Deploying Avaya Aura® Device Services

Release 8.0
Issue 1
July 2019

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 mediums which may include product information, 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. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Hosted Service

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

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way

any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: 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 Inc.

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

Contents

Chapter 1: Introduction

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*.

Prerequisites

Before deploying the product, ensure that you have the following knowledge, skills, and tools.

Knowledge

- System Manager
- Session Manager
- Presence Services
- Avaya Session Border Controller for Enterprise
- Solution Deployment Manager (SDM) and SDM client
- Cassandra database
- LDAP Server
- vSphere client
- Certificates
- Avaya Equinox® clients

Skills

- To deploy Session Manager.
- To set up the enterprise LDAP directory.
- To administer the System Manager console.

Tools

For information about tools and utilities, see Configuration tools and utilities.

Change history

Issue	Date	Summary of changes
Release 8.0, Issue 1	July 2019	• Updated New in this release on page 11. • Updated Planning checklist on page 17. • Updated Avaya Aura Device Services virtual machine resource requirements on page 24. • Updated VMware software requirements on page 24. • Updated Installation checklist on page 53. • Added Enabling IPv6 support at the system layer on page 82. • Added Enabling FIPS mode on page 83. • Updated Installing Avaya Aura Device Services on page 84. • Updated Performing a silent installation on page 93. • Updated Initial configuration with the Avaya Aura Device Services configuration utility on page 109. • Updated Configuring Avaya Aura Device Services using the configuration utility on page 110. • Updated LDAP configuration on page 115. • Added a new section, OAuth configuration on page 135. • Added Configuring Keycloak settings on page 136. • Added Starting and stopping the Keycloak service on page 138. • Added Enabling OAuth database replication in a cluster environment on page 142. • Updated Amazon Web Services deployments on page 65. • Minor rephrasing throughout the document.

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, and it can also provide file server capabilities, such as providing 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 Equinox®.

SIP endpoints, such as Avaya Equinox®, 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 Equinox® 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 Equinox®, you cannot manually force the software to update unless it is configured through Avaya Aura® Device Services.

New in this release

The following is a summary of new functionality that has been added to Avaya Aura® Device Services in Release 8.0.

FIPS

Avaya Aura® Device Services is FIPS 140-2 compliant. FIPS is a cryptographic security standard. You can choose to enable or disable FIPS mode during Avaya Aura® Device Services installation depending on your enterprise requirements.

Support for Internet Protocol version 6 (IPv6)

IPv6 is the successor to IPv4. IPv6 has several advantages over IPv4, including more efficient routing, simplified network configuration, and native support for IPSec. IPv6 can coexist with IPv4 networks, easing the transition process.

Note:

Amazon Web Services (AWS) deployments do not support IPv6.

SAML/OAuth

OAuth is an authorization mechanism that enables users to authenticate using a combination of enterprise credentials and other factors that the enterprise has chosen, including enterprise Single Sign-On (SSO) and two-factor authentication. The capabilities are provided by a third-party identity provider. Currently, Avaya Aura® Device Services only supports the Shibboleth identity provider.

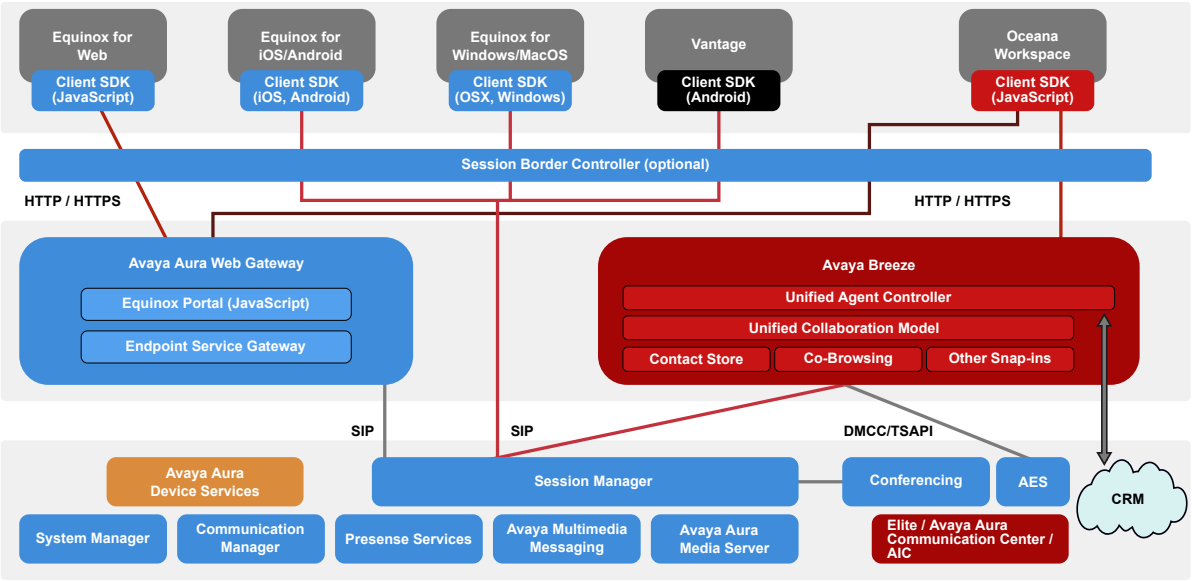
You need an activation code to activate and use OAuth.

Password masking

For security reasons, Avaya Aura® Device Services does not display the actual values for automatic configuration settings that represent passwords on the web administration portal. For these settings Avaya Aura® Device Services displays the special value **********.

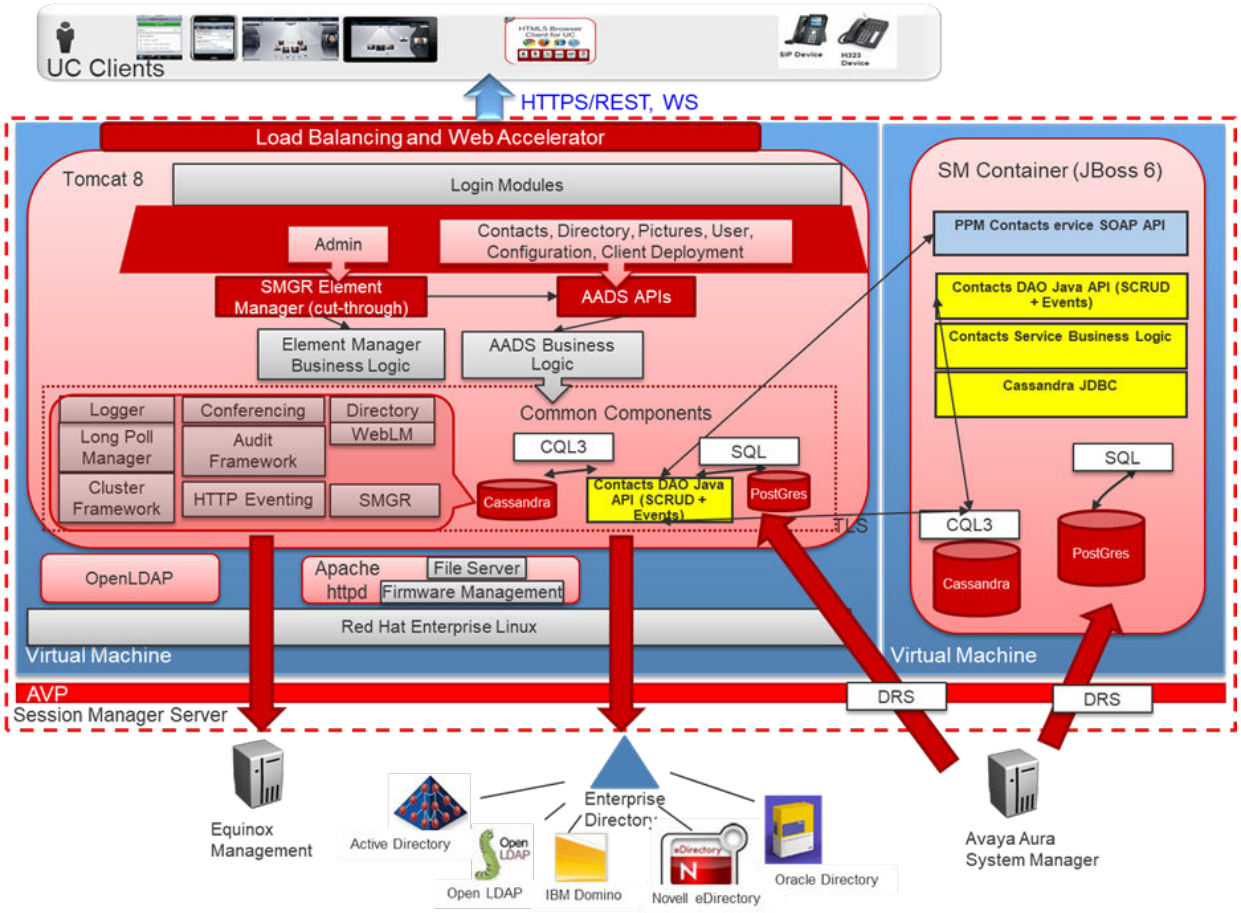
Solution topology

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



Avaya Aura® Device Services architecture topology

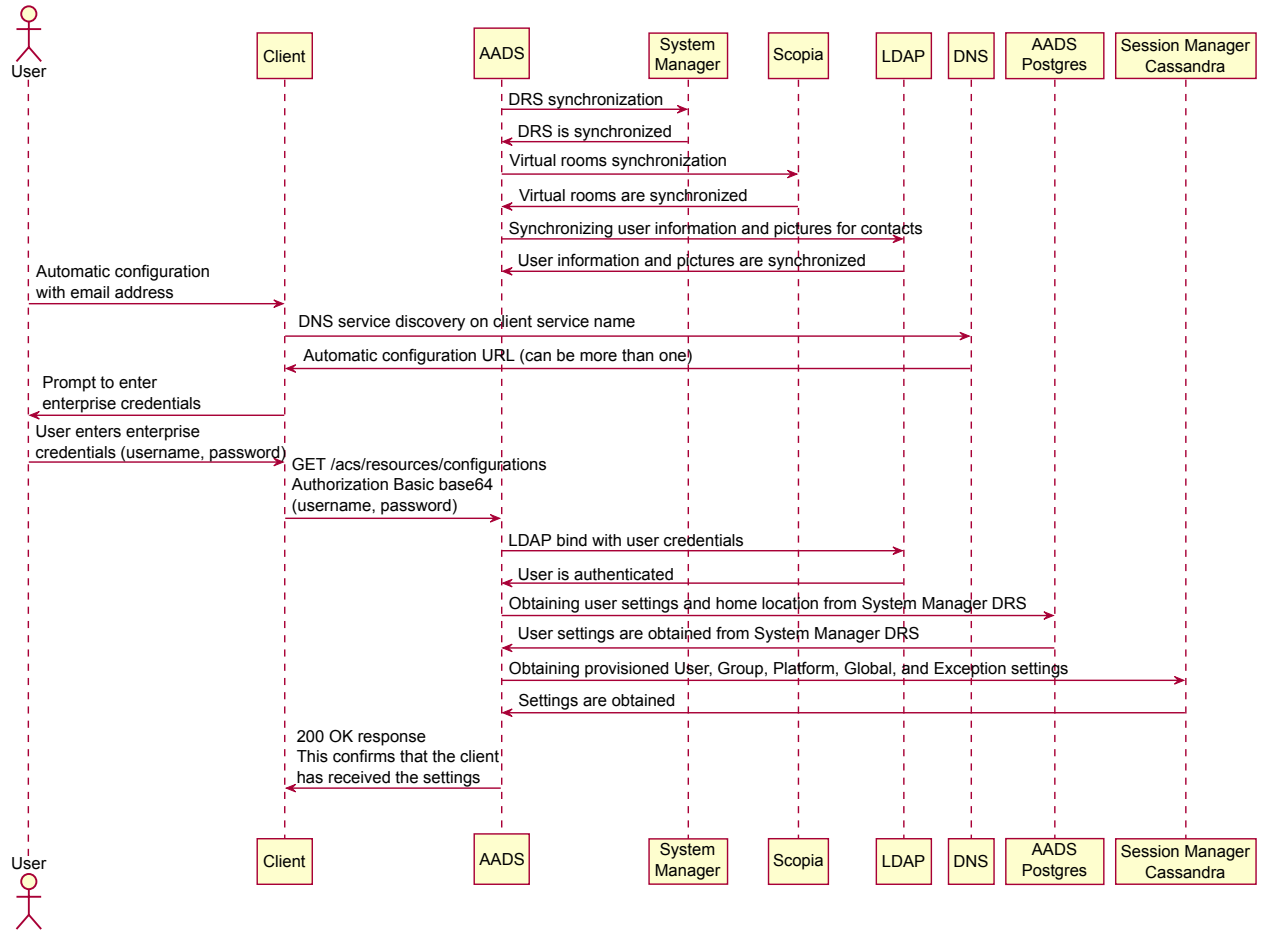
The following diagram shows the Avaya Aura® Device Services architecture:



Avaya Aura® Device Services is aligned with Session Manager, Appliance Virtualization Platform, and the VMware virtualized environment. The VMware license embedded in the Appliance Virtualization Platform does not support vCenter.

Automatic configuration flow

The following diagram shows the automatic client configuration flow.



Components

The following table lists key components that interwork with Avaya Aura® Device Services. 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. • 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.
Avaya Aura® Session Border Controller (Avaya SBCE)	Avaya SBCE 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 at the same time.
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.
Appliance Virtualization Platform	A platform that is a customized OEM version of VMware ESXi. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.
Solution Deployment Manager	The centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.

Virtualized components	Description
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
- Appliance Virtualization Platform

Chapter 3: Planning

Planning checklist

Review this chapter before installing the Avaya Aura® Device Services server. You can deploy Avaya Aura® Device Services using VMware, AWS, or Solution Deployment Manager.

Warning:

When you deploy Avaya Aura® Device Services, avoid copying and pasting commands directly from this document. This can introduce unwanted characters and errors. Double-check all inputs you copy or type them manually.

Ensure you follow the steps in sequence before deploying the Avaya Aura® Device Services OVA.

No.	Task	Notes	✔
1	Identify the hypervisor and verify that the capacity meets the OVA requirements.	See Avaya Aura Device Services virtual machine resource requirements on page 24. **Important:** As of Release 7.1.5, Avaya Aura® Device Services does *not* support Appliance Virtualization Platform (AVP) deployments on CSR3 and below. For more information, see Avaya Aura Device Services support for Appliance Virtualization Platform on page 24.	
2	Plan the staging and verification activities and assign the resources.	See AADS virtual machine resource requirements on page 24.	
3	Download the required Avaya Aura® Device Services OVA.	See Downloading software from PLDS on page 22. See Configuration tools and utilities on page 27. **Note:** Avaya Aura® Device Services is an entitlement, so it does *not* require any licenses.	

No.	Task	Notes	✔
4	Verify the md5sum of the OVA file matches with the md5sum on PLDS.		
5	Gather and keep configuration data ready.	See *Avaya Aura® Device Services Questionnaire* and Data required for installation on page 20.	
6	Deploy Avaya Aura® Device Services on the same subnet as the Session Manager management subnet.		
7	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 ms. • The Avaya Aura® Device Services servers, load balancers, and virtual IP are in the same subnet.		
8	Determine whether to install Avaya Aura® Device Services in a standalone or 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. For single node installations, see Deploying AADS OVA on page 57 and Post deployment configuration on page 143. For cluster node installations, in addition to Deploying AADS OVA on page 57 and Post deployment configuration on page 143, see Cluster node configuration on page 95.	

