script based ones.	

The NativeFirstName and NativeSurName parameters allow the user to identify the LDAP attributes used to store the user's native language given name and surname. These are mandatory parameters with defaults of givenName and sn.

The GivenName and SurName parameters allows the user to identify the LDAP attributes used to store the ASCII transliteration of the user's given name and surname, respectively. These are optional parameters and only used only if the Language used in Directory parameter is set to one of the non-Latin script languages.

The internationalization of the names must be done using the language tags specified in [RFC 3866](#).

To configure internationalization for Microsoft Active Directory, you must configure custom attributes for the native and the ASCII transliterations of the names, if both types of names are needed.

6. Click **Save** to apply changes and restart Avaya Aura® Device Services.

Configuring the user management parameters

About this task

Microsoft Active Directory (AD) users can be disabled by Administrators. The active state is tracked using one bit in the value of the attribute “userAccountControl”. The “whenChanged” attribute in AD is updated with the timestamp of the last time the object is updated.

This procedure describes how to configure the user management parameters for Microsoft Active Directory.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **LDAP Configuration > Advanced LDAP parameters**.
3. Configure the following settings:

Parameter	Description	Example
Active users search filter string	The active users search filter string contains the following elements: - objectClass: because the object needs to be of the “user” object class as this is the object class that AD uses to store AD user data. - objectCategory: because AD also uses the “user” object class for objects other than AD users. Notably, the “Computer” object is also of “user” object class. Adding this condition ensures that the object found is an AD user object. - userAccountControl: The string “1.2.840.113556.1.4.803” specifies a bitwise AND filter to check the second lowest bit in the value of “userAccountControl”, which is “1” if the user is disabled. Negating this filter using the “!” operator results in filtering for users that are NOT disabled. For details on bitwise filters and an example of using it to locate disabled users in AD, see: http://support.microsoft.com/kb/269181	<pre>(&(objectClass=user) (objectCategory=Person)(! (userAccountControl:1.2.840.113556.1.4.803:=2)))</pre>
Last updated time attribute	The value for AD is “whenChanged”.	whenChanged

Multiple authentication and authorization domains

Before Release 7.1.3, you could configure multiple LDAPs and have multiple base contexts on each LDAP, but you could only use one of them for authorization and authentication. With the single authentication and authorization domain restriction in place, users had to be provisioned multiple times so they existed in the authentication and authorization domain and in the other LDAPs used for search.

As of Release 7.1.3, the multiple authentication and authorization feature removes the requirement for a single domain for authentication and authorization and facilitates the following deployments:

- A single LDAP infrastructure belonging to a single organization with multiple configured domains.
- Two distinct LDAP infrastructures belonging to two separate organizations.

Avaya Aura® Device Services supports up to ten LDAP authentication and authorization domains.

When multiple directories are enabled for authentication, you must provide your FQDN to log in. For example: `username@avaya.com`. A short user name is not supported. If you do not have proper data in user name attributes, such as mail and userPrincipalName, you can assign a custom attribute that is used for the UID mapping of user names. All values in the custom attribute

must be a fully qualified user name of the form `username@domain`, where `domain` must match one of the base context DNSs defined for the LDAP.

During the initial Avaya Aura® Device Services installation procedure, you can configure only one LDAP server. If you want to add more LDAP servers, use the web administration portal. For more information, see “Adding a new enterprise LDAP server” in *Administering Avaya Aura® Device Services*.

Creating groups in LDAP

About this task

The procedure to create groups might differ depending on the type of enterprise directory used. This section describes the steps for creating LDAP groups in Active Directory.

Procedure

1. Access Active Directory.
2. Click the **roles** organizational unit.
3. Click the Create Group icon.
4. In the **Group name** field, type the group name and click **OK**.

You must create the following groups in the enterprise directory that you use:

- AADSAdmin
- AADSAuditor
- AADSUsers
- AADSServiceAdmin
- AADSSecurityAdmin
- AADSServiceMaintenance

5. To add a user to the group, right-click the user and click **Add to a group**.
6. In the **Enter the object names to select** field, type the group name, and click **OK**.

LDAP attribute mapping

Attribute mapping consists of associating the Avaya Aura® Device Services Application fields with attributes from the LDAP server configuration, depending on the organization requirement.

You can configure attribute mapping using the **Attribute Mapping** menu on the Avaya Aura® Device Services administration portal.

Configuration and data mapping use cases

Avaya Multimedia Messaging uses Avaya Aura® Device Services to validate addresses. Avaya Aura® Device Services brings the address information or handle data from Enterprise Directory and System Manager.

Enterprise Directory query

The query used is based on a URI from the Avaya Multimedia Messaging side, which should not contain a schema. Avaya Aura® Device Services uses the LDAP attribute mapping from the configuration to build the filter to query the LDAP. The filter can use the attributes mapped to EmailAddress, EmailAddress-1, IMHandle, IMHandle-1, or LyncAddress, and it is intended for the SMTP, SIP, and XMPP schema.

The following are sample default mappings:

Application Field Name	Directory Field Name
Email address	mail
EmailAddress-1	<not mapped>
IMHandle	<not mapped>
IMHandle-1	<not mapped>
LyncAddress	msrtcsip-primaryuseraddress
SMGRLoginname	userPrincipalName

If the Avaya Multimedia Messaging sends a validation request to Avaya Aura® Device Services for address j.doe@company.com, the Avaya Aura® Device Services will set the filter as follows:

```
OR: 8 items
Filter: (mail=j.doe@company.com)
Filter: (mail=sip:j.doe@company.com)
Filter: (mail=xmpp:j.doe@company.com)
Filter: (mail=smtp:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=sip:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=xmpp:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=smtp:j.doe@company.com)
```

Leave the IMHandle and IMHandle-1 attributes unmapped. Avaya Multimedia Messaging uses the EmailAddress value as the internal contact. When the EmailAddress and IMHandle mapping return different attribute values, the validation might fail.

System Manager query

Avaya Multimedia Messaging sends a query to Avaya Aura® Device Services, which first queries LDAP, brings back the information, and extracts the values returned for EmailAddress and SMGRLoginname. Avaya Aura® Device Services then queries System Manager using SMGRLoginName, and if that fails, then it uses EmailAddress.

Application Field Name	System Manager Field Name
SMGRLoginName	Login Name

Application Field Name	System Manager Field Name
Email address	Login Name, OR Microsoft Exchange Communication Address, OR Other Email Communication Address

This use case is not applicable for Avaya Aura® Device Services deployments in an environment without Avaya Aura®.

The user information is available in both Enterprise Directory and System Manager

If Avaya Aura® Device Services is able to retrieve data from both Enterprise Directory and System Manager, it merges these two data sets, and sends this information back to the Avaya Multimedia Messaging server.

If Avaya Aura® Device Services queries the System Manager data, and if it does not find any related information from System Manager, it sends back the data only from Enterprise Directory.

This use case is not applicable if Avaya Aura® Device Services is deployed in an environment without Avaya Aura®. In this case, the user information is available only in Enterprise directory.

The user information is available on System Manager but not on Enterprise Directory

The Avaya Multimedia Messaging server sends a query to Avaya Aura® Device Services. If the relevant user is not available on Enterprise Directory, the query is redirected to System Manager. Avaya Aura® Device Services attempts to use the received URI from Avaya Multimedia Messaging to match the System Manager, Login Name, Microsoft Exchange Communication Address, or Other Email Communication Address.

If a match is found, then Avaya Aura® Device Services extracts the SMGRLoginName, creates a query filter with the SMGRLoginName, and then sends another query to the Enterprise Directory.

The fetched data is merged with System Manager data and sent back to Avaya Multimedia Messaging. If the second query to Enterprise Directory fails to bring back data because no relevant data exists, then only System Manager data is sent back to the Avaya Multimedia Messaging server.

This use case is not applicable if Avaya Aura® Device Services is deployed in an environment without Avaya Aura®. In this case, the user information is available only in Enterprise directory.

User in Enterprise Directory and System Manager

Table 5: Avaya Multimedia Messaging server mappings

Application Field Name	Directory Field Name
Email address	mail
EmailAddress-1	<not mapped>
IMHandle	<not mapped>
IMHandle-1	<not mapped>
LyncAddress	msrtcip-primaryuseraddress
SMGRLoginname	userPrincipalName

Table 6: Enterprise Directory mappings

Enterprise Directory Field	Value
mail	j.doe@company.com
userPrincipalName	j.doe@north.company.com

Table 7: System Manager mappings

System Manager Field	Value
Login Name	j.doe@north.company.com
Avaya SIP handle	2001@sip.company.com
Avaya Presence/IM handle	j.doe@pres.north.company.com

Avaya Multimedia Messaging sends a validation request for j.doe@company.com to Avaya Aura® Device Services, which then sends a query to Enterprise Directory with the filter shown in [Enterprise Directory query](#) on page 293.

OR: 8 items

```
Filter: (mail=j.doe@company.com)
Filter: (mail=sip:j.doe@company.com)
Filter: (mail=xmpp:j.doe@company.com)
Filter: (mail=smtp:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=sip:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=xmpp:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=smtp:j.doe@company.com)
```

When Enterprise Directory gets a match for mail=j.doe@company.com, it returns:

```
mail=j.doe@company.com
userPrincipalName=j.doe@north.company.com
```

Avaya Aura® Device Services sends the following query to System Manager:

```
Filter: Login Name=j.doe@north.company.com
```

When System Manager gets a match on Login Name, it returns the Avaya SIP handle and the Avaya Presence or IM Handle.

Avaya Aura® Device Services merges the information and returns handles to Avaya Multimedia Messaging:

```
Contact = j.doe@company.com
SIP Handle= 2001@sip.company.com
XMPP Handle=j.doe@pres.company.com
```

Changing the PictureURL attribute

About this task

Use this procedure if you are using onboard Open LDAP and want to upload user images.

Procedure

1. Log in to the Avaya Aura® Device Services web administration interface.
2. Navigate to **Server Connections > LDAP Configuration**.
3. On the Enterprise Directory page, select the onboard Open LDAP tab.
4. In Server Address and Credentials area, click **Modify Attribute Mappings**.
5. For the PictureURL attribute, enter `jpegPhoto` in the **Custom Field Name** field.
6. Click **Save**.
7. To apply the changes immediately, click **Force LDAP Sync** on the Enterprise Directory page.

LDAP configuration best practices

Ensure you use the following best practices during LDAP configuration for Avaya Aura® Device Services.

- Map SMGRLoginName to the email address or User Principal Name (UPN) attribute. You can update the mapping on the Attribute Mapping page in the Avaya Aura® Device Services web administration portal.
- Turn on LDAP synchronization between System Manager and LDAP.

Even if the above best practices are not followed, make sure you include a Microsoft Exchange Server (SMTP) handle in System Manager for all user records. This facilitates correlation of System Manager user records with LDAP records.

These best practices are not applicable for Avaya Aura® Device Services deployments in an environment without Avaya Aura® because Avaya Aura® Device Services does not interact with System Manager in this environment type.

LDAP parameter descriptions

Parameter settings

The following table describes the parameter settings according to the search mechanism that you choose:

Parameter	Search mechanism #1: Find the user, extract the group DNs from the “memberOf” attribute, and get the role strings from each of the group objects		Search mechanism #2: Find the groups that the user belongs to and extract the role string from one of the attributes	
	Example	Description	Example	Description
Role Filter	(&(objectClass=user)(objectCategory=Person)(<UID attribute ID>={0}))	<UID Attribute ID> is the value of the “UID Attribute ID” parameter. “{0}” is the placeholder that will be replaced by the authenticating user ID.	(&(objectClass=group)(member={1}))	“{1}” is the placeholder to be replaced by the DN of the user object. The DN is identified during the authentication process. This filter looks for a group object whose “member” attribute contains a value of the authenticating user DN.
Role Context DN	ou=Users,dc=global,dc=example,dc=com	The purpose of the search is to find the user and then extract the role objects from the “memberOf” user attribute.	ou=Groups,dc=global,dc=example,dc=com	The purpose of the search is to find the roles whose “member” attribute contains the user.
Role Attribute ID	memberOf	This attribute contains the list of DNs of the groups to which the user belongs to.	CN	This contains the group’s name (for example, “AADSAdmin”, and so on.)
Role Attribute is DN	true	The “memberOf” values are the DNs of the group/mailling list objects.	false	The “Role Attribute ID” already contains the “role” string name.
Role Name Attribute	CN	The attribute defined by Role Name Attribute contains the group name. For example: AADSAdmin		Leave this parameter empty because “Role Attribute is DN” is false.

Parameter	Search mechanism #1: Find the user, extract the group DNs from the “memberOf” attribute, and get the role strings from each of the group objects		Search mechanism #2: Find the groups that the user belongs to and extract the role string from one of the attributes	
	Example	Description	Example	Description
Role Recursion	0	This configuration does not allow recursive search.  Note: Using this configuration, the users under the “AADSDelegates” group will not be able to use Avaya Aura® Device Services so this is not the recommended configuration for this example.	1 or higher	You must set this value to 0 if there are no subgroups or a value from 1 to 10 to support searches of users that are in subgroups. In this example, the recursive search is needed to find the user in the “AADSDelegates” group, so this value must be set to at least 1.

Role configuration

To search the role base context and under it, set **Search Scope** to 2 or `SUBTREE_SCOPE`. The configuration of the following roles is the same, regardless of the configured search mechanism:

Role	Description	Example
Administrator Role	This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Aura® Device Services server ADMIN application role.	AADSAdmin
User Role	This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Aura® Device Services server USERS application role.	AADSUsers
Auditor Role	This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Aura® Device Services server AUDITOR application role.	AADSAuditor
Service Administrator Role	Avaya Aura® Device Services does not currently use this role. Leave this setting blank.	
Services Maintenance and Support Role	Avaya Aura® Device Services does not currently use this role. Leave this setting blank.	
Security Administrator Role	This role is for updating web certificates from the web administration portal.	AADSSecurityAdmin

Chapter 12: SNMP server configuration

You can configure Avaya Aura® Device Services to send its alarms to an SNMP server.

- If you use Avaya Aura® Device Services in an Avaya Aura® environment, this is normally System Manager. However, if required, you can configure and use a third-party SNMP server.
- If you use Avaya Aura® Device Services in an environment without Avaya Aura®, you must configure and use a third-party SNMP server.

If FIPS is enabled, only SNMPv3 profiles are supported.

For more information, see *Administering Avaya Aura® System Manager*.

You can also view alarm details in the `/opt/Avaya/DeviceServices/<version>/logs/AADS_alarm.log` file.

Alarms configuration for System Manager

You can configure Avaya Aura® Device Services to send its alarms to an SNMP server. If you use Avaya Aura® Device Services in an Avaya Aura® environment, this is normally System Manager.

You must set up serviceability agents to receive Avaya Aura® Device Services alarms in System Manager. To configure serviceability agents, set up an SNMPv3 user profile and an SNMP target profile. Then assign the SNMPv3 user profile to the SNMP target profile.

Configuration Checklist

No.	Task	Notes	✓
1	Setup an SNMPv3 user profile.	See Setting up an SNMPv3 user profile on page 299.	
2	Setup an SNMP target profile.	See Setting up an SNMP target profile on page 300.	
3	Assign the SNMPv3 user profile.	See Assigning the SNMPv3 user profile on page 301.	

Setting up an SNMPv3 user profile

About this task

An SNMPv3 user profile enables you to define privileges so serviceability agents can read and write data in SNMP Management Information Bases (MIBs).

Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > SNMPv3 User Profiles**.
2. In the User Details section, click **Edit**.
3. In the **User Name** field, type `initial`.
4. In the **Authentication Protocol** field, select **SHA**.
The **MD5** setting is not supported.
5. In the **Authentication Password** field, type the authentication password.
The default authentication password is `avaya123`.
6. In the **Confirm Authentication Password** field, confirm the password.
7. In the **Privacy Protocol** field, select **AES**.
8. In the **Privacy Password** field, type the privacy password.
The default privacy password is `avaya123`.
9. In the **Confirm Privacy Password** field, confirm the password.
10. In the **Privileges** field, select **Read/Write**.
11. Click **Commit**.

Setting up an SNMP target profile

About this task

An SNMP target profile contains settings for sending alarms from Avaya Aura® Device Services to System Manager.

Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > SNMP Target Profiles**.
2. On the Target Details tab, click **Edit**.
3. In the **Name** field, type the name of the profile.
4. In the **Description** field, type a description for the profile.
5. In the **IP Address** field, type the System Manager IP address.
6. In the **Port** field, type `10162`.
7. In the **Notification Type** field, select **Trap**.
8. In the **Protocol** field, select **V3**.
9. Click **Commit**.

Assigning the SNMPv3 user profile

About this task

You must assign the SNMPv3 user profile to the target profile so System Manager can receive alarms from Avaya Aura® Device Services.

Before you begin

Associate the Avaya Aura® Device Services server with the configured Session Manager.

Set up an SNMPv3 user profile and an SNMP target profile.

Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.
2. Select the Avaya Aura® Device Services host name, and click **Manage Profiles**.
3. Click the **SNMP Target Profiles** tab.
4. In the Assignable Profiles section, click the SNMP target profile you created, and click **Assign**.
5. Click the **SNMPv3 User Profiles** tab.
6. In the Assignable Profiles section, select the SNMPv3 profile you created, and click **Assign**.
7. Click **Commit**.

Alarms configuration for a third-party SNMP server

You can configure Avaya Aura® Device Services to send its alarms to an SNMP server. If you use Avaya Aura® Device Services in an environment without Avaya Aura®, you must configure and use a third-party SNMP server.

Configuration Checklist

No.	Task	Notes	✓
1	Setup SNMPv3 on the third-party server.	See Setting up a third-party SNMPv3 server on page 302.	
2	Configure the Avaya Aura® Device Services server to send alarms to the third-party server.	See Configuring Avaya Aura Device Services to support a third-party SNMP server on page 302.	
3	Verify that the third-party server receives Avaya Aura® Device Services alarms.	See Verifying third-party SNMP server operation on page 303.	

Setting up a third-party SNMPv3 server

About this task

In order to send alarms to a third-part server, the following elements must be configured on that server:

- SNMPv3 server software such as SNMP Manager on Linux.
- An SNMP user account configured on the third-party server. A matching user is configured on the Avaya Aura® Device Services server.
- Firewall access to the SNMP server. The defaults for most SNMP server installations are port 161 (UDP and TCP) for SNMP client access and port 162 for SNMP traps (UDP and TCP).

Procedure

1. Using the documentation for the third-party server operating system and/or the SNMP server software, verify the installation of the SNMP server.
2. Check that the third-party server is accessible on the ports configured for SNMP.
3. Check that you have the details for the SNMP server configured on the third-party server for use by Avaya Aura® Device Services. The required details are:
 - The user name.
 - The user's authentication password.
 - The user's encryption password.
 - The encryption algorithm to use; AES or DES.
 - The IP address of the SNMP server.
 - The destination port for SNMP traps on the SNMP server.

Configuring Avaya Aura® Device Services to support a third-party SNMP server

About this task

This process:

- Creates an SNMP user on the Avaya Aura® Device Services to match the one configured on the third-party SNMP server.

Adds the third-party SNMP server as the destination for alarms from the Avaya Aura® Device Services server.

Before you begin

- Configure the third-party server for SNMPv3 and create an SNMP user on that server.

Procedure

1. Log in to the Avaya Aura® Device Services CLI.
2. Run the following command:

```
cdto misc
```

3. Run the following command:

```
sudo ./setSNMPTrapDestination.sh -u <username> -A <authentication password> -X <encryption password> -x <encryption algorithm> -i <destination address> -p <destination port>
```

where:

- *<username>* is replaced with the SNMP username.
- *<authentication password>* is the SNMP user's authentication password.
- *<encryption password>* is the SNMP user's encryption password.
- *<encryption algorithm>* is the encryption algorithm, either AES or DES.
- *<destination address>* is the IP address of the third-party server running SNMP manager.
- *<destination port>* is the IP port for SNMP traps on the third-party server.

For example:

```
sudo ./setSNMPTrapDestination.sh -u snmpadmin -A 12345678 -X 34567890 -x DES -i 10.133.32.69 -p 162
```

Verifying third-party SNMP server operation

About this task

This process sends a set of test alarms from the Avaya Aura® Device Services server. Use these to check that the alarms are shown by the third-party SNMP server.

Procedure

1. On the Avaya Aura® Device Services server, use the following commands to send a set of test alarms:

```
cdto bin
```

```
sudo ./snmpTest.sh 1
```

2. Check that the third-party SNMP server displays the test alarms.

Chapter 13: Reverse proxy configuration

Checklist for reverse proxy configuration

In networks where connections to an Avaya Aura® Device Services instance go through Avaya SBC placed in a DMZ, some additional configurations are required for the reverse proxy.

