Administering Avaya Aura® Device Services

Release 8.0.2
Issue 4
June 2020

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 ongoing administration, management, and maintenance tasks for Avaya Aura® Device Services. Use this document after deploying Avaya Aura® Device Services. For more information about deployment, see *Deploying Avaya Aura® Device Services*.

Change history

Issue	Release Date	Summary of changes
Release 8.0.2, Issue 4	June 2020	• Added Web administration portal roles on page 27. • Indicated that the Security Administrator role is required to access the Security Settings page on the web administration portal throughout the document. • Added Changing your Keycloak password on page 60. • Updated the URL for accessing Avaya Spaces throughout the document. • Removed the instruction to import the Avaya Spaces CA certificate from Checklist for configuring Avaya Spaces integration on page 76. • Added information about the **Status** and **License Information** fields to Setting up Avaya Spaces integration on page 79. • Indicated that you do not need to import the Avaya Spaces CA certificate manually in Setting up Avaya Spaces integration on page 79. • Added Uploading Avaya Spaces language and time zone settings to Avaya Aura Device Services on page 82. • Added Language file format on page 83. • Added Time zone file format on page 84. • Indicated that Avaya Aura® Device Services now displays license expiration information in Avaya Spaces user licenses on page 85.

Issue	Release Date	Summary of changes
		• Updated Registering enterprise users on Avaya Spaces on page 87. • Updated Removing an unregistered user on page 88. • Added new sections about configuring automatic registration of LDAP group users on Avaya Spaces under Automatic registration of LDAP group members on Avaya Spaces on page 88. • Added Viewing user information on page 93. • Updated Assigning a different license to Avaya Spaces users on page 95. • Added Cancelling user registration and license upgrade operations on page 98. • Added Updating Avaya Spaces integration parameters on page 99. • Added Viewing the Avaya Spaces connection status on page 101. • Indicated that automatic LDAP synchronization is required for automatic registration of LDAP group users on Avaya Spaces in Setting up user synchronization with the LDAP server on page 116. • Indicated that the Utility Server only supports HTTP for backing up H.323 files in Backing up H.323 phone settings on the Utility Server on page 145. • Added Enabling additional STIG hardening on page 200. • Added Disabling additional STIG hardening on page 201. • Added Configuring the SameSite cookie attribute on page 201. • Added information about Avaya Spaces connection alarms in Avaya Aura Device Services alarms list on page 209. • Indicated that a password must be used when creating backups in an archive or restoring backups from an archive in Backup and restore on page 217. • Updated upgrade paths in Avaya Aura Device Services upgrade and migration operations on page 223. • Added Avaya Spaces connectivity errors on page 280. • Added Avaya Aura Device Services does not contain the latest Avaya Spaces CA certificate on page 280.
Release 8.0.1, Issue 3	March 2020	Updated the command to restart the SpiritAgent service in System Manager does not show Avaya Aura Device Services alarms on page 265.
Release 8.0.1, Issue 2	March 2020	• Updated the names of some Avaya products. Specifically, Avaya Equinox® was renamed to Avaya IX™ Workplace Client. • Updated New in this release on page 18.

Issue	Release Date	Summary of changes
		• Added Data encryption on page 24 and Data retention on page 24. • Updated Configuring enhanced search options on page 29. • Added Integration with Avaya IX Workspaces for Oceana on page 33. • Added general information about OAuth authorization to Avaya Aura Device Services OAuth2 management on page 39. • Added Prerequisites for OAuth2 configuration on page 45. • Updated Checklist for OAuth2 authentication configuration on page 47. • Added procedures for configuring Office 365 integration under Avaya Aura Device Services integration with Office 365 for OAuth2 authentication on page 49. • Added a new chapter: Avaya Spaces integration on page 76. • Moved LDAP server management procedures to a new chapter: LDAP server management on page 102. • Updated LDAP server management on page 102. • Updated Adding a new enterprise LDAP server on page 103. • Added Testing connection to a LDAP server on page 111. • Updated Configuring additional base context DNs on page 111. • Updated Modifying the provenance priority on page 112. • Updated Modifying enterprise directory attribute mappings on page 113. • Updated Configuring Windows Authentication for Active Directory on page 114. • Updated Setting up user synchronization with the LDAP server on page 116. • Updated Changing the PictureURL attribute on page 122. • Moved certificate management procedures to a new chapter: Certificate management on page 123. • Moved procedures related to the Web Deployment service to a new chapter: Web Deployment service management on page 131. • Added Enabling access to the Utility Server using an HTTP connection on page 140. • Added Uploading settings files to the Utility Server on page 143. • Updated Administration of the Dynamic Configuration service on page 153.

Issue	Release Date	Summary of changes
		• Updated Viewing the Home location in System Manager on page 155. • Updated Publishing the configuration settings on page 164. • Updated Setting up the Windows Domain Controller on page 179. • Added Configuring the data retention period on page 185. • Added a new chapter: Security options on page 190, which includes information about managing disk encryption and the AIDE and ClamAV tools. • Updated Log management on page 204. • Added Configuring remote logging on page 204. • Updated Changing a logging level on page 205. • Updated Downloading logs on page 206. • Added sections about configuring serviceability agents under Alarms on page 207. • Updated Restoring Avaya Aura Device Services in a standalone environment on page 218. • Updated Restoring an Avaya Aura Device Services cluster on page 220. • Updated Avaya Aura Device Services upgrade and migration operations on page 223. • Added Disk encryption on page 224. • Added Changing the SELinux mode to permissive on page 227. • Added Checklist for updating the system layer on page 225. • Updated Installing a staged system layer update on page 228. • Added migration procedures for ESXi deployments under Migrating Avaya Aura Device Services on ESXi on page 244. • Updated Checking for DRS synchronization on page 257. • Added Primary System Manager fails on page 262. • Updated Allocating unused disk space to logical volumes on page 269. • Added Cannot register an enterprise user on Avaya Spaces on page 282. • Added Avaya Spaces user management operation fails on page 282. • Added Logs collected using the collectlogs command are encrypted on page 283. • Added *Avaya Aura® Device Services Data Privacy Controls Addendum* to Documentation on page 284.

Issue	Release Date	Summary of changes
		• Updated sys volmgt command on page 294. • Added passwdrules command on page 303. • Added information about disk encryption commands under Data encryption commands on page 304. • Minor rephrasing throughout the document. • Removed “Managing picture settings” because Unified Portal does not support the picture upload functionality anymore.
Release 8.0, Issue 1	July 2019	• Updated New in this release on page 18. • Updated Logging in to the Avaya Aura Device Services web administration portal on page 26. • Updated Enterprise LDAP Server Configuration field descriptions on page 105. • Added Enabling LDAP authentication for OAuth on page 113. • Updated Uploading the client installer on page 132. • Added a new chapter, Avaya Aura Device Services OAuth2 management on page 39 • Updated Logging in to the Utility Server on page 141. • Added Password masking on page 160. • Updated Overwriting an existing configuration on page 162. • Updated Testing configuration settings on page 163. • Updated Viewing published settings on page 165. • Updated Importing dynamic configuration settings using a file in the JSON format on page 167. • Added JSON file structure on page 167. • Added Managing automatic logging in to Avaya clients on page 173. • Updated Defaults field descriptions on page 174. • Added Setting up the Windows Domain Controller on page 179. • Added Enabling encryption for the domain user on page 182. • Updated Restoring an Avaya Aura Device Services cluster on page 220. • Updated Avaya Aura Device Services upgrade and migration operations on page 223. • Added “Virtual machine memory requirements”. • Updated Upgrading the existing AVP virtual machines on page 233.

Issue	Release Date	Summary of changes
		• Updated Upgrading Avaya Aura Device Services on ESXi or AWS on page 240. • Added “Allocating memory resources to the Avaya Aura® Device Services virtual machine”. • Updated Upgrading ESXi or AWS virtual machines on page 241. • Added OAuth2 authentication does not work as expected on page 275. • Updated collectlogs on page 291.

Chapter 2: Avaya Aura® Device Services overview

With Avaya Aura® Device Services, you can roll out multiple clients and seamlessly transition between devices. Avaya Aura® Device Services acts as a single point of administration for endpoints. It can also provide file server capabilities, such as firmware and settings files. Avaya Aura® Device Services can handle traditional IP phones, such as the 96xx Series Phones, and the complex configuration of SIP endpoints, such as Avaya IX™ Workplace Client[1].

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

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

As an administrator, you must maintain software-based soft clients on a limited set of versions to ensure consistent feature sets and security. With hard phones, such as 96xx Series Phones, you can initiate a firmware download by forcing the phone to reboot. With a soft phone, such as Avaya IX™ Workplace Client, 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 Releases 8.0.1 and 8.0.2.

Data privacy and personal data protection

Avaya Aura® Device Services provides measures to ensure data privacy and secure processing of personal data for GDPR and CCPA compliance. You can deploy Avaya Aura® Device Services in a secure mode to encrypt personal data and configure automatic deletion so that any internally generated logs and reports do not persist for more than 24 hours.

[1] This document also uses the term “client” when referring to Avaya IX™ Workplace Client.

Avaya Spaces integration

Avaya Spaces is a cloud-based team collaboration and meeting platform. Using the Avaya Aura® Device Services web administration portal, you can:

- Register users in your enterprise directory on Avaya Spaces. These users do not need to perform the user self-registration sign-up process. Starting from Release 8.0.2, you can automatically register enterprise users that belong to a specific LDAP group.
- Manage Avaya Spaces user licenses.

Security enhancements

To ensure the secure processing of user data and reduce security vulnerabilities, Avaya Aura® Device Services now supports the following hardening features:

- Disk encryption. When data encryption is enabled, all Avaya Aura® Device Services data, including operational data, configuration data, and log files are encrypted.
- Advanced Intrusion Detection Environment (AIDE) tool. AIDE monitors file system changes, verifies the integrity of the files and notifies you if it finds any differences with the reference values.
- ClamAV antivirus. ClamAV is an open-source antivirus tool for Linux. It can detect viruses, malware, trojans, and other malicious software on Avaya Aura® Device Services.
- Additional STIG hardening options. If your organization requires stricter STIG compliance, you can enable additional Linux STIG security hardening options.
- Protection against cross-site request forgery attacks. You can use the SameSite attribute to specify when Avaya Aura® Device Services sends cookies in response to cross-origin requests.
- Passwords for backup files. Now you can protect your Avaya Aura® Device Services backup files with passwords.

Support for Office365 as an identity provider

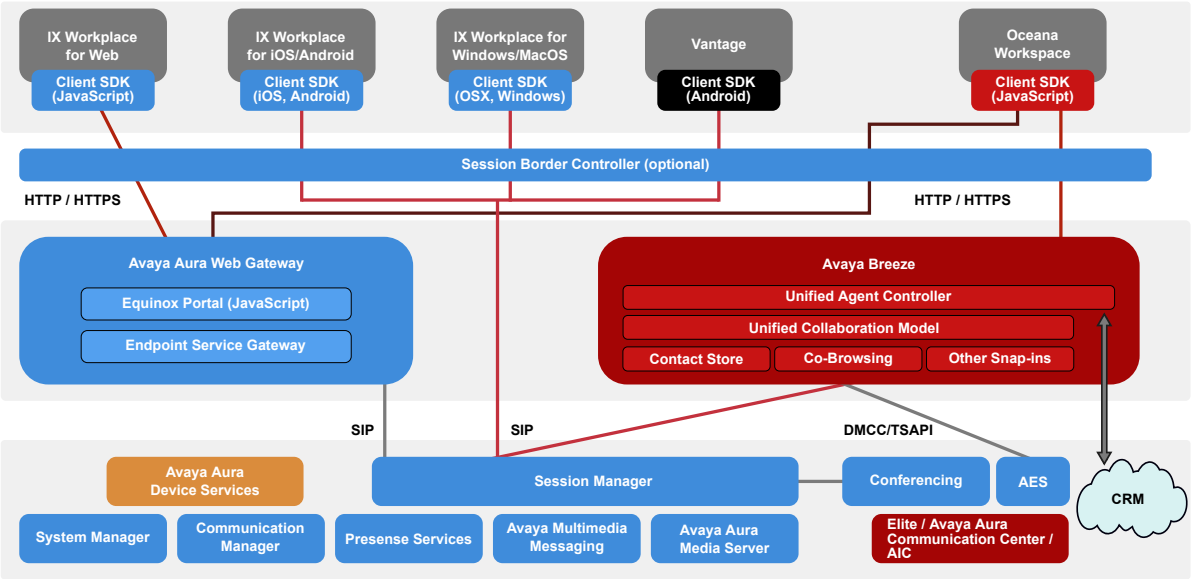
Avaya Aura® Device Services now supports Office365 as a SAML v.2 and OAuth2 identity provider.