No.	Task	Notes	✔
9	If you are using a single authentication directory, ensure that all users are in a single authentication domain. **Note:** This is not required if you are using multiple authentication directories.	The first LDAP domain added to the system 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.	
10	If you are planning to use third-party CA signed certificates, ensure that you have the following certificates: • System Manager root CA certificate. • Third-party root CA certificate. • Intermediate CA certificates. • Third-party CA-signed identity certificate chain to be used for Avaya Aura® Device Services.	See Third-party CA-signed certificates on page 25. Use third-party certificates if you are not using System Manager for certificate management.	
11	To use an external load balancer, review the external load balancer requirements.	See External load balancer requirements on page 26.	
12	To use OAuth, obtain the OAuth activation code.	Currently, the OAuth feature is a controlled introduction feature. To enable it, you must enter the activation code during Avaya Aura® Device Services installation. To obtain the activation code, contact Avaya product management. For more information, see *Avaya Aura® Device Services Release Notes* for Release 8.0.	

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.
- 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 2008, 2012, and 2016 • Microsoft Active Directory Lightweight Directory Services (LDS) 2008 and 2012 • IBM Domino Server 7.0 and 8.5.3 • Novell e-Directory 8.8 • Open LDAP 2.4.44 • Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1.7.0)		

Parameter	Notes	Value	✔
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 115 or Examples of Microsoft Active Directory LDAP property files on page 222.		
System Manager FQDN	You must know the System Manager FQDN before attempting installation.		
System Manager enrollment password	If you use System Manager for enrolling certificates, ensure you have the enrollment password. Go to System Manager home page, and click **Security** > **Enrollment Password** to check whether the enrollment password has expired. If the **Time Remaining** field displays zero, the password has expired and must be changed.		
Session Manager Asset IP	To view the Session Manager Asset IP address, go to the System Manager home page, and click **Session Manager** > **Session Manager Administration**. Then, in the **Session Manager Instances** tab, select a Session Manager instance, and click **View**. The Session Manager asset IP address is displayed in the **SIP Entity IP Address** field.		

Parameter	Notes	Value	✔
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**. Then, in the **Session Manager Instances** tab, select a Session Manager instance, and click **View**. The Session Manager management IP address is displayed in the **Management Access Point Host Name/IP** field.		
Keystore password	Set this while running the binary installer to any password of 6 characters or more.		
Avaya Aura® Device Services CLI user name	While running the binary installer, use the same user name that you specify while 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. By using the profile chosen during Session Manager deployment and the number of users you need to support, determine how many nodes you will need.		
IP addresses/ 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. For example, for deploying 3 nodes, you must have 4 IP addresses: one for each node, and one IP for the virtual IP address.		

Downloading software from PLDS

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. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from http://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. Enter http://plds.avaya.com in your Web browser 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 on the search icon (magnifying glass) for **Company Name**.
6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. 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.
13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

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 http://www.vmware.com/resources/guides.html.

Avaya Aura® Device Services support for Appliance Virtualization Platform

Appliance Virtualization Platform (AVP) deployments on CSR3 and below are not supported. As of Avaya Aura® Device Services Release 7.1.5, the required disk space has increased to a total of 250 GB, so you must use the updated Avaya Converged Platform (ACP) 130 server.

VMware software requirements

The following VMware software versions are supported:

- VMware vSphere ESXi 6.0, 6.5, and 6.7
- VMware vCenter Server 6.0 and 6.5

Avaya Aura® Device Services virtual machine resource requirements

	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
Session Manager Device Footprint	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	Up to 1200 Devices	Up to 2700 Devices	Up to 4200 Devices	Up to 6000 Devices	Up to 13,900 Devices
CPU Minimum	1150 MHz, 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*.

Supported servers

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

- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R610
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R620
- HP ProLiant DL360 G9
- Dell™ PowerEdge™ R630
- Dell™ PowerEdge™ R640

Third-party CA-signed certificates

If you do not 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 private or public certificate authority. You can import third-party CA certificates either during or after Avaya Aura® Device Services installation.

If you are planning to use third-party certificates specific to your organization, you must obtain the following certificates before installing Avaya Aura® Device Services:

- The System Manager root CA certificate in the 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.
- The 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

Installing Avaya Aura Device Services on page 84

External load balancer requirements

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

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.	The load balancer must be able to route requests based on the request URL. For example, requests that start with `/acs` on port 443 must be routed to Avaya Aura® Device Services.
The HTTP load balancer must support URL rewrite.	The load balancer must be able to modify the URL path of the request based on simple rules to remove or rename parts of the path.
The HTTP load balancer must support TLS 1.2.	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: `https://<AADS FQDN>:8457/health` To avoid leaving multple 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.

Requirement	Description
The HTTP load balancer must be able to insert custom headers to HTTP requests.	

Related links

Port configuration for an external load balancer on page 52

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

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			
/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	

Disk Volume	Volume Size (GiB)			
	Disk 1 (sda)	Disk 2 (sdb)	Disk 3 (sdc)	Disk 4 (sdd)
/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*.

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 app without arguments, the system displays the available subcommands. For example, the following commands give the same results • `sudo /opt/Avaya/DeviceServices/`*`version`*`/CAS/bin/backupAADS.sh` • `app backup`
svc	Provides commands for managing services, such as starting, stopping, and viewing status. If you type svc without arguments, the system displays the available subcommands. For example, to start Avaya Aura® Device Services services, run the `svc aads start` command.
cdto	Provides an easy way to navigate through directories of the installed application. If you type cdto without arguments, the system displays the available subcommands. For example, the following commands give the same results: • `cd /opt/Avaya/DevicesSerivces/`*`version`*`/CAS/`*`version`* • `cdto cas`

app commands

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

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

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
`cdto base`	`/opt/Avaya`
`cdto root`	`/opt/Avaya/DeviceServices`
`cdto active`	`/opt/Avaya/DeviceServices/<version>`
`cdto cas`	`/opt/Avaya/DeviceServices/<version>/CAS/<version>`
`cdto misc`	`/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc`
`cdto bin`	`/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin`
`cdto config`	`/opt/Avaya/DeviceServices/<version>/CAS/<version>/config`

Command	Navigation target
cdto logs	/opt/Avaya/DeviceServices/<*version*>/CAS/<*version*>/logs
cdto ilogs	/opt/Avaya/DeviceServices/.AADSInstallLogs
cdto tlogs	/opt/Avaya/DeviceServices/<*version*>/tomcat/<*Tomcat version*>/logs
cdto openldap	/opt/Avaya/DeviceServices/<*version*>/CAS/<*version*>/openldap

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, --hhelp
        Verbose help

Available commands:

    secconfig       [Manage security settings]
    versions        [Query version information]
    volmgt          [Manage disk volume sizes]
    smcvemgt        [Manage Spectre/Meltdown patches]
    ipv6config      [Manage server IPv6 configuration]
    extension       [Manage system layer extensions]

  Command invocation syntax:
     sys <command> <arguments>

  Command syntax
    sys <command> -h

[admin@server-dev ~]$
```

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 UCApp appliances. To obtain help with
each of these commands, use the "-h" (or "--help") argument for help
with command line syntax, and "-hh" (or "--hhelp") for verbose help.

secconfig
    Manages security-related settings.
```

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

volmgt
    Queries the sizes of existing disk volumes and extends their sizes.

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.
[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. 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. The following provides the command line syntax for this command:

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

Syntax:
    --help,                  -h
    --hhelp,                 -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 --hhelp

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

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

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 specfied,
        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
        mebibites, "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 ---------------------+
|                              |                       LVM        File System    |
| Num  Name     Size     Free |    Name               Size      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 ---------------------+
|                              |                       LVM        File System    |
| Num  Name     Size     Free |    Name               Size      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.

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 tunalbles 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 disbled 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 **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.
```

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

Appying 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
```

Resource profile specifications

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	vCPUs	Memory (GB)
AADS2100	4200 end points	c4.2xlarge	8	15
AADS5240	13900 end points	c4.2xlarge	8	15

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 http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_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, you must 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 Virtual Private Cloud (VPC) in the following ways:

Connection type	Resource
VPN connection	For information about VPN connections, see http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html.
Direct connection	For information about AWS direct connections, see https://aws.amazon.com/directconnect/.

Chapter 4: Preconfiguration

Pre-deployment checklist

Use this checklist to prepare your system before deploying the Avaya Aura® Device Services OVA file.

No.	Task	Description	Notes	✔
1	If you are using Session Manager Release 7.x, enable data storage clustering on Session Manager.	To pair a Session Manager instance with an Avaya Aura® Device Services instance, you must enable data storage clustering. If the **Enable Data Storage Clustering** field on the Session Manager Administration page is selected, all Session Manager servers are added to the Cassandra database cluster. If the **Enable Data Storage Clustering** field is not selected, all the Cassandra nodes run in standalone mode. Cassandra clustering should be done only when Avaya Aura® Device Services servers are configured and paired with Session Manager. See Enabling data storage clustering on page 43.	As of Avaya Aura® Release 8.0, Cassandra data storage clustering is enabled permanently on Session Manager.	
2	Add a data center.	See Adding a data center on page 43.		

No.	Task	Description	Notes	✔
3	Assign a Session Manager instance to a data center.	See Assigning Session Manager to a data center on page 44.		
4	Set the SSH keepalive timer.	See Configuring SSH terminal keepalive timer on page 43.		
5	Update DNS addresses and search domains.	See Updating DNS addresses and search domains on page 50.		
6	Update NTP addresses.	See Updating NTP addresses on page 51.		
7	If you do not use System Manager for certificate management and you are planning to use third-party CA-signed certificates, import CA certificates on servers that interact with Avaya Aura® Device Services.	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 Equinox® Conferencing Restart the server to activate the imported third-party certificates.		
8	If you use an external load balancer, configure external load balancer and firewall ports.	See Port configuration for an external load balancer on page 52		
9	If you are planning to enable FIPS on Avaya Aura® Device Services, ensure that FIPS mode is enabled on both System Manager and Session Manager.	For information about enabling FIPS on Session Manager, see the “Security” chapter in *Administering Avaya Aura® Session Manager*. For information about enabling FIPS on System Manager, see the “Security” chapter in *Administering Avaya Aura® System Manager*.		

Configuring SSH terminal keepalive timer

About this task

If the SSH terminal expires when installation is in progress, you will have to restart the installation.

Procedure

1. Open PuTTY.
2. In the Category section, click **Connection**.
3. In the **Seconds between keepalives** field, type an interval in milliseconds.

   When you set a non-zero value in this field, the system sends a keepalive message periodically, and prevents the session from timing out

Enabling data storage clustering

About this task

Use this procedure to enable data storage clustering to activate Cassandra data replication and assign Session Manager instances to discrete data centers for geo-redundancy. This process is enabled automatically with Avaya Aura® Release 8.0 or later, but with earlier releases you must perform this procedure.

You must use Data Center assignment when Session Manager servers are geographically separated.

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the **Global Settings** tab, click **Enable Data Storage Clustering**.
3. Click **Commit**.

Adding a data center

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, and then click **New**.

   The system displays the Edit Data Center page.
3. In the **Name** field, type the data center name.

4. In the **Description** field, type the description about the data center.
5. Click **Commit**.

Note:

The system might display a warning message. However, the process is unaffected, and you can proceed to add the data center.

Data Center page field descriptions

Name	Description
Data Center	The name of a data center.
Description	The description of a data center.
Details	The details of the Session Manager instances assigned to a data center.
# of assigned SMs	The number of core Session Manager instances assigned to a data center.
SM	The name of the core Session Manager assigned to a data center.
Description	The description of the core Session Manager.

Name	Description
New	Creates a new Data Center. Assigns Core Session Managers to any Data Center.
Edit	Modifies a Data Center name, description, or modifies assignment of Core Session Manager to any Data Center.
Delete	Deletes a data center if the data center is not assigned to a core Session Manager server.
View	Displays the read only view of Data Center.

Assigning Session Manager to a data center

Before you begin

Data Centers need to be added before the Session Manager assigning.

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.

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**.

   The system 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, the system 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, the system displays the assigned data center under the **SMs unassigned or assigned to other Data Center** section.
5. Click **Commit**.

   The system displays the Confirm Data Center assignments page.
6. Verify the data center and SM assignment.
7. Click **Confirm**.

Setting up the DNS server

About this task

You require the DNS setup only if the user uses an email address for automatic configuration. You do not need the DNS setup if the user uses a standard web address.

Create records on the DNS server of the enterprise to link your DNS server to the settings file. Use split-horizon DNS and the same FQDN for Session Border Controller and Session Manager if you want to prevent users from re-configuring their clients when working outside of the enterprise network.

Note:

You might need to discuss with your DNS provider if your level of service is sufficient to provide support for DNS Service Discovery (DNS-SD). For more information, see DNS-Based Service Discovery. Avaya Equinox® uses DNS PTR records consistent with the DNS-SD RFC, which in some cases might require an additional level of service from your DNS provider.

Before you begin

- Create the settings file.
- Configure a web server and save the settings file to that web server. You must know the URL of the file on the web server.
- Set the following information based on your DNS server policy:
  - SRV and TXT record time-to-live period in seconds. For example, 300. During this time, the client or intermediate servers might cache the retrieved record. Usually, the SRV and TXT record time-to-live periods share the same value.

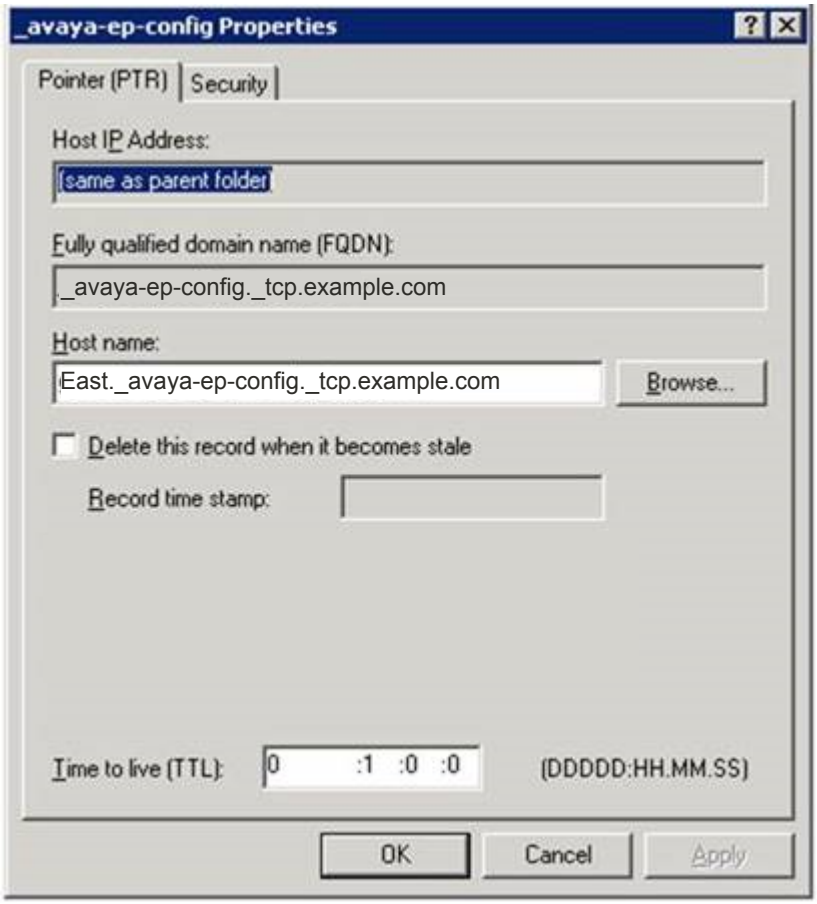
- Web server port number. You can enter 0 to keep the default port number for the protocol.
- SRV record priority. For example, 0.
- SRV record weight. For example, 0.

Procedure

1. Create a PTR record that links the descriptive name of your settings file to the domain of the enterprise.
   a. Ensure that you name the PTR record as `_avaya-ep-config._tcp.<domain>`.
   b. Use the descriptive name for the settings file as the target of the PTR record: `<Descriptive name>._avaya-ep-config._tcp.<domain>`.

   The following is an example of a PTR record: `_avaya-ep-config._tcp.example.com. IN PTR East._avaya-ep-config._tcp.example.com`.