No.	Task	Notes	✓
1	Configure Avaya Aura® Device Services with the appropriate front end certificate.	The Front-end IP or address configured during installation is used as the common name for the nginx certificate and published during resource discovery. The front-end certificate is used on port 443 and is located at <code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/nginx/certs/nginx.crt</code> .	
2	Generate certificate request on Avaya SBC by using the Avaya Aura® Device Services front-end FQDN.	See Creating a CSR on page 305.	
3	Issue certificate from Certificate Authority.	• If you use Avaya Aura® Device Services in an Avaya Aura® environment, see Creating an end entity on page 308 and Creating the certificate using a CSR on page 309. • If you use Avaya Aura® Device Services in an environment without Avaya Aura®, obtain a certificate from a third-party CA using the CSR.	
4	Ensure port 443 is open on both sides of Avaya SBC.		
5	Install server certificates on Avaya SBC.	See Uploading a certificate file on page 309 and Synchronizing and installing certificate in a multi-server deployment on page 311.	

No.	Task	Notes	✓
6	Install client certificates on Avaya SBC.	- If you use Avaya Aura® Device Services in an Avaya Aura® environment, see Downloading the System Manager PEM certificate on page 312 and Installing a CA certificate on page 312. - If you use Avaya Aura® Device Services in an environment without Avaya Aura®, obtain your third-party CA root certificate and install it as described in Installing a CA certificate on page 312.	
7	Create client and server TLS profiles.	See Creating a TLS server profile on page 313 and Creating a TLS client profile on page 316.	
8	Add reverse proxy.	See Adding a reverse proxy on page 318.	

Creating a CSR

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management > Certificates**.

The EMS server displays the Certificates window.

4. Click **Generate CSR**.

The EMS server displays the TLS Management Generate CSR window.

5. Enter the appropriate information in the TLS Management Generate CSR window and click **Generate CSR**.

Ensure that the **Key Encipherment** and **Digital Signature** check boxes are selected.

In the **Common Name** field, type the Avaya Aura® Device Services FQDN.

6. In the **Subject Alt Name** field, type the Avaya Aura® Device Services FQDN.
7. Click **Download CSR** and **Download Private Key**.

TLS certificates field descriptions

Certificates tab

Name	Description
Installed Certificates	Some Certificate Authority (CA) signed certificate or self-signed certificate. This certificate is incorporated into a server certificate profile and sent to clients to set up a TLS connection.  Note: All certificates, certificate authorities, and certificate revocation lists uploaded to the EMS must be valid X.509 certificates in the PEM format. Certificates not in this format might be converted using a proper SSL tool, such as the publicly available OpenSSL tool. You can access this tool from: https://www.openssl.org/
Installed CA Certificates	The unsigned public key certificates from a Certificate Authority (CA), which vouch for the correctness of the data contained in a certificate and verify the signature of the certificate.
Installed Certificate Revocation Lists	The Certificate Revocation Lists (CRLs) that contain the serial numbers of CSRs that have been revoked, or are no longer valid, and should not be relied upon by any system subscriber.
Installed Certificate Signing Requests	The installed certificate signing requests on the system.
Installed Keys	The installed keys for third party certificates.

Install Certificate

Name	Description
Type	The type of certificate that you want to install. The options are: • Certificate • CA Certificate • Certificate Revocation List
Name	The name of the certificate that you want to install. This field is optional, and if not specified, the filename of the uploaded certificate is used as the certificate name. Additionally, specifying a name same as another certificate will overwrite the existing certificate with the one being uploaded.
Overwrite Existing	An option to control whether uploading a certificate with the same name is permitted. If this field is cleared, uploading a certificate with the same name as another certificate causes failure. If this field is selected, when you upload a certificate with the same name overwrites an existing certificate.

Name	Description
Allow Weak Certificate/Key	An option to permit usage of a weak private keys. This option bypasses the check that requires strong private keys. By default, private keys with a key size less than 2048 bits, signed with a SHA-1 or MD5 based hash, or no key usage extension or extended key usage extension, will be rejected.
Certificate File	The location of the certificate on your system. Depending on your browser, click Browse or Choose file to browse for the file. If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBC. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.
Trust Chain File	The trust chain file used to verify the authenticity of the certificate. Depending on the browser, click Browse or Choose File to locate the file.
Key	The private key that you want to use. You can opt to use the ilexisting key from the filesystem or select a file containing another key.
Key File	This field is available when you select Upload Key File in the Key field. Depending on the browser, click Browse or Choose File to locate the file.
Key Passphrase	This field is available when you select Upload Key File in the Key field. A key passphrase is used to to protect the key file while installing certificates. You must use the same passphrase in the Key Passphrase which you created while creating the third party certificate. For successful encryption of the key, Avaya recommends not to use the dollar sign (\$) in Key Passphrase.

Generate CSR

Name	Description
Country Name	The name of the country within which the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Locality Name	The locality (city) where the certificate is being created.
Organization Name	The name of the company or organization creating the certificate.
Organizational Unit	The group within the company or organization creating the certificate.
Common Name	The name used to refer to or identify the company or group creating the certificate. It is recommended not to use wildcard (*) character in this field.
Algorithm	The hash algorithms (SHA256) to be used with the RSA signature algorithm.
Key Size (Modulus Length)	The certificate key length (2048 or 3072) in bits.
Key Usage Extension(s)	The purpose for which the public key might be used: Key Encipherment, Non-Repudiation, Digital Signature. The Digital Signature and Key Encipherment options are selected by default.

Name	Description
Subject Alt Name	An optional text field to further identify the certificate. You can provide multiple comma-separated entries in this field. You can make a maximum of 10 Subject Alt Name entries. Avaya SBC supports DNS hostname, IP address and SIP domain name as valid entries for Subject Alt Name field. Avaya SBC does not support SIP URI as a valid value for the Subject Alt Name field. Though wildcard (*) character is supported in this field, it is recommended not to use this character. Example of supported format: DNS: .test.com Examples of unsupported formats: DNS: * DNS: *.com
Passphrase	The password to encrypt the private key.
Confirm Passphrase	A verification field for the Passphrase.
Contact Name	The name of the point-of-contact within the issuing organization for issues related to the certificate.
Contact E-mail	The contact's e-mail address.

Creating an end entity

About this task

This procedure is not applicable for Avaya Aura® Device Services deployments in an environment without Avaya Aura®.

Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **RA Functions > Add End Entity**.
4. On the Add End Entity page, in **End Entity Profile**, select **INBOUND_OUTBOUND_TLS**.
5. Type the username and password.

The password is mandatory for each end entity. Without the password, you cannot generate the certificate from System Manager because you require the password to authenticate the certificate generation request.

6. Enter the relevant information in the fields.

The system automatically selects the following:

- **ID_CLIENT_SERVER** in **Certificate Profile**
- **tmdefaultca** in **CA**
- **User Generated** in **Token**

With **User Generated**, the system generates the certificate by using CSR.

The options are **P12 file**, **JKS file**, and **PEM file**.

7. Click **Add**.

The system displays the message `End Entity <username> added successfully`.

Creating the certificate using a CSR

About this task

This procedure is not applicable for Avaya Aura® Device Services deployments in an environment without Avaya Aura®.

Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. In the navigation pane, click **Public Web**.
4. On the public EJBCA page, click **Enroll > Create Certificate from CSR**.
5. To get your certificate, on the Certificate Enrollment from a CSR page, do the following:
 - a. Enter the same username and the password that you provided while creating the end entity.
 - b. In the text box, paste the PEM-formatted PKCS10 certification request.
 - c. Click **OK**.

A certificate in PEM format is generated. The certificate contains the values provided in the end entity.

Uploading a certificate file

Before you begin

Obtain the signed certificate from the Certificate Authority (CA). You might also receive a certificate trust chain if the CA did not directly sign the certificate. The certificate trust chain might be provided as a separate file or it might be concatenated directly onto the signed certificate.

If the signed certificate is not in a PEM-encoded format, re-encode the certificate in the PEM format before uploading it to the EMS.

An open-source SSL library with utilities for conversions is available at:

<http://www.openssl.org>

You can use this utility to convert a file with a DER-encoded format to a PEM format, as shown in the example below:

```
openssl x509 -in input.der -inform DER -out output.pem -outform PEM
```

You can convert a certificate with a .PEM extension to the .crt extension by renaming the file and changing the PEM extension to .crt.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management > Certificates**.
4. Click **Install**.
5. In the **Type** field, select **Certificate**.
6. In the **Name** field, type the name of the Certificate file.

Note:

You can type only letters, numbers, and underscores in the **Name** field. Enter the name of the Certificate file that is uploaded to the EMS. If the name of the Certificate file that you browse for uploading has a different name, that name will be changed with the Certificate name that is uploaded to the EMS.

7. In the **Certificate File** field, click **Browse** and browse to the location of the Certificate file.
8. In the **Key** field, select one of the following options:

- **Use Existing Key:** Select this option if you generated a CSR from the Generate CSR screen. In this option, the key file is already in the correct location on the EMS.

Note:

If you are using this option, ensure that the Common Name in the Generate CSR screen matches with the name of the install certificate.

- **Upload Key File:** Select this option if you generated a CSR by using an alternate method than the built-in Generate CSR screen.

In this option, you must upload the private key as described in Step 7.

9. In the **Key File** field, click **Browse** and browse to the location of the key file.
10. In the **Trust Chain File** field, click **Browse** and browse to the location of the trust chain file.

This step is required if the CA provided a separate certificate trust chain.

If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBC. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.

11. Click **Upload**.

The EMS server uploads the signed X.509 certificate and the key file, if necessary, to the SBC. The EMS server automatically synchronizes and installs the certificate and key on multi-server and single server deployments.

 Important:

For an HA pair, the certificate and key are uploaded to the primary device and synchronized to the secondary device. However, if you add a new certificate and key on the EMS, you must manually click **Synchronize to HA Peer** so that the certificate and keys are synchronized onto the secondary device.

Synchronizing and installing certificate in a multi-server deployment

About this task

A multi-server deployment can consist of one or more Avaya SBC HA pairs or multiple individual Avaya SBC servers. Use this procedure to synchronize and install certificates for each Avaya SBC server in the multi-server deployment.

Procedure

1. Using a terminal emulation program such as PuTTY, start a secure shell (SSH) connection to each Avaya SBC individually in a multiple server deployment.
2. In the **Host Name (or IP address)** field, type the IP address of an individual SBCE box.
3. In the **Port** field, type `222` and click **Open**.

A short delay might occur before connecting.

4. To log in to Avaya SBC, use `ipcs login` and password.
5. At the `$` prompt, type `sudo su` and press `Enter`.

The system displays a prompt to enter the password.

6. At the password prompt, type the `ipcs` password.
7. At the `#` prompt, type `clipcs` and press `Enter`.

The system displays the CLIPCS console commands level, which is one level below root-level. For a list and descriptions of available CLIPCS commands, see “CLIPCS Console Commands”.

8. When the system requests the key passphrase, enter the passphrase.

If you used the CSR generation utility that is built into Avaya SBC, the passphrase is the password you entered in the Generate CSR screen.

9. At the `#` prompt, type `exit` and press `Enter`.

The system exits the program level and displays the `$` prompt.

10. At the `$` prompt, type `exit` and press `Enter`.

The system exits the secure shell session. You can also exit the session by clicking the Cancel (X) button in the upper-right portion of the window.

11. Use the EMS web interface to restart the Avaya SBC application.

Downloading the System Manager PEM certificate

About this task

This procedure is not applicable for Avaya Aura® Device Services deployments in an environment without Avaya Aura®.

Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **CA Functions > CA Structure & CRLs**.
4. Click **Download PEM file**.

The system downloads the `.pem` file on your system.

Installing a CA certificate

Before you begin

Change the extension of the CA certificate to `.crt`.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management > Certificates**.
4. Click **Install**.
5. In the **Type** field, select **CA Certificate**.
6. In the **Name** field, type a name for the certificate.

7. Click **Browse** to locate the certificate file.
8. Click **Upload**.

Creating a TLS server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management > Server Profiles**.
The EMS server displays the Server Profiles screen.
4. Click **Add**.
The EMS server displays the New Profile window.
5. Administer the options as described in [TLS server profile screen field descriptions](#) on page 313.
6. Click **Finish**.

The EMS server creates, installs and lists the TLS server profile in the application pane.

TLS server profile screen field descriptions

Field	Description
TLS Profile	
Profile Name	The descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
SNI Options	Indicates whether the SNI group is required or not. The options are: • None: SNI functionality does not have any effect on the client server handshake process. The Avaya SBC server approves the handshake between the client and the server with and without the SNI request. • Optional: If there is an SNI request from the client and server_name extension in the client handshake packet matches with the CN or SAN fields of the TLS certificate. The Avaya SBC server approves the handshake between the client and server, otherwise TLS handshake is rejected. If there is no SNI request from the client, the TLS profile associated with the Signaling Interface will be used for communication. • Mandatory: If there is an SNI request from client and server_name extension in the client handshake packet matches with the CN or SAN fields of the TLS certificate. The Avaya SBC server approves the handshake between the client and server, otherwise handshake is rejected. If there is no SNI request from client, then also the Avaya SBC server rejects the TLS handshake.

Field	Description
SNI Group	Specifies the configured SNI groups. SNI Group field is accessible only if SNI Options is either Optional or Mandatory.
Certificate Verification	
Peer Verification	One of three check boxes indicating whether peer verification is required: • Required: The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the Required check box is a locked setting and cannot be deselected. • Optional: The incoming connection may optionally provide a certificate. If a certificate is provided, but is not contained in the Peer Certificate Authority list, or is contained in a Peer Certificate Revocation List, the connection will be rejected. • None: No peer verification will be performed.  Note: Peer Verification is always required for TLS Client Profiles, therefore the Peer Certificate Authorities, Peer Certificate Revocation Lists, and Verification Depth fields will be active.
Peer Certificate Authorities	The CA certificates to be used to verify the remote entity identity certificate, if one has been provided.  Note: Using Ctrl or Ctrl+Shift, any combination of selections can be made from this list. Using Ctrl+Shift, the user can drag to select multiple lines, and using Ctrl, the user can click to toggle individual lines.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether or not a peer certificate is valid.  Note: Using Ctrl or Ctrl+Shift, any combination of selections can be made from this list. Using Ctrl+Shift, the user can drag to select multiple lines, and using Ctrl, the user can click to toggle individual lines.
Verification Depth	The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.
Renegotiation Parameters	
Renegotiation Time	The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.

Field	Description
Renegotiation Byte Count	The amount of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Handshake Options	
Version	The TLS versions that the client or servers accepts or offers. For Release 10.1.0, the options are: • TLS 1.2 • TLS 1.1 • TLS 1.0 For Release 10.1.2, the options are • TLS 1.3 • TLS 1.2 The default value for this field is TLS 1.2. Ensure that you select an appropriate TLS version according to the TLS version that the server supports.
Ciphers	The level of security to be used for encrypting data. The options are: • Default: The cipher suite recommended by Avaya. • FIPS: The cipher suite recommended by Avaya for FIPS 140–2 compatibility. • Custom: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below.
Value	A field provided to contain a textual representation of the ciphers settings used by OpenSSL.  Note: The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure. For a full list of possible values, see the OpenSSL ciphers documentation at https://www.openssl.org/docs/manmaster/man1/openssl-ciphers.html. To get the list of cipher suites supported by Avaya SBC, run the following command: <pre>openssl ciphers -s -v -<TLS version> '<cipher string>',</pre> where <cipher string> is DEFAULT:!SHA for Default ciphers and FIPS:!ECDH:!ADH:!3DES:!KRB5 for FIPS ciphers. For example, run the following command to get the list of cipher suites supported by Avaya SBC for Default ciphers when using TLS version 1.2: <pre>openssl ciphers -s -v -tls1_2 'DEFAULT:!SHA'</pre>

 Note:

The only exception is regarding the Peer Verification parameter setting (see description below). This setting determines if a peer verification operation should be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**, while in a TLS server profile, the Peer Verification parameter may be set to one of three possible values: **Required**, **Optional**, or **None**.

Creating a TLS client profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management > Client Profiles**.
4. Click **Add**.

The EMS server displays the **New Profile** window.

5. Enter the requested information in the appropriate fields.
6. Click **Finish** to save the changes.

The EMS server installs and displays the new TLS client profile.

TLS client profile screen field descriptions

Name	Description
TLS Profile	
Profile Name	A descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
SNI	A check box to enable the SNI feature.
Certificate Verification	
Peer Verification	The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the Required is selected for this field.  Note: Peer Verification is always required for TLS Client Profiles, therefore the Peer Certificate Authorities, Peer Certificate Revocation Lists, and Verification Depth fields will be active.

Name	Description
Peer Certificate Authorities	The CA certificates to be used to verify the remote entity identity certificate, if one has been provided.  Note: Using Ctrl or Ctrl+Shift, any combination of selections can be made from this list. Using Ctrl+Shift, the user can drag to select multiple lines, and using Ctrl, the user can click to toggle individual lines.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether a peer certificate is valid.  Note: Using Ctrl or Ctrl+Shift, any combination of selections can be made from this list. Using Ctrl+Shift, the user can drag to select multiple lines, and using Ctrl, the user can click to toggle individual lines.
Verification Depth	The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.
Extended Hostname Verification	Determines whether or not server certificates will be verified only by the DNS entry in the Common Name or Subject Alt Name of the certificate served by the remote server.
Server Hostname	Permits the user to define a custom hostname that will be accepted if served by the remote server. This is primarily intended for use with legacy Avaya products. You must configure Server Hostname field for: • Non SIP traffic • Non HTTP traffic • PPM traffic Server Hostname field is accessible only if either Extended Hostname Verification or SNI or both of these check boxes are selected.
Renegotiation Parameters	
Renegotiation Time	The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Renegotiation Byte Count	The number of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Handshake Options	

Name	Description
Version	The TLS versions that the client or servers accepts or offers. For Release 10.1.0, the options are: • TLS 1.2 • TLS 1.1 • TLS 1.0 For Release 10.1.2, the options are • TLS 1.3 • TLS 1.2 The default value for this field is TLS 1.2. Ensure that you select an appropriate TLS version according to the TLS version that the client supports.
Ciphers	The level of security to be used for encrypting data. The options are: • Default: The cipher suite recommended by Avaya. • FIPS: The cipher suite recommended by Avaya for FIPS 140–2 compatibility. • Custom: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below.
Value	A field provided to contain a textual representation of the ciphers settings used by OpenSSL. For a full list of possible values, see the OpenSSL ciphers documentation at http://www.openssl.org/docs/apps/ciphers.html.  Note: The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure.

 Note:

The only exception is regarding the Peer Verification parameter setting. This setting determines whether a peer verification operation must be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**. In a TLS server profile, the Peer Verification parameter can be set to one of three possible values: **Required**, **Optional**, or **None**.

Adding a reverse proxy

About this task

Use this procedure to configure the reverse proxy with the listed IP towards the enterprise and connect the IP to the network outside the enterprise.

In a remote worker environment, ensure split DNS configuration for Avaya Aura® Device Services to function properly.

Procedure

1. On the Add Reverse Proxy page, do the following:
 - a. In the **Service Name** field, type the reverse proxy profile name.
 - b. Select the **Enabled** check box.
 - c. In the **Listen IP** field, click the external SBC IP address.
 - d. In the **Listen Protocol** field, select the protocol published towards remote workers.
If you select the HTTPS protocol, the system enables the **Listen TLS Profile** field.
 - e. In the **Listen TLS Profile** field, click the TLS profile you created.
The default TLS profiles, such as AvayaSBCServer have demonstration certificates. For optimum security, Avaya recommends that you do not use demonstration certificates.
 - f. In the **Listen Port** field, type 443 or the override port defined on Avaya Aura® Device Services.
 - g. In the **Server Protocol** field, click the protocol used for the Avaya SBC server.
For security reasons, Avaya recommends the use of HTTPS.
 - h. In the **Server TLS Profile** field, click the TLS profile that you created.
 - i. In the **Connect IP** field, click the IP address that Avaya SBC must use for communicating with the file servers.
 - j. In the **Server Addresses** field, type the Avaya Aura® Device Services server address and port.
This field accepts an IP address or FQDN, and port. Specify the FQDN and port in the **Server Addresses** field. This field must match the **Subject Alt Name** defined in the Avaya Aura® Device Services server certificate.
 - k. In the **Load Balancing Algorithm** field, select a load balancing algorithm.
 - l. Select the **Allow Web Sockets** check box.
 - m. In the **Whitelisted IPs** field, type the allowedlist IPs.
2. Click **Finish**.

Overriding port configuration in a cluster

About this task

If clients will not be connecting directly to the Avaya Aura® Device Services server, but rather using a proxy server as part of a remote access solution that is configured to receive connections

on a port other than the default port 443, you must change the front-end port for reverse proxy on the all nodes in the cluster. All nodes must use the same port number.