Dynamic Configuration service updates

You can now define your own platform types and publish settings for these platform types.

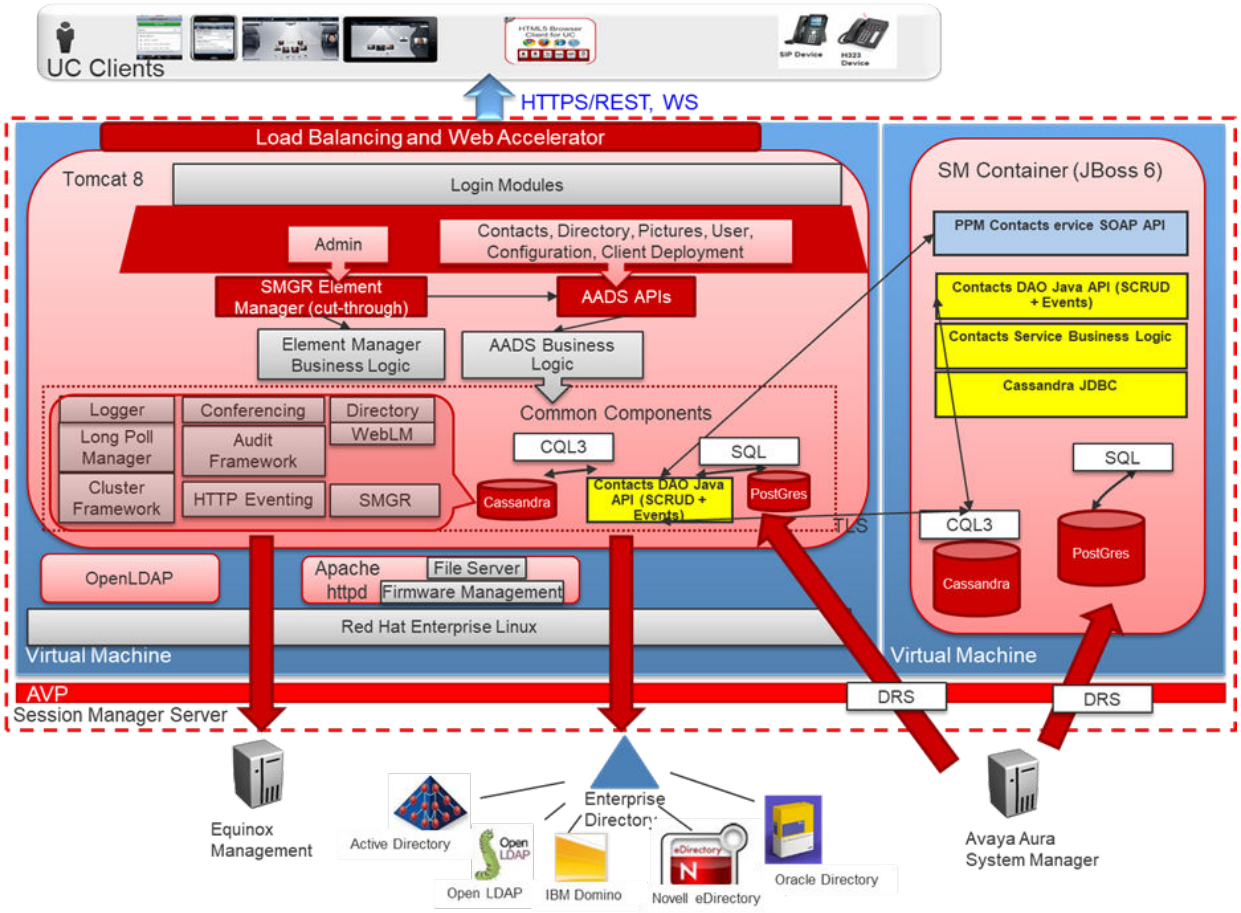
Solution topology

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:



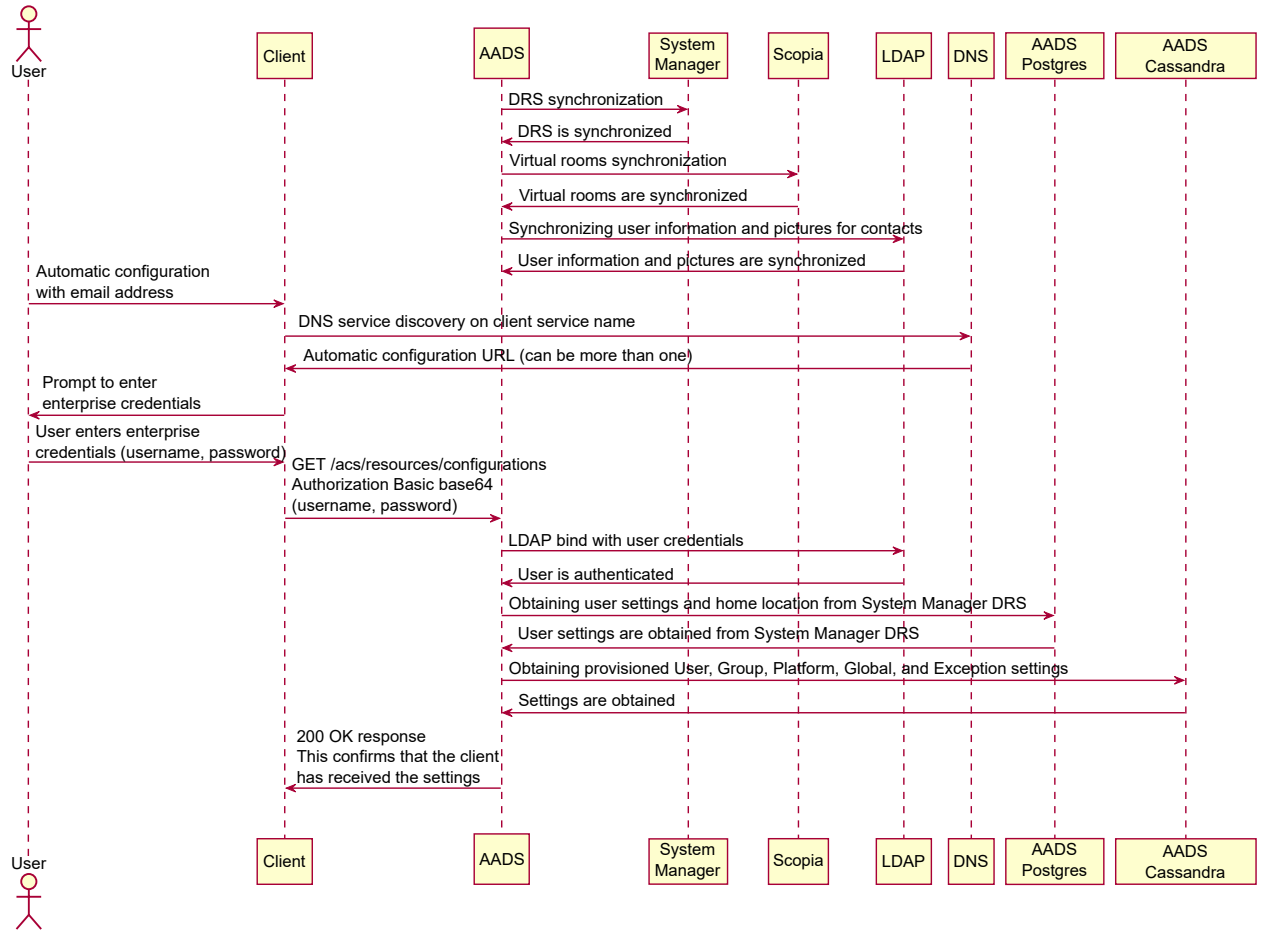
Avaya Aura® Device Services is aligned with Session Manager, Appliance Virtualization Platform, and the VMware virtualized environment. The VMware license embedded in the Appliance Virtualization Platform does not support vCenter.

Note:

You must deploy Avaya Aura® Device Services on the same subnet as the Session Manager management subnet.

Automatic configuration flow

The following diagram shows the automatic client configuration flow.



Components

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

Components	Description
Avaya Aura® core	Avaya Aura® Device Services requires the following key Avaya Aura® key components: • System Manager: For centralized management. System Manager also enables other capabilities, including licensing with Avaya WebLM. **Note:** Avaya Aura® Device Services does not support the System Manager Geographic Redundancy mode. • Session Manager: For registration and telephony functions, such as call escalation. • Communication Manager: For organizing and routing voice, data, image, and video transmissions. • Presence Services: For Presence and IM functionality.
Avaya Session Border Controller for Enterprise (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.

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

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

- Solution Deployment Manager
- vSphere Client
- vCenter server
- Appliance Virtualization Platform

Data retention

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

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

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

Data retention — log files

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

Data retention — Cassandra database

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

Related links

Configuring the data retention period on page 185

Data encryption

As of Release 8.0.1, you can enable or disable data encryption when deploying the Avaya Aura® Device Services OVA. When data encryption is enabled, all operational data and log files are encrypted.

You can only enable data encryption on Avaya Aura® Device Services if are using Appliance Virtualization Platform or a VMware Virtualized Environment. For Amazon Web Services (AWS) deployments, you must enable data encryption on AWS itself. For more information, see How to Protect Data at Rest with Amazon EC2 Instance Store Encryption.

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

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

Encryption of Avaya Aura® Device Services partitions

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

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

The sda boot disk is always unencrypted.

Related links

Data encryption management on page 185

Chapter 3: Management of Avaya Aura® Device Services with the web administration portal

Logging in to the Avaya Aura® Device Services web administration portal

About this task

You can access the Avaya Aura® Device Services web administration portal by using the Avaya Aura® Device Services URL or System Manager. To use System Manager for single sign on, you must add the Avaya Aura® Device Services instance to System Manager.

Before you begin

- In the DNS, add an entry to map the IP address with the FQDN.
- If the FQDN does not resolve through DNS, you must add the Avaya Aura® Device Services IP address and FQDN in the `hosts` file of the system from which you are accessing the Avaya Aura® Device Services web administration portal. The default path of the `hosts` file on a Microsoft Windows system is `C:\Windows\System32\drivers\etc\hosts`.

Procedure

1. Open your web browser.
2. Type the URL in one of the following formats:
   - `https://<FQDN>:8445/admin/`
   - `https://<IP_Address>:8445/admin/`

     If IPv6 support is enabled you can use either IPv4 or IPv6 addresses.

     The following are URL examples:

     - IPv4 address example: `https://192.0.2.44:8445/admin`
     - IPv6 address example: `https://[2001:db8::7334]:8445/admin`
3. Press `Enter`.

   If your browser does not have a valid security certificate, the browser displays a warning with instructions to load the security certificate.

4. **(Optional)** If you are certain your connection is secure, accept the server security certificate to access the Login screen.
5. On the Login screen, enter your user name and password.

   To access the web-based administration portal, use an account with an administrator role defined in the LDAP server configuration.

   Note:

   If OAuth is enabled on Avaya Aura® Device Services and LDAP authentication for OAuth is disabled, then you must use the credentials of the administrative user created during OVA deployment. For more information about enabling LDAP authentication, see Enabling LDAP authentication for OAuth on page 113.
6. Click **Log on**.