   In case of Microsoft DNS Manager, the following is an example of a PTR record:



Tip:

In the left pane of Microsoft DNS Manager, you must create the PTR, SRV, and TXT records at the *_avaya-ep-config* level. If the *_avaya-ep-config* level does not exist, you must manually create the same. Right-click *_avaya-ep-config* and then click **Other New Records**, select the resource record type, and then click **Create Record**.

2. Create an SRV record linking the descriptive name of your settings file to the web server where the file resides.

   If the URL to the settings file is `https://server.example.com/East_settings.txt`, then the server name is `server.example.com`.

   An SRV record also includes the following information:

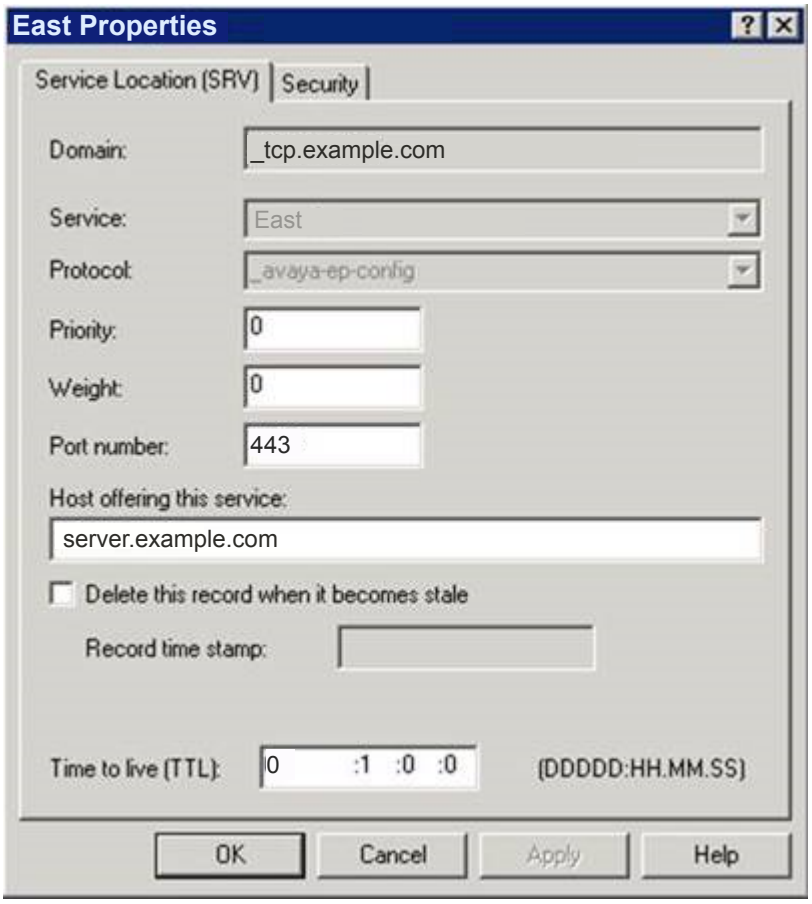
   - SRV *time-to-live* period in seconds during which the client or intermediate servers might cache the retrieved record.

   The following is an example of an SRV record: *East*`._avaya-ep-config._tcp.`*example.com*`. 300 IN SRV 0 0 443 server.example.com`.

   In this example:

   - 300 is the time-to-live period
   - The first zero is the priority, the second zero is the weight, and 443 is the port number.

   In case of Microsoft DNS Manager, the following is an example of a SRV record:



3. Create a TXT record linking the descriptive name of your settings file to the remaining URL information.

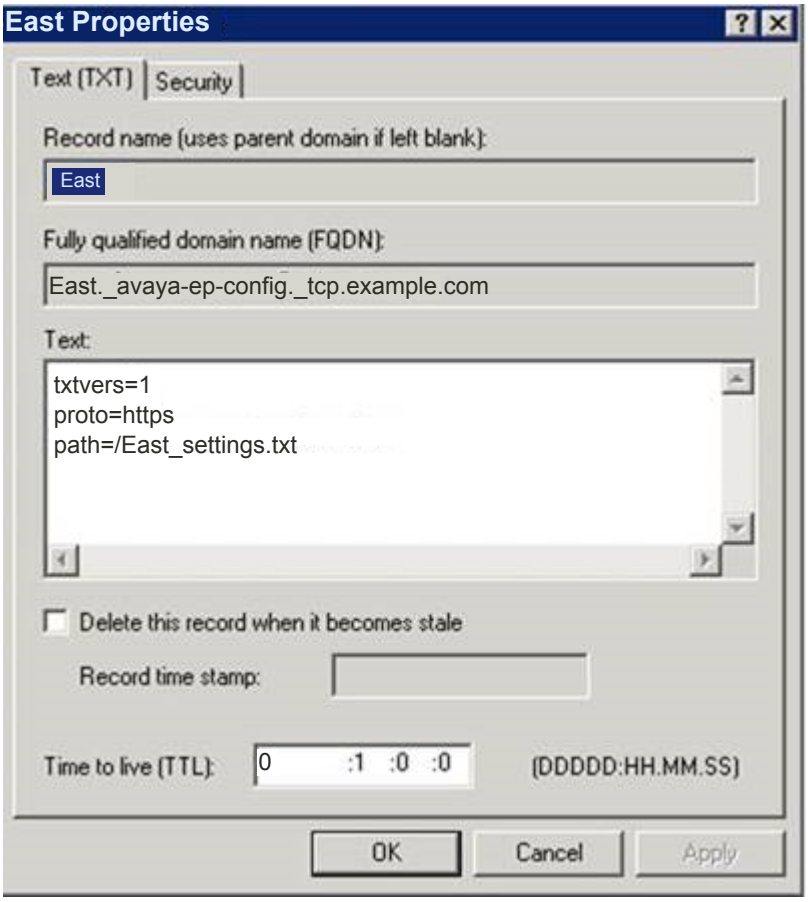
   TXT records are provisioned differently depending on the DNS server. However, all TXT records must have the following parameters:

   - *txtvers*: The text version of the TXT record. This value indicates the structure version of the record. You must always set the value to `1`.
   - *path*: The path to the settings file. An example value is `path=/East_settings.txt`.
   - *proto*: The web server access scheme. This value is usually `http` or `https`.

   The following is an example of a TXT record: `East._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/East_settings.txt"`

   In this example, 300 is the time-to-live period.

   In case of Microsoft DNS Manager, the following is an example of a TXT record:



Sample DNS SRV records configuration

Note:

You might need to discuss with your DNS provider if your level of service is sufficient to provide support for DNS Service Discovery (DNS-SD). For more information, see DNS-Based Service Discovery. Avaya Equinox® uses DNS PTR records consistent with the DNS-SD RFC, which in some cases might require an additional level of service from your DNS provider.

To support automatic configuration, you must configure the PTR, SRV, and TXT records in your DNS server configuration. For more information, see the documentation of your DNS server.

PTR records

Provides a list of configurations with multiple PTR records.

Format: `_avaya-ep-config._tcp.<domain>. IN PTR <Descriptive name>._avaya-ep-config._tcp.<domain>`

Examples:

- `_avaya-ep-config._tcp.example.com. IN PTR East._avaya-ep-config._tcp.example.com`
- `_avaya-ep-config._tcp.example.com. IN PTR West._avaya-ep-config._tcp.example.com`

SRV records

Provides a link from the descriptive name to the web server where you stored the file.

Format: `<Descriptive name>._avaya-ep-config._tcp.<domain>. <TTL> IN SRV <priority> <weight> <port number> <web server FQDN>`

Examples:

- `East._avaya-ep-config._tcp.example.com. 300 IN SRV 0 0 443 server.example.com`
- `West._avaya-ep-config._tcp.example.com. 300 IN SRV 0 0 443 server.example.com`

TXT records

Provides a link from the descriptive name to the URL information, protocol, and path.

Format: `<Descriptive name>._avaya-ep-config._tcp.<domain>. <TTL> IN TXT "txtvers=1" "proto=<http or https>" "path=<file path>"`

Examples:

- `East._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/East_settings.txt"`
- `West._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/West_settings.txt"`

Related links

Configuration tools and utilities on page 27

Updating DNS addresses and search domains

About this task

DNS address and search domains are configured while deploying the Avaya Aura® Device Services OVA. Use this procedure to configure DNS address and search domains after Avaya Aura® Device Services installation.

Procedure

1. Log in to Avaya Aura® Device Services using administrator credentials.
2. To create a local copy of the configuration file, type the following commands:

```
cd $HOME
cp /etc/resolv.conf .
cp ./resolv.conf ./resolv.conf.orig
```

3. To edit the local file with the new information, type `vi ./resolv.conf`.
4. Update the search domain and IP addresses as required.

   Search domains are space delimited, on a single line as per the following format: search *domain-name domain-name domain-name*....

   You can add one DNS name server on each line, as per the following format: nameserver *ipv4–address*.
5. To verify the changes, type `diff ./resolv.conf.orig ./resolv.conf`.
6. To replace the system file, type `sudo cp ./resolv.conf /etc/resolv.conf`.
7. To inspect the updated system copy, type `cat /etc/resolv.conf`.
8. To clean up local copies, type `rm ./resolv.conf ./resolv.conf.orig`.

Updating NTP addresses

Procedure

1. Log in to Avaya Aura® Device Services using administrator credentials.
2. To create a local copy of the configuration file use the following commands:

```
cd $HOME
cp /etc/ntp.conf .
cp ./ntp.conf ./ntp.conf.orig
```

3. To edit the local file with new information, type `vi ./ntp.conf`.

   The relevant entries are listed at the bottom of the file.

   Every configured NTP server has a pair of lines in the following format:

   - server *ipv4_address* iburst
   - restrict *ipv4_address* mask 255.255.255.255 nomodify notrap noquery
4. Add, update, or remove these pairs of lines for every NTP server.

   Replace the *ipv4_address* with the ipv4 address of the NTP server, keeping all remaining content for these lines unmodified.
5. To verify changes, type `diff ./ntp.conf.orig ./ntp.conf`.
6. To replace the system file, type `sudo cp ./ntp.conf /etc/ntp.conf`.
7. To inspect the system file, type `cat /etc/ntp.conf`.
8. To clean up the local files, type `rm ./ntp.conf ./ntp.conf.orig`.
9. To restart the machine so that the new settings to take effect, type `sudo reboot`.

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.
- 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 port 8448. As a result, port 8448 must be reachable from the load balancer through firewalls.

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

External load balancer requirements on page 26

Chapter 5: Initial setup

Deployment methods

Use the following sections to perform the initial VMware or AWS setup.

Important:

As of Release 7.1.5, Avaya Aura® Device Services does *not* support Appliance Virtualization Platform (AVP) deployments on CSR3 and below. You must use the ACP 130 server.

Note:

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

Installation checklist

The checklist describes the high level deployment process on VMware and AWS

No.	Task	Notes	✔
1	Deploy the OVA for the VMware or AWS environment.	The Avaya Aura® Device Services OVA file includes openjdk. Operating system updates for virtual machines include updates for openjdk.	
2	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 82. AWS deployments do not support IPv6.	

No.	Task	Notes	✔
3	Enable FIPS mode, if required.	You can only enable FIPS mode before installing the application layer. For more information, see Enabling FIPS mode on page 83.	
4	Install or restore the application layer as required.	For more information, see Installing Avaya Aura Device Services on page 84. **Note:** Avaya Aura® Device Services is an entitlement, so it does *not* require any licenses.	

VMware deployment options

Use one of the following deployment methods and then proceed to install the Avaya Aura® Device Services software.

Deploying Avaya Aura® Device Services OVA on VMware using vCenter vSphere client

Before you begin

FQDNs, where mentioned in the procedure, are mandatory.

Deploy Session Manager. For information about deploying Session Manager, see *Deploying Avaya Aura® Session Manager*.

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 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 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.

Procedure

1. In the vSphere client, click the host ESXi server.
2. Click **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, do one of the following to deploy the Avaya Aura® Device Services OVF package:
   - Click **Browse** and provide the Avaya Aura® Device Services OVA file location.
   - If the OVA file is on an http server, type the URL in the **Deploy from a file or URL** field.

   The system deploys the Avaya Aura® Device Services OVF package.
4. Click **Next**.
5. In the OVF Template Details window, verify the details of the Avaya Aura® Device Services OVA template and click **Next**.

   The system displays the End User License Agreement window.
6. Read the license agreement and click **Accept**.
7. Click **Next**.

   The system displays the Name and Location window.
8. In the **Name** field, type the name of the new virtual machine.
9. Click **Next**.

   The system displays the Deployment Configuration window.
10. In the **Configuration** field, click an Avaya Aura® Device Services profile that matches your requirement, and click **Next**.
11. In the Disk Format window, verify that the correct datastore location and available space information is displayed.
12. Accept the default disk format to store the virtual machine and virtual disks for the Avaya Aura® Device Services OVA and then click **Next**.
13. In the Network Mapping window, ensure that the correct network for that virtual machine is selected and then click **Next**.
14. Complete the **Management Network Settings** and **Account login Details** fields.

    For information about fields, see VM Deployment Configuration Parameters and Network Parameters field descriptions on page 56.

    Ensure that you deploy Avaya Aura® Device Services on the same subnet as the Session Manager to which the Avaya Aura® Device Services instance is associated.
15. Click **Next**.

    The system displays the Ready to Complete window.
16. Verify the deployment settings and click **Finish**.

    The system displays the progress of the tasks in the Deploying AADS window.

Related links

Avaya Aura Device Services virtual machine resource requirements on page 24
VM Deployment Configuration Parameters and Network Parameters field descriptions on page 56

VM Deployment Configuration Parameters and Network Parameters 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 Hostname or FQDN*	Specifies the host name or 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 to use for DNS queries. If there is more than one domain, separate each domain with a comma.
DNS Server IP Address*	Specifies the DNS server IP address of the virtual machine. If there are more than one 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 more than one NTP servers, separate each IP address or FQDN with a comma.
Timezone	Specifies the time zone of the virtual machine.
Account login Details	
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.
Admin Group name*	Specifies the group name of the administrative user.

Related links

Configuring Avaya Aura Device Services using the configuration utility on page 110
Front-end host, System Manager, and certificate configuration on page 111
LDAP configuration on page 115
Clustering configuration on page 129
Advanced configuration on page 132
Avaya Aura Device Services virtual machine resource requirements on page 24

Deploying Avaya Aura® Device Services OVA on vSphere connected directly to the host

Before you begin

Deploy Session Manager. For information about deploying Session Manager, see *Deploying Avaya Aura® Session Manager*.

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.

Procedure

1. In the vSphere client, click the host ESXi server.
2. Click **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, do one of the following to deploy the Avaya Aura® Device Services OVF package:
   - Click **Browse** and provide the Avaya Aura® Device Services OVA file location.
   - If the OVA file is on an http server, type the URL in the **Deploy from a file or URL** field.

   The system deploys the Avaya Aura® Device Services OVF package.
4. Click **Next**.
5. In the OVF Template Details window, verify the details of the Avaya Aura® Device Services OVA template and click **Next**.

   The system displays the End User License Agreement window.
6. Read the license agreement and click **Accept**.
7. Click **Next**.

   The system displays the Name and Location window.
8. In the **Name** field, type the name of the new virtual machine.
9. Click **Next**.

   The system displays the Deployment Configuration window.
10. In the **Configuration** field, click an Avaya Aura® Device Services profile that matches your requirement, and click **Next**.

11. In the Disk Format window, verify that the correct datastore location and available space information is displayed.
12. Accept the default disk format to store the virtual machine and virtual disks for the Avaya Aura® Device Services OVA and then click **Next**.
13. In the Network Mapping window, ensure that the correct network for that virtual machine is selected and then click **Next**.
14. Click **Next**.

    The system displays the Ready to Complete window.
15. Verify the deployment settings and click **Finish**.

    The system displays the progress of the tasks in the Deploying AADS window.

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 Appliance Virtualization Platform or an ESXi 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 Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Platform**, select a platform.