Procedure

1. On the seed node, run the `app configure` command.
2. Click **Front-end host, System Manager and Certificate Configuration**.
3. Set **Override port for reverse proxy** to `y` (yes).
4. In **Front-end port for reverse proxy**, enter the appropriate port number.
5. Provide the enrollment and keystore passwords.
6. Select **Apply** and press `Enter`.

Perform the following steps on the backup node first and then on all remaining non-seed nodes.

7. On the node, run the `app configure` command.
8. Click **Front-end host, System Manager and Certificate Configuration**.
9. Ensure that the **Front-end port for reverse proxy** field contains the port number that you set up on the seed node.
10. Provide the enrollment and keystore passwords.
11. Select **Apply** and press `Enter`.

Avaya Aura® Device Services generates new certificates and updates firewall rules with the new front-end port value.

Chapter 14: Remote access configuration

You can configure Avaya Aura® Device Services to be accessible to remote workers using Avaya Workplace Client clients from outside the enterprise network. The following configuration methods are available:

- Virtual private Network (VPN)
- Avaya Session Border Controller (Avaya SBC)
- Application Delivery Controllers (formerly named Reverse Proxies)

The following section contains an example for configuring the remote access feature using Avaya Session Border Controller and instructions for configuring the A10 Thunder ADC.

Configuring remote access

About this task

You can use the Avaya SBC for relaying HTTP and HTTPS traffic between Avaya Aura® Device Services enabled application clients (such as the Avaya Workplace Client clients) and Avaya Aura® Device Services. For more information about relay services configuration in Avaya SBC, see *Administering Avaya Session Border Controller*.

Before you begin

- If a reverse proxy or relay is configured to listen on a port other than the default port 443, the **Override port for reverse proxy** setting from the **Front-end host, System Manager and Certificate Configuration** menu must be set to *y* (yes). You must also set a value for the **Front-end port for reverse proxy** parameter.
- HTTPS traffic relay for Avaya Aura® Device Services requires that you configure an external IP address for Avaya SBC.

Note:

To use the remote worker functionality, you must configure one of the following:

- Implement Split-Horizon DNS: Avaya recommends the use of this configuration. This configuration optimizes traffic so that clients connect to Session Manager directly on the internal network and only use Avaya SBC when external.
- Use Public cloud model: All FQDNs or URLs must point to the reverse proxy or Avaya SBC. This configuration is used for cloud deployments and also for on premise deployments. By using this configuration, calls are preserved during any network

transition from Wi-Fi to cellular data when the client IP address can change during an active call.

- Implement for internal access only and all remote devices must use VPN: This configuration is used when a security policy is in place such that all traffic must be either internal or via VPN. The VPN solution that is deployed must have sufficient bandwidth and latency to support the expected volume of VoIP calls.

Procedure

1. In the Avaya SBC, navigate to **Device Specific Settings > Relay Services**.
2. In the **Remote Configuration** field, configure the parameters with the following values:
 - **Remote Domain:** the Avaya Aura® Device Services server domain.
 - **Remote IP:** the IP address of the Avaya Aura® Device Services server.
 - **Remote Port:** the **Front-end port for reverse proxy** configured during the Avaya Aura® Device Services server installation. The default value is 443.
 - **Remote Transport:** TCP.
3. In the **Device Configuration** field, configure the parameters with the following values:
 - **Published Domain:** the Avaya Aura® Device Services server domain.
 - **Listen IP:** the External Avaya SBC IP address created for Avaya Aura® Device Services relay.
 - **Listen Port:** 8443 or 443.
 - **Connect IP:** the internal Avaya SBC IP address.
 - **Listen Transport:** TCP.

A10 Thunder Application Delivery Controller Configuration

Before you configure the A10 Thunder Application Delivery Controller (ADC) for interworking with the Avaya Aura® Device Services, ensure that:

- The A10 Thunder 1030s software version is 2.7.1 P3 or higher.
- You have reviewed the following guides:
 - A10 Networks Apache Web Server deployment guide
 - A10 Thunder Series and AX Series System Configuration and Administration Guide

Importing the A10 Client SSL Certificate

About this task

The following procedure describes how to import the A10 Client SSL Certificate.

Before you begin

Obtain an X509 certificate and the associated private key from a Certificate Authority.

! Important:

To successfully establish the SSL connection with the A10 server, the Avaya Aura® Device Services enabled client must import the root certificate of the CA that you use in your deployment. In an Avaya Aura® environment, this is the System Manager root certificate by default. If you do not use System Manager for certificate management or if you use Avaya Aura® Device Services in an environment without Avaya Aura®, this is the third-party CA root certificate.

Procedure

1. Log in to the ACOS administration interface.
2. In the **Config Mode** tab, select **SLB > SSL Management > Certificate**.
3. Click **Import**.
4. Enter the required information:
 - The name of the certificate file.
 - The source for importing the certificate: local, remote, or text.
 - The certificate file format.
 - The source for importing the Key file: local, remote, or text.
 - The key file format.

*** Note:**

In order for the Split-Horizon DNS to work properly, you must provide the certificate Common Name with a FQDN and not an IP address. The A10 external FQDN must also match the Avaya Aura® Device Services internal FQDN.

5. Click **OK** and then click **Save**.

Importing the A10 Server SSL Certificate**About this task**

The following procedure describes how to import the A10 Server SSL Certificate.

Before you begin

Obtain an X509 certificate and the associated private key from a Certificate Authority.

! Important:

The A10 server will not be able to establish an SSL connection with the backend Avaya Aura® Device Services server if the Server SSL certificate has not been provisioned.

Procedure

1. Log in to the ACOS administration interface.

2. In the Config Mode tab, select **SLB > SSL Management > Certificate**.
3. Click **Import**.
4. Enter the required information:
 - The name of the certificate file.
 - The source for importing the certificate: local, remote, or text.
 - The certificate file format.
 - The source for importing the Key file: local, remote, or text.
 - The key file format.
5. Click **OK** and then click **Save**.

Importing the CA root certificate

About this task

You must import the root certificate of the CA which certificates you use in your deployment into A10. In an Avaya Aura® environment, this is the System Manager root certificate by default. If you do not use System Manager for certificate management or if you use Avaya Aura® Device Services in an environment without Avaya Aura®, this is the third-party CA root certificate.

Before you begin

Obtain a copy of the root certificate from your CA.

For information about obtaining the System Manager root certificate, see the *Administering Avaya Aura® System Manager*.

Procedure

1. Log in to the ACOS administration interface.
2. In the Config Mode tab, select **SLB > SSL Management > Certificate > Import**.
3. Enter the required information:
 - The name of the certificate.
 - The source for importing the certificate.
 - The certificate format.
 - The certificate source.
 - The source for importing the key.
 - The private key source.
4. Click **OK** and then click **Save**.

Creating the A10 server SSL template

About this task

The following procedure describes how to create the A10 Server SSL certificate template.

Procedure

1. Log in to the ACOS administration interface.
2. In the Config Mode tab, select **SLB > Template > SSL > Server SSL**.
3. Click **Add**.
4. Enter the required information:
 - The name of the SSL server.
 - The name of the certificate file.
 - The name of the key file.
 - Pass phrase and pass phrase confirmation.
 - TLS/SSL version.
 - Close notification.
 - Session ticket.
 - SSL forward proxy.
 - The size and time-out of the Session Cache.
 - Server certificate error.
5. Click **OK** and then click **Save**.

Creating the A10 client SSL template

About this task

The following procedure describes how to create the A10 client SSL certificate template.

Procedure

1. Log in to the ACOS administration interface.
2. In the Config Mode tab, select **SLB > Template > SSL > Client SSL**.
3. Click **Add**.
4. Enter the required information:
 - The name of the certificate
 - The chain certificate name
 - The name of the key file
 - Pass phrase and pass phrase confirmation
 - Whether to bypass SSLv2
 - Session cache size and timeout
 - Session ticket lifetime

- SSL false start
 - Whether to reject requests for SSLv3
 - Server name indication
5. Click **OK** and then click **Save**.

Creating an IP source NAT

About this task

The following procedure describes how to import the Avaya Aura® System Manager root certificate into A10.

Before you begin

Obtain a copy of the root certificate from System Manager.

For information about obtaining the System Manager root certificate, see the *Administering Avaya Aura® System Manager*.

Procedure

1. Log in to the ACOS administration interface.
2. In the Config Mode tab, select **IP Source NAT > IPv4 Pool**.
3. Enter the required information:
 - The name of the IPv4 pool.
 - The start IP address.
 - The end IP address.
 - The net mask.
 - The gateway.
 - The HA group.
 - The IP-RR.
 - The source for importing the key.
 - The private key source.
4. Click **OK** and then click **Save**.

Creating the Avaya Aura® Device Services backend server

About this task

The following procedure describes how to create the Avaya Aura® Device Services backend server.

Procedure

1. Log in to the ACOS administration interface.

2. In the Config Mode tab, select **SLB > Service > Server**.
3. Click **Add** twice.
4. Enter the required information:
 - The name of the backend server.
 - The host name or IP address of the backend server.
 - The GSLB external IP address.
 - The IPv6 mapping of GSLB.
 - Weight.
 - Health monitor.
 - Connection limit.
 - Connection resume.
 - Slow start.
 - Spoofing cache.
 - Firewall.
 - Stats data.
 - Extended stats.
 - Server template.
 - HA priority cost.
 - Description.
5. (Optional) Create an alternate server.
6. Expand the **Port** section and configure the connection details for the Avaya Aura® Device Services backend servers.
7. Click **OK** and then click **Save**.

Creating a virtual server

About this task

The following procedure describes how to create a virtual server using the A10 interface.

Procedure

1. Log in to the ACOS administration interface.
2. In the Config Mode tab, select **SLB > Service > Virtual Server**.
3. Click **Add**.
4. Enter the required information:
 - The name of the virtual server.

- The IP address or the CIDR subnet.
 - Enable or disable the virtual server.
 - The condition for disabling the virtual server.
 - Enable or disable the ARP status.
 - Enable or disable the Stats Data.
 - Enable or disable Extended Stats.
 - Flag for redistribution.
 - HA group.
 - Virtual server template.
 - Policy template.
 - Description.
5. Expand the **Port** section and configure the connection details for the virtual server.
 6. Click **OK** and then click **Save**.

Creating a service group

About this task

The following procedure describes how to create a service group using the A10 interface.

Procedure

1. Log in to the ACOS administration interface.
2. In the Config Mode tab, select **SLB > Service > Service Group**.
3. Click **Add**.
4. Enter the required information:
 - The name of the service group.
 - The service group type.
 - The service group algorithm.
 - Enable or disable the Auto Stateless Method.
 - The traffic replication.
 - The health monitor.
 - The server template.
 - The server port template.
 - The policy template.
 - Enable or disable minimum active members.
 - Enable or disable priority affinity.

- Enable sending a client reset when the server selection fails.
 - Enable sending log information for the backup server events.
 - Enable or disable Stats Data.
 - Enable or disable Extended Stats.
 - Priority.
 - Description.
5. Expand the **Server** section and configure the servers of the service group.
 6. Click **OK** and then click **Save**.

Creating a virtual service

About this task

The following procedure describes how to create a virtual service using the A10 interface.

Procedure

1. Log in to the ACOS administration interface.
2. In the Config Mode tab, select **SLB > Service > Virtual Service**.
3. Click **Add**.
4. Enter the required information:
 - The name of the virtual service
 - The virtual service type
 - The virtual service port
 - The virtual service address
5. Click **OK** and then click **Save**.

Configuring A10 for LDAP searches

About this task

The following procedure describes how to perform A10 configuration to enable LDAP searches for clients.

Procedure

1. To create an LDAP backend server, do the following:
 - a. In the ACOS administrative interface, click the **Config Mode** tab.
 - b. Select **SLB > Service > Server**.
 - c. Click **Add** twice.
 - d. In the General section, configure the name and the host or IP address of the LDAP backend server.

- e. In the Port section, configure the port and the weight.
 - f. Click **OK** and then click **Save**.
2. To create a service group, do the following:
 - a. In the ACOS administrative interface, click the **Config Mode** tab.
 - b. Select **SLB > Service > Service Group**.
 - c. Click **Add**.
 - d. In the Service Group section, configure the name of the LDAP service group.
 - e. In the Server section, select the servers to add to the service group.
 - f. Click **OK** and then click **Save**.
3. To create a virtual service, see [Creating a virtual service](#) on page 329.
4. To edit a virtual server, do the following:
 - a. In the ACOS administrative interface, click the **Config Mode** tab.
 - b. Select **SLB > Service > Virtual server**.
 - c. Click **Edit**.
 - d. Edit the configuration of the virtual server.
 - e. Click **OK** and then click **Save**.

Configuring A10 for LDAP authentication

About this task

The following procedure describes how to configure A10 for performing LDAP authentication before the HTTP requests are redirected to the backend Avaya Aura® Device Services server.

Procedure

1. To create an LDAP server, do the following:
 - a. In the ACOS administrative interface, click the **Config Mode** tab.
 - b. Select **Security > Authentication > Server**.
 - c. Click **Add** twice.
 - d. In the General section, configure the connection details for the LDAP server.
 - e. Click **OK** and then click **Save**.
2. To enable HTTP log on, do the following:
 - a. In the ACOS administrative interface, click the **Config Mode** tab.
 - b. Select **Security > Authentication > Logon**.
 - c. Click **Add**.
 - d. Configure the HTTP logon settings.

- e. Click **OK** and then click **Save**.
3. To configure the HTTP relay, do the following:
- a. In the ACOS administrative interface, click the **Config Mode** tab.
 - b. Select **Security > Authentication > Relay**.
 - c. Click **Add**.
 - d. Configure the authentication relay settings.
 - e. Click **OK** and then click **Save**.
4. To create an authentication template, do the following:
- a. In the ACOS administrative interface, click the **Config Mode** tab.
 - b. Select **Security > Authentication > Template**.
 - c. Click **Add**.
 - d. Configure the authentication template.
 - e. Click **OK** and then click **Save**.
5. To edit a virtual service, do the following:
- a. In the ACOS administrative interface, click the **Config Mode** tab.
 - b. Select **SLB > Service > Virtual Service**.
 - c. Click **Edit**.
 - d. Edit the virtual service.
 - e. Click **OK** and then click **Save**.

Chapter 15: Troubleshooting

This section describes troubleshooting issues related to deploying Avaya Aura® Device Services.

Avaya Workspaces Client cannot connect to Avaya Aura® Device Services

Condition

Avaya Workspaces Client is unable to connect to Avaya Aura® Device Services.

The browser displays the following error:

For example,

```
Your connection is not private
Attackers might be trying to steal your information from aads.xyz.avaya.com (for
example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Subject: aads.xyz.avaya.com
Issuer: System Manager CA
Expires on: Nov 14, 2024
Current date: Jul 31, 2023
PEM encoded chain:-----BEGIN CERTIFICATE-----
MIIEvTCCA6WgAwIBAgIULIWE+z6Rgvi68M5o99kcxpm0avMwDQYJKoZIhvcNAQEL
BQAwOzEaMBGGA1UEAwRU3lzdGVtIE1hbmFnZXIgdQ0ExDTALBgNVBAsMBE1HTVQx
```

The browser console logs displays the following error:

For example,

```
GET https://aads.xyz.avaya.com/abc/resources net::ERR_CERT_AUTHORITY_INVALID
GET https://aads.xyz.avaya.com/abc/resources net::ERR_CERT_AUTHORITY_INVALID
```

Cause

Avaya Aura® Device Services is using ID certificates issued by System Manager/ Private/ Third-party CA and this CA certificate is not available out of the box for the browser and it does not trust the System Manager/ Private/ Third-party CA.

Solution

Install Enterprise CA certificate.

For example, System Manager/ Private/ Third-party CA's on the user's machine, where the user is accessing Workspaces in the browser. So that the browser can trust System Manager/ Private/ Third-party CA certificate and can access the Avaya Aura® Device Services APIs for search.

Service unavailable

Condition

Avaya Aura® Device Services is not available and displays a 503 error.

Cause

- Traffic exceeds acceptable limits.

- Avaya Aura® Device Services is not paired to Session Manager.

This option is only applicable if Avaya Aura® Device Services is deployed in an Avaya Aura® environment.

- DRS synchronization is not complete.

This option is only applicable if Avaya Aura® Device Services is deployed in an Avaya Aura® environment.

Solution

1. Wait for traffic to reduce to acceptable limits.

The following options are only applicable if Avaya Aura® Device Services is deployed in an Avaya Aura® environment:

2. Ensure that DRS synchronization is done.

3. Log in to Session Manager and check whether Avaya Aura® Device Services is paired to the Session Manager.

Admin user is not prompted for password in sudo su

Solution

The "90-cloud-init-users" file in /etc/sudoers.d/ gets created by cloud-init and adds the following rule for admin user:

For example, for an admin or administrative user, cloud-init adds the rule `admin ALL=(ALL) NOPASSWD:ALL`.

This file has limited permission. Even the "root" user has read-only access.

To overcome this problem, move "90-cloud-init-users" file to user's home dir.

For example, `mv /etc/sudoers.d/90-cloud-init-users /home/admin/`

Avaya Workplace Client cannot connect to Avaya Aura® Device Services

Condition

Avaya Workplace Client is unable to connect to Avaya Aura® Device Services to complete the mutual authentication for client identity certificates.

Cause

On Avaya Aura® Device Services, on the HTTPS Clients screen, the administrator has set the Client-Device Certificate Policy as Required.

Solution

On the HTTP Clients screen, the administrator must set the Client-Device Certificate Policy as None.

Avaya Aura® Device Services installation fails if the DNS forward and reverse lookup zones are not configured properly

Cause

The DNS reverse lookup zone for Session Manager is not configured properly.

This is only applicable if Avaya Aura® Device Services is deployed in an Avaya Aura® environment.

Solution

1. Check the DNS forward and reverse lookup zone.
2. Verify the System Manager enrollment password.

Avaya Aura® Device Services installation or upgrade fails due to invalid System Manager certificates

Condition

In an Avaya Aura® environment, Avaya Aura® Device Services installation or upgrade fails due to invalid System Manager certificates.

Cause

During the installation or upgrade process, Avaya Aura® Device Services connects to System Manager to obtain certificates required for installation. If the System Manager certificates contain

unsupported critical extensions, expired, or the certificate start date is in the future, Avaya Aura® Device Services does not import these certificates and stops the installation or upgrade process.

Solution

Contact the System Manager administrator.

Avaya Aura® Device Services installation fails if third-party certificates are used on other Avaya Aura® elements

Condition

Avaya Aura® Device Services installation fails when both of the following conditions are met:

- Third-party CA-signed certificates are used on other Avaya Aura® components, such as System Manager or Session Manager.
- Avaya Aura® Device Services uses certificates generated by System Manager.

This issue is only applicable for deployments without Avaya Aura®.

Cause

If Avaya Aura® elements use third-party certificates, Avaya Aura® Device Services does not receive the third-party trust chain from System Manager during Avaya Aura® Device Services installation.

Solution

See the Product Support Notice (PSN) at <https://downloads.avaya.com/css/P8/documents/101051932>.

Avaya Aura® Device Services installation fails when using third-party CA identity certificates

Condition

In an Avaya Aura® environment, Avaya Aura® Device Services installation fails if you use identity certificates signed by a third-party CA. The installation log contains entries related to issues with:

- Certificate validation. For example:

```
Invalid format :Not able to validate certificateInappropriate
certificate data
Failed to import certificate.
```

- DRS service. For example:

```
Executing # Sending registration information to DRS master
ERROR # 1 : Sending registration information to DRS master.
Terminating configuration process .....
```



```
/opt/Avaya/DeviceServices/10.2.0.0.70/drs/8.1.3.5.0-38243-  
SDK-1.0/bin/start_aggregation.sh failed with exit  
code: 1, exiting...
```

Cause

Starting from Release 10.1.1, if you use identity certificates signed by a third-party CA, the Avaya Aura® Device Services truststore does not contain System Manager CA certificates. If you use identity certificates signed by a third-party CA, ensure that System Manager also uses an identity certificate signed by the same CA.

Solution

Ensure that System Manager uses an identity certificate signed by the same CA that signs the Avaya Aura® Device Services identity certificates as described in [Configuring third-party identity certificates for System Manager](#) on page 44.

app commands do not work after a failed installation

Condition

After a failed or incomplete installation, **app** commands, such as **app uninstall** or **app configure**, do not work.

Cause

app is an alias command that provides a convenient way to run commonly used application-specific commands. Avaya Aura® Device Services sets up aliases, including **app**, during installation. If the installation process fails, aliases are not set up properly, so you cannot use them.