Related links

Web administration portal roles on page 27

Web administration portal roles

Role	Description
Administrator	Enables full access to most web administration portal pages except for the Security Settings page. You can perform any administration operation on the pages you can access.
Services Administrator	
Security Administrator	Enables full access to all web administration portal pages, including the Security Settings page. You can perform any administration operation with this role.
Auditor	Provides read-only access to web administration portal pages. You cannot modify any settings.
Services Maintenance and Support	

Related links

Logging in to the Avaya Aura Device Services web administration portal on page 26

Starting or stopping Avaya Aura® Device Services

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Service Control** > **Application Management**.
2. Select the **Device Services** check box and then do one of the following:
   a. Click **Start** to start Avaya Aura® Device Services.

b. Click **Stop** to stop Avaya Aura® Device Services.

Managing application sessions

About this task

Use this procedure to:

- Set a timeout period for terminating inactive, idle, or unattended sessions.
- Manage concurrent HTTP sessions.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Service Control** > **Application Management**.
2. In the Application Properties area, complete the required settings, which are described in Application Properties field descriptions on page 28.
3. Click **Save**.

Application Properties field descriptions

Name	Description
Admin HTTPSession Timeout (minutes)	The timeout period for the Avaya Aura® Device Services web administration portal. You can enter a value between 1 and 60 minutes. The default value is 15 minutes.
Application HTTPSession Timeout (minutes)	The timeout period for application components. You can enter a value between 1 and 60 minutes. The default value is 15 minutes.
Maximum Concurrent HTTP Sessions	The maximum number of active sessions that are available for application components. If the number of sessions exceeds the configured value for any component, a 503 error, which indicates that service is unavailable, is generated by that component. You can enter a value between 100 and 1,000,000. The default value is 200,000.
Concurrent HTTP Sessions per User	The number of active sessions that are available per user. If the number of sessions exceeds the configured value for any user, a 429 error, which indicates that there are too many requests, is sent as a response to the user's request. You can enter a value between 10 and 1000. The default value is 50.

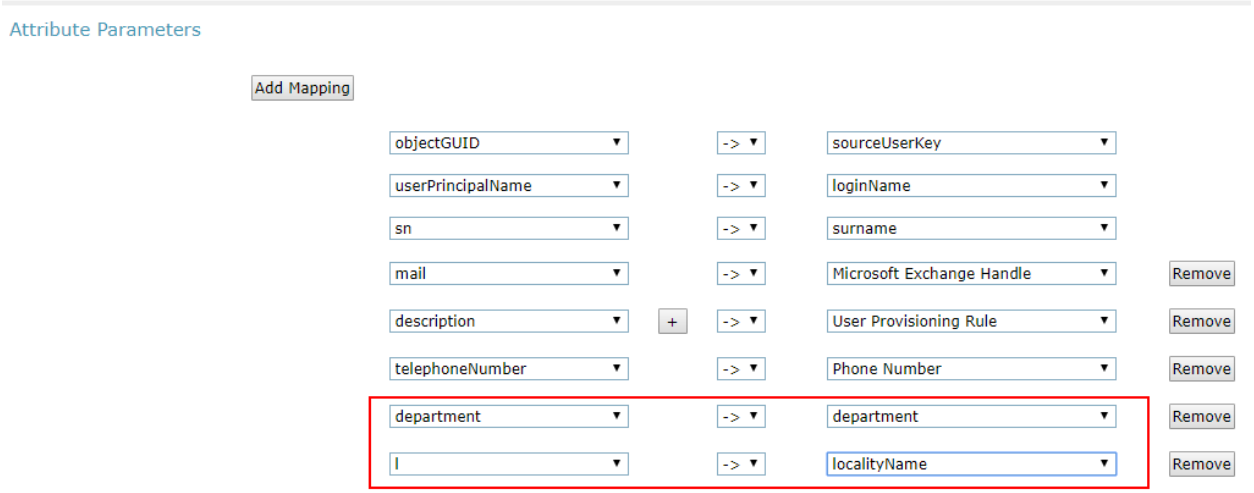
Configuring enhanced search options

About this task

The enhanced search feature enables Avaya IX™ Workplace Client users to search by name, location, or department. Use this procedure to configure the department search capability in the Avaya Aura® Device Services web administration portal.

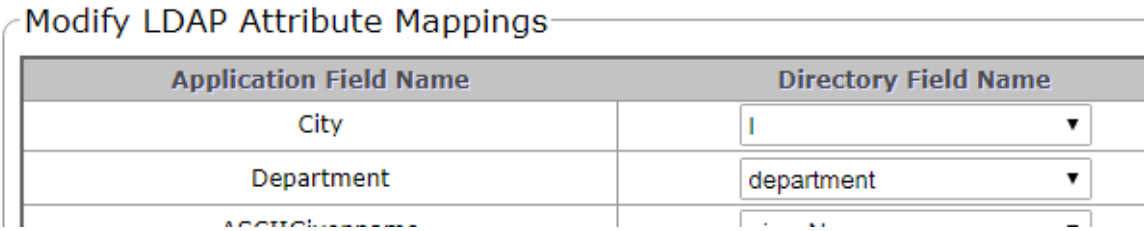
Before you begin

- On System Manager, configure the mapping from the LDAP directory server to System Manager for the department and city attributes. For example:



  For more information, see “Directory synchronization” in *Administering Avaya Aura® System Manager*.

- Ensure that the mapping for the Department and City attributes is configured on each Avaya Aura® Device Services LDAP directory server. For example:



  For more information, see Modifying enterprise directory attribute mappings on page 113.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Client Administration** > **Enhanced Search Configuration**.
2. From the **Department** drop-down list, select one of the following options:
   - **startsWith**: Searches for department names that start with the search text entered. The relevant users from the departments are displayed.

- **contains**: Searches for department names that contain the search text entered. The relevant users from the department are displayed.

3. Click **Save**.

Enabling an external load balancer

About this task

Use this procedure to enable an external load balancer. When you enable the external load balancer, the internal load balancer is disabled.

Before you begin

- Configure the external load balancer. For more information about the external load balancer requirements and configuration options, see “External load balancer requirements” and “Port configuration for an external load balancer” in *Deploying Avaya Aura® Device Services*.
- Disable the virtual IP on all nodes.
- Set the Avaya Aura® Device Services front-end FQDN to the FQDN of the external load balancer on all nodes.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **External Access** > **Load Balancer Check**.
2. Select the **Enable use of an external load balancer** check box.
3. Click **Save**.

Certificate management

You can use the Avaya Aura® Device Services web administration portal to view and manage certificates. For more information, see the sections under Certificate management on page 123.

Client certificate policy administration

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.

Configuring the client certificate policy using the Avaya Aura® Device Services web administration portal

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.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Client Administration** > **HTTP Clients**.

   Avaya Aura® Device Services displays the Client-Device Certificate Policy page.

2. To set the client certificate policy for the REST request, in the **REST** field, select the appropriate setting.

   Note:

   If the client certificate policy for an interface is set to **OPTIONAL**, **OPTIONAL_NO_CA**, or **REQUIRED** client certificates, when presented to the client:

   - Must have digitalSignature key usage if key usage information is present.
   - Must have id-kp-clientAuth if extended key usage is present. This is the TLS WWW client authentication extended key usage.

   If the certificate does not have key usage information, the certificate allows all key usages.

3. To set the client certificate policy for the administrator UI (OAMP), in the **OAMP** field, select the appropriate setting.
4. Click **Save**.

Client-Device Certificate Policy field descriptions

Name	Description
REST	Specifies certificate processing options for REST requests. The options are: • **NONE**: The server does not check for a certificate. The connection is established with or without a valid certificate. • **OPTIONAL**: The server requests a certificate. The connection is established with or without a certificate, but the process stops if a client

Name	Description
	provides an invalid or untrusted certificate, and the system returns the error code `HTTP 400`. • **OPTIONAL_NO_CA**: The server requests a certificate. The connection is established with any valid certificate even if CA is untrusted, but the process stops if a client provides an invalid certificate, and the system returns the error code `HTTP 400`. • **REQUIRED**: The server requests a certificate. The server rejects a connection if a client fails to provide a valid certificate, and the system returns the error code `HTTP 400`. The default value is: **OPTIONAL**.
OAMP	Specifies certificate processing options for OAMP. The options are: • **NONE**: The server does not check for a certificate. The connection is established with or without a valid certificate. • **OPTIONAL**: The server requests a certificate. The connection is established with or without a certificate, but the process stops if a client provides an invalid or untrusted certificate, and the system returns the error code `HTTP 400`. • **OPTIONAL_NO_CA**: The server requests a certificate. The connection is established with any valid certificate even if the CA is untrusted, but the process stops if a client provides an invalid certificate, and the system returns the error code `HTTP 400`. • **REQUIRED**: The server requests a certificate. The server rejects a connection if a client fails to provide a valid certificate, and the system returns the error code `HTTP 400`. The default value is: **OPTIONAL**.

Button	Description
Save	Saves the changes made to the settings.
Cancel	Ignores your changes and resets the settings to default values.

Integration with Avaya IX™ Workspaces for Oceana®

Avaya IX™ Workspaces is a browser-based application with which contact center agents can handle inbound customer operations. Avaya IX™ Workspaces uses Avaya Aura® Device Services for certain functionality. For example, the Avaya IX™ Workspaces address book uses Avaya Aura® Device Services to search for enterprise directory contacts. For information about integrating Avaya Aura® Device Services with Avaya IX™ Workspaces, see “Configuration for Avaya IX™ Workspaces” in *Administering Avaya IX™ Workspaces for Oceana®*.

Enabling Avaya Breeze® platform authorization

About this task

Use this procedure to enable Single Sign-On (SSO) capabilities for Avaya Aura® Device Services users that previously authenticated using the Avaya Breeze® platform Authorization application.

To enable authorization, you must import the Avaya Breeze® platform authorization certificate to Avaya Aura® Device Services. If the certificate is changed, then you must re-upload it to Avaya Aura® Device Services.

For more information about Authorization Service, see “Authorization Service” in *Administering Avaya Breeze® platform*.

Before you begin

Obtain the Avaya Breeze® platform authorization certificate file in the `.PEM` format. For more information, see *Administering Avaya Breeze® platform*.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the “Security administrator” role.
2. Navigate to **Security Settings** > **Authorization**.
3. Click **Choose File** and select the `.PEM` file that you exported from the Avaya Breeze® platform node.
4. Click **Save**.

Dynamic Configuration service management

With the Dynamic Configuration service, Avaya Aura® Device Services can dynamically retrieve and deploy the device configuration settings to Avaya IX™ Workplace Client. For more information about the Dynamic Configuration service, see the sections under Administration of the Dynamic Configuration service on page 153.

Messaging server address discovery management

Avaya Aura® Device Services provides clients with the Presence Services or Avaya Multimedia Messaging server FQDN and port values using the ESMSRVR and ESMPORT parameters respectively. When clients receive a server FQDN, they resolve it to a single IP address and then try to connect to this address. Previously, Avaya Aura® Device Services used System Manager user profiles as the primary source for server FQDN values.

If the server FQDN resolves to multiple FQDN addresses, there might be an issue when clients resolve the FQDN and try to connect to a failed IP address, but do not try to use other IP addresses. To prevent this issue, as of Release 7.1.5, Avaya Aura® Device Services can perform automatic DNS SRV service lookup to resolve the server FQDN and port. Avaya Aura® Device Services sets the values of ESMSRVR and ESMPORT based on the first matching record it finds during the DNS SRV query.

Avaya Aura® Device Services supports the following discovering methods for the messaging server FQDN value:

1. Publishing the ESMSRVR and ESMPORT values using the Dynamic Configuration service.
2. Obtaining the FQDN value from the System Manager user profile. This method can be enabled or disabled using the legacy ESM_MULTISITE_ENABLED parameter.
3. Performing DNS SRV service lookup on the FQDN that is found in the System Manager user profile. This method can be enabled using the new AUTO_AMM_LOOKUP_ENABLED parameter.