      The system displays the host name in the **Platform FQDN** field.

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

   The page 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. In 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.

10. Click **Deploy**.
11. Click **Accept the license terms**.

    In the Hosts for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Location <location name> page.

12. 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: • **AVP**: An Appliance Virtualization Platform platform • **Customer VE**: A customer-provided VMware ESXi platform • **SWONLY**: A customer-provided operating system platform
SSH Status	The SSH service status. The values are enabled and disabled.
Platform Certificate Status	The certificate status of Appliance Virtualization Platform 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 host 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	Refreshes the status of the platforms.
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 host. When enabled successfully, the system displays `SSH enabled successfully`.
More Actions > **SSH** > **Disable SSH**	Disables SSH on the Appliance Virtualization Platform host. When disabled, the system displays `Disabling SSH for AVP host with <IP address> <FQDN>, <username>`.

Button	Description
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.
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 > **AVP Cert. Management** > **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 host only. • **Accept Certificate**: To accept a valid certificate for the platform or vCenter. • **Decline Certificate**: To decline the certificate for the Appliance Virtualization Platform host only. 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.

Button	Description
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.
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, 8.0.
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.

Name	Description
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.
More Actions > **Restart**	Starts the selected applications that were stopped earlier.
More Actions > **Refresh VM**	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.

Amazon Web Services deployments

Amazon Web Services (AWS) is a cloud services platform that enables enterprises to securely run applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

When you deploy Avaya Aura® Device Services in an AWS environment, you must 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.

AWS deployments *do not* support IPv6.

Note:

Use the AWS Command Line Interface (CLI) for managing AWS services from your computer. For more information about setting up the AWS CLI, see https://aws.amazon.com/cli and http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html#cli-quick-configuration.

Signing in to the Amazon Web Services Management console

Before you begin

Ensure that you have an AWS account.

Procedure

1. In your web browser, type the URL https://aws.amazon.com/.
2. Click **Sign In to the Console**.

   The system displays the Amazon Web Service page and auto-populates the **Account** field.
3. In the **User Name** field, type the user name or registered email ID.
4. In the **Password** field, type the password.
5. Click **Sign In**.

   The system displays the AWS Management Console page.

Configuring AWS details using the AWS CLI

About this task

The first time that you use the AWS CLI, you must configure the AWS details.

Before you begin

Set up the AWS CLI on a computer with access to AWS. For more information, see http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html.

Procedure

1. Start a command line interpreter on the computer with the installed AWS CLI.

   Note:

   The AWS CLI supports different Windows and Linux command line interpreters, such as PowerShell or Bash.
2. From the command line interpreter, run the command `aws configure`, and do the following:
   a. For **AWS Access Key ID**, type the AWS access key ID.
   b. For **AWS Secret Access Key**, type the AWS secret access key ID.
   c. For **Default region name**, type the region name.

      For example: `us-west-2`.
   d. For **Default output format**, type `text` or `json`.

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.

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.

OVA to AMI conversion

Creating a bucket for uploading the OVAs for AMI conversion

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Storage**, and click **S3**.

   The system displays the S3 Management Console page.
3. Click **Create bucket**.

   The system displays the Create bucket dialog box.
4. In **Bucket name**, type a unique bucket name.

   Only use lowercase letters for the name.
5. In the **Region** field, click a region for your bucket.

   For more information about creating a bucket and selecting a region, see Amazon S3 Documentation.

6. Click **Create**.

Next steps

Upload the Avaya Aura® Device Services OVA.

Creating a service role

About this task

Use this procedure to create a role named `vmimport` for importing files into the S3 bucket.

Use the AWS CLI to run the commands in this procedure.

Procedure

1. Start a command line interpreter on a computer with the installed AWS CLI.
2. Run the following command to create a role named `vmimport` and let the AWS image import service assume this role:

   ```
   aws iam create-role --role-name vmimport --assume-role-policy-document <file://
   trust-policy.json>
   ```

   In this command, `<file://trust-policy.json>` is a path to the `trust-policy.json` file. This file is included in the AWS configuration files artifact.
3. Open the `role-policy.json` file, and in each `"Resource":"arn:aws:s3:::<disk-image-file-bucket>"` string, replace `<disk-image-file_bucket>` with the actual S3 bucket name.

   For example:

   ```
   "Resource": "arn:aws:s3:::my-s3-bucket"
   ```
4. Run the following command to allow the `vmimport` role to perform importing procedures:

   ```
   aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-
   document <file://role-policy.json>
   ```

   In this command, `<file://rule-policy.json>` is a path to the `rule-policy.json` file. This file is included in the AWS configuration files artifact.

Uploading the Avaya Aura® Device Services OVA

Before you begin

Download the OVAs from the Avaya PLDS website at http://plds.avaya.com/.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Storage**, and click **S3**.

   The system displays the S3 Management Console page.
3. From the All Buckets area, select a bucket.
4. Click **Upload**.

5. In the dialog box that is displayed, click **Add Files** and upload the Avaya Aura® Device Services OVA with the `-aws-001-ova` suffix.

Importing the OVA for AMI conversion

About this task

You can use files in the JSON format that are included in the AWS configuration files artifact. The AWS configuration files artifact also contains single-node and multi-node CloudFormation template generators that you use for AWS server deployment. The AWS configuration file contains the following:

- `trust-policy.json`
- `role-policy.json`
- `Single-Node-Cloud-Template-Gen.html`
- `Multi-Node-Cloud-Template-Gen.html`

For more information, see http://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html.

Use the AWS CLI to run the commands in this procedure.

Before you begin

You need the following to convert the OVA file to an Amazon Machine Image (AMI), to deploy the AMI, and configure Avaya Aura® Device Services:

- Avaya Aura® Device Services OVAs with the `-aws-001.ova` suffix has been uploaded to an S3 bucket.

Ensure that you also convert the `*.pem` file to the `*.ppk` format and configure PuTTY for establishing an SSH connection.

Ensure that you updated AWS details using the AWS CLI. For more information, see Configuring AWS details using the AWS CLI on page 66.

Procedure

1. Start a command line interpreter on a computer with the installed AWS CLI.
2. Run the following command to check whether the S3 bucket is ready to use:

   ```
   aws s3 ls
   ```

   The system displays the S3 bucket that you created.
3. To view the content of the S3 bucket, run the `aws s3 ls s3://<nameofbucket>` command.
4. To import the ova for conversion, run the following command:

   ```
   >aws ec2 import-image --cli-input-json "{ \"Description\": \"<server.ova>\",
   \"DiskContainers\": [ { \"Description\": \"<text description of task>\",
   \"UserBucket\": { \"S3Bucket\": \"<your_bucket_name>\", \"S3Key\" : \"<server.ova>
   \" } } ]}"
   ```

   The system displays the Status and the ImportTaskId parameters.

In the following example, when the system converts the CM Simplex OVA, ImportTaskId is `import-ami-ffmanv5x`.

```
{
    "Status": "active",
    "Description": "<version>-aws-001.ova",
    "Progress": "2",
    "SnapshotDetails": [
        {
            "UserBucket": {
                "S3Bucket": "<version>-dev",
                "S3Key": "<version>-aws-001.ova"
            },
            "DiskImageSize": 0.0
        }
    ],
    "StatusMessage": "pending",
    "ImportTaskId": "import-ami-fftlelct"
}
```

5. To check the status of the import image, run the following command:

   ```
   aws ec2 describe-import-image-tasks --cli-input-json "{ \"ImportTaskIds\":
   [\"<Your_ImportTaskId>\"], \"NextToken\": \"abc\", \"MaxResults\": 10 } "
   ```

   The conversion process takes up to 30 minutes. You can run the above command repeatedly.

   In the following example, the process is preparing the AMI and is 76% complete:

   ```
   IMPORTIMAGETASKS x86_64 CM-Simplex-07.1.0.0.xxx-aws-001.ova import-ami-ffgji45r
   BYOL Linux 76 active preparing ami
   ```

   The output format varies depending on the selection of the text or JSON format on the AWS CLI configuration.

6. Sign in to the Amazon Web Services Management console.
7. Go to **Services** > **Compute** and then click **EC2**.

   The system displays the EC2 Management Console page.

8. In the left navigation pane, click **IMAGES** > **AMIs**.

   You can search the converted AMI with ImportTaskId. The system displays the newly converted AMI ImageId in the AMI ID column.

Next steps

Create CloudFormation templates, which can be used to create a stack.

Creating CloudFormation templates

About this task

Use CloudFormation templates to create an AWS stack.

Important:

To create CloudFormation templates, use one of the following web browsers:

- Google Chrome
- Mozilla Firefox

Internet Explorer and Microsoft Edge are *not* supported.

Before you begin

Download the compressed artifact that contains the configuration files to your computer. Extract the two CloudFormation generator HTML files from the compressed file.

Procedure

- To create a single-node CloudFormation template, do the following:
  1. In your web browser, run the template generator by opening the `Single-Node-Cloud-Template-Gen.html` file.
  2. In **Product**, select the required application and profile size.
  3. If you are planning to use the Utility Server, select the **Utility server** check box.
  4. Click **Generate template**.
  5. Save the file to your computer.
- To create a multi-node CloudFormation template, do the following:
  1. In your web browser, run the template generator by opening the `Multi-Node-Cloud-Template-Gen.html` file.
  2. In **Product**, select the required application and profile size.
  3. In **Number of nodes**, set the number of servers required for the cluster.
  4. In **Number of subnets**, set the number of subnets required for the cluster.

     You can set two or three subnets.
  5. If you want to create new subnets for availability zones, select the **Create subnets** check box.

     Do not select **Create subnets** if you are planning to use existing subnets.
  6. If you are planning to use the existing subnets, do not select **Create subnets**.
  7. If you are planning to use the Utility Server, select the **Utility server** check box.
  8. Click **Generate template**.
  9. Save the file to your computer.

Next steps

Deploy the CloudFormation stack:

- For a single-node system, see Deploying a single-node CloudFormation stack on page 72.
- For a multi-node system, see Deploying a multi-node CloudFormation stack on page 75.

Deploying a single-node CloudFormation stack

About this task

Use this procedure to deploy a standalone instance by using a single-node CloudFormation template.

Before you begin

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud (VPC) settings and Security Groups.
- Generate a single-node CloudFormation template.
- Ensure that you have network access to the Amazon VPC before deploying an AMI.

Procedure

1. Sign in to the AWS console and navigate to **Services** > **Management Tools** > **CloudFormation**.

   CloudFormation is an AWS service used to create a stack. A stack is a graph of objects such as EC2 instances and EBS volumes inside the Amazon cloud. CloudFormation is used to create the objects required for a single-node Avaya Aura® Device Services system within a subnet of an existing virtual network.

2. On the CloudFormation page, click **Create Stack**.
3. On the Create Stack page, click **Select Template**.
4. On the Select Template page, in the Choose a template area, click **Choose file**.
5. Select the single-node `yaml` CloudFormation template file that you generated.
6. Click **Next**.
7. On the Specify Details page, in the **Stack name** field, type the stack name.

   The host name for the node is derived from the stack name.

   Note:

   The stack name must start with a letter and must contain letters, numbers, and dashes.

8. In **Amazon Machine Image ID**, type the Amazon Machine Image ID (AMI ID) of the instance that you created.

   For example, `ami-fda9369d`.

   Tip:

   To obtain the AMI ID of an image, go to **Services** > **EC2** > **Images** > **AMIs**

9. In the Network area, select the required **Virtual Private Cloud** and **Subnet**.
10. In **DNS domain**, type the name of the private DNS domain to use.

    This domain name represents the domain name that clients use to access service.

11. If the domain is a new domain in this VPC, set **Create domain** to **Y**. Otherwise, set it to **N**.
12. In the Security area, select **SSH key for administrator login**.
13. Click **Next**.
14. **(Optional)** On the Options page, in the Tag area, add tags that can help you find and organize your AWS objects.
15. In the Permissions area, leave the default values for both **IAM Role** and **Enter role arn**.
16. Click **Next**.
17. On the Review page, confirm the stack information.
18. Click **Create** to create the stack.

    The system displays the Stacks page, which shows the stack creation status.
19. Wait until the status displays `CREATE_COMPLETE`.

    You can monitor the status of the stack creation and review the properties using the tabs at the bottom of the Stacks page.
20. Click the **Resources** tab.
21. Click the Physical ID of the EC2 instance for the node, for example, `i-0fccb4a222a32dcc9`.

    The system displays the Instances page using a filter that displays the newly created AMI.
22. **(Optional)** Click the **Actions** menu to change the instance state.

    For example, you can start, stop, or reboot the AMI virtual machine.

Next steps

To complete the first-login configuration, log in using `admin@Instance.hostname` or `admin@instance_IP` as the login credentials are not provided. Accept the license agreement and set the password.

AWS cluster deployments

Use the information in the following subsections for multi-node AWS clusters.

For traffic distribution, use the AWS load balancer. A virtual IP address for clusters is not available on AWS.

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.

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, and 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. **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.

Deploying a multi-node CloudFormation stack

About this task

Use multi-node CloudFormation to create a cluster.

Note:

You cannot expand an AWS single node into a AWS cluster. You must create AWS clusters from the beginning. However, after an AWS cluster is created it can be expanded. For more information, see Expanding an existing cluster on page 78.

Before you begin

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud (VPC) settings and Security Groups.
- Ensure that you have network access to the Amazon VPC before deploying an AMI.
- Create a multi-node CloudFormation template as described in Creating CloudFormation templates on page 70.
- Create and apply load balancer certificates. The ARN value created during the certificate import is required for this procedure.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Navigate to **Services** > **Management Tools** > **CloudFormation**.
3. Click **Create Stack**.

   The AWS EC2 Management console displays the first page of the Create stack wizard.
4. On the Select Template page, in the Choose a template area, click **Choose File**.
5. Select the multi-node `yaml` CloudFormation template file that you generated.
6. Click **Next**.

   The system displays the Specify Details page.
7. In **Stack name**, type a name for the stack.

   This stack name must match the stack name portion of the FQDN of the load balancer.
8. In **Amazon Machine Image ID**, type the Amazon Machine Image ID (AMI ID) of the image that you imported.

   For example, `ami-fda9369d`.

   Tip:

   You can obtain the AMI ID of an image from the EC2 AMI page. On a separate browser tab, navigate to **Services** > **EC2** > **Images** > **AMIs**.
9. In Network area, select the required **Virtual Private Cloud**.
10. Do one of the following depending on whether you selected the **Configure subnets** check box in step 2 on page 71 when creating the multi-node CloudFormation template:

    - If you selected the check box, configure the required IPv4 address range in each subnet CIDR block field.

      In CIDR notation, the number of bits in the network portion of the address follows a slash. For example, 10.143.11.192/28. The address range for the subnets must fall within the address range of the VPC and must not overlap any existing subnet within the VPC.
    - If did not select the check box, select the required subnets from each **Subnet** field.

      Note:

      When using existing subnets, each subnet must be in a different availability zone.
11. In **DNS domain**, type the name of the private DNS domain to use.

    This domain name must match the domain name used in the FQDN of the load balancer.
12. If the domain is a new domain in this VPC, set **Create domain** to **Y**.

    Otherwise, set it to **N**.

13. If you selected to install the Utility Server when creating a CloudFormation template, in **Utility server host name**, provide a name for the Utility Server.

    Use a name that is similar to the stack name that you provided in step 7. For example, if the stack name is “aads716–dev”, use “aads716–us” as the Utility Server host name.

14. If you are planning to connect Avaya Aura® Device Services to the Avaya Aura® Web Gateway, in **Hostname for server-to-server**, provide a host name.

    The Avaya Aura® Web Gateway uses this host name to connect to Avaya Aura® Device Services.

    Note:

    - The host name must *not* match either of the following host names:
      - Load balancer host name.
      - Any of cluster node host names.
    - If you are not planning server-to-server communication, leave **Hostname for server-to-server** blank.