Solution

Reinstall the Avaya Aura® Device Services application.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following commands to uninstall Avaya Aura® Device Services:

```
cd /opt/Avaya/DeviceServices/<version>/CAS/<version>/uninstaller/  
sudo ./uninstallAADS.sh
```

3. Install Avaya Aura® Device Services.

Related links

[Installing Avaya Aura Device Services](#) on page 179

[Aliases](#) on page 57

[app commands](#) on page 57

DNS entries disappear from the `/etc/resolv.conf` file after restarting Avaya Aura® Device Services

Condition

DNS entries disappear from the `/etc/resolv.conf` after restarting Avaya Aura® Device Services.

Cause

The NetworkManager service controls the content of the `/etc/resolv.conf` file. This service automatically changes the content of the file to the “default” state when Avaya Aura® Device Services is restarted.

Solution

1. Open the `/etc/NetworkManager/NetworkManager.conf` file in a text editor.

For example: `vi /etc/NetworkManager/NetworkManager.conf`

2. Navigate to the `[main]` section in the file and do one of the following:

- If the `[main]` section contains an entry starting with `dns`, replace this entry with the `dns=none` entry.
- If the `[main]` section does not contain an entry starting with `dns`, add the `dns=none` entry to the `[main]` section.

For example:

```
[main]
dns=none
```

3. Save the file.
4. Run the following command to restart the NetworkManager service:

```
systemctl restart NetworkManager
```

runUserDiagnostics tool

The **runUserDiagnostics** tool is used with the `clitool-acs.sh` tool for collecting and dumping user and contact-related information.

You can run the command for a user by:

- specifying the user’s email ID
- specifying a filename that contains comma separated email IDs of more than one user

The tool generates an excel file for each user. The file name contains the email address of the user to distinguish the file name for each user.

Syntax

```
sudo ./clitool-acs.sh runUserDiagnostics [-e email_address] [-f
<absolute_filepath><filename>] [-d <email_address>] [-a]
```

e	Creates an excel file in /opt/Avaya/ directory that contains contact-related information for the email ID specified
f	Creates excel files in /opt/Avaya/ directory that contains contact-related information for each email ID specified in the text file
d	Deregisters a registered user and removes all user related data from Avaya Aura® Device Services
a	Creates an excel file in /opt/Avaya/ directory that contains the number of contacts in Session Manager and Avaya Aura® Device Services for all registered Avaya Aura® Device Services users
email_address	Email address of a user
filename	Filename containing comma separated email IDs. The file must be accessible from the misc directory for clitool and stored under opt/Avaya or a sub-directory.
absolute_filepath	Absolute filepath of the directory where the filename containing comma separated email IDs is stored.

Example

The following examples show how the runUserDiagnostics tool can be used with the available features.

```
sudo ./clitool-acs.sh runUserDiagnostics -e email1@domain.com
```

Creates an output file for containing contact related information for email1@domain.com.

```
sudo ./clitool-acs.sh runUserDiagnostics -f /opt/Avaya/filelist.txt
```

Creates output files containing contact related information for every email specified in /opt/Avaya/filelist.txt.

```
sudo ./clitool-acs.sh runUserDiagnostics -d email1@domain.com
```

Deregisters email1@domain.com and removes all data related to this user from Avaya Aura® Device Services.

```
sudo ./clitool-acs.sh runUserDiagnostics -a
```

Checks the number of contacts in Session Manager and Avaya Aura® Device Services for all registered Avaya Aura® Device Services users and creates a file opt/Avaya/Contacts.xls.

Files

The following files are associated with the runUserDiagnostics tool:

- opt/Avaya/DeviceServices/version/CAS/version/misc/clitool-acs.sh
- /opt/Avaya/Contact.xls

Data on Cassandra is corrupted

Condition

Data on Cassandra is corrupted.

Solution

Uninstall Avaya Aura® Device Services and reinstall again.

Primary System Manager fails

Condition

The primary System Manager fails. Geographic redundancy is enabled in System Manager.

Cause

Avaya Aura® Device Services does not support the System Manager geographic redundancy mode. Therefore, Avaya Aura® Device Services cannot switch to the secondary System Manager automatically.

Solution

If the primary System Manager fails and you need to use Avaya Aura® Device Services before it is restored, perform the following steps to enroll Avaya Aura® Device Services against the secondary System Manager. In a cluster environment, perform these steps on each cluster node.

Important:

After the primary System Manager is back online, you must re-enroll against the primary System Manager.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the `app configure` command.
3. Select **Front-end host, System Manager and Certificate Configuration**.
4. Select **System Manager FQDN** and provide the FQDN of the secondary System Manager.
5. Select **System Manager Enrollment Password** and provide the enrollment password of the secondary System Manager.
6. Click **Apply**.
7. When the primary System Manager is back online, repeat this procedure and provide the FQDN and the enrollment password of the primary System Manager.

Open LDAP replication fails

Condition

Open LDAP replication fails. The `/var/log/Avaya/openldap/openldap.log` file contains entries such as the following:

- Server unwilling to perform
- ldap bind failed
- syncrepl: consumer state is newer than provider

Solution

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
sudo systemctl restart slapd
```

3. Repeat the steps above on all remaining nodes in the cluster.
4. Review the `/var/log/Avaya/openldap/openldap.log` file and ensure that it does not contain any error messages.

If the `/var/log/Avaya/openldap/openldap.log` file still contains error messages, do the following:

5. On all nodes in the cluster, run the following commands:

```
cdto openldap  
sudo ./recover_openldap.sh
```

6. Enable Open LDAP replication again.

Related links

[Enabling Open LDAP replication](#) on page 255

Open LDAP replication fails if Avaya Aura® Device Services uses a custom identity certificate for server interfaces

Condition

When you use a custom identity certificate for an Avaya Aura® Device Services service interface, Open LDAP replication might fail. The `/var/log/Avaya/openldap/openldap.log` file contains the `TLS negotiation failure` entry.

Cause

The custom identity certificate is applied to a single node and not to the entire cluster.

Solution

Re-import the custom certificate as described in “Managing server interface certificates” in *Administering Avaya Aura® Device Services*. Ensure that you select **Apply For Cluster** when importing the certificate.

Avaya Workplace Soft Clients are logging out due to a mismatch in the ETAG

Condition

Avaya Workplace Soft Clients are logging out due to mismatch in ETAG.

Cause

This issue is due to a lack of ability to copy a settings file around to all Utility servers on AADS with matching modified timestamps for that file down to the nanosecond (9 digits past the decimal point). The `copy -p` function does not include even milliseconds (3 digits).

Solution

If the settings files is copied to Utility servers individually, that same settings file will have different modified timestamps. To ensure that the web server ETags are generated identically for the files, it is important that the file timestamps match to the millisecond across all nodes.

1. Upload the settings file on the seed node.
2. Check the timestamp on the seed node using the command line.

```
stat -c '%y' 46xxSettings.txt
```

3. Copy the same file to the non-seed nodes using a root user (use the `-p` option (preserve) or `--preserve=mode, ownership, timestamps` when copying the files)

```
scp -p user@<seed node IP>:/var/www/html/custom/46xxSettings.txt  
user@<non-seed node IP>:/var/www/html/custom/
```

4. Compare the timestamps of the file of seed node and non-seed node. If they are different, delete the file from the seed node and copy it back from the non-seed node.

The timestamps should match now.

```
rm 46xxSettings.txt
```

```
scp -p user@<non-seed node IP>:/var/www/html/custom/  
46xxSettings.txt user@<seed node IP>:/var/www/html/custom/
```

Chapter 16: Resources

Documentation

The following table lists related documentation. All Avaya documentation is available at <https://support.avaya.com>. Many documents are also available at <https://documentation.avaya.com/>.

Title	Use this document to:	Audience
Implementing		
<i>Deploying Avaya Aura® Device Services</i>	Deploy Avaya Aura® Device Services.	Sales engineers, solution architects, implementation engineers, support personnel
<i>Deploying Avaya Aura® Session Manager</i>	Deploy the Session Manager OVA.	Sales engineers, solution architects, implementation engineers, support personnel
Administering		
<i>Administering Avaya Aura® Device Services</i>	Administer Avaya Aura® Device Services.	System administrators, support personnel
<i>Administering Avaya Aura® Session Manager</i>	Administer the Session Manager interface.	System administrators, support personnel
<i>Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows</i>	Perform system planning and configuration for: • Avaya Workplace Client for Android • Avaya Workplace Client for iOS • Avaya Workplace Client for Mac • Avaya Workplace Client for Windows	System administrators, support personnel
<i>Using Avaya Spaces</i>	Administer Avaya Spaces.	System administrators, support personnel
Using		

Title	Use this document to:	Audience
<i>Using Avaya Device Enrollment Services to Manage Endpoints</i>	Use Device Enrollment Services to manage endpoints or devices.	Non-Avaya users, such as service providers and resellers
Other		
<i>Avaya Aura® Device Services Data Privacy Controls Addendum</i>	Understand how Avaya Aura® Device Services processes user's personal data.	Customers, service providers, system administrators, support personnel
<i>Port Matrix for Avaya Aura® Device Services</i>	Understand ports for Avaya Aura® Device Services.	Solution architects, implementation engineers, system administrators, support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

You can select multiple items in each filter category. For example, you can select a product and multiple user roles.

- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** () to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** () to add a topic to your watchlist so you are notified when the content is updated or removed.

- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
- Unwatch the selected content or all topics.
- Send feedback for a topic.

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.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: Avaya Aura® Device Services certificate configuration

The Avaya Aura® Device Services server has multiple options for certificate management, which include:

- Importing local or public certificates.
- Importing local certificates that are signed by an intermediate Certificate Authority.
- Viewing the details for a certificate.

The following sections outline the manual command line and configuration utility processes for setting up certificates during the Avaya Aura® Device Services installation process. After you import a certificate, you must restart Avaya Aura® Device Services for the changes to take effect.

You can also manage and update certificates using the Avaya Aura® Device Services web administration portal. For more information about working with the web administration portal, see *Administering Avaya Aura® Device Services*.

Important:

The web administration portal is the preferred method for managing certificates. Use the configuration utility process to configure certificates for troubleshooting purposes, but after this is done, perform certificate management from the web administration portal when possible.

For information about managing the Avaya Aura® Device Services root certificate and for managing identity certificates, see *Administering Avaya Aura® System Manager*.

If you do not use Avaya Aura® System Manager certificates, the Avaya Aura® Device Services server requires four PEM certificates and their corresponding key files:

- The REST interface certificate is used for the communication with the clients.
- The OAMP interface certificate is used for the OAMP GUI.
- The node certificate is used for internode communication such as cluster notifications. The node certificate is also used for encrypting database traffic.

Avaya Aura® Device Services supports PKCS12-format certificates. The signing authority certificate file is also required.

! Important:

- All certificates must contain Subject Alternate Names for the FQDN of the Avaya Aura® Device Services server and the FQDN of the local Avaya Aura® Device Services node.
- The Common Name of the Node certificate must contain the FQDN of the local Avaya Aura® Device Services node. In a cluster, every Avaya Aura® Device Services node has a different FQDN.

Command for viewing certificate details

You can view certificate details by running `displayCertificate.sh` from the `misc` directory.

```
sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/displayCertificates.sh
<cert-type>
```

You can enter one of the following `<cert-type>` values:

- oam
- rest
- lync
- node
- ca
- licensing
- ldap
- psng

Example

The following is an example output of the command:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4043459183551203610 (0x381d40b44b5c491a)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: CN=System Manager CA, OU=MGMT, O=AVAYA
    Validity
      Not Before: Jun 24 12:49:18 2016 GMT
      Not After : Jun 24 12:49:18 2018 GMT
    Subject: CN=AWSDev-14.cnda.avaya.com, O=Avaya, C=US
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (1024 bit)
      Modulus:
        00:96:48:38:bb:64:aa:86:86:79:9a:ab:b5:a5:58:
        c7:d7:9a:ee:ee:c3:39:f9:47:1a:9b:d4:f0:f9:5b:
        02:c6:92:5d:aa:73:43:d2:c8:f6:e6:af:1a:77:91:
        6d:0d:d9:0a:f8:17:64:4c:be:7c:18:e3:56:60:fa:
        ec:b0:fb:75:38:b9:96:f1:78:8d:99:12:9a:2b:38:
        e8:9c:f9:75:d2:2a:8d:63:83:d3:72:b7:6f:78:d8:
```

```

3d:b7:48:a8:90:ec:5d:c3:67:68:11:69:d2:0a:ff:
48:be:b8:6f:35:3a:b6:ed:d8:63:9e:0e:6e:c1:58:
5b:87:5e:78:5e:7c:a3:8e:8d
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Alternative Name:
    DNS:AWSDev-14.cnda.avaya.com
  X509v3 Basic Constraints: critical
    CA:FALSE
  X509v3 Authority Key Identifier:
    keyid:03:1B:17:D2:B9:C7:0B:78:45:51:56:86:F1:4A:48:1A:3D:00:D4:D0

  X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
  X509v3 Subject Key Identifier:
    58:EF:09:4E:87:03:89:FC:49:A4:58:DD:9F:3C:21:0A:46:BC:52:7E
  X509v3 Key Usage: critical
    Digital Signature, Non Repudiation, Key Encipherment, Data
Encipherment, Key Agreement
  Signature Algorithm: sha1WithRSAEncryption
    89:ed:f3:6d:59:67:5f:38:a1:77:ee:50:15:20:a8:2f:f3:e3:
    39:7e:ff:2d:4a:7d:48:8e:c8:2d:f1:ac:f0:0c:f0:26:a4:c8:
    e8:09:e6:a5:e1:c8:56:9d:a8:35:b1:40:4d:a0:d2:04:91:b6:
    dd:f8:67:27:c2:bc:b8:01:96:45:29:28:0b:5b:8c:7b:e5:b7:
    7a:e2:e3:50:88:b9:c9:f2:d7:0f:77:0f:2c:7e:16:02:25:2e:
    1e:e1:dc:2b:cf:ca:8f:25:cb:73:65:d5:f6:52:b9:d3:67:8f:
    f6:e5:9f:49:7a:58:20:87:90:af:64:8a:2a:d4:46:95:ed:ea:
    aa:b2:f2:6a:a1:be:46:98:c2:b0:e6:bf:89:41:6b:e5:63:a2:
    5b:d9:ec:48:47:4f:dd:84:cd:cb:da:9a:5a:ec:12:4c:84:25:
    6a:dd:31:90:64:03:cd:e3:5e:50:25:0a:6a:ab:77:5c:69:c3:
    c2:86:62:bd:38:41:31:3a:73:14:77:1f:f0:e8:92:06:39:36:
    5b:49:cc:a5:4b:24:60:68:0c:b4:86:51:cf:49:bf:8e:d5:f1:
    ca:7f:15:4e:e4:b4:ff:df:2e:11:cd:5c:57:9a:df:78:c0:b1:
    03:12:50:5c:a2:1b:51:1f:18:50:7e:e3:bb:af:a3:28:db:01:
    fe:43:b6:1b
SHA1 Fingerprint=DB:3E:FB:84:80:76:74:DC:25:E4:93:85:CE:D6:84:4F:B6:71:DB:33

```

Importing the Avaya Aura® System Manager trusted certificate

About this task

If you use Avaya Aura® System Manager for certificate management, you must configure the System Manager connection details, enable using System Manager for certificate management, and enter the enrollment password.

The following procedure describes how to configure the Avaya Aura® Device Services server for certificate management using Avaya Aura® System Manager.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **Front-end host, System Manager and Certificate Configuration**.
3. Set **Use System Manager** to `y` (yes).

4. Configure the System Manager connection details:
 - **System Manager FQDN**
 - **System Manager HTTPS Port** or the **Front-end port for reverse proxy**, if applicable

To configure the reverse proxy port number, you must first set the **Override port for reverse proxy** setting to *y* (yes).
 5. Configure the **System Manager Enrollment Password** and **Keystore password** options.
- These options are used for adding the certificates to the trust store of the client applications.
6. After you finish configuring the Avaya Aura® Device Services server, check the configuration utility log files to ensure that the System Manager configuration was made successfully.
 7. Restart Avaya Aura® Device Services after adding certificates for the changes to take effect.

Importing third-party CA-signed certificates

About this task

If you do not use Avaya Aura® System Manager for certificate management, Avaya Aura® Device Services enables you to use certificates specific to your organization and have the certificates signed by a local or public certificate authority (CA).

The following procedure describes how to import third-party certificate files and corresponding key files using the configuration utility.

Before you begin

Import third-party root and all intermediate CAs into the following trust stores in order:

- The trust stores of each server that interacts with Avaya Aura® Device Services in your deployment, including System Manager, Session Manager, Avaya Aura® Session Border Controller, and Avaya Meetings Management servers.
- The Avaya Aura® Device Services trust store. This is required for intra-cluster communications where the Avaya Aura® Device Services identity certificate is presented to other servers within the cluster.

Important:

You must perform the importing in order. Otherwise, a loss of service can occur because Avaya Aura® Device Services cannot communicate with some or all of the mentioned servers.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.

2. Select **Front-end host, System Manager and Certificate Configuration** and do one of the following:
 - If you use Avaya Aura® Device Services in an Avaya Aura® environment, continue from step 3.
 - If you use Avaya Aura® Device Services in an environment without Avaya Aura®, continue from step 6.

3. Configure the System Manager connection details:

- **System Manager FQDN**
- **System Manager HTTPS Port** or the **Front-end port for reverse proxy**, if applicable

To configure the reverse proxy port number, you must first set the **Override port for reverse proxy** setting to *y* (yes).

4. Configure the **System Manager Enrollment Password** option.

The System Manager enrollment password is used for adding the certificates to the trust store of the client applications.

5. Set **Use System Manager** to *n* (no).

The menu displays options for importing individual certificate files and the corresponding key files.

6. Configure the following options to provide the paths to the certificate and key files:

- REST interface key file
- REST interface certificate file
- OAM interface key file
- OAM interface certificate file
- node key file
- node certificate file
- signing authority certificate file

The certificate and the corresponding key file must be present on the server when they are imported. If one pair of files is not imported because one or both files are missing, the other files may still be imported so that you can selectively replace individual certificates. To generate certificates, you can also use Avaya Aura® System Manager and replace individual certificates, such as the front-end certificates.

7. Configure the **Keystore password** option.

This password is used for adding the certificates to the trust store of the client applications. The role of the keystore password is similar to the role of the Avaya Aura® System Manager enrollment password in the configurations that use the Avaya Aura® System Manager root certificate.

8. Restart Avaya Aura® Device Services and check the configuration utility log files to ensure that the certificates were imported successfully.

Importing intermediate CA certificates

About this task

In some deployments where certificates are imported rather than generated by Avaya Aura® System Manager, server certificates are signed by an intermediate Certificate Authority (CA) rather than a root CA. To use the certificates, a chain of trust is required: The root CA signs the intermediate CA certificate, and the intermediate CA signs the server certificate.

To create a certificate chain, you must concatenate the PEM-format certificate files for the server and the intermediate CA so that the server certificate is first.

! Important:

The node and back-end certificates do not support intermediate CAs, and importing certificate chains for those certificates fails.

The following procedure describes how to concatenate the PEM-format certificate files and import the files using the configuration utility.

Procedure

1. Copy the server certificate file to a new file for concatenation.

For example:

```
cp server.crt certificate-chain.crt
```

2. Concatenate the intermediate certificate file to the file created in the previous step.

For example:

```
cat intermediateca.crt >> certificate-chain.crt
```

3. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
4. Select **Front-end host, System Manager and Certificate Configuration** and do one of the following:
 - If you use Avaya Aura® Device Services in Avaya Aura® environment, continue from step [5](#) on page 352.
 - If you use Avaya Aura® Device Services in an environment without Avaya Aura®, continue from step [8](#) on page 353.
5. Configure the System Manager connection details:
 - **System Manager FQDN**
 - **System Manager HTTPS Port** or the **Front-end port for reverse proxy**, if applicable

To configure the reverse proxy port number, you must first set the **Override port for reverse proxy** setting to `y` (yes).
6. Configure the **System Manager Enrollment Password** option.

The System Manager enrollment password is used for adding the certificates to the trust store of the client applications.

7. Set **Use System Manager** to **n** (no).

The menu displays options for importing individual certificate files.

8. Select one of the following options to provide the path to the concatenated certificate file:

- **REST interface certificate file**
- **OAM interface certificate file**

9. Import the key file of the certificate using the corresponding menu option:

- **REST interface key file**
- **OAM interface key file**

The key file does not require alteration. Import the key file as if you are importing individual certificates.

10. Configure the **Keystore password** option.

This password is used for adding the certificates to the trust store of the client applications. The role of the keystore password is similar to the role of the Avaya Aura® System Manager enrollment password in the configurations that use the Avaya Aura® System Manager root certificate.

11. Restart Avaya Aura® Device Services and check the configuration utility log files to ensure that the certificates were imported successfully.