By default, automatic DNS lookup is disabled, so Avaya Aura® Device Services uses server FQDN and port values that are configured in the System Manager user profile. If you want to resolve the server FQDN using DNS SRV lookup, you must set the AUTO_AMM_LOOKUP_ENABLED parameter to `1` using the Dynamic Configuration service.

In a migration scenario, Avaya Aura® Device Services continues to use the values configured before migration. In this case, automatic DNS lookup is enabled only if ESM_MULTISITE_ENABLED was set to 0 before migration.

The following table shows which ESMSRVR and ESMPORT values Avaya Aura® Device Services provides to clients depending on the ESM_MULTISITE_ENABLED and AUTO_AMM_LOOKUP_ENABLED values.

Dynamic Configuration parameter value		Value Avaya Aura® Device Services provides to clients	
ESM_MULTISITE_ENABLED	**AUTO_AMM_LOOKUP_ENABLED**	**ESMSRVR**	**ESMPORT**
1	Not published. Derived value is 0	The value configured in the System Manager user profile. If the value is not found, then the published ESMSRVR value is used, if available.	The ESMPORT value published using the Dynamic Configuration service is used, if available.

Dynamic Configuration parameter value		Value Avaya Aura® Device Services provides to clients	
ESM_MULTISITE_ENABLED	**AUTO_AMM_LOOKUP_ENABLED**	**ESMSRVR**	**ESMPORT**
0	Not published. Derived value is 1	The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMSRVR value is used, if available.	The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMPORT value is used, if available.
Not published. Derived value is 1	Not published. Derived value is 0	The value configured in the System Manager user profile. If the value is not found, then the published ESMSRVR value is used, if available.	The ESMPORT value published using the Dynamic Configuration service is used, if available.
1	0	The value configured in the System Manager user profile. If the value is not found, then the published ESMSRVR value is used, if available.	The ESMPORT value published using the Dynamic Configuration service is used, if available.
1	1	The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMSRVR value is used, if available.	The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMPORT value is used, if available.
0	1	The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMSRVR value is used, if available.	The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMPORT value is used, if available.
0	0	The ESMSRVR value published using the Dynamic Configuration service is used, if available.	The ESMPORT value published using the Dynamic Configuration service is used, if available.

When the DNS SRV query fails, Avaya Aura® Device Services assumes that no matching DNS records were found. Avaya Aura® Device Services then uses ESMSRVR and ESMPORT values that are set according to the rules listed in the table.

LDAP server management

You must configure the enterprise LDAP server to authenticate the users and administrators of Avaya Aura® Device Services. The LDAP Configuration screen on the Avaya Aura® Device Services web administration portal displays the enterprise LDAP server that you configured during deployment.

You cannot perform all LDAP server management tasks with the configuration utility. Use the Avaya Aura® Device Services web administration portal to do the following:

- Configure multiple LDAP directories.
- Specify an order in which Avaya Aura® Device Services accesses LDAP directories.
- Select which LDAP directories are used for authentication.
- Configure multiple base context Distinguished Names (DNs).
- Set up LDAP synchronization.
- Configure attribute mappings.

For information about LDAP server management, see the sections under LDAP server management on page 102.

Cross-origin resource sharing

Using the Cross-origin resource sharing (CORS) technology, you can access the webpage resources from different domains. With CORS, a browser can send a cross-origin HTTP request to the web servers to access the resources from a different domain. Also it facilitates a secure cross-domain data transfer.

You can enable and configure CORS on the Avaya Aura® Device Services server using the Avaya Aura® Device Services web administration portal or the Avaya Aura® Device Services configuration utility.

You can enable CORS for the service and administrator interfaces.

Service Interface

The Service Interface page displays the CORS configuration for the Avaya Aura® Device Services server using service port 443.

Administrator Interface

The Admin Interface page displays the CORS configuration for the Avaya Aura® Device Services server using port 8445.

Related links

Configuring the SameSite cookie attribute on page 201

Enabling Cross-origin resource sharing for the Service Interface

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **CORS Configuration** > **Service Interface**.

   Avaya Aura® Device Services displays the Cross-Origin Resource Sharing for Service interface page.

2. Select the **Enable Cross-Origin Resource Sharing** check box.

   Avaya Aura® Device Services displays the **Allow access from any origin** and **Specific Domain(s)** fields.

3. Do one of the following:

   - To allow access to the Avaya Aura® Device Services resources from any domain, select the **Allow access from any origin** check box.
   - To allow access to the Avaya Aura® Device Services resources from specific domains, in the **Specific Domain(s)** field, type the comma-delimited list of the domain names.

4. Click **Save**.

   Avaya Aura® Device Services saves the specified CORS configuration in the Cassandra database and in `/opt/Avaya/DeviceServices/<aads_version>/nginx/1.8.0-1/conf/cors-service.conf`. Avaya Aura® Device Services then reloads the Nginx configuration to apply CORS changes.

   For service interface, Avaya Aura® Device Services applies the CORS configuration for the root `/`.

Enabling Cross-origin resource sharing for the Administrator Interface

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **CORS Configuration** > **Admin Interface**.

   Avaya Aura® Device Services displays the Cross-Origin Resource Sharing for Admin interface page.

2. Select the **Enable Cross-Origin Resource Sharing** check box.

   Avaya Aura® Device Services displays the **Allow access from any origin** and **Specific Domain(s)** fields.

3. Do one of the following:
   - To allow access to the Avaya Aura® Device Services resources from any domain, select the **Allow access from any origin** check box.
   - To allow access to the Avaya Aura® Device Services resources from specific domains, in the **Specific Domain(s)** field, type the comma-delimited list of the domain names.
4. Click **Save**.

   Avaya Aura® Device Services saves the specified CORS configuration in the Cassandra database and in `/opt/Avaya/DeviceServices/<aads_version>/nginx/1.8.0-1/conf/cors-service.conf`. Avaya Aura® Device Services then reloads the Nginx configuration to apply CORS changes.

   Avaya Aura® Device Services applies the specified CORS configuration for the administrator interface to `/admin/webdeployment/upload URL`, for example, `https://<aads_server>:8445/admin/webdeployment/upload`.

Web Deployment service management

The Web Deployment service enables appcast for Avaya IX™ Workplace Client desktop applications. You can upload and download of the client installer and edit or delete appcast items. For more information about the Web Deployment service, see the sections under Web Deployment service management on page 131.

Chapter 4: Avaya Aura® Device Services OAuth2 management

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 multi-factor authentication. As of Release 8.0, you configure Avaya Aura® Device Services to support OAuth2, so that your enterprise users can log in to Avaya IX™ Workplace Client using SSO.

Before configuring OAuth2, ensure that you: understand core OAuth2 concepts and gathered all required information

- Understand core OAuth2 concepts.
- Gather information required for configuring OAuth2.

Related links

Prerequisites for OAuth2 configuration on page 45
Checklist for OAuth2 authentication configuration on page 47
Checklist for configuring Office 365 integration using SAML v2.0 on page 49
Checklist for configuring Office 365 integration using OAuth2 on page 54

Components to support OAuth2

Avaya Aura® Device Services OAuth2 involves the following key components:

- Avaya Aura® Device Services
- Keycloak
- External third-party identity provider

Avaya Aura® Device Services

Avaya Aura® Device Services implements an OAuth2 authorization code flow for Avaya IX™ Workplace Client. Avaya Aura® Device Services initiates the OAuth2 flow, but Avaya Aura® Device Services itself is not an identity provider. Therefore, Avaya Aura® Device Services relies on an embedded third-party component called Keycloak for token management and brokering to an external third-party identity provider.

Keycloak

Keycloak is a third-party open source component that implements a fully functional identity provider. Keycloak also supports federation and brokering to external third-party identity providers. Avaya Aura® Device Services supports the following Keycloak configurations:

- Direct integration with an enterprise directory.
- Brokering to an external third-party identity provider. Typically, this is your enterprise's identity provider.

For more information about Keycloak, see Keycloak documentation.

External third-party identity provider

An identity provider manages identification information and authenticates users.

When Keycloak is configured to broker to an external identity provider, the Avaya IX™ Workplace Client user is redirected to the identity provider's Login page. The user logs in directly with the identity provider, so the user's credentials are only exchanged with the identity provider and are never passed through Avaya Aura® Device Services. The following are additional benefits of brokering:

- The Avaya IX™ Workplace Client user logs in using a familiar Login screen, which is used by all other SSO-enabled applications.
- The identity provider can implement additional authentication requirements, such as multi-factor authentication.

Avaya Aura® Device Services supports the following identity providers:

- Shibboleth (SAML v2.0)
- Office 365 (SAML v2.0 and OAuth2)
- CA SiteMender (SAML v2.0)

Authentication flows

Request flow

When OAuth2 is enabled on Avaya Aura® Device Services, the following occurs:

1. The client's authentication request is forwarded to the embedded Keycloak service.
2. Keycloak forwards this request to the third-party identity provider, which prompts the Avaya IX™ Workplace Client user to log in.

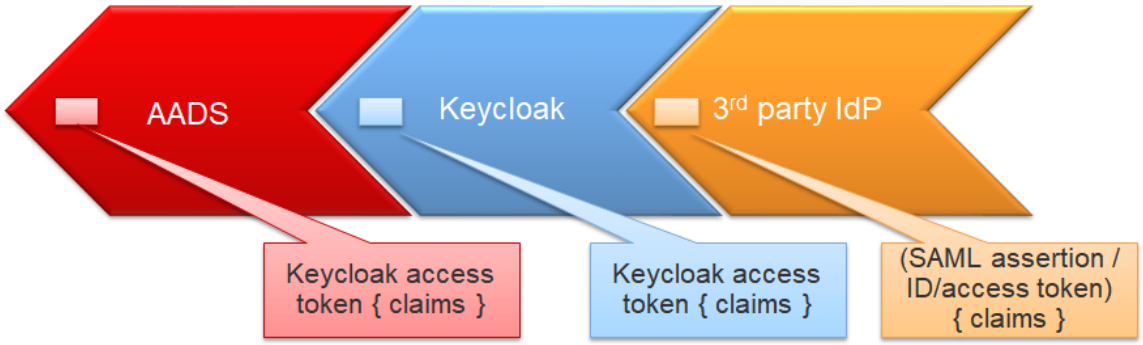
The following diagram illustrates this flow:

The third-party identity provider authenticates the Avaya IX™ Workplace Client user login credentials and notifies Keycloak whther the login was successful. Avaya Aura® Device Services only receives an OAuth2 token and returns it to the client.

Response flow

The third-party identity provider passes information about the authenticated user to Keycloak using a SAML assertion or the ID or access token. The exact method depends on how Keycloak is integrated with the identity provider.

The following diagram illustrates a response flow:



The SAML assertion or the ID token contains user authentication information, such as the first name, last name or email address. The identity provider determines which information the SAML assertion or token contain. In most cases, the identity provider takes this information from an enterprise directory source.

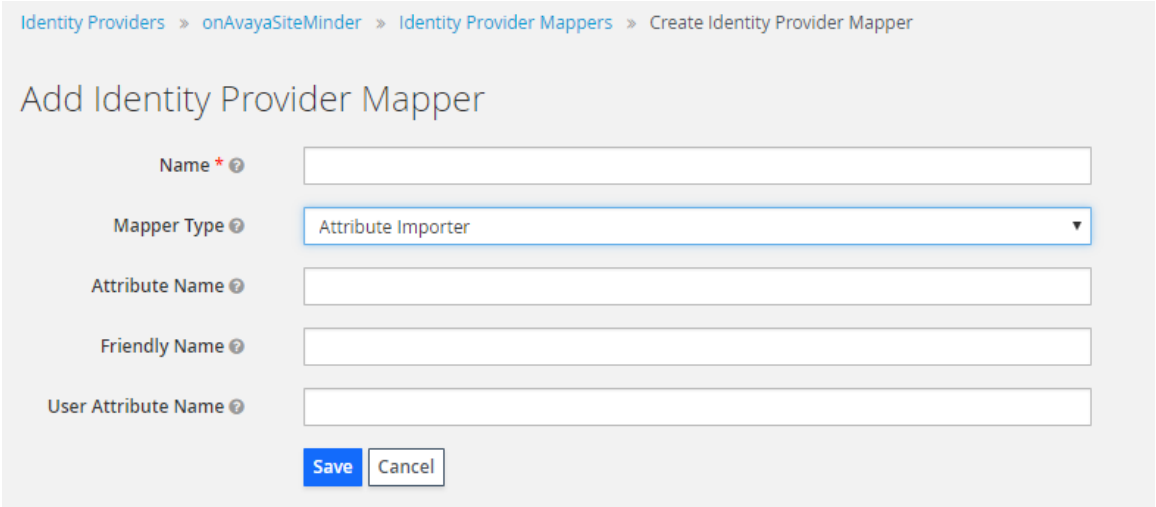
Note:

The SAML assertion or the ID token can contain custom attributes, such as “memberOf”, which contains the LDAP group name that Avaya Aura® Device Services associates with the user role. For information about configuring a third-party identity provider to include custom attributes to SAML assertions or ID tokens, see documentation for the specific identity provider.