15. In the Security area, select **SSH key for administrator login**.
16. Copy the ARN saved in the Details section and paste it into the **Load balancer certificate ARN** field.

    For information on copying the ARN, see Creating and applying load balancer certificates on page 73.

17. If you selected to install the Utility Server when creating a CloudFormation template, Copy ARNs saved in the Details section and paste it into the **Main load balancer certificate ARN** and **Utility server load balancer certificate ARN** fields.

    For information on copying the ARN, see Creating and applying load balancer certificates on page 73.

18. Click **Next**.

    The system displays the Options page.

19. **(Optional)** In the Tags area, add tags to help you find and organize your AWS objects.
20. In the Permissions area, keep the default values for both **IAM Role** and **Enter role arn**.
21. Click **Next**.

    The system displays the Review page.

22. Click **Create** to create the stack.

    The system displays the Stacks page, which shows the stack creation status.

23. Wait until the status displays `CREATE_COMPLETE`.

    You can monitor the status of the stack creation and review the properties using the tabs at the bottom of the Stacks page.

24. Click the **Resources** tab.
25. Click the Physical ID of the EC2 instance for the node, for example, `i-0fccb4a222a32dcc9`.

    The system displays the Instances page using a filter that displays the newly created AMI.
26. **(Optional)** Click the **Actions** menu to change the instance state.

    For example, you can start, stop, or reboot the AMI virtual machine.

Next steps

- To complete the first-login configuration, log in using `admin@Instance.hostname` or `admin@instance_IP` as the login credentials are not provided. Accept the license agreement and set the password.
- If you are planning to connect Avaya Aura® Device Services to the Avaya Aura® Web Gateway, then after installing Avaya Aura® Device Services application, create and apply a new certificate containing information about the FQDN used for server-to-server communication. For more information, see Configuring certificates to connect Avaya Aura Device Services to the Avaya Aura Web Gateway on page 213.

Expanding an existing cluster

About this task

An existing AWS cluster can be expanded with additional nodes by updating the stack that represents the cluster.

Note:

You cannot expand a single AWS node into an AWS cluster. You must create AWS clusters from the beginning.

Procedure

Add nodes to a cluster by updating the CloudFormation stack that represents the cluster.

For information about updating a stack, see the AWS management information in *Administering Avaya Aura® Device Services*.

Creating a hybrid cloud for client access

About this task

Servers deployed in AWS are contained within a Virtual Private Cloud (VPC). End user clients are present within a separate network but require access to the servers in AWS. You must create a VPN to enable client access.

You must configure VPN gateways at both ends of the tunnel:

- The address range assigned to the VPC must route to the gateway on your side of the tunnel.
- Within AWS, the address range that clients use must route to the AWS-side gateway.

Use this procedure to configure AWS so that the address range that clients use routes to the AWS-side of the gateway.

Before you begin

- Deploy the required EC2 instances.
- Assign an IP address range to the VPC that does not overlap with any subnet in your network.

Procedure

1. Sign in to the AWS console.
2. Navigate to **Services** > **Management Tools** > **CloudFormation** and select the required stack.
3. Click the **Resources** tab.
4. Click the physical ID link for one of the nodes.

   The system displays a page with the details of the node.
5. Copy the value from the **Subnet ID** field of the Description tab. For example, `subnet-99942eff`.
6. Navigate to **Services** > **Networking & Content Delivery** > **VPC** > **Subnets**.
7. Paste the subnet ID into the **Search Subnets** filter.
8. Select the subnet that the system displays.
9. Select the row that contains the previously noted ID in the Route Table ID column.
10. Select the **Route Table** tab.
11. Click the route table ID link that is located next to the **Edit** button. For example, `rtb-bc53a2db`.
12. Select the route that the system displays.
13. Select the Routes tab.
14. Click **Edit**.
15. Click **Add another route** to add each required client address range and do the following:
    a. In the Destination column, enter the address range.
    b. In the Target column, select an AWS-side gateway that can reach the destination.
16. Click **Save**.

Configuring on-premise DNS resolution of VPC addresses

About this task

This configuration allows on-premise clients to access the servers hosted in the AWS VPC. Use this procedure to configure your local, on-premise DNS server with a new DNS forwarding zone so

that client DNS resolution requests are forwarded to a DNS server located within the VPC. The DNS server located within the VPC then performs the final address resolution to the servers hosted in the AWS VPC.

Before you begin

Ensure that you have:

- Access to your on-premise DNS server so that you can add a new DNS forwarding zone.
- Enabled your corporate firewall to permit outgoing UDP traffic toward the AWS VPC.
- Routes on your AWS VPC VPN gateway that direct UDP port 53 traffic from the enterprise toward the VPC.
- The IP address of the DNS server in the AWS VPC.
- A list of the VPC domains that the on-premise DNS server must resolve to the AWS DNS server. For example, if your VPC servers must resolve `server.example.com` and `server.example.net`, then the list of required VPC domains is `example.com` and `example.net`.
- A test FQDN that is configured in the VPC DNS.

Procedure

1. Log on to your local on-premises DNS server.
2. Add a new “Forward Zone” or “Forward Lookup Zone” DNS by following the instructions provided by your DNS server manufacturer.
3. Add a new forward zone with the following details for each required VPC domain:
   a. A zone name: Use the same name as the domain name. For example, `example.com`.
   b. The forwarding address: Use the IP address and port of the DNS server in the AWS VPC. For example, `10.1.2.3@53`.
   c. Forward First: Enable Forward First if your DNS server supports this feature. This feature causes resolution requests for the zone to be forwarded to the VPC DNS server before attempting to resolve them locally.
4. Enable the DNS server changes by reloading the configuration or restarting the DNS server.
5. Verify that the DNS resolution completes by performing a lookup of the test FQDN using a DNS resolution utility, such as `nslookup` or `dig`.

   For example, you can run the following `nslookup` command:

```
>  nslookup server.example.com
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:    server.example.com
Address: 10.1.2.165
```

Logging in to the EC2 instance

Procedure

Log in to the EC2 instance using the SSH console or PuTTY.

For information about how to use PuTTY, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html?icmpid=docs_ec2_console.

Note:

You must use the key that you specified during stack creation.

Completing the first-login configuration

About this task

The first time you access a newly deployed EC2, you must complete a one-time system procedure to accept the license agreement, configure the OS, and select network preferences.

Before you begin

Access the EC2 instance by logging in using PuTTY or SSH from the command line. Use the Avaya Aura® Device Services administrator credentials and the EC2 DNS or IP address for the first log in as follows:

```
<admin_name>@<instance_dns_or_ip_address>
```

For example:

```
ammapp@ec2-198-51-100-1.compute-1.internal
```

or

```
ammapp@198.51.100.1
```

Procedure

1. Do the following when you see the license agreement banner, which is displayed when you log in for the first time:
   a. Press `Enter` to display the license agreement.
   b. Press the `Space bar` to navigate through the license agreement.
   c. When prompted, type `yes` to accept the license agreement.
2. Enter a password for the system administrator.
3. To configure the NTP servers, do one of the following:
   - Press `Enter` to accept the default Amazon NTP time servers.
   - Enter one or more comma separated NTP server IP addresses or FQDNs and then press `Enter`.

Important:

The NTP servers that you configure must be reachable from this server. The default Amazon NTP time serves are on the Internet and might not be reachable.

4. Select your time zone preferences.
5. Review the summary of your selections and type one of the following:
   - `y` to apply the settings to the system.
   - `n` to make changes to your selections.

Next steps

Install the Avaya Aura® Device Services application software using the `app install` command as described in Deployment methods on page 53.

Complete the required configuration and commissioning procedures after the initial installation. If you are installing a cluster, you must follow the instructions for using an external load balancer.

Obtaining the virtual server instance user ID

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Compute**, and click **EC2**.

   The system displays the EC2 Management Console page.
3. In the left navigation pane, click **Instances**.
4. Select a server instance, and click **Connect**.

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 deployments *do not* support IPv6.

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 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 38.

3. Follow the system prompts to complete the procedure.

Next steps

Enable IPv6 at the application layer during Avaya Aura® Device Services installation. For more information, see Installing Avaya Aura Device Services on page 84.

Enabling FIPS mode

About this task

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

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

Ensure that FIPS mode is enabled on both System Manager and Session Manager. For more information about enabling FIPS on System Manager, see *Administering Avaya Aura® System*

Manager. For more information about enabling FIPS on Session Manager, see *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 secconfig --fips --enable
   ```

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

   ```
   sys secconfig --fips --query
   ```

Related links

Disabling FIPS mode on page 108
sys secconfig command on page 31

Installing Avaya Aura® Device Services

About this task

Use this procedure to install Avaya Aura® Device Services as a standalone instance or as a seed node in a cluster deployment.

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 25.
  - 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.
- If you are planning to use FIPS, enable it as described in Enabling FIPS mode on page 83. 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 82.
- To use OAuth, contact Avaya product management to obtain an activation code. For more information, see *Avaya Aura® Device Services Release Notes* for Release 8.0. The OAuth feature is currently restricted, so you need a code to enable it.

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. 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.p12`
   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
      ```
3. Go to `/opt/Avaya/` and run the following command:

   ```
   app install
   ```

   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. **(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:
   - You can only enable the Utility Server when installing or upgrading Avaya Aura® Device Services. You cannot enable the Utility Server using the Avaya Aura® Device Services web administration portal or configuration utility.
   - If you are installing 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. Select **OAuth2 activation code** .
   c. Enter the activation code and then select **OK**.

      If you entered an incorrect code, Avaya Aura® Device Services prompts you that the code is incorrect and you need to re-enter the code.
   d. Select **Return to Main Menu** and press `Enter`.

   Note:

   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:

   - You can only enable IPv6 when installing or upgrading Avaya Aura® Device Services. You cannot enable IPv6 using the Avaya Aura® Device Services web administration portal or configuration utility.
   - AWS deployments *do not* support IPv6.
8. In the Initial Installation Configuration screen, select **Cluster Configuration** and press `Enter`.
9. In the Clustering screen, ensure that the value of the **Initial cluster node** field is `y`.
10. For cluster deployments, ensure that the **Local Node IP address** option is set to the IP address of the node.
11. Select **Return to Main Menu** and press `Enter`.
12. **(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.

    Note:

    If you enabled FIPS mode, SSL encryption for internode communication is enabled by default and the **Cassandra Encryption** menu is unavailable.
13. In the Initial Installation Configuration screen, select **Front-end host, System Manager and Certificate Configuration** and press `Enter`.
14. 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 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 6 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.

15. 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 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.
16. If you are using 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 **Yes**.
    b. For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS file**, enter the path to the `identity.p12` file.
    c. Select **Signing authority certificate configuration**.
    d. In **Is the Signing Authority certificate in PKCS12 format?**, select **No**.
    e. In **Signing Authority PEM certificate file**, enter the path to the `cert-chain.pem` file that you created in step 2.
17. Select **Return to Main Menu** and press `Enter`.
18. In the Initial Installation Configuration screen, select **Session Manager Configuration** and press `Enter`.
19. 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.

20. Select **Return to Main Menu** and press `Enter`.
21. If you want to use 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.
    e. In **Administrator's password**, provide a password for the Open LDAP administrator.
    f. Select **Return to Main Menu** and press `Enter`.

    Important:

    - You can only install Open LDAP when installing or upgrading Avaya Aura® Device Services. You cannot install Open LDAP using the Avaya Aura® Device Services web administration portal or configuration utility.
    - You cannot install Open LDAP if you enabled FIPS mode.
22. In the Initial Installation Configuration screen, select **Continue** and press `Enter`.
23. In the Configuration Summary screen, select **Accept and continue** and press `Enter`.
24. In the Results of Configuration Checks screen, select **Continue** and press `Enter`.

    The system displays the End User License Agreement.
25. Select **Accept** and press `Enter`.

    The system installs the required RPMs, downloads certificates from System Manager, creates database schema, and performs the required initial configuration. After successful installation, the system displays the Results of Installation Script screen.
26. In the Results of Installation Script screen, select **Continue** and press `Enter`.
27. 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.
28. In the LDAP Configuration screen, set values for the following parameters:
    - Use LDAP for authentication

      This option is only available when OAuth is enabled.

- 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 148.
  - If you are using the LDAPS protocol, you cannot use IP addresses in the server URL. LDAPS only supports FQDNs.
- 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, the system skips validation and directly saves the configuration in the database. For more information, see testUser validations on page 92.

29. Select **Advanced LDAP Parameters** and press `Enter`.
30. In the Advanced LDAP Paramters screen, verify the default values for the parameters and update them if required.
31. Select **Return to previous menu** and press `Enter`.
32. In the LDAP Configuration screen, select **Apply** and press `Enter`.
33. In the LDAP Configuration screen, select **Yes** and press `Enter`.
34. In the Results of LDAP Parameter Configuration screen, select **Continue** and press `Enter`.
35. Select **Return to previous menu** and press `Enter`.

If you are deploying a standalone system, continue from step 41 on page 90. The steps 36 to 40 are for cluster deployments.

36. In the Main Menu screen, select **Clustering Configuration** and press `Enter`.
37. 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.
38. 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.
39. Select **Apply** and press `Enter`.
40. Select **Return to previous menu** and press `Enter`.
41. 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 45 on page 91. Steps from 42 to 44 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.
42. 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 92.

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**.

43. Select **Apply** and press `Enter`.
44. Select **Continue** and press `Enter`.
45. In the Main menu screen, select **Continue** and press `Enter`.
46. **(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.
- 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 135.
- 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 142 .
- 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 134.
- 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 143 and Pairing Session Manager with an Avaya Aura Device Services node on page 145.

Related links

Configuring Avaya Aura Device Services using the configuration utility on page 110
Avaya Aura Device Services virtual machine resource requirements on page 24
VM Deployment Configuration Parameters and Network Parameters field descriptions on page 56
Configuring RSA public and private keys for SSH connections in a cluster on page 102
Configuring Keycloak settings on page 136
Avaya Aura Device Services installation fails if third-party certificates are used on other Avaya Aura elements on page 196

testUser validations

You can optionally choose to 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**, the system 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 AVP 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.

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

To use OAuth, contact Avaya product management to obtain an activation code. For more information, see *Avaya Aura® Device Services Release Notes* for Release 8.0. The OAuth feature is currently restricted, so you need a code to enable it.

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.

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 109.

   You can leave some of the settings blank and then configure them manually after the installation is complete.

3. **(Optional)** To enable OAuth, set INCLUDE_OAUTH to `y` and configure the following parameters:
   - OAUTH_ACT_CODE: The OAuth activation code.
   - 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 thrid-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.
4. **(Optional)** To enable the Utility Server, set INCLUDE_UTILITY_SERVER to `y`.
5. **(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.

6. Run the Avaya Aura® Device Services binary with a parameter that represents the full path to the properties file.

   For example:

   ```
   sudo ./aads-<version>.bin /home/avaya/installation.properties
   ```

7. **(Optional)** To start the Avaya Aura® Device Services service, run the following command:

   ```
   svc aads start
   ```

8. 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*.

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.

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 84.

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 102.

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 84.

Installing additional non-seed nodes

About this task

You must use this procedure for the second node or for any subsequent nodes in the cluster.

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 2 of Installing Avaya Aura Device Services on page 84.

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. Run the `app install` command.

   The system displays the Avaya Aura Device Services Installer dialog box.

   Note:

   Do not resize the SSH console during the installation and configuration of Avaya Aura® Device Services.

3. When prompted, type the administrative user password.
4. **(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:

   - You can only enable the Utility Server when installing or upgrading Avaya Aura® Device Services. You cannot enable the Utility Server using the Avaya Aura® Device Services web administration portal or configuration utility.
   - If you are installing 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*.

5. If you want to enable OAuth, do the following:
   a. In the Initial Installation Configuration screen, select **OAuth**.
   b. Select **OAuth2 activation code** .
   c. Enter the activation code and then select **OK**.

      If you entered an incorrect code, Avaya Aura® Device Services prompts you that the code is incorrect and you need to re-enter the code.
   d. Select **Return to Main Menu** and press `Enter`.

   Note:

   OAuth is unavailable if you enabled FIPS mode.
6. 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:

   - You can only enable IPv6 when installing or upgrading Avaya Aura® Device Services. You cannot enable IPv6 using the Avaya Aura® Device Services web administration portal or configuration utility.
   - AWS deployments *do not* support IPv6.
7. In the Initial Installation Configuration screen, select **Cluster Configuration** and press `Enter`.
8. In the Clustering screen, set **Initial cluster node** to `n`.
9. 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`.
10. 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`.
11. In the Clustering screen, set **User ID of product user on seed node**, type the UID of the seed node, and then click `Enter`.
12. Select **Return to Main Menu** and then press `Enter`.
13. In the Initial Installation Configuration screen, select **Front-end host, System Manager and Certificate Configuration** and press `Enter`.
14. In the Front-end host, System Manager and Certificate Configuration screen, set values for the following:
    - For a cluster, specify the FQDN of the virtual IP as the Front-end FQDN.
    - 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 6 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.

15. 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.
16. If you are using 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 **Yes**.
    b. For each of the REST, OAM, and NODE interface certificate configuration options, in **Interface PKCS file**, enter the path to the `identity.p12` file.
    c. Select **Signing authority certificate configuration**.
    d. In **Is the Signing Authority certificate in PKCS12 format?**, select **No**.
    e. In **Signing Authority PEM certificate file**, enter the path to the `cert-chain.pem` certificate chain file.
17. Select **Return to Main Menu** and then press `Enter`.
18. In the Initial Installation Configuration screen, select **Session Manager Configuration** and then press `Enter`.
19. In the Session Manager Cassandra Configuration screen, set values for the following:
    - Session Manager Management IP
    - Session Manager Asset IP
20. Select **Return to Main Menu** and then press `Enter`.
21. 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`.

22. Select **Continue** and then press `Enter`.
23. In the Configuration Summary screen, verify the values, select **Accept and Continue** and then press `Enter`.

    The installer performs pre-install checks.
24. In the Results of configuration checks screen, select **Continue** and then press `Enter`.

    The system displays the End User License Agreement.
25. Select **Accept** and then press `Enter`.

    The system displays the progress of the tasks in the Running Installer Script window. The system installs the required RPMs, downloads certificates from System Manager, creates database schema, and performs the required initial configuration. After successful installation, the system displays the Results of Installation Script screen.
26. Select **Continue** and then press `Enter`.
27. In the Main Menu screen, select **Clustering Configuration** and then press `Enter`.
28. 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.
29. 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.

30. Select **Apply** and then press `Enter`.
31. In the Clustering Configuration screen, select **Return to Main Menu** and then press `Enter`
32. 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.

33. 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.

    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 92.

    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.

34. Select **Apply** and press `Enter`.
35. Select **Continue** and press `Enter`.
36. 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.
37. Select **Continue** and then press `Enter`.

    The system displays a message for Avaya Aura® Device Services service restart.
38. Select **Yes** and press `Enter`.
39. 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, after all additional nodes are installed, configure Keycloak settings. For more information, see OAuth configuration on page 135 .
- If you enabled OAuth, after all additional nodes are installed, enable OAuth database replication. For more information, see Enabling OAuth database replication in a cluster environment on page 142 .
- 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 134.

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 node by using the Linux administrator account credentials.

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**.

   The system 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 the system 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 the system prompts you to enter a user name for a node, enter the username for the Linux administrator account that you used to perform the installation.
8. If the system prompts you to replace the existing keys, enter `y` (yes).
9. If the system displays the following error, type `yes` and then press `Enter`:

   ```
   The authenticity of the host can't be established.
   ```
10. When the system prompts you to enter a password, enter the password for the Linux administrator account that you used to perform the installation.
11. When the configuration is complete, press `Enter`.
12. From the main menu select **Continue** and then select **Yes** to restart services and 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
   ```
5. 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