Generating Certificate Signing Requests

About this task

Use this procedure to generate a Certificate Signing Request (CSR).

Important:

You must use this procedure if you are not using System Manager as the only Certificate Authority (CA) to sign certificates for all solution components.

Before you begin

Ensure that Avaya Aura® Device Services is successfully installed with System Manager signed certificates. This is the default setting for installation.

Procedure

1. Run the following command:

```
mkdir /tmp/AADSPortalCerts
chmod 770 /tmp/AADSPortalCerts
```

The system creates an `AADSPortalCerts` directory in `/tmp/` for the output of the script that will generate the CSRs.

2. Run the following command to navigate to the directory containing the script:

```
cdto misc
```

3. To generate a CSR, run the following command:

```
sudo ./createCSR.sh /tmp/AADSportalCerts frontEndFQDN localFQDN organizationName  
organizationUnit locality stateOrProvince countryCode emailAddress
```

 Important:

This command is a single Linux command and must be entered as a single line even if it appears as several lines in the document.

The parameters for this script are:

- **frontEndFQDN:** For a cluster installation, this is the FQDN of the Virtual IP or external load balancer. For simple, non-clustered installations, this is the FQDN of the server where Avaya Aura® Device Services is installed.
 - **localFQDN:** The FQDN of the server.
 - **organizationName:** The name of the organization.
 - **organizationUnit:** The name of the unit or sub-organization. For example, “Design”.
 - **locality:** The name of the city or town.
 - **state:** The two-digit state or province code.
 - **countryCode:** The two-digit country code.
 - **emailAddress:** The administrator email address.
4. Verify that `/tmp/AADSportalCerts` contains the `.key` and `.csr` files for front-end, node, OAMP, and LYNC.

Creating a Certificate Signing Request (CSR) using OpenSSL

About this task

Use this procedure to generate a CSR using OpenSSL.

You can also generate a CSR using the Avaya Aura® Device Services web administration portal.

Before you begin

Ensure that you have the OpenSSL utility.

Procedure

1. Create an OpenSSL configuration file.

For example:

```
[ req ]  
req_extensions = v3_req
```

```
distinguished_name = req_distinguished_name

[req_distinguished_name]

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = dnsserver10927.company.com
DNS.2 = dnsserver10938.company.com
DNS.3 = dnsserver10955.company.com
```

The `alt_names` section defines the Subject Alternative Names list and must contain FQDNs of all nodes in the cluster. For Open LDAP, the `alt_names` section must also contain the `localhost.localdomain` and, for IPv6, `localhost6.localdomain` records.

2. Run the following command:

```
openssl req -out <CSR_request_file>.csr -newkey rsa:2048 -nodes -keyout
<CSR_key_file>.key -config <configuration_file>
```

In this command:

- `<CSR_request_file>.csr` specifies a CSR file name.
- `<CSR_key_file>.key` specifies a file containing a private key that is used to add the signed certificate to the system.
- `<configuration_file>` specifies the OpenSSL configuration file that was created in the previous step.

For example:

```
openssl req -out createCSR.csr -newkey rsa:2048 -nodes -keyout keyCSR.key -config
configCSR.config
```

Signing identity certificates for Avaya Aura® Device Services using third-party CA certificates

About this task

You can use the following procedure to sign identity certificates for Avaya Aura® Device Services using third-party CA certificates.

* Note:

In the following procedure, the third-party CA certificate can be a public CA or an internal private CA.

Before you begin

- Create a CSR with the following X509 extensions:
 - keyUsage = nonRepudiation, digitalSignature, keyEncipherment
 - extendedKeyUsage = serverAuth, clientAuth
- Ensure that the CSR contains the following:
 - If the certificate is only used on the Avaya SBC, the request contains the subjectAltName extension that lists the cluster FQDN in the SAN.
 - If the certificate is used on both Avaya SBC and the Avaya Aura® Device Services server, the request contains the subjectAltName extension that lists the cluster FQDN as well as the FQDN of each cluster member in the SAN. For OpenLDAP, the subjectAltName extension must also include the `localhost.localdomain` and, for IPv6, `localhost6.localdomain` records.

Note:

From the security perspective, Avaya recommends that you generate separate certificates for each node, including the cluster FQDN and the individual cluster node FQDN in subjectAltName.

- Do *not* provide the password for a key because password protected keys are not supported.
- Ensure that the key generated along with the CSR is stored safely.
- Ensure that once the certificate is generated, you have received the identity certificate, root CA certificate, and all intermediate CA certificates in the `.PEM` format from the certification authority. If these certificates are not in the `.PEM` format, you can convert these certificates using the OpenSSL tool.
- Generate the identity certificate chain.
- If you use System Manager certificates in your deployment, obtain the System Manager root CA certificate.
- Generate the trust certificate chain by concatenating the following certificates into a `trustchain.PEM` file:
 - All intermediate CA certificates.
 - The root CA certificate.
 - The System Manager root CA certificate.

Note:

The System Manager root CA certificate is *not* required for deployments without Avaya Aura®.

Procedure

1. Log on to Avaya Aura® Device Services using your SSH credentials.
2. If you are using reverse proxy on the Avaya SBC to Avaya Aura® Device Services, import the intermediate CA certificate and the root CA certificate to the Avaya SBC trust store.
3. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.

4. Do the following to import intermediate CA certificates to Avaya Aura® Device Services:
 - a. Select **Add a Certificate to the TrustStore**.
 - b. Click **Select**.
 - c. Enter the path to the certificate file and then click **OK**.
 - d. Click **Apply** to import the certificate.
 - e. Repeat these steps for all intermediate CA certificates.

Avaya Aura® Device Services does not import a certificate into the truststore if the certificate has unsupported critical extensions, expired, or if the certificate start date is in the future.

5. Click **Front-end host, System Manager and Certificate Configuration**.
6. Click **Use System Manager for Certificates** and type `n` to not use System Manager for certificates.
7. Click **REST Interface certificate configuration**. If the certificate is not in the PKCS12 format, type `n` on the REST Interface certificate configuration screen.
8. Add the key file to the REST interface PEM key file and the certificate chain to the REST interface PEM certificate file.
9. Click **Signing authority certificate configuration** on the Front-end host, System Manager and Certificate Configuration screen.
10. If the CA root certificate is not in the PKCS12 format, type `n`.
11. Click **Signing Authority PEM certificate file** and add the `trustchain.PEM` trust certificate chain that you have created.
12. Click **Return to previous menu**.
13. Click **Apply**.

Configuring System Manager to trust third-party root CA certificates

About this task

This procedure is not applicable for deployments without Avaya Aura®.

Procedure

1. Log on to the System Manager web console.
2. Click **Home > Services > Inventory > Manage Elements**.
3. Select System Manager from the **Elements**.
4. Click **Configure Trusted Certificates** in the **More Actions** list.

5. Click **Add** and select **Import from file**.
6. Click **Choose File** and browse to the third-party root CA certificate.
7. Click **Commit**.
8. Restart the System Manager JBOSS™ process.

From the SSH session on the System Manager, run the following command as a root user:

```
service jboss restart
```

 Note:

The `service jboss restart` command affects the service for the System Manager.

Viewing the current CA used to sign the Session Manager certificate

About this task

This procedure is not applicable for deployments without Avaya Aura®.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory > Manage Elements**.
2. Select the primary Session Manager from the list, and click **More Actions**.
3. Click **Configure Identity Certificates**.
4. Click **Security Module HTTPS**.

The system displays the Certificate details. In the **Issuer Name** field, you can view which CA issued the certificate.

Importing SIP CA certificate to the Avaya Aura® Device Services trust store

About this task

Before release 6.3.8, Session Manager used the default SIP CA to sign the certificate used by PPM HTTP. After release 6.3.8, the System Manager CA is used. You must manually import SIP CA certificate to the Avaya Aura® Device Services trust store if you had Session Manager 6.3.8 or earlier, and upgraded to a later release.

This procedure is not applicable for deployments without Avaya Aura®.

Procedure

1. Log in to the Avaya Aura® Device Services server.
2. Type `sudo keytool -importcert -file <CA_Certificate>.cer -keystore /opt/Avaya/DeviceServices/<version>/CAS/<version>/cert/ssl-ts.jks -alias "CA_alias"`

Here, *CA_Certificate* is the name of the CA certificate file in PEM or DER format. *CA_alias* is the alias you want to assign this certificate

LDAP certificates

By default, Avaya Aura® Device Services uses an unsecured LDAP connection. For secure connectivity, you must import an LDAP certificate file to the Tomcat trust store.

You can import the certificate using the configuration utility or the web administration portal. This section describes the configuration utility procedure. For information about importing the certificate from the web administration portal, see *Administering Avaya Aura® Device Services*.

Importing a trusted LDAP certificate

About this task

Use this procedure to import the LDAP certificate to enable secure LDAP.

You cannot import a certificate if:

- The certificate contains an unsupported critical extension.
- The certificate expired.
- The start date of the certificate is in the future.

Avaya Aura® Device Services displays a warning message if a certificate cannot be imported.

Procedure

1. Log in to Avaya Aura® Device Services as the administrative user.
You must use the administrative user defined during the OVA deployment.
2. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
3. In the Avaya Aura Device Services Configuration Utility dialog box, navigate to **LDAP Configuration** and click **Select**.
4. On the LDAP Configuration page, select **Import Secure LDAP trusted certificate** and click **Select**.

*** Note:**

To use secure LDAP, you must first import a secured and trusted LDAP certificate. This helps to validate the connection with a secure LDAP.

5. On the Import Secure LDAP trusted certificate page, select **Certificate file** and click **Select**.

The system displays a page to specify the path to the certificate.

6. In the text box, type the full path and file name of the LDAP trusted certificate.

The file must be in the .pem or .der format.

7. Ensure that the URL of the secured LDAP Server is: `ldaps://<LDAP server FQDN>:<SECURE_PORT>`.

In this URL, *LDAP server FQDN* is the FQDN of the LDAP server and *SECURE_PORT* is 3269.

8. Click **Apply** to save and apply the LDAP configuration settings.

Configuring the client certificate policy using the command line interface

About this task

You can configure client certificates to establish a secure connection. As per your requirement, you can choose how the server validates certificates for Avaya Aura® Device Services clients. Changing the certificate setting might affect the client's ability to connect to Avaya Aura® Device Services.

Use this procedure if you accidentally changed the administrator interface (OAMP) client certificate policy and are no longer able to access the system interface. To change the certificate, you must access the Avaya Aura® Device Services seed node. Use this procedure to change the setting through the command line interface (CLI).

Procedure

1. On the SSH terminal, log in as an administrator.
2. Run one of the following commands:

- To change the setting to **None**:

```
sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-acs.sh
clientCertificateVerificationConfig oampGuiClient off
```

- To change the setting to **Optional**:

```
sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-acs.sh
clientCertificateVerificationConfig oampGuiClient optional
```

- To change the setting to **Required**:

```
sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-acs.sh
clientCertificateVerificationConfig oampGuiClient on
```

After you run the appropriate command, it will take several minutes for the changes to take effect.

Uploading and hosting CA certificate files on Avaya Aura® Device Services server

About this task

Use this procedure to upload CA certificate files to host on Avaya Aura® Device Services server.

Procedure

1. Upload CA certificate files to Avaya Aura® Device Services to the `/home/admin/` directory.
2. Run the following commands to transfer the CA certificate files to the `/opt/Avaya/DeviceServices/ClientInstallers` directory:

```
cdto misc
sudo ./copyCertsIntoClientInstallers.sh /home/admin/<CA_CERTIFICATE_NAME>
```

In this command, `<CA_CERTIFICATE_NAME>` is the name of the CA certificate or certificates that you uploaded in the previous step.

3. To verify that the certificate download link is valid, open the following URL in the web browser:

```
https://<AADS_SERVER_ADDRESS>/acs/resources/webdeployment/
downloads/<certificate-file>
```

In this command, `AADS_SERVER_ADDRESS` is the Avaya Aura® Device Services front-end FQDN or virtual IP address.

* Note:

You can combine all the CA certificate files into a single file or set the autoconfiguration setting `SET TRUSTCERTS` to the following:

```
SET TRUSTCERTS https://
<aads-server-fqdn>:8443/acs/resources/webdeployment/downloads/
cert1.crt,https://<aads-server-fqdn>:8443/acs/resources/
webdeployment/downloads/cert2.crt, https://<aads-server-
fqdn>:8443/acs/resources/webdeployment/downloads/cert23.crt.
```

Setting up a TLS link for Avaya Scopia® Management

About this task

Avaya Scopia® certificates are signed by VeriSign. Avaya Aura® Device Services certificates can be signed by System Manager or a third-party CA that you use in your deployment. Therefore, because Avaya Scopia® and Avaya Aura® Device Services uses certificates signed by different CAs, TLS links are not established until you import both CA certificates to Avaya Aura® Device Services.

Procedure

1. Log in to Avaya Aura® Device Services by using SSH.
2. Import Avaya Scopia® CAs to the Avaya Aura® Device Services truststore.

```
Type sudo keytool -importcert -file
ScopiaCA1.cer -keystore /opt/Avaya/DeviceServices/<version>/CAS/
<version>/cert/cas-serverAuth.jks -alias "ScopiaCA1".
```

```
Type sudo keytool -importcert -file
ScopiaCA1.cer -keystore /opt/Avaya/DeviceServices/<version>/CAS/
<version>/cert/cas-serverAuth.jks -alias "ScopiaCA2".
```

```
Type sudo keytool -list -keystore /opt/Avaya/DeviceServices/
<version>/CAS/<version>/cert/cas-serverAuth.jks.
```

3. Access the Avaya Meetings Management site at `http://<IVIEW>:8080/iview/`, and do the following:

- If you have Avaya Meetings Management 8.3, set the `com.radvision.icm.mcuproxy.xmlapi.useSSL` Avaya Scopia® parameter to true and set the `com.radvision.icm.mcuproxy.xmlapi.ssl.port` Avaya Scopia® parameter to 3346.

The `com.radvision.icm.mcuproxy.xmlapi.useSSL` parameter must be set to true for TLS mode and false for TCP mode.

The default port for TLS is 3346 and for TCP is 3336.

- If you have Avaya Meetings Management 9.0, set the `com.vnex.vcms.core.aadsIP` Avaya Scopia® parameter to the Avaya Aura® Device Services address and restart Avaya Meetings Management to apply the changes.

Avaya Aura® Device Services accepts the incoming connection if the address matches the address on the Avaya Meetings Management synchronization page on the Avaya Aura® Device Services web administration portal.

4. Log in to the Avaya Aura® Device Services web administration portal.
5. Click **Server Connections > iView Synchronization**.
6. In the **Version number** field, select the Avaya Meetings Management version.

Avaya Aura® Device Services supports only one Avaya Meetings Management version at a time. Therefore, you must select either 8.3 or 9.0 from the **Version Number** field.

7. In the **IP address** field, type the IP address or FQDN for Avaya Meetings Management.
For example, type `alphaiview1.dr.avaya.com`.
8. If you have Avaya Meetings Management 8.3, do the following:
 - a. In the **Port to bind the connection** field, type the port number.
 - b. Select the **Secure connection** check box to use TLS connection between Avaya Aura® Device Services and Avaya Meetings Management 8.5.
9. Click **Save**.
10. Restart the Avaya Aura® Device Services.

Appendix B: LDAP examples and search results

Examples of Microsoft Active Directory LDAP property files

Examples of Microsoft Active Directory LDAP configuration that uses the user ID as the account name

```
# Binding parameters
ldapUrl=ldaps://gdc.global.example.com:3269
bindDN=global\AADSAssistant
bindCredential=admin123

# Authentication parameters
uidAttrID=sAMAccountName
baseCtxDN=dc=global,dc=example,dc=com
allowEmptyPasswords=false

# Authorization parameters based on method #2 by searching for the groups
roleFilter=(&(objectClass=group)(member={1}))
rolesCtxDN=ou=Groups,dc=global,dc=example,dc=com
roleAttrID=cn
roleAttrIsDN=false
roleNameAttrID=
roleRecursion=false
searchScope=2
adminRole=AADSAdmin
usersRole=AADSUsers
auditorRole=AADSAuditor

# Internationalization parameters
language=en

# User management parameters
activeUsersFilter=(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
lastUpdatedTimeAttr=whenChanged
```

Examples of Microsoft Active Directory LDAP configuration that uses the email address as the account name

```
# Binding parameters
ldapUrl=ldaps://gdc.global.example.com:3269
bindDN=global\AADSAssistant
bindCredential=admin123

# Authentication parameters
uidAttrID=mail
baseCtxDN=dc=global,dc=example,dc=com
```

```

allowEmptyPasswords=false

# Authorization parameters based on method #2 by searching for the groups
roleFilter=(&(objectClass=group)(member={1}))
rolesCtxDN=ou=Groups,dc=global,dc=example,dc=com
roleAttrID=cn
roleAttrIsDN=false
roleNameAttrID=
roleRecursion=false
searchScope=2
adminRole=AADSAdmin
usersRole=AADSUsers
auditorRole=AADSAuditor

# Internationalization parameters
language=en

# User management parameters
activeUsersFilter=(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
lastUpdatedTimeAttr=whenChanged

```

LDAP search results and referrals

Search Request Responses

Search Result:

The results of the search operation are returned as zero or more `SearchResultEntry` and/or `SearchResultReference` messages, followed by a single `SearchResultDone` message.

Each `SearchResultEntry` represents an entry found during the search. Each `SearchResultReference` represents an area not yet explored during the search.

Referral:

The referral result code indicates that the contacted server is unable to run the operation, while another server might be able to run the same.

LDAP Search Result Reference

If the server was able to locate the entry referred to by the `baseObject` but could not search one or more non-local entries, the server may return one or more `SearchResultReference` messages, each containing a reference to another set of servers for continuing the operation.

If Avaya Aura® Device Services receives a `SearchResultReference`, it will attempt to resolve the returned *LDAP URI*, and launch a new query for each returned reference, with the same filter unless a new filter is included in the reference. Any new references will also be followed.

The following is an example of a case when a reference would be returned when a domain is queried about another domain in the forest.

```

Ie
Source domain, dc=ottawa,dc=valley,dc=eh
Child domain, dc=upper,dc=ottawa,dc=valley,dc=eh

ldapsearch -v -H ldap://ottawa.valley.eh:389 -b "dc=ottawa,dc=valley,dc=eh"
"samaccountname=a.upper" mail msrtcsip-primaryuseraddress telephonenumber

```

```
ldap_initialize( ldap://ottawa.valley.eh:389/??base )
filter: samaccountname=a.upper
requesting: mail
# extended LDIF
#
# LDAPv3
# base <dc=ottawa,dc=valley,dc=eh> with scope subtree
# filter: samaccountname=a.upper
# requesting: mail
#
# search reference
ref: ldap://upper.ottawa.valley.eh/DC=upper,DC=ottawa,DC=valley,DC=eh
# search reference
ref: ldap://DomainDnsZones.ottawa.valley.eh/DC=DomainDnsZones,DC=ottawa,DC=valley,DC=eh
# search result
search: 2
result: 0 Success
# numResponses: 3
# numReferences: 2
```

LDAP Reference with Active Directory:

If you have Active Directory as your Enterprise source and it uses integrated DNS, the forest root will have a `ForestDnsZones` partition, while all domains with integrated DNS will have a `DomainDnsZones` partition. The forest root will also contain the `Configuration` partition.

This means any query to the Active Directory source will return references to all of these partitions.

The following is an example of querying the forest root.

```
ldapsearch -v -H ldap://west.bytown.city:389 -b "dc=west,dc=bytown,dc=city"
"samaccountname=a.west" mail
ldap_initialize( ldap://west.bytown.city:389/??base )
filter: samaccountname=a.west
requesting: mail
# extended LDIF
#
# LDAPv3
# base <dc=west,dc=bytown,dc=city> with scope subtree
# filter: samaccountname=a.west
# requesting: mail
#
# Able West, West Users, west.bytown.city
dn: CN=Able West,OU=West Users,DC=west,DC=bytown,DC=city
mail: a.west@Bytown.City
# search reference
ref: ldap://DomainDnsZones.west.bytown.city/DC=DomainDnsZones,DC=west,DC=bytown,DC=city
# search reference
ref: ldap://ForestDnsZones.west.bytown.city/DC=ForestDnsZones,DC=west,DC=bytown,DC=city
# search reference
ref: ldap://west.bytown.city/CN=Configuration,DC=west,DC=bytown,DC=city
# search result
search: 2
```

```
result: 0 Success
# numResponses: 5
# numEntries: 1
# numReferences: 3
```

LDAP Referral

The referral result code indicates that the contacted server is unable to run the operation, and that one or more other servers might be able to. Reasons for this include:

- The target entry of the request is not held locally, but the server has knowledge of its possible existence elsewhere.
- The operation is restricted on this server, perhaps due to a read-only copy of an entry to be modified.