Attribute mapping between Keycloak and a third-party identity provider

A third-party identity provider sends an authentication response to Keycloak. This response contains user attributes, such as first name, last name, phone number, or email address. To send these authentication data to Avaya IX™ Workplace Client in an access token, Keycloak maps the received user attributes to the attributes of the access token. You can use the Identity Provider Mapper in Keycloak to map attributes identity provider attributes to Keycloak attributes.

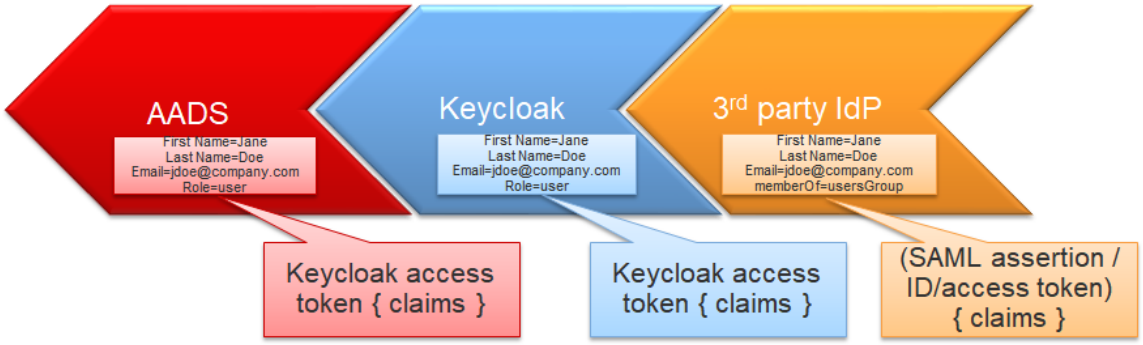
The following is an Identity Provider Mapper screen for a SAML v2.0 identity provider:



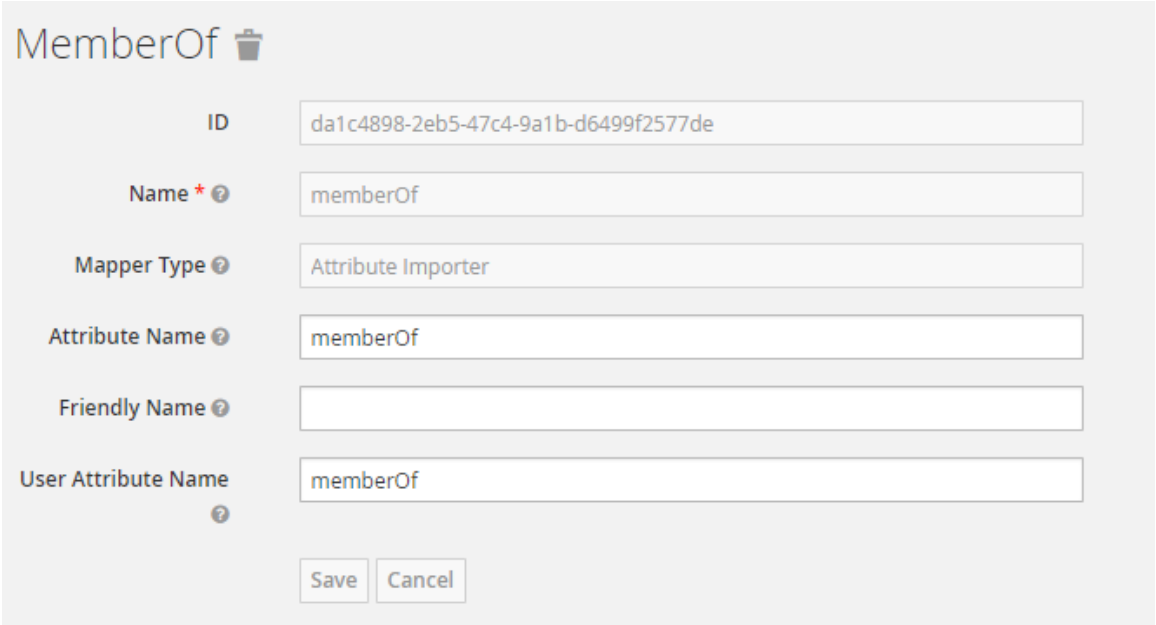
The **Attribute Name** or **Friendly Name** is the name of the attribute that Keycloak receives from the third-party provider. Keycloak uses an attribute defined in **User Attribute Name** to pass the value received from the identity provider to Avaya IX™ Workplace Client in access tokens.

For some attributes, direct mapping is not enough. Instead, you must map the attribute value received from the third-party provider and then transform it into a different value. The most common example is transforming a group value into a role.

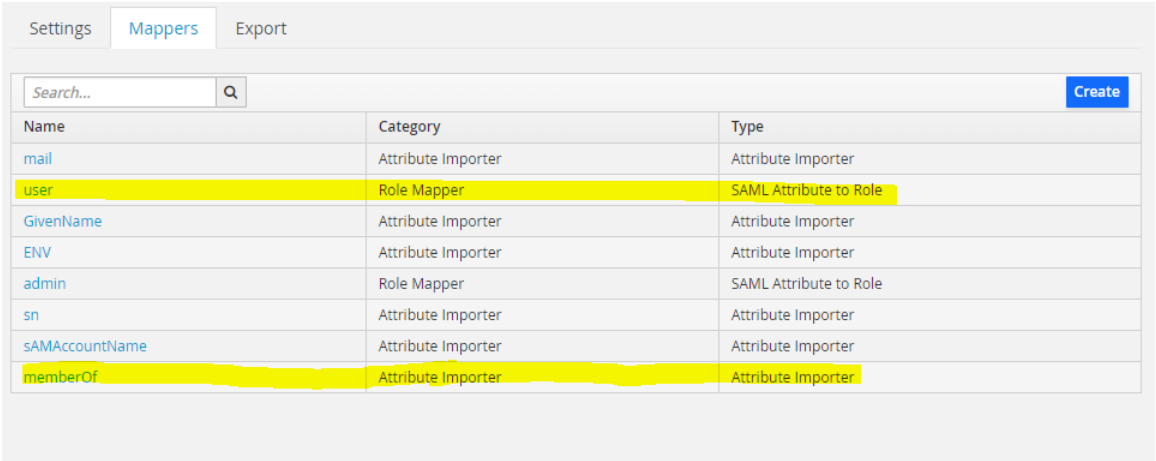
In the following example, the identity provider releases the “memberOf” attribute with the userGroup value.



First, Keycloak uses the Attribute Importer mapper to map this attribute to an attribute with the same name, “memberOf”.



Then Keycloak transforms this attribute into a role using the Role Mapper. The value of the "memberOf" attribute is mapped to the role, and Keycloak sends this role to Avaya IX™ Workplace Client. The following image shows the Identity Mapper configuration for this transformation:



Token authentication realm

Avaya Aura® Device Services OAuth2 access and refresh tokens, which are tied to a realm named "SolutionRealm" by default. Tokens that are received from Avaya Aura® Device Services can be used to access other solution elements that support the same authentication realm, such as Avaya Aura® Web Gateway and Presence Services.

Before enabling support for these tokens on other solution elements, ensure that:

- You imported the public key from the Avaya Aura® Device Services Client ID Mapping into other solution elements.
- You configured all solution elements that use Avaya Aura® Device Services for the “SolutionRealm”.

For more information, see documentation about client mapping configuration for the corresponding solution element.

Access and refresh token expiry times

At the end of the OAuth2 with SAML v2.0 redirect flow, Avaya Aura® Device Services returns an access and refresh token pair to Avaya IX™ Workplace Client, which uses the access token to access services on Avaya Aura® Device Services, such as contact operations or directory search. The same access token can also be used in the Unified Communication solution to access services provided by Avaya Aura® Web Gateway and Presence Services. Therefore, access tokens are as important as user name and password details.

All tokens have a configured expiry time. After the token expires, it cannot be used to access Avaya Aura® Device Services, Presence Services, or Avaya Aura® Web Gateway. Avaya recommends limiting the lifetime of access tokens for security purposes.

However, if the access token lifetime is too short, then Avaya IX™ Workplace Client will prompt the user to re-authenticate, which might affect user experience. To avoid that, the associated refresh token is provided to Avaya IX™ Workplace Client so that it can get a new access token without prompting the user to log in again. When the access token is refreshed using the refresh token, a new refresh token is provided and both the access and refresh tokens have their expiry times reset. Refresh tokens also have the expiry time, which is usually longer than the expiry time for access tokens.

You can use the following main settings on the Avaya Aura® Device Services Keycloak service to configure the expiration time of access and refresh tokens:

Setting	Description	Recommendations
Access Token Lifespan	Sets the expiry time for access tokens. If the access token is expired, the refresh token is used to get a new access token without prompting the Avaya IX™ Workplace Client user to re-authenticate.	Less than 1 hour.
SSO Session Idle	Sets the expiry time for refresh tokens. If the refresh token is not used by the expiry time, then the Avaya IX™ Workplace Client user needs to log in again to get new access and refresh tokens.	Several hours.

Setting	Description	Recommendations
SSO Session Max	Sets the overall maximum time period for refresh tokens. During this time, refresh tokens can be used to obtain new access tokens. If no server or network errors occur, Avaya IX™ Workplace Client will not have to log in again until the **SSO Session Max** time elapses.	The time period, which is defined by your password expiration policy. For example, if your set up user passwords to expire every 180 days, then set **SSO Session Max** to a value that is less or equal to 180 days. **Note:** Password expiration dates might be different for most users, therefore you can set SSO Session Max to a half of the password expiration period to ensure that users are required to re-authenticate with their new passwords.

For information about other parameters, see Keycloak documentation.

Important:

When configuring expiry times for refresh tokens, you must consider the following:

- The shorter the token lifetime, the more additional network traffic is generated.
- Very short token lifetimes causes Avaya IX™ Workplace Client to contact Avaya Aura® Device Services more often to refresh access tokens. On mobile clients, this might decrease the battery life.

Related links

Configuring access and refresh token expiry times on page 72

Prerequisites for OAuth2 configuration

Before configuring OAuth2 authentication on Avaya Aura® Device Services, gather the following information and configure an SSO application on the identity provider that you are planning to use:

SAML v2.0

- Determine the attribute names that the identity provider sends in SAML responses for the following:
  - First name
  - Last name
  - Email address
  - Group/Role indicator
- Configure the NameID format. Avaya Aura® Device Services uses the emailAddress format for NameID.

- Ensure that the identity provider supports the Service Provider-initiated (SP-initiated) flow and the SP-initiated flow is enabled and configured on the identity provider.
- Configure an SSO application on the third-party identity provider's side.
  - If you use Office 365 as an identity provider, configure an SSO application on the Microsoft Azure portal.
  - If you use other identity providers, such as Shibboleth, contact the identity provider administrator for information about configuring the Avaya Aura® Device Services as a new service provider application.
- Obtain the SAML v2.0 identity provider's IDPSSODescriptor metadata file.