You must configure a virtual IP for the cluster seed node only before installing other cluster nodes. Configuring virtual IP is necessary only if the cluster Nginx load balancer is used.

Note:

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.

Procedure

1. Log in to Avaya Aura® Device Services with administrator credentials.
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 click **Select**.
5. Type the FQDN of the virtual IP and click **OK**.
6. Click **Local frontend host** and click **Select**.
7. Type the FQDN of the node to which you have logged in and click **OK**.
8. Click **Apply**.
9. Click **Clustering Configuration** and click **Select**.
10. Click **Virtual IP Configuration** and click **Select**.
11. Click **Enable Virtual IP**.

    The system enables the virtual IP address that forms the interface for client requests in the clustered environment. The system 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 click **Select**.
14. Type the IP address that forms the front end to the clients and click **OK**.
15. Click **Virtual IP Interface** and 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 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 click **Select**.
20. Type a value between 1 and 255 and 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.

    The system 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 configruation.

    The system restarts Avaya Aura® Device Services services.
27. Run the `app configure` command for another node in the cluster and repeat the 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 UI, go to **Cluster Configuration** > **Cluster Nodes** to confirm whether Avaya Aura® Device Services are running.

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.

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.

Uninstalling Avaya Aura® Device Services

About this task

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.

   This command restores the system to the point before deploying Avaya Aura® Device Services.

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 135.

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 108.
2. Run the following command:

   ```
   sys secconfig --fips --disable
   ```

Related links

sys secconfig command on page 31

Chapter 6: 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 1: 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.

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, LYNC, or NODE.

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.

Table 2: 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 `/etc/hosts` 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 Avaya Aura® System Manager that signs the Avaya Aura® Device Services certificates.	`SYSTEM_MGR_IP`
System Manager web admin username	The System Manager web administration portal user name. This field is optional.	`SMGR_USER_NAME`
System Manager web admin password	The System Manager web administration portal password. This field is optional.	`SMGR_USER_PASSWORD`
System Manager web version	The version number of Avaya Aura® System Manager.	`SYSTEM_MGR_VERSION`

Item name	Description	Equivalent properties file parameter
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.	`SYSTEM_MGR_HTTPS_PORT`
System Manager Enrollment Password	The Avaya Aura® System Manager enrollment password.	`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**. **Note:** If this parameter is changed after the installation, all of the nodes in a cluster must be restarted using the `svc aads restart` command to apply the change. For more information about overriding ports in a clustered environment, see Overriding port configuration in a cluster on page 183.	`OVERRIDE_FRONTEND_PORT` For the **Front-end port for reverse proxy** setting, the equivalent parameter is `REST_FRONTEND_PORT`.
Current Listen Port	Specifies the port Avaya Aura® Device Services uses to receive connections. This is the read-only field.	—

Item name	Description	Equivalent properties file parameter
Use System Manager for certificates	Specifies if the certificates are retrieved from Avaya Aura® System Manager or from imported files. Select `y` (yes) to retrieve certificates from Avaya Aura® System Manager or `n` (no) to retrieve certificates from imported files. If you select `n` (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 • LYNC interface key file • LYNC interface certificate file • OAM interface key file • OAM interface certificate file • node key file • node certificate file • signing authority certificate file	`USE_SMGR` If the `USE_SMGR` option is set to `n` (no), you must configure the following parameters for importing the certificate files: • `REST_KEY_FILE` • `REST_CRT_FILE` • `SIP_KEY_FILE` • `SIP_CERT_FILE` • `OAM_KEY_FILE` • `OAM_CRT_FILE` • `NODE_KEY_FILE` • `NODE_CRT_FILE` • `CA_CRT_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. 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.	`LOCAL_FRONTEND_HOST`

Item name	Description	Equivalent properties file parameter
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 • other supported characters: exclamation point (!), at symbol (@), hash (#), percent sign (%), caret (^), star (*), question mark (?), underscore (_), dot (.)	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 as described in Verifying the LDAP server configuration settings on page 128.

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.

Table 3: LDAP configuration settings

Item name	Description	Equivalent properties file parameter
Use LDAP for Authentication	Specifies whether LDAP is used for authentication. This check box is only available when OAuth is enabled.	—
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	pathToLdapPropertiesFile

Item name	Description	Equivalent properties file parameter
	manually. The **Path to properties file** option is for configuring the absolute path to this file. The LDAP properties file must contain the *equivalent properties file parameters* specified in this table. The default value for this setting is `<install_dir>/config/ldap.properties`, where `<install_dir>` is the Avaya Aura® Device Services installation directory.	
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 `/etc/openldap/certs/nginx.crt`. **Important:** Only configure these settings if you need a Secure LDAP connection.	LDAP_TRUSTSTORE_CERTFILE LDAP_TRUSTSTORE_PASSWORD
Directory Type	The LDAP directory type of the enterprise. The supported directory types are the following: • 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 2008, 2012, and 2016	ldapType

Item name	Description	Equivalent properties file parameter
	• Microsoft Active Directory Lightweight Directory Services (LDS) 2008 and 2012 • Novell e-Directory 8.8 • OpenLDAP 2.4.44 • 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.	

URL for LDAP server	The URL for gaining access to the LDAP server. This is a mandatory setting.
	The URL must have one of the following formats:
	`ldap://<LDAP server FQDN or IP address>:<port>`
	`ldaps://<LDAP server FQDN>:<port>`
	For example:
	`ldap://myserver.mycompany.com:3268`
	`ldaps://myserver.mycompany.com:3269`
	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:
	`ldaps://localhost.localdomain:3269`
	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.
		ldapUrl

Item name	Description	Equivalent properties file parameter
	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. 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 148.	
Bind DN	The Distinguished Name (DN) of the user that has read and search permissions for the LDAP server users and roles. This is a 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 "domain\user",	bindDN

Item name	Description	Equivalent properties file parameter
	"user@domain", as well as the actual DN of the user object.	
Bind Credential	The password that the Avaya Aura® Device Services server requires for the LDAP bind operation. This is a mandatory setting.	bindCredential **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 a mandatory setting. This parameter is used for searching users in the LDAP server. For example: `sAMAccountName` **Note:** When the UID attribute is set to `mail` 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.	uidAttrID
Base Context DN	The DN of the context used for LDAP authentication. For example: `ou=aadsusers,dc=example,dc=com`	baseCtxDN
Administrator Role	The list of LDAP roles that match the Avaya Aura® Device Services Administrator role. For example: If the role is configured as `AADSAdmin,AADSxyz`, any user whose list of roles contains `AADSAdmin` or `AADSxyz` is mapped to the Avaya Aura® Device Services Administrator role.	adminRole

Item name	Description	Equivalent properties file parameter
	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.	
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 `AADSSecurityAdmin,AADSxyz`, any user whose list of roles contains `AADSSecurityAdmin` or `AADSxyz` 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 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.	securityAdminRole
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 `AADSAuditor,AADSxyz`, any user whose list of roles contains the `AADSAuditor` or `AADSxyz` role is	auditorRole

Item name	Description	Equivalent properties file parameter
	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.	
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 `AADSUser,AADSxyz`, any user whose list of roles contains the `AADSUser` or `AADSxyz` 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 `AADSUser,AADSxyz`, any user whose list of roles contains the `AADSUser` or `AADSxyz` role is mapped to the 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	serviceAdminRole

Item name	Description	Equivalent properties file parameter
	the LDAP roles to the Avaya Aura® Device Services application roles to succeed.	
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 `AADSUser,AADSxyz`, any user whose list of roles contains the `AADSUser` or `AADSxyz` 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.	serviceMaintenanceRole
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	testUser

Item name	Description	Equivalent properties file parameter
	validation and directly saves the configuration in the database.	

Table 4: Advanced LDAP attributes

The following table contains the LDAP configuration settings accessible through the **Advanced LDAP attributes** menu:

Item name	Description	Equivalent properties file parameter
Role Filter	The string to use for role filtering. The format of the string depends on the LDAP server configuration. For example: `(&(objectClass=group)(member={1}))`	`roleFilter`
Role Attribute ID	The Role Attribute ID parameter has a different meaning, depending on the value of RoleAttributeIsDN: • If RoleAttributeIsDN is true, this is the attribute that contains the DN used to find the object that contains the role name. • If RoleAttributeIsDN is false, this is the name of the attribute that contains the role name. For example: `memberOf`	`roleAttrID`
Roles Context DN	The Roles Context DN to use for searching roles. The roles search in LDAP is performed by using the Roles Context DN in combination with the Role Filter. For example: `ou=aadsusers,dc=example,dc=com`	`rolesCtxDN`

Item name	Description	Equivalent properties file parameter
Role Name Attribute	This parameter has a different meaning, depending on the value of RoleAttributeIsDN: • If RoleAttributeIsDN is true, the value of the attribute set in RoleAttributeID 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 RoleAttributeIsDN is false, this parameter is ignored. For example: `cn`	`roleNameAttrID`
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 `true`, the role is stored in the attribute defined by the *Role Name Attribute* parameter. If you set this parameter to `false`, the role attribute of the user contains the name of the role.	`roleAttrIsDN`
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.	`roleRecursion`
Allow Empty Passwords (true/false)	The setting to determine if empty passwords are allowed in the LDAP directory.	`allowEmptyPasswords`

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 *Role Context DN* and uses the *Role Filter*. 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`

Item name	Description	Equivalent properties file parameter
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 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)).`	`activeUsersFilter`
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)).`	—

Item name	Description	Equivalent properties file parameter
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. If this parameter is not configured, the User 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.	`lastUpdatedTimeAttr`
Load parameter defaults	The script to load the default values for the parameters.	—

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\\`.

Verifying the LDAP server configuration settings

About this task

Use this procedure to modify the LDAP configuration settings so that they are consistent with the Avaya Aura® Device Services settings

Procedure

1. Click the **LDAP Configuration** tab.
2. Modify the LDAP configuration settings as needed.

   The settings are described in LDAP configuration on page 115.
3. Ensure that **UID Attribute ID** is set to the same value that is in Avaya Aura® Device Services.
4. Modify or update other parameters related to LDAP as required and then click **Save**.
5. Click **Test Connection** to verify the connection.

   If the test fails, check the configured LDAP address FQDN, port, and protocol, and then run the test again.

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.

Table 5: Cassandra database settings

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`

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

Table 6: Cluster Utilities

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 `installation.properties` 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 from the seed node after installing the other nodes in the cluster.	This setting does not have an equivalent parameter in the `installation.properties` 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.

Table 7: Virtual IP Configuration Settings

Item name	Description	Equivalent properties file parameter
Enable virtual IP	The setting to enable the usage of a virtual IP address. If you select `n` (no), the configuration script does not configure the virtual IP address. If you select `y` (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 `eth0`. • 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 (VRRP) installations and it is limited to cluster deployments.	`KA_ENABLED` If you set this parameter to `y` (yes), you must also configure the following parameters: • `KA_VIRTUAL_IP` • `KA_INTERFACE` • `KA_MASTER_YN` • `KA_AUTHENTICATION_PASSWORD` • `KA_ROUTER_ID`

Item name	Description	Equivalent properties file parameter
	• 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
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**.	SYSTEM_MANAGER_PW

Advanced configuration

Table 8: Advanced configuration settings

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.
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`

Item name	Description	Equivalent properties file parameter
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 `/etc/alternatives/jre`.	—

Configuring the Avaya Aura® Device Services server firewall

About this task

Use this procedure to reset the firewall settings back to the defaults, or to allow additional ports through the server firewall.

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.

Enabling Open LDAP replication

About this task

Use this procedure to 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.log` file.

   The following is an example of a `/var/log/Avaya/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.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 198

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 Avaya Equinox® clients and UC servers

When OAuth is enabled on Avaya Aura® Device Services, you must provision the following parameters for all Avaya Equinox® clients 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 OAuth, ensure that they use the same Keycloak realm.

- ACSSSO: Set the value to `3`, so that Avaya Equinox® clients use Avaya Authorization for Avaya Aura® Device Services.
- ESMSSO: Set the value to `3`, so that Avaya Equinox® clients use Avaya Authorization for Presence and Multimedia Messaging.
- AUTOCONFIG_USE_SSO: Set the value to `3` so that Avaya Equinox® clients use 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`

Configuring Keycloak settings

About this task

Use this procedure to set up a Keycloak administrator account. You can also upload an identity provider entity descriptor file in XML format. 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 do not upload an entity descriptor file using the Avaya Aura® Device Services configuration utility, you must configure the identity provider settings using the Keycloak web administration portal. Otherwise, OAuth will not work.