The following is an example of when a source will return referral when a query is sent to a source that is not authoritative in the base context.

```
source domain, dc=upper,dc=ottawa,dc=valley,dc=eh

    send query with base context of dc=ottawa,dc=valley,dc=eh

ldapsearch -v -H ldap://upper.ottawa.valley.eh:389 -b "dc=ottawa,dc=valley,dc=eh"
"samaccountname=a.ottawa" mail msrtcsip-primaryuseraddress telephonenumber
ldap_initialize( ldap://upper.ottawa.valley.eh:389/??base )
filter: samaccountname=a.ottawa
requesting: mail msrtcsip-primaryuseraddress telephonenumber
# extended LDIF
#
# LDAPv3
# base <dc=ottawa,dc=valley,dc=eh> with scope subtree
# filter: samaccountname=a.ottawa
# requesting: mail msrtcsip-primaryuseraddress telephonenumber
#
# search result
search: 2
result: 10 Referral
text: 0000202B: RefErr: DSID-03100781, data 0, 1 access points
      ref 1: 'ottawa.valley.eh'

ref: ldap://ottawa.valley.eh/dc=ottawa,dc=valley,dc=eh
# numResponses: 1
```

If the Avaya Aura® Device Services receives a Referral, it will attempt to resolve the returned LDAP URI and launch a new query for each returned referral, with the same filter. This is unless specified otherwise in the referral.

Typically, the referred to URI will be equal to the base context in the query.

Recommendations

Minimize the number of queries sent to the Enterprise source for any given transaction. This might improve Avaya Aura® Device Services performance, and also minimize the impact on the source.

Base Context:

To avoid referrals when choosing base context DN, choose the highest granularity that your enterprise source is authoritative in.

Active Directory:

The `ForestDNSZones`, `DomainDNSZones`, and `Configuration` partitions are not replicated to the global catalog. Therefore, search requests to global catalog will not return references to said partitions. Thus if possible it is advisable to use the global catalog on Active Directory instead of the standard LDAP source.

Multiple Domains:

If the Enterprise is built on Active Directory, it is advisable to use global catalog, instead of counting on referral or reference. This might minimize the number of queries. If using alternate Enterprise sources, you might experience degradation if many or all queries require referral to another source.

Appendix C: FIPS validated cryptographic modules

When FIPS is enabled, Avaya Aura® Device Services uses the following FIPS validated cryptographic modules:

Module	Certificate number	Description
Bouncy Castle FIPS Java API (BC-FJA)	3152	The Bouncy Castle FIPS Java API is a comprehensive suite of FIPS-approved algorithms implemented in pure Java. All key sizes and modes are implemented to allow flexibility and efficiency. Additional algorithms are available in non-approved operation as well.
Red Hat Enterprise Linux OpenSSL Cryptographic Module	3538	The OpenSSL FIPS Runtime module is a general purpose cryptographic library designed to provide FIPS 140-2 validated cryptographic functionality for use with the high-level APIs of the OpenSSL library.

For more information about FIPS validated cryptographic modules, see [Cryptographic Module Validation Program](#).

Appendix D: Best Practices for VMware performance and features

For information on the hardware requirements for Avaya Aura® Device Services, see *Installing the Avaya Solutions Platform 130 Series*, which is available at <https://support.avaya.com>.

Related links

[Timekeeping](#) on page 370

[VMware Tools](#) on page 371

[VMware networking best practices](#) on page 372

[Storage](#) on page 375

[VMware features supported by Avaya Aura](#) on page 378

Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that the NTP service can communicate with the external NTP servers.

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command `/usr/bin/vmware-toolbox-cmd timesync status`.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine. If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the **chronyc sources -v** command from a command window. The results from this command:

- Verify if the NTP service is getting time from a network time source.
- Indicate which network time source is in use.
- Display how closely the guest OS matches the network time.
- Display how often the guest OS checks the time.

The guest OS polls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding **chronyd**. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

Related links

[Best Practices for VMware performance and features](#) on page 370

VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see *Overview of VMware Tools* at <http://kb.vmware.com/kb/340>.

Important:

Do not upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

Related links

[Best Practices for VMware performance and features](#) on page 370

VMware networking best practices

You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

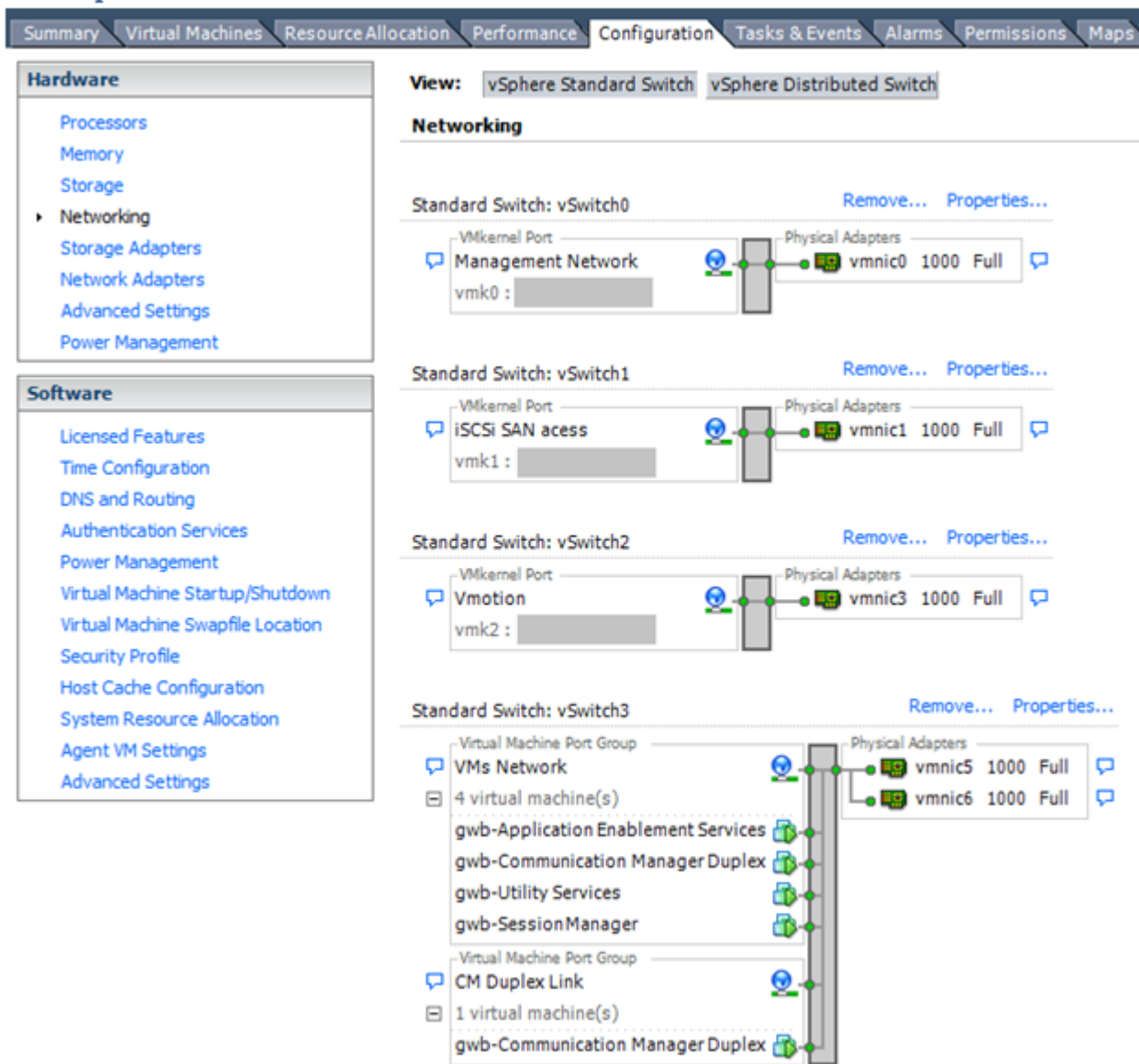
This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernel vNICs to be the same IP Maximum Transmission Unit (MTU).

Disclaimer: The images in this section represent older ESXi versions and may vary for the latest ESXi versions.

Networking Avaya applications on VMware ESXi – Example 1

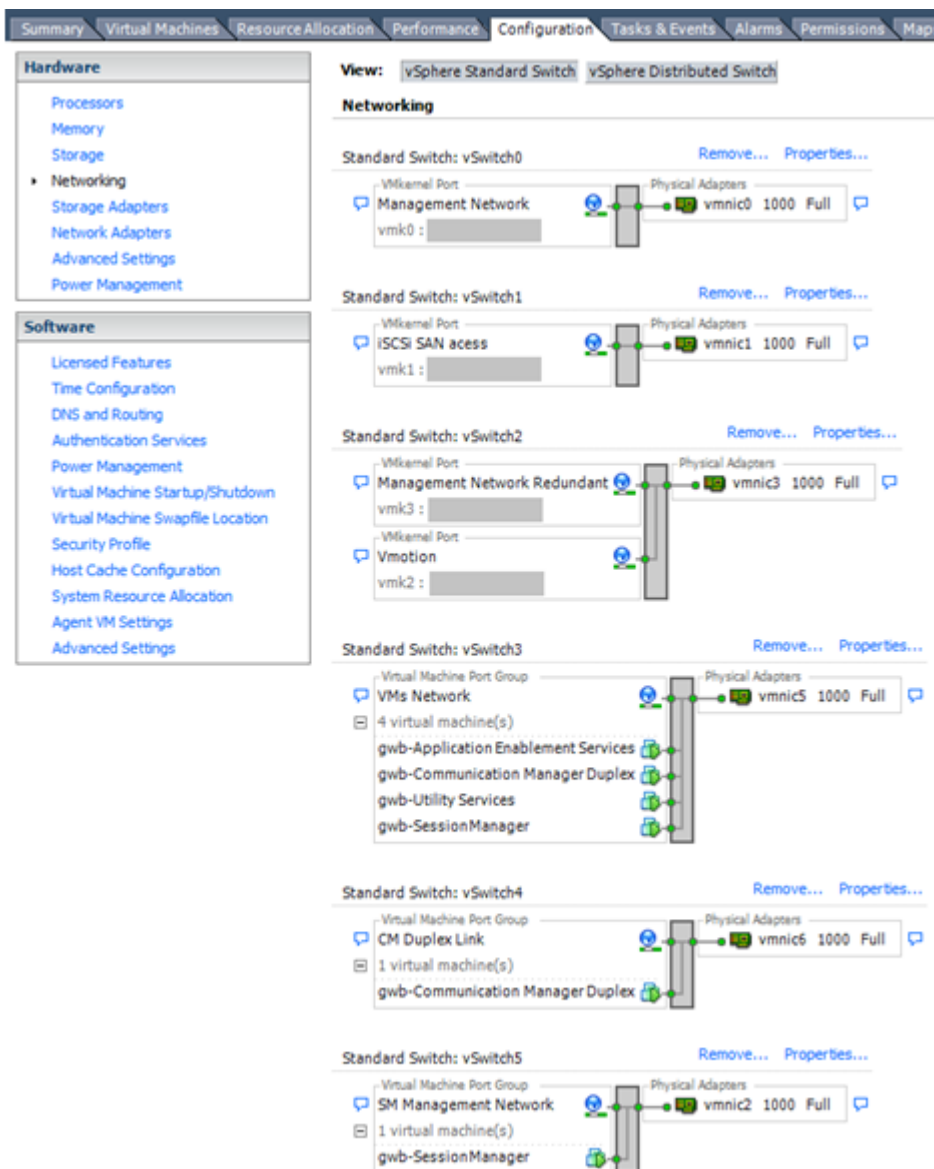


This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In example 2, the virtual machine network of vSwitch3

can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



This configuration shows a complex situation using multiple physical network interface cards. The key differences between example 1 and example 2 are:

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.

References

Title	Link
Product Support Notice PSN003556u	Go to https://support.avaya.com and search for PSN003556u.
VMware vSphere 8.0 Documentation	Go to https://www.vmware.com/support/pubs/ and search for <i>VMware vSphere 8.0 Documentation</i> .
VMware vSphere 7.0 Documentation	Go to https://www.vmware.com/support/pubs/ and search for <i>VMware vSphere 7.0 Documentation</i> .
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Related links

[Best Practices for VMware performance and features](#) on page 370

Storage

There is no stipulation on the underlying storage vendor type and storage technology used. Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are different storage technologies supported by VMware vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning these resources to virtual machines.

Related links

[Best Practices for VMware performance and features](#) on page 370

Best Practices for VMware features

VMware High Availability

VMware High Availability (HA) provides automatic detection of hardware failures, server failures, and operating system failures. In the event of a physical server failure, VMware HA automatically restarts the affected virtual machine on other production servers that have spare capacity. In the event of an operating system failure, VMware HA restarts the affected virtual machine on the same server.

VMware HA ensures that capacity is available to restart all virtual machines that are affected by a service failure. HA continuously monitors capacity utilization and reserves spare capacity to restart virtual machines.

VMware HA helps users identify abnormal configuration settings detected within HA clusters. The VMware vSphere client interface reports relevant operating status and potential error conditions along with suggested remediation steps.

For more information, see the VMware website at https://www.vmware.com/pdf/ha_datasheet.pdf.

 Note:

- All virtual machines and their configuration files must be on shared storage, e.g. Fibre Channel SAN, iSCSI SAN, or SAN iSCSI NAS.
- The console network must have redundant network paths to have reliable failure detection for HA clusters. VMware HA monitors the heartbeat between hosts on the console network for failure detection.
- VMware HA uses virtual machine priority to decide order of restart.
- VMware HA only works across a LAN. VMware HA does not work across a WAN.

Related links

[Best Practices for VMware performance and features](#) on page 370

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.
- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or under-performing servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

Related links

[Best Practices for VMware performance and features](#) on page 370

VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

 Caution:

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Only take snapshots during a maintenance window.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.

If your virtual machine contains snapshots that are more than 72 hours old, system performance might be impacted. When you no longer need a snapshot, remember to delete it.

- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
 - In the Take Virtual Machine Snapshot window, clear the **Snapshot the virtual machine's memory** check box.

- Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

*** Note:**

If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots

Related links

[Best Practices for VMware performance and features](#) on page 370

VMware features supported by Avaya Aura®

This section does not cover Avaya Solutions Platform (ASP) 130 and ASP S83000. Avaya does not support advanced VMware features on its ASP 130 and ASP S8300 hardware. It supports the basic VMware features as listed in the following table. For more information about support and limitations on ASP 130 and ASP S8300, see <https://download.avaya.com/css/public/documents/101062774>.

*** Note:**

For more information about Avaya Aura® Media Server, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

The following table lists the VMware features supported on customer-provided Virtualized Environment for various Avaya Aura® Release10.2 components.

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
ESXi 7.0	Yes	Yes	Yes	Yes	Yes	Yes
ESXi 8.0	Yes	Yes	Yes	Yes	Yes	Yes
vCenter See foot note ⁵	Yes	Yes	Yes	Yes	Yes	Yes
vSphere WebClient (HTML5)	Yes	Yes	Yes	Yes	Yes	Yes
VMFS 6	Yes	Yes	Yes	Yes	Yes	Yes
VMware vMotion See foot note ⁶	Yes	Yes	Yes	Yes	Yes	Yes
Storage vMotion	Yes	Yes	Yes	Yes	Yes	Yes
VMware Snapshot See foot note ⁷	Yes	Yes	Yes	Yes	Yes	Yes
VMware Live Snapshot	Not supported	Not supported	Not supported	Not supported	Not supported	No
VMware High Availability	Yes	Yes	Yes	Yes	Yes	Yes
Proactive High Availability	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)
Storage DRS	Yes	Yes	Yes	Yes	Yes	Yes
Hyperthreading	Yes	Yes	Yes	Yes	Yes	Yes
Hyperthreading ratio for Virtual CPUs and Physical CPU	2:1	2:1	2:1	2:1	2:1	2:1

⁵ Limited to deployment, managing VMs, basic monitoring, and making VMs part of a vCenter cluster.

⁶ Ensure that vMotion occurs when an Avaya Aura® application virtual machine is in maintenance mode.

⁷ Snapshots should be used when patching the products. As per the backup mechanism provided in the product-specific documentation, you should perform daily backups instead of using snapshots of the products. Applicable for Communication Manager, Session Manager, System Manager, and Application Enablement Services.

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
VMware DRS (Compute and Memory) See foot note ⁸	Yes	Yes	Yes	Yes See foot note ⁹	Yes	Yes
Secure boot for virtual machine	Yes	Yes	Yes	Yes	Yes	Yes
Content Library	Yes	Yes	Yes	Yes	Yes	Yes
VMware Fault Tolerance (FT)	Not supported	Not supported	Not supported	Yes See foot note ¹⁰	Not supported	Yes
vSphere Standard Switch	Yes	Yes	Yes	Yes	Yes	Yes
vSphere Distributed Switch	Yes	Yes	Yes	Yes	Yes	Yes
Hot Pluggable Virtual Hardware	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
Reservation Required see foot note ¹¹	Yes	Yes	Yes	Yes	Yes	Yes
vSAN support See foot note ¹²	Yes	Yes	Yes	Yes	Yes	Yes
Thin Provisioning	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported

Related links

[Best Practices for VMware performance and features](#) on page 370

⁸ With two conservative modes - Applicable for Communication Manager, Session Manager, System Manager, and Application Enablement Services.

⁹ DRS supports In-cluster migration - Applicable for Avaya SBC for Enterprise.

¹⁰ For more information about the Fault Tolerance for Application Enablement Services, see *Avaya Aura Application Enablement (AE) Services 7.x, 8.x, and 10.x High Availability (HA) White Paper*.

¹¹ Avaya Aura® does not support reservationless deployments on ASP 130. Avaya recommends always making reservations when choosing a reservationless deployment. It is crucial to strictly adhere to the guidelines outlined in the Application Notes. For more information on reservationless deployment, see the *"Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware"* at <https://support.avaya.com>.

¹² If you are using vSAN, use Thick Provisioning. Even though VMware supports vSAN with Thin Provisioning, Avaya Aura® does not support it.

Appendix E: Creating RHEL virtual machine on Nutanix

Uploading the RHEL ISO to Nutanix server

About this task

You can install RHEL on Nutanix 6.5 and later, after uploading the standard RHEL ISO image on the Nutanix server.

Note:

The RHEL ISO must be customer-provided. Avaya is not responsible for the RHEL ISO image.

Procedure

1. Log in to Nutanix server using Nutanix Prism web console.
2. Navigate to **Home > Settings > Image Configuration**.
3. In the **Image Configuration** screen, click **Upload Image**.
Nutanix Prism web console displays the **Create Image** window.
4. In the **Name** field, enter a name for the image.
5. In the **Image Type** field, select the ISO image to upload.
6. In the **Storage Container** field, select the required option.
7. Under **Image Source** field, either browse for the ISO image through URL or upload the image file if stored in your local machine.
8. Click **Save**.

You can view the image upload status from the drop-down list on top of the **Home** page.

Next steps

Installing RHEL on Nutanix 6.5 and later.

Installing RHEL on the Nutanix server

Before you begin

- Upload the RHEL image on Nutanix 6.5 and later.
- Log in to Nutanix 6.5 server using the Nutanix Prism web console.

Procedure

1. Navigate to **Home > VM**.
2. In the **VM** page, click **Create VM**.
3. In the **Create VM** window under **General Configurations**, enter appropriate values in the **Name**, **Description**, and **Timezone** fields.
4. In the **vCPUs** field under **Compute Details**, enter the number of CPUs required for the application.
5. In the **Number of Cores per vCPU** field, enter the required value.
6. In the **Memory** field, enter appropriate memory in GiB.
7. Under **Boot Configuration**, select **UEFI**.
8. Under **Disks**, click the Edit icon for the CD-ROM disk type, and do the following:
 - a. In the **Type** field, ensure **CD-ROM** is displayed.
 - b. In the **Operation** field, select **Clone from Image Service**.
 - c. In the **Bus Type** field, Avaya recommends selecting **IDE**.
 - d. In the **Image** field, select the RHEL ISO Image.
 - e. Click **Update**.

The CD-ROM and the disk size are displayed.

9. Click **Add New Disk** next to **Disks**, and do the following:
 - a. In the **Type** field, select **Disk**.
 - b. In the **Operations** field, select **Allocate on Storage Container**.
 - c. In the **Bus Type** field, select the same bus type which you selected while updating the disk.
 - d. In the **Storage Container** field, select the appropriate storage container.
 - e. In the **Size** field, enter the required GiB size.
 - f. Click **Add**.
10. Under **Network Adapters (NIC)**, do the following:
 - a. Click **Add New NIC** to add a Network Interface Card (NIC).
 - b. In the **Create NIC** window, select the **Subnet Name**.