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

  You must import this metadata file into Keycloak when enabling OAuth authentication support on Avaya Aura® Device Services or after Avaya Aura® Device Services is installed.
- Obtain the SPSSODescriptor metadata file.

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

  `https://<AADS FQDN>:<AADS PORT>/auth/realms/SolutionRealm/broker/<SAML V2 PROVIDER NAME>/endpoint/descriptor`

  For example, if the Avaya Aura® Device Services front-end FQDN is aads.company.com, the AADS front-end port is the default port 443, and you created on SAML v2.0 identity provider on Keycloak with the name mySAMLProvider, then the URL for retrieving the SPSSODescriptor file is:

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

OAuth2

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

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

Checklist for OAuth2 authentication configuration

The following checklist lists the OAuth2 configuration tasks that you can perform using the Keycloak web administration portal. Some tasks are mandatory and others are only relevant if you did not configure Keycloak using the configuration utility.

If you use Office 365 as an identity provider, see configuration checklists in Avaya Aura Device Services integration with Office 365 for OAuth2 authentication on page 49.

When possible, Avaya recommends using the Avaya Aura® Device Services configuration utility. For more information, see “OAuth configuration” in *Deploying Avaya Aura® Device Services*.

No.	Task	Notes	✔
1	Determine which identity provider you are using: • If you are using Office 365, continue with either Checklist for configuring Office 365 integration using OAuth2 on page 54 or Checklist for configuring Office 365 integration using SAML v2.0 on page 49, depending on the integration method you are planning to use. • If you are using other identity providers, such as Shibboleth, continue with this checklist.		
2	Ensure that you gathered all required information and configured an SSO application on your third-party identity provider.	See Prerequisites for OAuth2 configuration on page 45. Before configuring authentication settings on Keycloak, you must configure an SSO application on the identity provider’s side and obtain the IDPSSODescriptor file from the identity provider. For more information, contact your identity provider.	
3	Ensure that the realm is created.	The realm, which is called SolutionRealm by default, is typically created automatically when you configure Keycloak in the Avaya Aura® Device Services configuration utility. Verify this when you log in to the Keycloak web administration portal. If the realm was not created automatically, contact Avaya support. Ensure that the realm value is properly provisioned to Avaya IX™ Workplace	

No.	Task	Notes	✔
		Client soft phones and other UC servers configured to use the Authorization service. For more information, see Authorization realm configuration on UC servers and Avaya IX Workplace Client on page 60.	
4	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 61.	
5	Obtain the client secret.	See Obtaining the client secret on page 63. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
6	Create client mapping.	See Creating client mapping on page 63. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 64.	
7	Optional: Import a third-party identity provider.	See Importing a third-party identity provider on page 66. This task is only required if you did not import the identity provider using the Avaya Aura® Device Services configuration utility. If the third-party identity provider uses a certificate signed by a private CA, you must import the CA certificate chain for the identity provider to the default Java truststore. For more information, see Importing third-party identity provider private CA certificates on page 65.	
8	Optional: Select the OAuth identity provider to use for authorization.	See Selecting the default identity provider on page 67. This task is only required if you did not import an identity provider using the Avaya Aura® Device Services configuration utility.	
9	Optional: Modify the attribute mapping between the third-party identity provider and Keycloak.	Perform this task if the identity provider uses different attribute names than the ones in the default mapping. See Configuring the LDAP UID mapping on page 70.	

No.	Task	Notes	✔
10	Configure the LDAP UID mapping	See Configuring the LDAP UID mapping on page 70.	
11	Test the integration with the identity provider.	See Testing the integration with an identity provider from the Google Chrome web browser on page 71.	
12	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 72.	

Related links

Checklist for configuring Office 365 integration using SAML v2.0 on page 49
Checklist for configuring Office 365 integration using OAuth2 on page 54
Prerequisites for OAuth2 configuration on page 45

Avaya Aura® Device Services integration with Office 365 for OAuth2 authentication

If you use Office 365 in your deployment, you can configure SSO capabilities for authentication on Avaya IX™ Workplace Client. You can use one of the following methods to integrate with Office 365 for OAuth2 authentication and authorization:

- SAML v2.0
- OAuth2

Keycloak supports both these methods. However, the OAuth2 method might have limitations comparing to SAML v2.0. For example, integration with OAuth2 currently requires you to add the user role to all users that must authenticate using Office 365.

Integration with Office 365 using SAML v2.0

Checklist for configuring Office 365 integration using SAML v2.0

The following checklist lists the configuration tasks that you perform on the Microsoft Azure web portal and the Keycloak web administration portal to set up integration with Office 365 using SAML v2.0.

No.	Task	Notes	✔
1	Ensure that you gathered all required information for configuring integration.	See Prerequisites for OAuth2 configuration on page 45.	

No.	Task	Notes	✔
2	Create and configure an application for SSO on Microsoft Azure.	See Creating a new application and configuring SSO using SAML v2.0 on page 51.	
3	Set up ownership for the application.	See Assigning an owner to the application on page 52.	
4	Enable the application to read data from the Microsoft Azure Active Directory.	See Allowing the application to read Microsoft Azure directory data on page 52.	
5	Select Microsoft Azure Active Directory users and groups that can use SSO capabilities.	See Assigning users and groups to the application on page 53.	
6	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 61.	
7	Configure an Office 365 SAML v2.0 identity provider on Keycloak.	See Configuring an Office 365 SAML v2.0 identity provider on Keycloak on page 53.	
8	Configure attribute mapping between the Office 365 SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 67. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for Office 365 SAML v2.0 identity provider on page 70.	
9	Obtain the client secret.	See Obtaining the client secret on page 63. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
10	Create a client mapping.	See Creating client mapping on page 63. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 64.	
11	Configure the LDAP UID mapping	See Configuring the LDAP UID mapping on page 70.	
12	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 67.	
13	Test the integration with Office 365.	See Testing the integration with an identity provider from the Google Chrome web browser on page 71.	

No.	Task	Notes	✔
14	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 72.	

Related links

Checklist for OAuth2 authentication configuration on page 47
Prerequisites for OAuth2 configuration on page 45

Creating a new application and configuring SSO using SAML v2.0

About this task

Use this procedure to configure a new application for SSO on the Microsoft Azure portal.

When configuring the application, you obtain an identity provider alias and configuration file. You will need this data later when configuring an Office 365 SAML v2.0 identity provider on Keycloak.

Procedure

1. Log in to https://portal.azure.com as a cloud application administrator or as an administrator of a Microsoft Azure Active Directory tenant.
2. Navigate to **Azure Active Directory** > **Enterprise Applications**
3. On the Enterprise applications — All applications page, click **New application**.
4. In the Add an application section, click **Non-gallery application**.
5. In **Name**, provide a name for your application.
6. Click **add**.

   Microsoft Azure displays an Overview page for your application.
7. In the Getting Started section, click **Set up single sign on**.
8. In the Select a single sign-on method section, click **SAML**.

   Microsoft Azure displays the Single Sign-On with SAML — Preview page.
9. In the upper-right corner of the Basic SAML Configuration section, click ✎ to edit SAML configuration and update the following settings:
   a. In **Identifier**, enter `https://<AADS FQDN>/auth/realms/SolutionRealm`
   b. In **Reply URL**, enter `https://<AADS FQDN>/auth/realms/SolutionRealm/broker/<IDP alias>/endpoint`

   In these strings, `<AADS FQDN>` is the Avaya Aura® Device Services front-end FQDN. `<IDP alias>` is an identity provider alias of your choice. For example, `office365SAML`.
10. Remember the identity provider alias you used in the previous step.

    You will use this alias later when creating an Office 365 SAML v2.0 provider on Keycloak.
11. Click **Save**.

12. In the SAML Signing certificate section, click **Download** next to Federation Metadata XML to download an XML file with federation metadata.

    You will use this XML configuration file later when creating an Office 365 SAML v2.0 provider on Keycloak.

Assigning an owner to the application

About this task

After creating an SSO application, you must determine which Microsoft Azure administrative users can modify application settings.

Before you begin

Create an application for SSO. For more information, see Creating a new application and configuring SSO using SAML v2.0 on page 51.

Procedure

1. On Microsoft Azure, from **Enterprise Applications**, navigate to the application that you created.
2. In the Manage section on the left-hand side of the screen, click **Owners**.
3. Click **Add**.

   Microsoft Azure displays the list of administrators on the right.
4. Select the required administrator and then click **Select**.
5. Repeat the previous step if you need to select other administrators.

Allowing the application to read Microsoft Azure directory data

About this task

You must allow the SSO application you created to read data in your organization's directory. Users must consent to having their data read or you can grant administrative consent on behalf of all users.

Before you begin

Create an application for SSO as described in Creating a new application and configuring SSO using SAML v2.0 on page 51.

Procedure

1. On Microsoft Azure, from **App registration**, navigate to your SSO application.
2. To grant consent on behalf of all users in your organization's directory, do the following:
   a. In Configured permissions, click **Grant admin consent for <your admin name here>** to grant consent on behalf of all users in your organization's directory.
   b. In the Confirmation window, enter your administrator credentials to confirm changes.
3. In the Manage section on the left-hand side of the screen, click **API permissions**.
4. Click **Add a permission**.

5. In the Request API permission section, click **Azure Active Directory Graph**.

   Microsoft Azure displays the Permission Properties window.
6. Select **Delegated permissions**.
7. In the Select permissions area, click **Directory** and select the **Directory.Read.All** check box.
8. Click **Add permissions**.
9. **(Optional)** If Microsoft Azure prompts you to enter your administrator credentials, repeat step 2.

Assigning users and groups to the application

About this task

Use this procedure to select users or groups from your Microsoft Azure Active Directory that can use SSO to log in to Avaya IX™ Workplace Client.

Procedure

1. On Microsoft Azure, from **Enterprise Applications**, navigate to the SSO application that you created.
2. In the Manage section on the left-hand of the screen, click **Users and groups**.

   Microsoft Azure displays the list of users and groups in the Active Directory.
3. Click **Add user**.
4. On the Add Assignment page, click **Users and groups**.
5. Select one or more users or groups and then click **Select**.

Configuring an Office 365 SAML v2.0 identity provider on Keycloak

About this task

To use Office 365 SSO capabilties and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

- Copy the alias you used when creating a new SSO application on Microsoft Azure. For more information, see step 9 on page 51 in Creating a new application and configuring SSO using SAML v2.0 on page 51.
- Ensure that you have the Federation Metadata XML file. For more information, see 12 on page 52.
- If the identity provider uses a certificate signed by a private CA, you must import the CA certificate chain for the identity provider to the default Java truststore. For more information, see step Importing third-party identity provider private CA certificates on page 65.

Procedure

1. From the Keycloak web administration interface, click **Identity Provider**.

2. Click **Add provider** and then select **SAML v2.0**.

   Keycloak displays the Add identity provider page.

3. In **Alias**, enter the name that you used when configuring basic SAML settings for your SSO application on Microsoft Azure.

   For example, `office365SAML`. For more information, see step 9 on page 51.

4. Navigate to the Import External IDP Config section.

5. Click **Select file** next and then navigate to the Office 365 Federation Metadata XML file that is stored on your computer.

   Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.

6. Click **Save**.

Next steps

Configure attribute mapping between Keycloak and the Office 365 identity provider.

Integration with Office 365 using OAuth2

Checklist for configuring Office 365 integration using OAuth2

The following checklist lists the configuration tasks that you perform on the Microsoft Azure web portal and the Keycloak web administration portal to set up integration with Office 365 using OAuth2.

No.	Task	Notes	✔
1	Ensure that you gathered all required information for configuring integration.	See Prerequisites for OAuth2 configuration on page 45.	
2	Register an application for SSO purposes on Microsoft Azure.	See Registering an application for SSO purposes on page 55.	
3	Enable the application to read data from the Microsoft Azure Active Directory.	See Allowing the application to read Microsoft Azure directory data on page 52.	
4	Obtain the following application data: • Application ID • Application Client secret.	See Obtaining the application ID on page 56 and Obtaining the application client secret on page 56. You must have this data when you configure an identity provider on Keycloak.	
5	Configure an Office 365 OAuth2 identity provider on Keycloak.	See Adding an Office365 OAuth2 identity provider to Keycloak on page 57.	