Note:

Currently, Avaya Aura® Device Services only supports the Shibboleth identity provider.

Before you begin

- Install Avaya Aura® Device Services.
- Obtain the third-party identity provider configuration file in the XML format. For Shibboleth, you can download it 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.
4. If you want to configure a third-party identity provider for authentication, do the following:
   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 identity provider configuration file that you uploaded to the system.
   d. Configure the mapping between attributes used by the identity provider and attributes used by Keycloak:
      - **Last Name attribute**: The Last Name attribute that is used by the identity provider. For example: `sn`.
      - **First Name attribute**: The First Name attribute that is used by the identity provider. For example: `givenName`.
      - **Membership attribute**: The Membership attribute containing role information that is used by the identity provider. For example: `memberOf`.
      - **User Role value**: 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`.
      - **Administrator Role value** 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`.
5. Select **Apply**.
6. 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 142.

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>:<AADS PORT>/auth/admin`

   In this URL:

   - `<AADS IP or FQDN>` is either the Avaya Aura® Device Services front-end FQDN or IP address.
   - `<AADS PORT>` is the Avaya Aura® Device Services front-end FQDN service port.
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 139.

Creating client mapping

About this task

In the authorization flow, Avaya Aura® Device Services interacts with Keycloak on behalf of Avaya Equinox® clients. 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.

Before you begin

Obtain the client secret as described in Obtaining the client secret on page 138.

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**, enter `Equinox`.

      This value is case sensitive.

   b. In **OIDC Discovery URL**, enter `https://<AADS front-end FQDN>:<AADS PORT>/auth/realms/<Realm>/.well-known/openid-configuration`

      In this string:

      - `<AADS front-end FQDN>` is the Avaya Aura® Device Services front-end FQDN.
      - `<AADS 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 that you copied from the Keycloak web administration interface.
5. Click **OK**.

Modifying the attribute mapping between the third-party identity provider and Keycloak

About this task

To authenticate a user, a thrid-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.

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.

   The system 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.

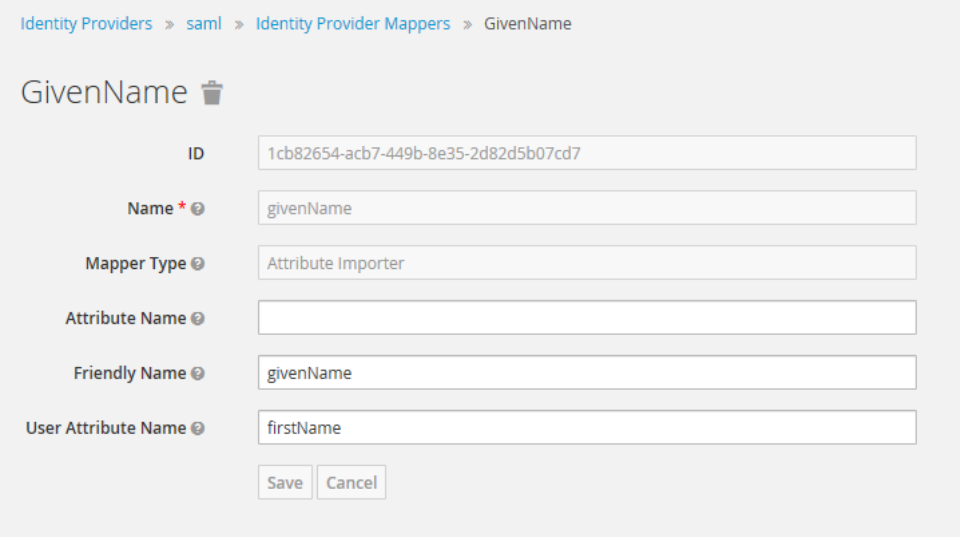
   - The **User Attribute Name** field contains the attribute name that Keycloak passes to clients in access tokens.

     For a person's given name, last name, and email address, use the following **User Attribute Name** values:

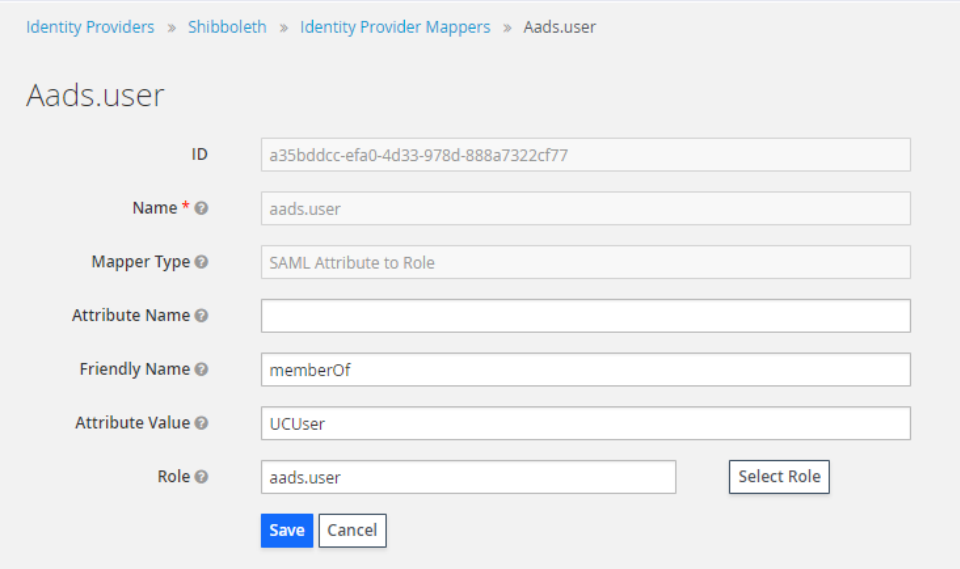
     - Given name: `givenName`.
     - Last name: `lastName`.
     - Email address: `email`

     These values are case sensitive.

   The following image shows the givenName attribute.



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 upgrading Avaya Aura® Device Services
- After rolling back Avaya Aura® Device Services
- Before restoring Avaya Aura® Device Services

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 136.

Procedure

Perform steps 1 to 5 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 **Yes** and then select **Apply**.
6. 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.
7. On all non-seed nodes, run the `svc aads restart` command to restart Avaya Aura® Device Services.

Chapter 7: Configuring Session Manager for cluster environments

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 Equinox® 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.

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 node while adding a Session Manager instance or after adding the Session Manager instance using the **Edit** button.

Repeat these steps for all Avaya Aura® Device Services nodes in the cluster.

For example, for a Session Manager cluster with two nodes, SM01 and SM02, to deploy an Avaya Aura® Device Services 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 home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the Session Manager Administration page, click the **Session Manager** Instances tab.
3. In the **Session Manager Instances** section, select a Session Manager instance, and click **Edit**.

   The system displays the Edit Session Manager page.
4. From **Data Center**, select a data center if one is not already assigned.

   If you do not assign the Session Manager instance to a data center, the system displays the following message: `Session Manager must be assigned to a Data Center to pair with an Avaya Aura Device Services Server.`
5. From **Avaya Aura Device Services Server Pairing**, select an Avaya Aura® Device Services server.

When an AADS server is already paired with a Session Manager instance, the system does not display that Avaya Aura® Device Services Server in the **Avaya Aura Device Services Server Pairing** drop-down list.

6. Click **Commit**.

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**.

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.

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*.

Chapter 8: LDAP settings configuration

Avaya Aura® Device Services uses the LDAP servers for user authentication, user authorization, and retrieving user details.

The following sections provide tasks and configuration examples for the LDAP settings.

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 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

Before you begin

Ensure to login to active directory system as an administrator.

Note:

This procedure is applicable only for active directory.

Procedure

1. Open the command prompt.
2. Type `regsvr32 schmmgmt.dll` to register `schmmgmt.dll` on your system.
3. Click **Start**.
4. Click **Run**.
5. Run the `mmc /a` command.

6. In the Console window, click **File** > **Add or Remove Snap-in**
7. In the Add or Remove Snap-in window, under **Available snap-ins** select the **Active Directory Schema** and click **Add**.
8. Click **OK** to add the schema to your console.
9. Click **Save** to save this console on the **File** menu.

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

Ensure to install the LDAP schema snap-in.

Procedure

1. Open the command prompt.
2. Run the `mmc /a` command.

   The system displays **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 on the selected attribute and click **Properties**

   The system displays the selected attribute's properties window.
6. Under 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 Enterprise Directory Mappings window are indexed on Active Directory.
7. Click **Apply** and then click **OK** to save the property changes done to 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

- ASCIIDisplayname
- ASCIIGivenname
- ASCIISurname
- 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 Avaya Aura® Device Services as the administrative user.

2. At the command prompt, type `clitool.sh ldapConfiguration > ~/ldap_settings.txt`.

   The system copies the existing LDAP configuration to the `ldap_settings.txt` file.

   You must not cut and paste to a file from a terminal because pasting from a terminal might introduce some unwanted white space.

Setting up user synchronization with LDAP after deployment

About this task

Important:

Before using Avaya Aura® Device Services, you must synchronize the user with LDAP Server.

Procedure

1. Log on 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**.

   The system displays the Enterprise LDAP Server Configuration page.
3. In the User Synchronization Update Instructions section, do the following:
   a. Click **Force LDAP Sync**.

      The system 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**.

      The system displays the following message:

      ```
      Starting update.
      ```

   c. Click **OK**.
   d. Ensure that system 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 tasks follow the LDAP configuration example provided in this section, 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 and 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 217.

LDAP configuration example

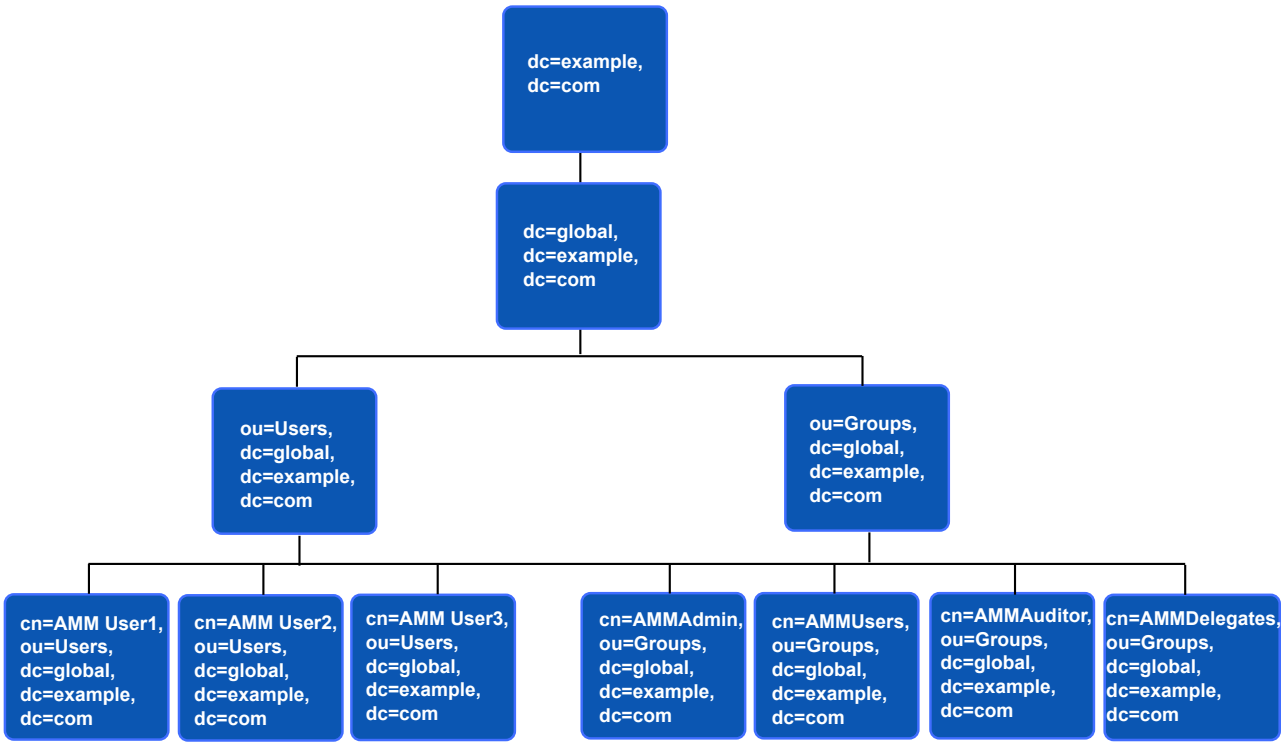


Figure 1: LDAP configuration example

- 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 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 as 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 148. • 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 “sAMAccoutName”. See MultipleActiveDirectorydomains 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.	sAMAccoutName 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 *Allow Empty Passwords* 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 DNs 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 DNs 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 166.
4. Configure the attributes as described in Role configuration on page 168.

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), as well as the language 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 how to configure 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**.

   The system 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.	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	(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
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 DNs 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

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.

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.

User in Enterprise Directory and System Manger

Table 9: 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	msrtcsip-primaryuseraddress
SMGRLoginname	userPrincipalName

Table 10: Enterprise Directory mappings

Enterprise Directory Field	Value
mail	j.doe@company.com
userPrincipalName	j.doe@north.company.com

Table 11: 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 querySystem Manager queryThe user information is available in both Enterprise Directory and System Manager on page 161.

```
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
```

Attribute mapping use case: changing the address attribute

About this task

The following task provides a use case for attribute mapping when the Directory Service Response contains `address` as `postalCode`, instead of `StreetAddress`.

By default, the `address` application field in the directory service response contains the `streetAddress` LDAP attribute value of the user.

To configure the `address` application field to contain the postal address, perform the following actions:

Procedure

1. Log in to the Avaya Aura® Device Services administration portal.

   The URL for gaining access to the administration portal is `https://<hostname>:8445/admin`.

   Important:

   For the host name, always use the same Avaya Aura® Device Services server FQDN that you use for generating certificates. You will be redirected to the Login page if you use the IP address instead of the FQDN.

   To gain access to the web-based administration portal, you must use an account that has the Administrator role defined in the LDAP server configuration.
2. Select **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. Click **Modify Attribute Mappings**.
4. Find the `address` application field.
5. In the combo box next to the `address` application field, select `postalCode`.
6. Click **Save**.
7. To apply the changes immediately, click **Force LDAP Sync** on the Enterprise Directory page.

Attribute mapping use case: adding the language to the directory service response

About this task

The following task provides a use case for attribute mapping when the Directory Service Response contains the language of the user.

The attribute used for determining the language of a user depends on each organization.

By default, the `language` field does not have a default attribute mapping. The `preferredLanguage` attribute used in the following example is not a pre-loaded attribute. You must type the `preferredLanguage` name in the custom attribute field.

Important:

Before you type the name of a custom attribute, ensure that the attribute is available in your Directory configuration and that the attribute is available or part of the global catalogue.

The following procedure describes how to map the `preferredLanguage` attribute to the `language` application field by using the custom attribute field.

Procedure

1. Log in to the Avaya Aura® Device Services administration portal.

The URL for gaining access to the administration portal is `https://<hostname>:8445/admin`.

Important:

For the host name, always use the same Avaya Aura® Device Services server FQDN that you use for generating certificates. You will be redirected to the Login page if you use the IP address instead of the FQDN.

To gain access to the web-based administration portal, you must use an account that has the Administrator role defined in the LDAP server configuration.

2. Select **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. Click **Modify Attribute Mappings**.
4. Find the `language` application field.
5. In the **Custom Attribute Field** column that corresponds to the `language` application field, click the cell and type `preferredLanguage`.
6. Click **Save**.
7. To apply the changes immediately, click **Force LDAP Sync** on the Enterprise Directory page.