- c. In the **Network Connection State** field, select **Connected**.
 - d. Click **Add**.
 - e. To add multiple NICs, repeat 10.a to 10.d.
11. Under **VM Host Affinity**, click **Set Affinity** and do the following:
- a. In the **Set VM Host Affinity** window, select the hosts.
Select multiple hosts to ensure one node (virtual machine) runs in case another node fails.
 - b. Click **Save**.
- After the successful creation of virtual machine, virtual machine appears in the VM page.
12. Select the newly created VM and click **Power On**.
13. Click **Launch Console**.

 Note:

The **Launch Console** button is enabled only when the virtual machine is Powered On.
After the RHEL boots, Red Hat Enterprise Linux 8.10 welcome screen appears.

14. Click **Continue**.
15. In the **Installation Summary** screen, under **LOCALIZATION**, click **Language Support** to select the supported language.
16. Click **Time & Date** to set the required timezone.
17. Under **SOFTWARE**, click **Software Selection**.
18. Select **Minimal Install** and then click **Done**.
19. Under **SYSTEM**, click **Installation Destination** and do the following:
- a. Under **Storage Configuration**, select the **Custom** radio button and click **Done**.
 - b. In the **Manual Partitioning** window, set the partitioning as required.
 - c. Click the **+** icon to create a new mount point.
 - d. Select the available partition from the **Mount Point** drop-down menu. To add custom partitions, type the required partition name. For eg: `/etc/opt/defty`.
 - e. Enter the capacity in GiB in the **Desired Capacity** field and then click **Add Mount Point**.
 - f. In the **Manual Partitioning** window, click **Done**.
 - g. In the **Summary of Changes** window, click **Accept Changes**.
 - h. Click **Done**.

20. Click **Network & Host Name** and do the following:
 - a. Enter a name in the **Host Name** field and click **Apply**.
 - b. To configure the IP, click **Configure**.
 - c. Click **IPV4 Settings** and select the required option from the **Method** drop-down menu.
 - d. Click **Done**.
21. Under **USER SETTINGS**, click **Root Password**.

In the **Root Password** window, set a password for the root user and then click **Done**.
22. Click **User Creation** and in the Create User window, enter the details and click **Done**.
23. Click **Begin Installation**.

The RHEL virtual machine is installed on the Nutanix 6.5 server and later.
24. Click **Reboot System** to reboot the RHEL virtual machine.

Appendix F: Virtual Machine Backup (clone) in ASP R6.0.x (KVM on RHEL 8.10)

Virtual Machine Backups (clone) as an alternative to snapshots

Avaya Aura® documentation refers to snapshots at the application level for various procedures. Snapshots apply to a VMware environment.

With the introduction of the alternative hypervisor in Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), RHEL 8.10 does not support snapshots and Linux does not support issues relating to the use of snapshots.

Virtual machine backup is a similar feature to snapshots. Virtual machine backups use the cloning feature. Use virtual machine backups in place of snapshots for ASP R6.0.x (KVM on RHEL 8.10).

You should only keep backups for a maximum 48 hours in order to ensure sufficient storage is available. You may need to remove them earlier.

 Note:

The images and screenshots in this document are for illustration purposes only. The actual user interface may slightly vary due to updates and design changes.

Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to create a clone for backup purposes.

Before you begin

- Ensure there is sufficient space to create the Virtual Machine Backup (clone). Clones are created as “thick provisioned” and require the same size as the virtual machine you are cloning.

- Refer to application documentation for guidelines on storage requirements for different application profiles.
- Shut down the virtual machine for which you are creating a backup (clone). This is a service impacting activity. Perform these steps within a customer-approved maintenance window.

*** Note:**

You must be root or use `sudo` with `custadm` account for CLI commands, and you must enable Administrative access when using the Cockpit user interface.

*** Note:**

These clones must be created through the CLI as the Cockpit UI does not support the necessary required options.

Procedure

1. Log in to the KVM Cockpit web console as `custadm` in the following format: `https://<IP address or FQDN of KVM host>:9090`.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

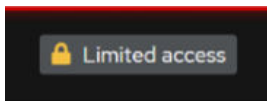


Figure 5: Limited access button

*** Note:**

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for `custadm`.

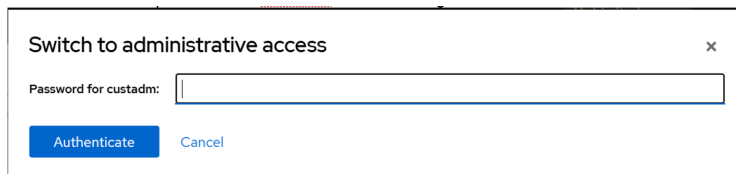


Figure 6: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

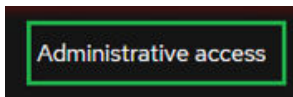


Figure 7: Administrative access button

4. Navigate to **System > Virtual Machines > Storage Pools**.

The Name `guest_images` is a label for `/var/lib/libvirt/images`. If you select `guest_images`, you can see additional information. If you select `Storage Volumes`, you can view all images in the `/var/lib/libvirt/images` directory.

- Review the images and remove any of them that you no longer use.

Images that do not have a 'Used by' value are typically safe to remove.

- Confirm that you have the necessary space for your clone.
- Log in to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
- Run the following command to obtain a list of all virtual machines:

```
sudo virsh list --all
```

Example output:

```
[custadm@asp130-r660xs-a3lp ~]# sudo virsh list --all
```

Id	Name	State
1	8HDD-RHEL-810-Fiotester2	running
2	8HDD-RHEL810-Fiotester1	running
-	8HDD-RHEL-810-Fiotester3	shut off
-	8HDD-RHEL-810-Fiotester3-Clone	shut off
-	8HDD-RHEL-810-Fiotester3-clone	shut off
-	Agent_Testing	shut off
-	Agent_Testing-Clone	shut off
-	Agent_Testing2	shut off
-	Agent_Testing3	shut off

In this example, the virtual machine `Agent_Testing3` is shut off state, ready for backup (clone).

- Run the following command to backup (clone) the virtual machine. You must use the `nonsparse` option to ensure the clone is created as thick provisioned.

```
sudo virt-clone --original <Domain-to-be-cloned> --auto-clone --nonsparse
```

Example output:

```
sudo virt-clone --original Agent_Testing3 --auto-clone --nonsparse
Allocating 'RHEL810-agenttestvm3-fat-clone.qcow2' | 50 GB 00:01:06
Clone 'Agent_Testing3-clone1' created successfully.
```

This command creates a backup (clone) with default values. You can create a clone with any name for the virtual machine and QCOW2 labels by specifying a full path and using the following command:

```
sudo virt-clone --original <VM Domain> --name <Clone VM Label> --file /var/lib/libvirt/images/<VM Domain QCOW2 file name>.qcow2 --nonsparse
```

Example for single QCOW2 image:

```
sudo virt-clone --original RHEL810-fiotester1 --name RHEL810-  
fiotester2 --file /var/lib/libvirt/images/RHEL810-fiotester2.qcow2  
--nonsparse
```

Example for multiple QCOW2 images:

```
sudo virt-clone --original Duplex_Active_974  
--name Duplex_Active_974_CloneTest --file /var/lib/  
libvirt/images/Duplex_Active_974_CloneTest_system.qcow2  
--nonsparse --file /var/lib/libvirt/images/  
Duplex_Active_974_CloneTest_Var_Disk.qcow2 --nonsparse
```

*** Note:**

Completion time varies depending on the size of original virtual machine disk.

Calculating space for the clone

About this task

Use this procedure to figure out if you have the necessary space for the clone. This example refers to System Manager but the same information applies to all Avaya Aura® components.

You can use the Cockpit user interface to calculate this information. You can also use the Command Line Interface (CLI). The units of measure may differ. The Cockpit user interface (UI) uses International Electrotechnical Commission (IEC) values, such as Gibibyte. The CLI uses International System of Units (SI) values, such as Gigabyte.

Procedure

1. Log in to the KVM Cockpit web console as **custadm** in the following format: `https://<IP address or FQDN of KVM host>:9090`.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

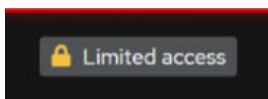


Figure 8: Limited access button

*** Note:**

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **custadm**.

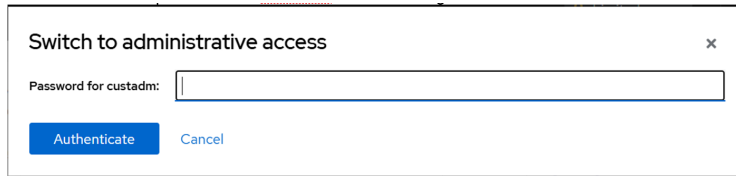


Figure 9: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

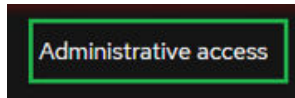


Figure 10: Administrative access button

4. Navigate to **System > Virtual Machines > Storage Pools**.
5. View the information on the **Storage Pools** screen.
6. Divide the amount of used and available space to get the percentage.

In this example, approximately 18% of the available storage is used ($579.51/3299 \sim 18\%$).

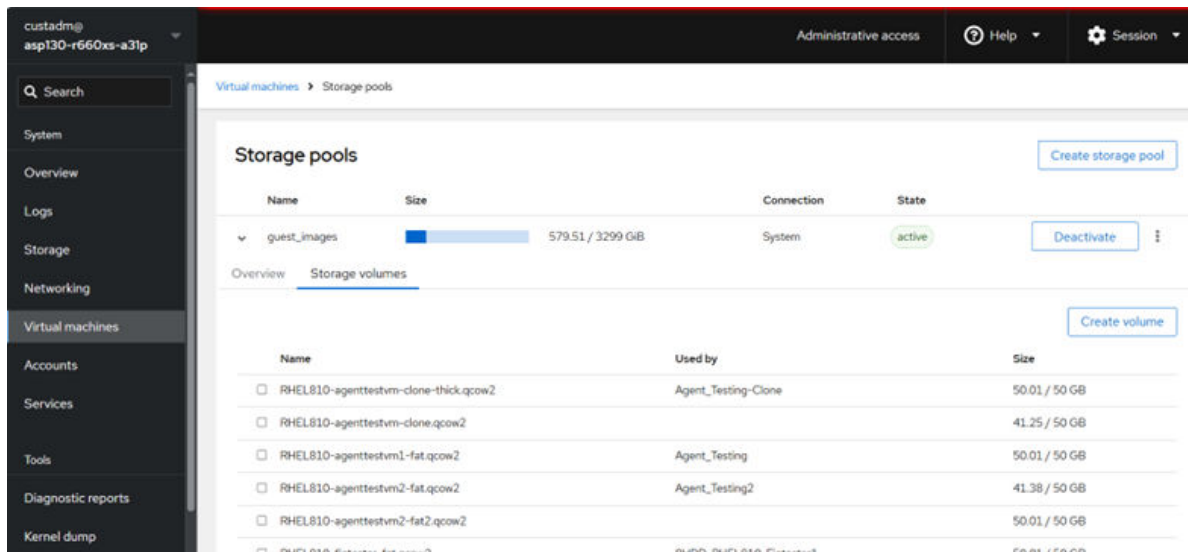


Figure 11: Example size

7. **(Optional)** Log in to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
8. Change the directory to `/var/lib/libvirt/images` and identify the available space.

In the example below, 18% of available storage is being used on the host.

Example output:

```
[custadm@asp130-r660xs-a31p ~]$ cd /var/lib/libvirt/images
[custadm@asp130-r660xs-a31p images]$ df -h .
```

Filesystem	Size	Used	Avail	Use%	Mounted on
dev/mapper/vg_system-lv_libvirt	3.3T	580G	2.7T	18%	/var/lib/libvirt

Validating a Virtual Machine Backup (clone)

Procedure

1. Login to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
2. Run the following command to validate the backup (clone):

```
sudo virsh list --all
```

Example output:

```
[custadm@asp130-r660xs-a3lp ~]# sudo virsh list --all
```

Id	Name	State
1	8HDD-RHEL-810-Fiotester2	running
2	8HDD-RHEL810-Fiotester1	running
-	8HDD-RHEL-810-Fiotester3	shut off
-	8HDD-RHEL-810-Fiotester3-Clone	shut off
-	8HDD-RHEL-810-Fiotester3-clone	shut off
-	Agent_Testing	shut off
-	Agent_Testing-Clone	shut off
-	Agent_Testing2	shut off
-	Agent_Testing3	shut off
-	Agent_Testing3-clone	shut off

In this example, the virtual machine `Agent_Testing3-clone` is the cloned virtual machine.

3. Confirm that the clone is thick provisioned by running the following command on the clone and ensuring that the virtual size is the same as the disk size:

```
cd /var/lib/libvirt/images
```

```
sudo qemu-img info <clone name>
```

Example output:

```
cd /var/lib/libvirt/images
```

```
sudo qemu-img info Agent_Testing3-clone.qcow2
```

```
image: Agent_Testing3-clone.qcow2
```

```
file format: qcow2
```

```
virtual size: 50 GiB (53687091200 bytes)
```

```
disk size: 50 GiB
```

```
cluster_size: 65536
```

```
Format specific information:
```

```
compat: 1.1
```

```
compression type: zlib
lazy refcounts: true
refcount bits: 16
corrupt: false
extended l2: false
```

4. Run the following command to ensure that the virtual machine is cloned with the same disk name that is provided during the backup (clone):

```
sudo virsh domblklist <cloned VM name>_8_1
```

For example, the output of the command appears as follows:

```
hda /var/lib/libvirt/images/RHEL810-fiotester2.qcow2
```

5. Log in to the KVM Cockpit web console as **custadm** in the following format: `https://<IP address or FQDN of KVM host>:9090`.
6. For administration actions, on the top-right of the window, click on the **Limited access** button.

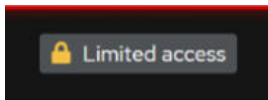


Figure 12: Limited access button

*** Note:**

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

7. In the Switch to administrative access window, enter the password for **custadm**.

Figure 13: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

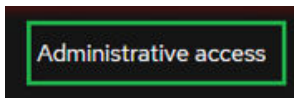
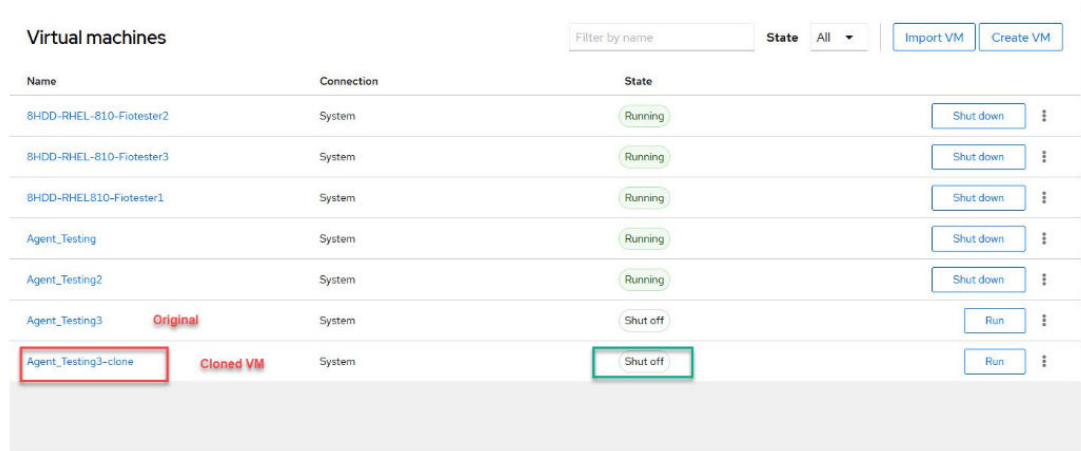


Figure 14: Administrative access button

8. Navigate to **System > Virtual Machines**.

9. View the cloned virtual machine in the virtual machines list.



Virtual machines			Filter by name	State	All	Import VM	Create VM
Name	Connection	State					
8HDD-RHEL-810-Fioteater2	System	Running				Shut down	⋮
8HDD-RHEL-810-Fioteater3	System	Running				Shut down	⋮
8HDD-RHEL810-Fioteater1	System	Running				Shut down	⋮
Agent_Testing	System	Running				Shut down	⋮
Agent_Testing2	System	Running				Shut down	⋮
Agent_Testing3	System	Shut off	Original			Run	⋮
Agent_Testing3-clone	System	Shut off	Cloned VM			Run	⋮

Figure 15: Virtual machines list

Rolling back using the Virtual Machine Backup (clone)

About this task

If you experience a problem during an upgrade, you can roll back to a state using the cloned virtual machine.

Procedure

1. Log in to the KVM Cockpit web console as **custadm** in the following format: `https://<IP address or FQDN of KVM host>:9090`.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

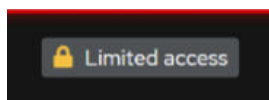


Figure 16: Limited access button

* Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **custadm**.

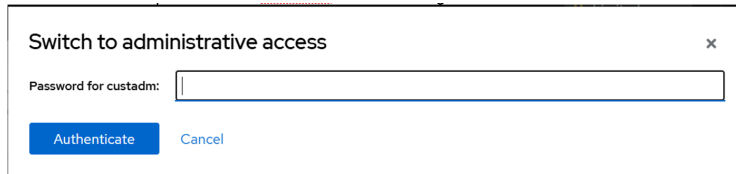


Figure 17: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

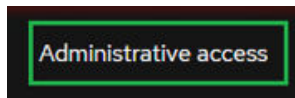


Figure 18: Administrative access button

4. Navigate to **System > Virtual Machines**.
5. Shut down the original virtual machine.
6. Rename the original virtual machine.

For example: `Virtual_Machine_Broken`

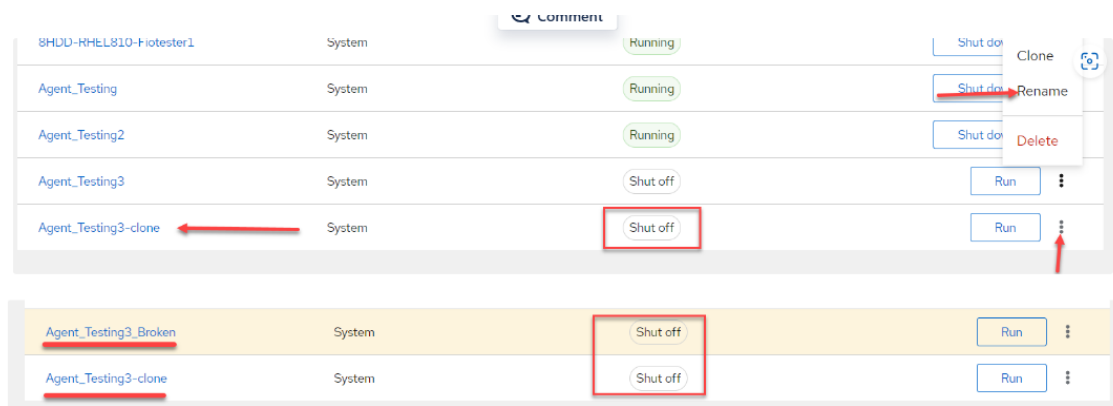


Figure 19: Roll back VM backup

7. While still in a power off state, edit the virtual machine clone Label to match the original virtual machine label. This ensures that the cloned virtual machine becomes the original virtual machine.

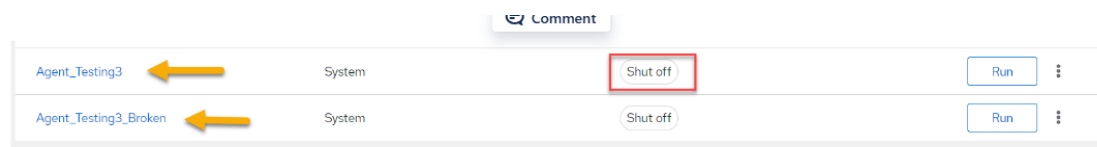


Figure 20: Edit Virtual Machine name

8. Configure the virtual machine that you renamed in step 5 to ensure the network interfaces and state match the broken virtual machine.