No.	Task	Notes	✔
6	Set up the redirect URI for your application on Microsoft Azure.	See Setting up a redirect URI on your Microsoft Azure application on page 57	
7	Disable the identity provider redirector.	See Disabling the identity provider redirector on page 58.	
8	Add a hard-coded user role in Keycloak	See Adding a hard-coded user role in Keycloak on page 58.	
9	Optional: Configure attribute mapping between the Office 365 SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 67. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for Office 365 SAML v2.0 identity provider on page 70.	
10	Configure the LDAP UID mapping	See Configuring the LDAP UID mapping on page 70.	
11	Test the integration with Office 365.	See Testing the integration with an identity provider from the Google Chrome web browser on page 71.	
12	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 72.	

Related links

Checklist for OAuth2 authentication configuration on page 47
Prerequisites for OAuth2 configuration on page 45

Registering an application for SSO purposes

About this task

Register an application in Microsoft Azure. When configuring this application, you obtain data that are required to configure the Office 365 identity provider on Keycloak to enable your enterprise users to log in to Avaya IX™ Workplace Client with Office 365 credentials.

Before you begin

Ensure that you have an Office 365 account with privileges for creating applications.

Procedure

1. Log in to https://portal.azure.com as an Office 365 administrator.
2. Navigate to **Azure Active Directory** > **App registrations**.

   Microsoft Azure displays the App registrations page.
3. At the top of the page, click **New registration**.

Microsoft Azure displays the Register an application page.

4. In **Name**, provide a name for the application.

   For example, `AADS`.

5. In **Supported account type**, select **Accounts in any organizational directory (Any Azure AD directory — Multitenant)**.
6. Ensure that **Redirect URI** is blank.
7. Click **Register**.

   Microsoft Azure displays the Overview page for your application.

Obtaining the application ID

About this task

Use this procedure to obtain the ID for the application you registered on Microsoft Azure. Avaya Aura® Device Services uses this application ID when adding a new identity provider.

Before you begin

Register an application on Microsoft Azure as described in Registering an application for SSO purposes on page 55.

Procedure

1. On Microsoft Azure, navigate to **Azure Active Directory** > **App registrations**.
2. Navigate to your application.
3. On the Overview page, click the **Copy** icon next to the **Application ID** field and save it in a safe location.

Obtaining the application client secret

About this task

When obtaining authentication tokens, Avaya Aura® Device Services uses a client secret to authenticate with Microsoft Azure Active Directory. You will use the client secret when configuring an identity provider on Avaya Aura® Device Services Keycloak. Use this procedure to generate and obtain a client secret for your SSO application on Microsoft Azure.

Important:

You must copy and save a client secret immediately after creating it. You *cannot* see the secret again after you leave the Client secret configuration page.

Before you begin

Register an application on Microsoft Azure as described in Registering an application for SSO purposes on page 55.

Procedure

1. On Microsoft Azure, navigate to **Azure Active Directory** > **App registrations**.
2. Navigate to your application.

3. In the Manage area, click **Certificates & secrets**.
4. In the Client secrets area, click **New client secret**.
5. Provide a description for the client secret.
6. Select the expiration time for the client secret.
7. Click **Add**.

   Microsoft Azure generates a new client secret.
8. Click **Copy** next to the client secret and save it in a safe location before leaving the page.

Adding an Office365 OAuth2 identity provider to Keycloak

About this task

To use SSO capabilities and authenticate users using Office365, you must configure the Office365 identity provider on Keycloak.

When you create an Office 365 identity provider, Keycloak automatically generates a redirect URI. Your Microsoft Azure application sends authentication tokens to this URI.

Before you begin

Obtain the application ID and client secret for the application you registered on Microsoft Azure.

Procedure

1. On the Keycloak web administration interface, navigate to **Identity Providers**.
2. Click **Add provider** and select **Microsoft**.

   Keycloak displays the Add identity provider page.
3. In **Client ID**, enter the application ID you copied from your Microsoft Azure application.
4. In **Client Secret**, enter the client secret you copied from your Microsoft Azure application.
5. Copy the **Redirect URI** value to a safe location, which you can access later.
6. Click **Save** to create the identity provider.

Setting up a redirect URI on your Microsoft Azure application

About this task

To send auth tokens to Keycloak, Microsoft Azure Active Directory uses a redirect URI configured on your Microsoft Azure application. Keycloak automatically generates this URI when you configure the Office 365 identity provider. Use this procedure to enter this URI on your Microsoft Azure application.

Before you begin

Obtain the redirect URI generated for the Office 365 identity provider on Keycloak. For more information, see Adding an Office365 OAuth2 identity provider to Keycloak on page 57.

Procedure

1. On Microsoft Azure, navigate to **Azure Active Directory** > **App registrations**.

2. Navigate to your application.
3. In the Manage area, click **Authentication**.
4. In the Redirect URIs section, in **Type**, select **Web**.
5. In **Redirect URI**, enter the redirect URI you copied from Keycloak.
6. Click **Save**.

Disabling the identity provider redirector

About this task

When you configure Office 365 integration for authentication purposes using OAuth2, the identity provider redirector must be disabled on Keycloak.

Procedure

1. On the Keycloak web administration portal, in the left pane, click **Authentication**.
2. On the Flows tab, click the drop-down field and select **Browser**.
3. For **Identity Provider Redirector**, select **Disabled**.

Adding a hard-coded user role in Keycloak

About this task

Authentication tokens generated by Keycloak must contain role information to enable Avaya IX™ Workplace Client to use SSO capabilities. In Avaya Aura® Device Services deployments that do not use the Enterprise SSO capability, the user role is assigned to users that belong to the LDAP group configured as the user role. Avaya Aura® Device Services does not restrict access to users that do not belong to the user group. Therefore, you can add a hard-coded user role to the Keycloak configuration for OAuth2 identity providers that cannot provide group membership information. In this case, Keycloak assigns this hard-coded user role to all users that successfully authenticate with the OAuth2 identity provider.

If you configured integration with Office 365 using OAuth2, you cannot use the Keycloak web administration portal to create attribute mappings from the OAuth2 token to a role. You can only use the “Hardcoded Role” mapper type.

Procedure

1. Log in to the Keycloak web administration interface.

   For more information, see Logging in to the Keycloak web administration portal on page 59.
2. On the Keycloak web administration interface, navigate to your Office 365 OAuth2 identity provider.
3. Click the **Mappers** tab.
4. Click **Create**.

   Keycloak displays the Add Identity Provider Mapper page.
5. In **Name**, provide a name for the mapper.

For example: `user.groups`

6. From **Mapper Type**, select **Hardcoded Role**.
7. Click **Select Role**.

   Keycloak displays the Role Selector page.
8. From the **Client Roles** drop-down list, select **aads**.
9. In the area below the **Client Roles** drop-down list, select **user**.
10. Click **Select client role**.
11. On the Add Identity Provider Mapper page, click **Save**.

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.

For more information about installation and initial configuration, see *Deploying Avaya Aura® Device Services*.

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.

   For more information, see “Configuring Keycloak settings” in *Deploying Avaya Aura® Device Services*.

Changing your Keycloak password

About this task

From the Avaya Aura® Device Services configuration utility, you can change the password that you use to access the Keycloak web administration portal.

Procedure

1. Log in to the Avaya Aura® Device Services seed node as an administrator.

   For more information, see Upgrading ESXi or AWS virtual machines on page 241
2. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
3. Select **Keycloak Configuration**.
4. In **Keycloak Admin user**, type the user name of the Keycloak administrator for which you want to change the password.
5. In **Keycloak Admin user's password**, type a new password.
6. In **Update Keycloak Admin user's password**, type `y`.
7. In **Keycloak Admin user's current password**, type the current password.
8. In **Keycloak Admin user's new password**, re-type the new password.
9. Confirm your new password.
10. Select **Apply**.
11. Select **Continue**.

Authorization realm configuration on UC servers and Avaya IX™ Workplace Client

When OAuth is enabled on Avaya Aura® Device Services, you must provision the following parameters for all Avaya IX™ Workplace Client soft phones 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 IX™ Workplace Client use Avaya Authorization for Avaya Aura® Device Services.

- ESMSSO: Set the value to `3`, so that Avaya IX™ Workplace Client use Avaya Authorization for Presence and Multimedia Messaging.
- AUTOCONFIG_USE_SSO: Set the value to `3` so that Avaya IX™ Workplace Client 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.

Before you begin

- Install Avaya Aura® Device Services.
- Ensure that you gather all information and configured an SSO application on the third-party identity provider. For more information, see Prerequisites for OAuth2 configuration on page 45.
- Obtain the IPDSSODescriptor configuration file in the XML format from the third-party identity provider.

  For example, for the Shibboleth identity provider, 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.

   Important:

   After setting the password, you *cannot* change it using the configuration utility.

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 IPDSSODescriptor configuration file that you uploaded to Avaya Aura® Device Services.
   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

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.

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 63.

Creating client mapping

About this task

In the authorization flow, Avaya Aura® Device Services interacts with Keycloak on behalf of Avaya IX™ Workplace Client. 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 63.

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**.

Regenerating the Keycloak client secret

About this task

Use this procedure if you need to regenerate a new Keycloak client secret. For example, this is useful if your company requires you to change your password periodically.

Procedure

1. On the Keycloak web administration interface, navigate to your realm and then click **Clients**.

   The default realm created by Avaya Aura® Device Services is “SolutionRealm”.

2. From the Clients table, select **aads**.
3. Click the **Credentials** tab.
4. Click **Regenerate Secret**.

Next steps

Update the identity provider to client mapping.

Related links

Updating the identity provider mapping on page 64

Updating the identity provider mapping

About this task

Use this procedure to review or edit identity provider mapping settings. You must update the mapping after regenerating the Keycloak client secret.

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. Select a client mapping configuration.
4. Click **Edit**.
5. Update the fields as required.
6. Click **OK**.

Importing third-party identity provider private CA certificates

About this task

If you integrate Avaya Aura® Device Services with a third-party identity provider that is using a private CA, you must import the private CA certificates into the Java truststore. This allows you to import the third-party identity provider configuration XML file directly from the identity provider.

In cluster deployments, perform this procedure on the seed node first and then on all non-seed nodes.

If you redeploy the virtual machines, you must perform this procedure again.

Before you begin

Obtain the root and, if required, intermediate CA certificates in PEM format for the CA that signs the provider's identity certificate.

Procedure

1. Transfer the CA certificates to the Avaya Aura® Device Services node using a file transfer program, such as SFTP or SCP.
2. Log in to the Avaya Aura® Device Services node using an SSH connection.
3. Navigate to `/etc/pki/java`.
4. Run the following command to import the root certificate into the truststore:

   ```
   sudo keytool -importcert -keystore ./cacerts -alias idpca -file <PATH>
   ```

   In this command, `<PATH>` is the full path to the CA certificate in PEM format.

   Note:

   The keystore password is `changeit`.
5. Repeat the previous step for all required intermediate CA certificates.

Importing a third-party identity provider

About this task

To use SSO capabilties and authenticate users, you must import a third-party identity provider. Avaya Aura® Device Services currently only supports the Shibboleth SAML v2.0 identity provider.

Use this procedure if you want to import the provider using the Keycloak web administration portal. You can also import a third-party identity provider using the Avaya Aura® Device Services configuration utility as described in *Deploying Avaya Aura® Device Services*.

Before you begin

- Obtain the identity provider configuration file in XML format from the provider.
- If the identity provider uses a certificate signed by a private CA, you must import the CA certificate chain for the identity provider to the default Java truststore. For more information, see Importing third-party identity provider private CA certificates on page 65.

Procedure

1. On the Keycloak web administration interface, navigate to your realm and then click **Identity Providers**.
2. Click **Add provider** and then select **SAML v2.0**.
3. In the **Alias** field, enter a name of your choice.