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. Click **Modify Attribute Mappings**.
5. For **PictureURL**, select **jpegPhoto** from the drop-down list.
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.

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.

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 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 (e.g. "AADSAdmin", etc.)
Role Attribute is DN	true	The "memberOf" values are the DNs of the group/mailing 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 empty because "Role Attribute is DN" is false.
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 9: Reverse proxy configuration

Checklist for reverse proxy configuration

In networks where connections to an Avaya Aura® Device Services instance go through Avaya SBCE 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 `/opt/Avaya/DeviceServices/<version>/CAS/<version>/nginx/certs/nginx.crt`.	
2	Generate certificate request on Avaya SBCE by using the Avaya Aura® Device Services front-end FQDN.	See Creating a Certificate Signing Request on page 170.	
3	Issue certificate from Certificate Authority.	See Creating an end entity on page 172 and Creating the certificate using a CSR on page 173.	
4	Ensure port 443 is open on both sides of Avaya SBCE.		
5	Install server certificates on Avaya SBCE.	See Uploading certificate file on page 173 and Synchronizing and installing certificate in a multi-server deployment on page 175.	
6	Install client certificates on Avaya SBCE.	See Downloading the System Manager PEM certificate on page 176 and Installing CA certificate on page 176.	
7	Create client and server TLS profiles.	See Creating a new TLS server profile on page 177 and Creating a client profile on page 179.	

No.	Task	Notes	✔
8	Add reverse proxy.	See Adding a reverse proxy on page 182.	

Creating a Certificate Signing Request

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Certificates**.

   The EMS server displays the Certificates screen.
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 screen, and click **Generate CSR**.

   Ensure that the **Key Encipherment** and **Digital Signature** check boxes are selected. Do not clear these check boxes.

   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 screen 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/.

Name	Description
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.

Install Certificate

Name	Description
Type	The type of certificate that you want to install. Options are: **Certificate**, **CA Certificate**, or **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.
Allow Weak/Certificate Key	An option to permit usage of a weak private keys. This option bypasses the check that requires strong private keys. EMS rejects private keys lesser than 2048 bits or signed with an MD5 based hash by default.
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 SBCE. 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 existing key from the filesystem or select a file containing another key.
Key File	The button that is displayed when you select **Upload Key File** in the **Key** field. Depending on the browser, click **Browse** or **Choose File** to locate the file.

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.

Name	Description
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. You cannot provide wildcard (*) characters 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 4096) 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.
Subject Alt Name	An optional text field that can be used to further identify this certificate. You can provide multiple comma-separated entries in this field. You cannot provide wildcard (*) characters in this field. Avaya SBCE does not support SIP URI as a valid value for the **Subject Alt Name** field.
Passphrase	The password used when encrypting the private key.
Confirm Passphrase	A verification field for the Passphrase.
Contact Name	The name of the individual within the issuing organization acting as the point-of-contact for issues relating to this certificate.
Contact E-mail	The e-mail address of the contact.

Creating an end entity

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. You can also select **P 12 file**.

7. Click **Add**.

   The system displays the message `End Entity <username> added successfully.`

Creating the certificate using a CSR

Before you begin

Create an end entity as described in Creating an end entity on page 172.

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-formated PKCS10 certification request.
   c. Click **OK**.

      A certificate in PEM format is generated. The certificate contains the values provided in the end entity.

Uploading 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, reencode 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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 from Filesystem**: 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. **(Optional)** 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 SBCE. 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 EMS.

Next steps

Synchronize the certificate to Avaya SBCE through a secure shell (SSH) session.

Synchronizing and installing certificate in a multi-server deployment

About this task

A multi-server deployment can consist of one or more Avaya SBCE HA pairs or multiple individual Avaya SBCE servers. Use this procedure to synchronize and install certificates for each Avaya SBCE 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 SBCE 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 SBCE, 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. At the # prompt, type `certsync` and press `Enter`.

   Avaya SBCE synchronizes with EMS and displays the list of available certificates.
9. Type `certinstall` *`certificate_file_name`*, where *certificate_file_name* is the name of the certificate file that you want to install.

   If the **`certinstall`** command does not accept the certificate file name that you enter, rename the file with extension .crt and enter the filename again.
10. When the system requests the key passphrase, enter the passphrase.

If you used the CSR generation utility that is built into Avaya SBCE, the passphrase is the password you entered in the Generate CSR screen.

11. At the # prompt, type `exit` and press `Enter`.

    The system exits the program level and displays the $ prompt.

12. 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.

13. Use the EMS web interface to restart the Avaya SBCE application.

Downloading the System Manager PEM certificate

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 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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 new TLS server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.

   The EMS server displays the Server Profiles screen.
4. Click **Add**.

   The EMS server displays the New Profile window.
5. Enter the requested information into the appropriate fields.
6. Click **Finish**.

Result

The EMS server creates, installs and lists the TLS server profile in the application pane.

TLS server profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS Client Profile Pop-up Screen Field Descriptions on page 180

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**.

Field	Description
TLS Profile	
Profile Name	The descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	

Field	Description
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.
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	

Field	Description
Version	The TLS versions that the client or servers accepts or offers. The options are: • TLS 1.2 • TLS 1.1 • TLS 1.0 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. Available selections 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.

Creating a client profile

Procedure

1. Log in to Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click **Add**.

   The system displays the **New Profile** window.
4. Enter the requested information in the appropriate fields.
5. Click **Finish**.

   The system installs and displays the new TLS client profile.

TLS client profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS server profile pop-up window field descriptions on page 177.

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**.

Name	Description
TLS Profile	
Profile Name	A descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
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.
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.

Name	Description
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.
Custom Hostname Override	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.
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	
Version	The TLS versions that the client or servers accepts or offers. The options are: • TLS 1.2 • TLS 1.1 • TLS 1.0 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. Available selections 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.

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. Log in to the EMS.web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **DMZ Services** > **Relay**.

   The EMS server displays the Relay Services page.
4. In the **Reverse Proxy** tab, click **Add**.
5. 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 SBCE 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 SBCE 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 whitelisted IPs.

6. 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 10: Remote access configuration

You can configure Avaya Aura® Device Services to be accessible to remote workers using Avaya Equinox® clients from outside the enterprise network. The following configuration methods are available:

- Virtual private Network (VPN)
- Avaya Session Border Controller for Enterprise (Avaya SBCE)
- Application Delivery Controllers (formerly named Reverse Proxies)

The following section contains an example for configuring the remote access feature using Avaya Session Border Controller for Enterprise and instructions for configuring the A10 Thunder ADC.

Configuring remote access

About this task

You can use the Avaya SBCE for relaying HTTP and HTTPS traffic between Avaya Aura® Device Services enabled application clients (such as the Avaya Equinox® clients) and Avaya Aura® Device Services. For more information about relay services configuration in Avaya SBCE, see *Administering Avaya Session Border Controller for Enterprise.*

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 SBCE.

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 SBCE when external.
- Use Public cloud model: All FQDNs or URLs must point to the reverse proxy or Avaya SBCE. 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 SBCE, 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 SBCE IP address created for Avaya Aura® Device Services relay.
   - **Listen Port**: 8443 or 443.
   - **Connect IP**: the internal Avaya SBCE 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:

The Avaya Aura® Device Services enabled client must import the System Manager's Root Certificate in order to successfully establish the SSL connection with the A10 server.

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 System Manager root certificate

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 **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 192.
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 11: Troubleshooting

This section describes troubleshooting issues related to deploying Avaya Aura® Device Services.

Service unavailable

Condition

Avaya Aura® Device Services is not available and displays a 503 error.

Cause

Avaya Aura® Device Services is not paired to Session Manager.

DRS synchronization is not complete.

Traffic exceeds acceptable limits.

Solution

1. Log in to Session Manager and check whether Avaya Aura® Device Services is paired to the Session Manager.
2. Wait for traffic to reduce to acceptable limits.
3. Ensure that DRS synchronization is done.

Avaya Equinox® cannot connect to Avaya Aura® Device Services

Condition

Avaya Equinox® 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 zone is not configured properly

Cause

The DNS reverse lookup zone for Session Manager is not configured properly.

Solution

1. Check the DNS forward and reverse lookup zone.
2. Verify the System Manager enrollment password.

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.

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.

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.

Open LDAP replication fails

Condition

Open LDAP replication fails. The `/var/log/Avaya/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.log` file and ensure that it does not contain any error messages.

If the `/var/log/Avaya/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 134

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.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.

Chapter 12: 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		
Deploying Avaya Aura® Device Services	Deploy Avaya Aura® Device Services.	Sales engineers, solution architects, implementation engineers, support personnel
Deploying Avaya Aura® Session Manager	Deploy the Session Manager OVA.	Sales engineers, solution architects, implementation engineers, support personnel
Administering		
Administering Avaya Aura® Device Services	Administer Avaya Aura® Device Services.	System administrators, support personnel
Administering Avaya Aura® Session Manager	Administer the Session Manager interface.	System administrators, support personnel
Planning for and Administering Avaya Equinox® for Android, iOS, Mac, and Windows	Perform system planning and configuration for: • Avaya Equinox® for Android • Avaya Equinox® for iOS • Avaya Equinox® for Mac • Avaya Equinox® for Windows	System administrators, support personnel
Using		
Using Avaya Device Enrollment Services to Manage Endpoints	Use Device Enrollment Services to manage endpoints or devices.	Non-Avaya users, such as service providers and resellers

Title	Use this document to:	Audience
Other		
Port Matrix for Avaya Aura® Device Services	Understand ports for Avaya Aura® Device Services. **Note:** This document is only available on the Avaya Support website. You might need to be logged in to access the document.	Solution architects, implementation engineers, system administrators, support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.

  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:

  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at 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 http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.
   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

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 LYNC interface certificate is used for integration with Lync or Skype for Business.
- 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 PKS12-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 provides you with the possibility of using certificates that are specific to your organization and have the certificates signed by a local or public certificate authority.

The following procedure describes how to import the certificate files and the 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, including Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Session Border Controller, and the Equinox Management server.
- 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, 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**.
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
   - LYNC interface key file
   - LYNC interface certificate file
   - OAM interface key file
   - OAM interface certificate file
   - node key file
   - node certificate file
   - signing authority certificate file

   Both 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. You can also generate certificates using 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**.
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 by 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:

   ```
   sudo mkdir /opt/Avaya/AADSportalCerts
   sudo chmod 770 /opt/Avaya/AADSportalCerts
   ```

   The system creates an `AADSportalCerts` directory in `/opt/Avaya/` 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 /opt/Avaya/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.
- `orgnizationName`: 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 `/opt/Avaya/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.

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
```

Configuring certificates to connect Avaya Aura® Device Services to the Avaya Aura® Web Gateway

About this task

If you are planning to connect Avaya Aura® Device Services to the Avaya Aura® Web Gateway, in addition to providing the host name for server-to-server communication in the CloudFormation template, you also need a certificate containing information about the FQDN that is used for server-to-server communication. Otherwise, this FQDN will not be part of the SAN, and Avaya Aura® Device Services will not connect to the Avaya Aura® Web Gateway.

This procedure describes the high-level certificate configuration process, which is performed in the Avaya Aura® Device Services web administration portal.

Before you begin

- When deploying a CloudFormation stack, provide the host name that is mapped directly to Avaya Aura® Device Services nodes in the **Hostname for server-to-server** field. For more information, see Deploying a multi-node CloudFormation stack on page 75.
- Install Avaya Aura® Device Services.

Procedure

Perform these steps in the web administration portal. For more information, see “Creating a CSR required to connect Avaya Aura® Device Services to the Avaya Aura® Web Gateway” in *Administering Avaya Aura® Device Services*.

1. Generate a CSR containing the FQDN that is used for server-to-server communication. This FQDN consists of the following parts:
   - Host name that you provided in the **Hostname for server-to-server** field when you deployed a CloudFormation stack.
   - Avaya Aura® Web Gateway domain.
2. Provide the CSR file to the System Manager CA for signing.
3. Assign the signed certificate to the Internal Avaya Aura® Device Services server interface.

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 SBCE, the request contains the subjectAltName extension that lists the cluster FQDN in the SAN.
  - If the certificate is used on both Avaya SBCE 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.

    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.
- Obtain the System Manager root CA certificate.
- Generate the trust certificate chain by concatenating the root CA, all intermediate CA, and the System Manager root CA certificates into a `trustchain.PEM` file.

Procedure

1. Log on to Avaya Aura® Device Services using your SSH credentials.
2. Import the intermediate CA certificate and the root CA certificate to the Avaya SBCE trust store if you are using reverse proxy on the Avaya SBCE to Avaya Aura® Device Services.
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.
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 you have created.
12. Click **Return to previous menu**.
13. Click **Apply**.

Configuring System Manager to trust third-party root CA certificates

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

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.

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 the secure LDAP certificate using the configuration utility

Before you begin

- Ensure that the certificate file is in the `.PEM` format. If it uses a different format, such as `.DER`, you must first convert the file to the `.PEM` format using the **`openssl`** command in the Avaya Aura® Device Services CLI.

  For example:

  ```
  openssl  x509 -inform DER -outform PEM -in certificate.der -out certificate.pem
  ```

- Ensure that the FQDN that is configured as the address of the LDAP source is defined in the LDAP certificate in one of the following places:
  - The Common Name in the Subject field.
  - Subject Alternative Name.

You can use the following command to verify the certificate content:

```
openssl s_client -connect <ldap server:port> | openssl x509 -noout -text
```

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **LDAP Configuration** > **Import Secure LDAP trusted certificate**.
3. In the **Trusted LDAP certificate settings** menu, configure the following settings:
   - **Certificate file**: The path and file name for the LDAP trusted certificate. This file must be in the PEM format.

   Note:

   If you perform a silent installation, the equivalent parameter that you must configure in the `installation.properties` file is `LDAP_TRUSTSTORE_CERTFILE`.

Importing a trusted LDAP certificate

About this task

Use this procedure to import the LDAP certificate to enable secure LDAP.

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. Go to, `/opt/Avaya/DeviceServices/ClientInstallers` on both Avaya Aura® Device Services servers and transfer the CA certificate files in this directory.
2. Run the following command to change the ownership of the certificate file:

   ```
   sudo chown ucapp:ucgrp <certificate-file>
   ```

3. To verify that the certificate download link is valid, open the following URL in the web browser:

   `https://<aads-server-fqdn>/acs/resources/webdeployment/downloads/<certificate-file>`

   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 and Avaya Aura® Device Services certificates are signed by System Manager. Therefore, TLS links are not established until you import both CAs 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 Equinox® Management site at `http://<IVIEW>:8080/iview/`, and do the following:
   - If you have Avaya Equinox® 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 Equinox® Management 9.0, set the com.vnex.vcms.core.aadsIP Avaya Scopia® parameter to the Avaya Aura® Device Services address and restart Avaya Equinox® Management to apply the changes.

     Avaya Aura® Device Services accepts the incoming connection if the address matches the address on the Avaya Equinox® 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 Equinox® Management version.

   Avaya Aura® Device Services supports only one Avaya Equinox® 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 Equinox® Management.

   For example, type `alphaiview1.dr.avaya.com`.
8. If you have Avaya Equinox® 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 Equinox® Management 8.5.
9. Click **Save**.
10. Restart the Avaya Aura® Device Services.

Appendix B: 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=sAMAccoutName
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=1
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=1
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
```

Appendix C: 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=val
 ley,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.

Related links

Changing the password of the Avaya Aura Device Services virtual machine on VMware through SSH on page 227

Changing the password of the Avaya Aura® Device Services virtual machine on VMware through SSH

About this task

When you log in to the system for the first time, change the password and then log in again.

Procedure

1. Log in to the system as `admin`.

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

   The system prompts you to type the password.

2. Type the password.

   The system 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.

   After you change the password, the system closes the SSH session.

Related links

LDAP search results and referrals on page 224

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 Equinox® clients 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

D

E

F

G

I

K

L

M

N

O

P

R

S

T

U

V

W