For example: `bridge0` and `state = up`

Comment

Network interfaces						Add network interface
Type	Model type	MAC address	Source	State		
bridge	virtio	52:54:00:b1:6f:b1	Bridge <code>bridge0</code>	up		Unplug Edit ⋮

Figure 21: Network interfaces

9. Power on the virtual machine that you renamed in step 5.

Comment

Agent_Testing3	System	Running	Shut down ⋮
Agent_Testing3_Broken	System	Shut off	Run ⋮

Figure 22: Power on

10. Delete any unused backups.

Glossary

Cassandra	Third party NoSQL database, which is used by Avaya Multimedia Messaging to store messaging data and configuration information. For more information, see https://cassandra.apache.org/ .
Domain Name System (DNS)	A system that maps and converts domain and host names to IP addresses.
Endpoints	Refers to Avaya Vantage™ and supported hard phones, including the J100 and 9600 series phones. Avaya Workplace Client softphones are referenced separately in this document.
Fully Qualified Domain Name (FQDN)	A domain name that specifies the exact location of the domain in the tree hierarchy of the Domain Name System (DNS).
Network Time Protocol (NTP)	A protocol used to synchronize the real-time clock in a computer.
Secure Shell (SSH)	Secure Shell (SSH) is a group of standards and an associated network protocol that the system can use to establish a secure channel between a local and a remote computer. SSH uses public-key cryptography to mutually authenticate a user and a remote computer. SSH uses encryption and message authentication codes to protect the confidentiality and integrity of the data that is exchanged between the two computers.
Simple Network Management Protocol (SNMP)	A protocol for managing devices on IP networks.
SSL (Secure Sockets Layer) Protocol	The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.
TCP	Transmission Control Protocol.
TLS	Transport Layer Security

UDP

User Datagram Protocol. This is a communication method, similar to TCP.

Index

Special Characters

_Admin user is not prompted for password in sudo su	333
_REPLACE THIS TEXT, OR DELETE THIS ENTIRE INDEXTERM ELEMENT IF YOU DO NOT NEED IT	265

Numerics

10.2.0.1	18
10.2.1	18
10.2.1.1	17

A

A10 configuration	322 , 326
configuring LDAP authentication	330
configuring LDAP searches	329
creating virtual service	329
service group	328
virtual server	327
AADS 10.2.0.1	18
Active Directory	
indexing attributes	282
Add End Entity	308
adding	
data center	47
reverse proxy	318
additional node	
installing	199 , 206
additional seed node	217
administrative user	
creating	103
AIDE	
creating baseline database	225
alarms	
overview	299
System Manager	299
third-party SNMP	301
verify	303
aliases	57
app commands do not work	336
Amazon Web Services	
creating security groups	118
deploying virtual machines	113
managing load balancers	128
app command	57
does not work after failed installation	336
application layer	
installation checklist	177
Applications	87
ASP	
considerations	31

assign	
firewall rules to virtual machines	164
assigning	
data center	48 , 49
attributes replication	280
authentication domain	
requirements	42 , 280
automatic backups	
changing default password	226
Avaya Aura Device Services	270
Azure virtual machine resource requirements	35 , 36
installation	179
installing in environment without Aura	189
overview	17
supported servers	31
virtual machine resource requirements	34
Avaya Aura Device Services VM deployment	
configuration parameters	81
Avaya Aura® application	
ESXi version	32
KVM version	33
Avaya InSite Knowledge Base	346
Avaya support website	345
Avaya Workplace Soft Clients are logging out due to a mismatch in the ETAG	341
Avaya Workspaces Client cannot connect to Device Services	332
AWS	
manage load balancer certificates	116
Utility Server virtual IP and FQDN	189
AWS resource profiles	
specifications	37

B

best practices	296
performance and features	370
VMware networking	372

C

CA certificate files	361
CA signed certificates	355
Cassandra	
clustering	46
installation time	188
Cassandra clustering	47
configuration on Session Manager	47
cdto command	58
certificate	
signing identity certificates using CA certificates	355
Certificate Enrollment	309
certificate file	

certificate file (<i>continued</i>)			
uploading	309	collection (<i>continued</i>)	
certificate signing requests	354	edit	343
generating	353	generating PDF	343
certificate using CSR		sharing content	343
create	309	commands	
certificates	347	system layer	58
intermediate CA certificate	352	components	22
LDAP certificate	359	Avaya Aura Device Services	22
load balancer certificates for AWS deployment	116	configuration	
System Manager	334, 335	advanced configuration	252
System Manager certificate	349	automatic configuration flow	21
third party CA signed certificates	350	Avaya SBCE for remote access	321
third-party certificates required for installation	42	certificates	230
viewing details	348	client certificate policy using CLI	360
changes to platform support	13	cluster configuration	249
changing password		database settings	248
Avaya Aura Device Services	75	firewall configuration	254
characters in passwords	56	front-end host	230
checking		LDAP advanced parameters in Configuration Utility	244
Chrony status	111	LDAP parameters in Configuration Utility	234
DRS synchronization	224	LDAP settings	280
checking connection		remote access	321
Session Manager	111	system manager	230
System Manager	111	tools and utilities	56
checklist		Utility Server	251
Cassandra clustering configuration on Session		configuration tasks	228
Manager	47	configure	
Device Services application installation	177	run configuration script	229
virtual machine deployment on Google Cloud		configuring	
Platform	164	additional ports in server firewall	254
Chrony service		additional seed node	217
checking status	111	firewall rules for Hyper-V	140
client mapping		Keycloak for OAuth	258
creating	260	Microsoft Azure load balancer	155
clone	388	network for virtual switch	135
cluster		OAuth database replication	264
change cassandra password	248	password rules	69
change cassandra username	248	RSA public and private keys	213
change LDAP parameters after install	214	secure boot	96
changing seed node	214	SSH connections	213
configuring data center	47	virtual IP address	215
configuring ports	319	connection types	38
configuring Session Manager	268	considerations	
configuring virtual IP address	215	migrating from standalone to cluster environments	39
enabling LDAP replication	255	content	
enabling OAuth database replication	264	publishing PDF output	343
install cluster	198	searching	343
installation	198	sharing	343
installing initial node	199	sort by last updated	343
clustering		watching for updates	343
geographically distributed system considerations	41	CPU	
large deployment considerations	40	Hyper-V settings	139
network latency requirements	41	create	
topology configuration	40	administrative user	103
collection		creating	
delete	343	baseline database for AIDE	225
		client mapping	260

creating (<i>continued</i>)		diagram (<i>continued</i>)	
CSR	305	automatic configuration flow	21
disk partitioning for Microsoft Azure	149 , 173	solution architecture	19
Elastic load balancer on AWS	128	disabling	
Hyper-V virtual machine	136	FIPS	94
LDAP groups	292	STIG hardening	95
load balancers on Google Cloud Platform	170	disk partitioning	37
Microsoft Azure load balancer	154	create for software-only AWS	124
security groups for Azure VMs	150	create for software-only VMware	102 , 140
TLS client profile	316	for Microsoft Azure	149 , 173
TLS server profile	313	LVM	173
virtual hard disks for Google Cloud Platform	172	DNS	
virtual hard disks for Hyper-V	138	server addresses disappear	337
virtual hard disks for Microsoft Azure	147	document changes	14
creating a key pair	118	documentation center	343
creating an end entity	308	finding content	343
Creating certificate using certificate signing request	309	navigation	343
cryptographic module validation program	369	documentation portal	343
CSR		downloading	
creating	305	System Manager PEM certificate	312
D		downloading software	
		using PLDS	74
data center	47	E	
adding	48	EASG	
data corruption	339	enabling from CLI	222
data encryption		enabling	
encryptionPassPhrase command	70	additional RPMs for software-only	107
field descriptions	81	EASG	222
overview	24	FIPS	93
data encryption commands	70	FIPS for software-only systems	106
encryptionRemoteKey	71	Hyper-V	134
encryptionStatus	71	IPv6	93 , 112
data replication	255	LVM on Google Private Cloud	173
data retention	24	PPM rate limiting	273
deploying		root access for AWS VM	124
Microsoft Azure virtual machines	146	root access on GCP	168
OVA using Host Client	83	root access on Microsoft Azure	148
OVA using KVM Cockpit	275	STIG hardening	95
OVA using vSphere Client	78	encryptionPassphrase	70
Deploying OVA file		encryptionRemoteKey	71
Avaya Aura Device Services	86	encryptionStatus	71
deploying virtual machines		end entry	
on Google Cloud Platform	165	create	308
deployment methods	73	environment without Aura	
Amazon Web Services	113	installing Avaya Aura Device Services	189
Google Cloud Platform	157	equinox management	
Hyper-V	131	settings for Avaya Aura Device Services	362
Microsoft Azure	141	ESXi	378
OVA-based	77	ESXi version	
VMware	98	Avaya Aura® application	32
deployment options	25	external load balancer	
descriptions		Nginx requirements	52
LDAP parameter	296	port configuration	52
device authorization flow			
prerequisites	54		
diagram			

F

features best practices	370
field description	
TLS certificates	306
field descriptions	
Applications	87
Locations	87
new profile	316
new server profile screen	313
Platforms	87
file system	
creating baseline database	225
finding content on documentation center	343
FIPS	
cryptographic modules	369
disabling	93 , 94
haveged service	105
firewall	
assigning firewall rules	164
firewall rules	
configuring on Google Cloud Platform	161

G

generating	
certificate signing requests	353
geographic redundancy	
System Manager	39
geographical redundancy	
data center	47
geographically distributed system	
considerations	41
topology	20
global catalog	
attributes replication	280
Google Cloud Platform	
adding virtual hard disks	172
configuring firewall rules	161
creating load balancer	170
deploying virtual machines	157 , 165
instance group	169
peering	161
redirection rules for port 443	175
reimaging operating system disk	167

H

haveged	
enabling	105
Host Client	83
hosts	
enabling editing	174
Hyper-V	
adding virtual hard disks	138
configuring CPU settings	139
configuring ports	140

Hyper-V (continued)

creating virtual machine	136
creating virtual switch	135
deploying virtual machines	131
disabling time synchronization	138
enabling	134
host requirements	35
network settings for virtual switch	135
Hyper-V Manager	134

I

identity certificates	355
identity provider	
mapping Keycloak attributes	262
importing	
LDAP certificate	359
SIP CA certificate	358
trusted certificate	359
Importing Certificate	266
incoming call	268
indexed attributes	282
indexing attribute	282
initial setup	
Amazon Web Services	113
Google Cloud Platform	157
Hyper-V	131
Microsoft Azure	141
VMware	77 , 98
install	
additional node	199 , 206
installation	
checklist	77 , 99 , 131
checklist for AWS software-only	113 , 142
checklist for Google Platform Cloud	157
fails	334 , 335
on customer-provided physical servers or virtual machines	98
third-party certificates	42
installation checklist	177
installation data	27
installation fails	
Avaya Aura elements use third-party certificates	335
installation time	
for Cassandra	188
for Keycloak	188
installing	
additional RPMs for software-only	107
Avaya Aura Device Services	179
CA certificate	312
certificate to SBCE	311
Device Services in environment without Aura	189
RHEL	101
system layer for software-only	108
installing LDAP schema snap-in	280
installing RPMs for software-only	105
instance group	169

IPv6		
enabling	93 , 112	
K		
KB		
Support site	346	
key pair		
creating	118	
Keycloak		
configuration	257	
configuring	258	
creating client mapping	260	
installation time	188	
mapping identity provider attributes	262	
obtaining client secret	260	
realm configuration for UC servers	257	
starting and stopping	259	
web administration portal	260	
Keycloak configuration	267	
Keycloak Truststore	266	
KVM version		
Avaya Aura® application	33	
L		
latency		
requirements for clustering	41	
LDAP	267	
advanced Configuration Utility settings	244	
authentication domain requirements	42 , 280	
configuration	296	
Configuration Utility settings	234	
global catalog	280	
indexing attributes	282	
multiple authentication and authorization domains	291	
secure connection	359	
supported characters	243	
validation	188	
LDAP configuration		
Active Directory authentication parameters	288	
Active Directory binding parameters	287	
Active Directory internationalization parameters	289	
Active Directory role search parameters	289	
Active Directory user management parameters	290	
attribute mapping	292	
attribute value requirements	281	
change LDAP parameters after installing cluster	214	
configuring photoURI attribute	295	
Microsoft Active Directory	284	
property file examples	364	
System Manager login name use cases	293	
LDAP parameter		
descriptions	296	
LDAP referrals	365	
LDAP search results	365	
LDAP server		
LDAP server (<i>continued</i>)		
user synchronization after deployment	284	
LDAP server certificate	265	
license	73	
load balancer		
configuring on Google Cloud Platform	170	
configuring on Microsoft Azure	154 , 155	
for AWS software-only installation	128	
Google Cloud Platform instance groups	169	
Nginx requirements	52	
requirements	50	
load balancer certificates		
AWS deployment	116	
Locations	87	
LVM		
enabling in Google Private Cloud	173	
M		
Microsoft Azure		
adding virtual hard disks	147	
assigning security groups	152	
configuring load balancer	155	
configuring secondary network interface	146	
configuring traffic rules	150	
creating load balancer	154	
deploying virtual machine	146	
deploying virtual machines	141	
resource profile specifications	35 , 36	
multiple authentication domains	291	
N		
network parameters for VM deployment	81	
networking considerations		
Amazon Web Services	38	
new in release	17 , 18	
new in this release		
Release 10.2	18	
Nginx		
requirements	52	
non-Aura deployment	25	
non-Aura environment		
installing Avaya Aura Device Services	189	
Non-Aura environment		
third-party certificates	42 , 45	
non-root administrative user		
creating	103	
NTP time source	370	
Nutanix	381 , 382	
O		
OAuth		
configuring Keycloak	258	
conifugration	257	

OAuth (<i>continued</i>)	
enabling database replication	264
web administration portal	260
Open LDAP	
configuring photoURI attribute	295
replication	256
Open LDAP replication	
replication is failed	340
TLS negotiation failure error	340
OpenLDAP	
enabling data replication	255
OpenSSL	354
optional RPMs	107
OVA	
data encryption field descriptions	81
deploying using Host Client	83
deploying using vSphere Client	78
OVA-based deployments	
deploying virtual machines	77
overview	
Avaya Aura Device Services	17
P	
packages	
RHEL package management	107
pairing Session Manager	
with Device Services node	272
password	
changing default password for automatic backups	226
password rules	
configuring	69
supported characters	56
peering	161
performance best practices	370
pinging	
Session Manager	111
System Manager	111
Platforms	87
PLDS	
downloading software	74
port	
external load balancer	52
port configuration	
cluster	319
ports	
SNMP	302
post-installation script	
running	223
PPM rate limiting	
enabling	273
prerequisites	
for device authorization flow configuration	54
for SAML v2.0/OAuth2 SSO configuration	53
for SSO configuration	52
for Workspaces SSO configuration	55
system layer installation on AWS	126

prerequisites (<i>continued</i>)	
system layer installation on Azure	153
system layer installation on Google Cloud Platform ...	174

R

Red Hat subscription	107
Reestablish Connection	87
related documentation	342
remote worker configuration	
A10 client SSL certificate	322
A10 client SSL template	325
A10 server SSL certificate	323
A10 server SSL template	324
creating IP source NAT	326
importing root certificate	324
required	
skills and knowledge	27
requirements	
external load balancer	50
for Hyper-V host machine	35
LDAP attribute values	281
network latency for clustering	41
Nginx	52
resolv.conf	
does not contain DNS addresses	337
resources	
server	30
reverse proxy	
checklist	304
port configuration	319
reviewing	
data encryption status	71
RHEL	381
additional RPMs	104
installing	101
packages	107
RHEL Installation	382
RSA public and private keys	213
running	
post-installation script	223
runUserDiagnostics	337

S

SAML v2.0/OAuth2 SSO	
prerequisites	53
saving	
LDAP settings	283
searching for content	343
secure boot	96
checking status	96
secure LDAP connection	359
security groups	
assigning in Microsoft Azure	152
configuring for eth1 on AWS	123
seed node	

seed node (<i>continued</i>)		
configuring additional seed node	217	
installation	179	
seed node installation	199	
service unavailable	333	
serviceability agents	299	
Session Manager		
configuring for cluster environments	268	
Session Manager Service States		
effect on Avaya Aura Device Services	274	
setting up		
user synchronization after deployment	284	
settings		
Hyper-V virtual machine	138	
sharing content	343	
silent installation	217	
single sign-on		
enabling OAuth database replication	264	
skills and knowledge	27	
snapshots	376, 385, 390, 392	
SNMP	299, 301	
installation	302	
Send to a third-party server	302	
verify	303	
SNMP target profile		
setting up	300	
SNMPv3 user profile		
assigning	301	
setting up	299	
software requirements	31	
software-only		
additional packages	107	
additional RPMs	104	
Amazon Web Services		
prerequisites for software-only		
installation	115	
Amazon Web Services installation prerequisites	115	
checklist		
AWS software-only installation	113, 142	
software-only installation	99, 131	
configuring DNS settings	123	
configuring idle timeout	131	
configuring security groups for eth1	123	
create disk partitioning on AWS	124	
create disk partitioning on VMware	102, 140	
creating disk partitioning for Google Cloud Platform	173	
creating disk partitioning for Microsoft Azure	149	
creating security groups for AWS	118	
creating target groups on AWS	127	
disk partitions	101	
enabling Haveged service	105	
enabling IPv6	93, 112	
enabling root access for AWS VM	124	
enabling root access on GCP	168	
enabling root access on Microsoft Azure	148	
Google Cloud Platform		
deployment prerequisites	160	
Microsoft Azure (<i>continued</i>)		
Google Cloud Platform installation prerequisites	160	
installation checklist	99, 131	
installation checklist for AWS	113, 142	
installation checklist for Google Cloud Platform	157, 164	
installing RHEL on AWS	121	
Microsoft Azure		
deployment prerequisites	145	
Microsoft Azure installation prerequisites	145	
system layer installation	108	
system layer prerequisites for AWS	126	
system layer prerequisites for Azure	153	
system layer prerequisites for Google Cloud		
Platform	174	
uninstalling system layer	227	
software-only deployments	98	
Amazon Web Services	113	
Google Cloud Platform	157	
Hyper-V	131	
Microsoft Azure	141	
VMware	98	
software-only installation		
creating administrative users	103	
solution topology	19	
sort documents	343	
special characters	56	
for LDAP attributes	243	
specifications		
virtual disk volume	37	
SSH connections		
cluster	213	
SSH timeout	72	
SSO		
prerequisites	52	
standalone environment		
considerations for migrating to cluster	39	
standalone installation	179, 189	
starting		
Keycloak service	259	
virtual machine	92	
stickiness attribute	127	
STIG hardening		
disabling additional hardening options	95	
enabling	95	
stopping		
Keycloak service	259	
storage	375	
subscription		
Red Hat subscription	107	
support	345	
supported hardware and resources	30	
synchronizing		
certificate to SBCE	311	
sys	58	
sys ipv6config	67	
sys secconfig	60	
sys smcvmgt	65	

sys versions	60
sys volmgt	61
system layer	
commands	58
for software-only	108
ipv6config	67
seconfig	60
smcvemgt	65
versions	60
volmgt	61
system manager	
adding	270
System Manager	
geographic redundancy mode support	39
primary System Manager fails	339
System Manager certificates	334

T

target groups	127
third-party certificates	42
for Avaya Aura Device Services environment	43
for environment without Avaya Aura	45
System Manager	44
third-party root CA	357
time synchronization	
checking status	111
timekeeping	370
timeout	72
TLS client profile	
creating	316
TLS negotiation failure	340
TLS server profile	
creating	313
tmux	72
topology	
geographically distributed system	20
traffic rules	
Avaya Aura Device Services security group	121
Google Cloud Platform	162 , 163
traffic rules for security groups	
Avaya Aura Device Services	119 , 151
Device Services load balancer	120
Utility Server	120 , 152
troubleshooting	274 , 334
app uninstall is not working	336
Avaya Aura Device Services installation fails	335
DNS entries in resolv.conf	337
overview	332
System Manager certificates	334
third-party certificates	335

U

UEFI	96
UEFI secure boot	
checking status	96

uninstalling	
Avaya Aura Device Services	226
system layer for software-only application	227
Update Static Routing	87
upload	
certificate file	309
uploading CA certificate files	361
user data retention	24
Utility Server	189
configuring secondary network interface	146
configuring virtual IP	251
considerations	42

V

validate LDAP settings	188
videos	345
viewing	
certificate details	348
current CA	358
virtual IP	
migration from standalone to cluster environments	39
virtual IP address	
configuring	215
virtual IP and FQDN in AWS deployments	189
virtual machine	
Azure resource requirements	35 , 36
resource requirements	34
Virtual Machine	381
virtual machine backups	
creating	385
space	388
virtual machine backups (clone)	
definition	385
rolling back	392
validating	390
virtual switch	135
configuring network settings	135
vMotion	376
VMware	378
changing Avaya Aura Device Services password	75
deploying virtual machines	77 , 98
VMware deployment options	78
VMware High Availability	375
VMware networking	
best practices	372
VMware software requirements	31
VMware Tools	371
VMware_Features	378
VPC peering	161
vSphere	378
vSphere Client	78

W

watchlist	343
web administration portal	

web administration portal (<i>continued</i>)	
Keycloak	260
Windows firewall	
configuring ports for Hyper-V	140
Workspaces SSO	
prerequisites	55