   For example: `Shibboleth`

   Other fields are optional.
4. To import configuration data from the identity provider configuration file, do one of the following:
   - To upload the configuration file downloaded from the provider, click **Select file** and then select the configuration file that is stored on your computer.
   - To upload the configuration file directly from the provider, in the **Import from URL**, enter the configuration file URL.

     For example, for Shibboleth, the URL is `https://<shibboleth site address>:<port>/idp/shibboleth`

   Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.
5. Click **Save**.

Next steps

Select the OAuth identity provider.

Related links

Selecting the default identity provider on page 67

Selecting the default identity provider

About this task

If you have multiple identity providers configured, you can select which identity provider you want to use for authorization. Ohterwise, Keycloak will prompt Avaya IX™ Workplace Client users to select an identity provider to authenticate.

If you have a single identity provider configured, use this procedure if you configured the provider using the Keycloak web administration portal. If you configured the identity provider using the configuration utility, the provider is already selected.

Before you begin

Configure the required identity provider.

Procedure

1. On the Keycloak web administration portal, navigate to your realm and then click **Authentication**.
2. Click the **Flows** tab.
3. From the drop-down list, select **Browser**.
4. In the Identity Provider Redirector row, click **Actions** and then select **Config**.

   Avaya Aura® Device Services displays the Create authenticator configuration window.
5. In the **Alias** field, enter a name of your choice.

   For example: `Shibboleth`.
6. In the **Default Identity Provider**, enter the alias of the configured identity provider for OAuth.

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

About this task

To authenticate a user, a third-party identity provider sends to Keycloak an authentication response that contains various user attributes, such as first name, last name, phone number, and email address. Keycloak then maps this user information to the attributes of the access token that is generated and sent back to clients.

The Avaya Aura® Device Services configuration utility provides a default attribute mapping. The identity provider you are using, however, might use attribute names that differ from the attribute names provided in the default mapping. In this case, you must update the default mapping. Use this procedure to modify the default attribute mapping.

If you are configuring attribute mapping for the Office 365 SAML v2.0 identity provider, you must configure the mappers listed in Attribute mapping parameters for Office 365 SAML v2.0 identity provider on page 70.

Before you begin

Configure a third-party identity provider on Keycloak.

Procedure

1. On the Keycloak web administration portal, navigate to your realm and then click **Identity Providers**.
2. Select the identity provider.
3. Click **Mappers**.
4. From the table, select an appropriate attribute.

   Avaya Aura® Device Services displays the attribute mapping for the selected attribute.

   - The **Friendly Name** field contains the attribute name that the identity provider passes to Keycloak.

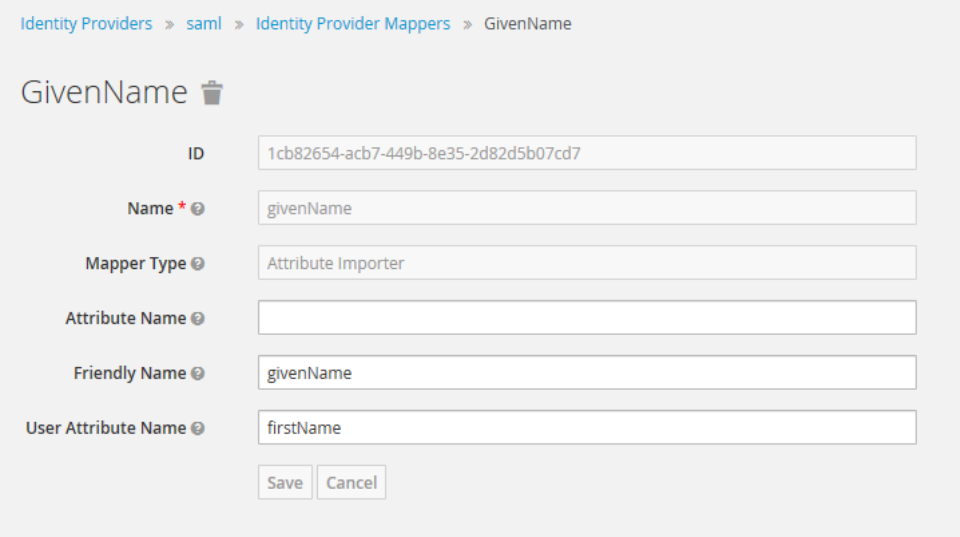
     If the identity provider does not provide a value for the **Friendly Name** field, use the **Attribute Name** field instead.
   - The **User Attribute Name** field contains the attribute name that Keycloak passes to clients in access tokens.

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

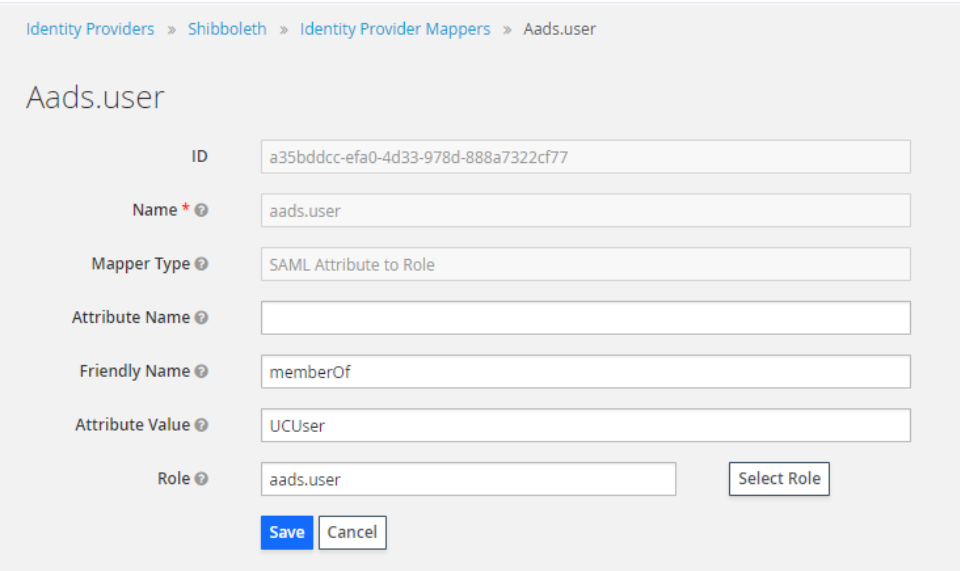
     - Given name: `givenName`.
     - Last name: `lastName`.
     - Email address: `email`

     These values are case sensitive.

   The following image shows the givenName attribute.



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**.



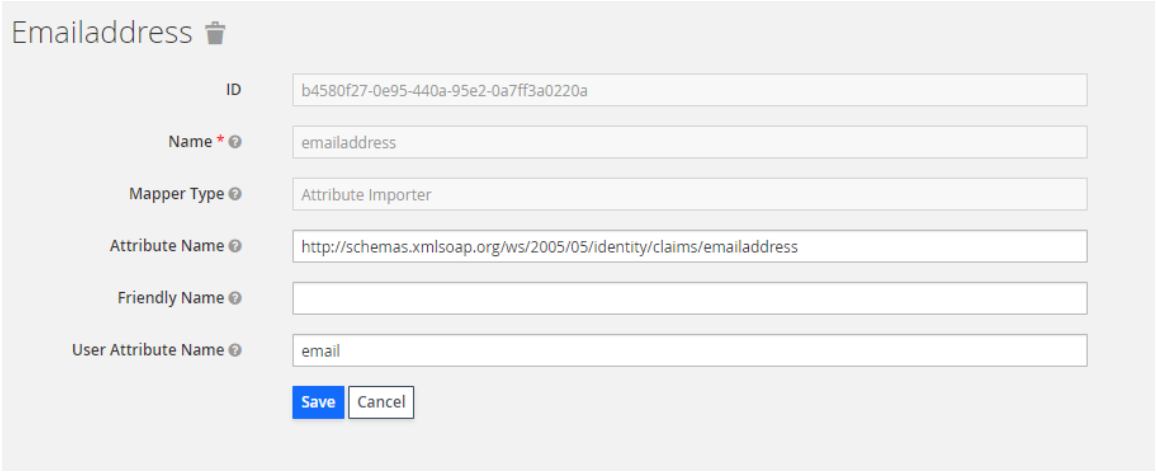
7. Click **Save**.
8. Repeat the above steps for any other attributes you need to map.

Attribute mapping parameters for Office 365 SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using Office 365 SAML v2.0 identity provider:

Mapper name	Mapper type	Attribute name	User Attribute Name	Role
user.groups	Hardcoded Role	—	—	aads.user
givenname	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	firstName	—
surname	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	lastName	—
emailaddress	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email	—

The following image shows the emailaddress mapper configuration:



Configuring the LDAP UID mapping

About this task

When configuring OAuth2, you must ensure that the value of the UID mapping attribute set for each LDAP server is equal to the value of **Access token email address attribute**, which is provided in the identity provider mapping.

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 **Edit**.

   Avaya Aura® Device Services displays the identity provider mapping settings.
4. Record the **Access token email address attribute** value.
5. Click **Cancel**.
6. Navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
7. Click the appropriate LDAP server.
8. In **UID Attribute ID**, enter the recorded value.
9. If additional LDAP servers are configured on Avaya Aura® Device Services, repeat steps 7 to 8 for each LDAP server.

Testing the integration with an identity provider from the Google Chrome web browser

About this task

Use this procedure to verify that the integration with an identity provider using OAuth2 is configured correctly. Use the Google Chrome web browser for this procedure.

Important:

For testing purposes, you will disable the web security of the Chrome browser when performing the procedure. After performing this procedure, you *must* close this browser instance and then restart the browser.

Before you begin

You must have an Avaya IX™ Workplace Client user account.

Procedure

1. Do the following to run the Google Chrome web browser with web security disabled:
   a. Use the CLI to navigate to the Chrome web browser executable file location.

      For example: `cd "\Program Files (x86)\Google\Chrome\Application"`
   b. Run the following command:

      ```
      chrome --disable-web-security --user-data-dir=%TMP%
      ```
2. In the browser address bar, enter the following URL:

```
https://<AADS FQDN>:<AADS PORT>/acs/resources/authorize?
client_id=Equinox&app_cb_uri=https://<AADS FQDN>:<AADS PORT>/
```

In this address, <AADS FQND> is the Avaya Aura® Device Services front-end FQDN and <AADS PORT> is the Avaya Aura® Device Services front-end service port.

3. If more than one identity provider is configured on Keycloak, on the Login page, click the identity provider you want to test.

   For example, if you want to test the integration with Office 365, click **Microsoft**.

4. If you are logging in for the first time, on the Permissions page, click **Accept**.
5. Enter your Avaya IX™ Workplace Client credentials.

   If the authentication process completes successfully, Chrome displays a JSON response containing information about an access token and a refresh token. The following is an example of the response:

```
{
  "access_token":"<access token value>,
  "expires_in":1800,
  "refresh_expires_in":3600,
  "refresh_token":<refresh token value>,
  "token_type":"bearer",
  "not-before-policy":0,
  "session_state":<session state value>,
  "scope":"profile pmm aads email"
}
```

6. Close the web browser instance.

Configuring access and refresh token expiry times

About this task

The access token lifetime determines the time period during which Avaya IX™ Workplace Client does not prompt the user to re-authenticate. Refresh tokens are used to refresh the access token lifetime. You can use the Keycloak service to configure the lifetime for access and refresh tokens. The main settings are the following:

- **Access Token Lifespan**: Sets the expiry time for access tokens.
- **SSO Session Idle**: Sets the expiry time for refresh tokens. If the refresh token is not used by the expiry time, then the Avaya IX™ Workplace Client user needs to log in again to get new access and refresh tokens.
- **SSO Session Max**: Sets the overall maximum time period for refresh tokens. During this time, refresh tokens can be used to obtain new access tokens.

The choice of a lifespan for tokens is a trade-off between security and user experience impact:

- If the token lifespan is too long, it increases the opportunity for a malicious actor to capture the tokens.
- If the token lifespan is too short, Avaya IX™ Workplace Client frequently prompts users to log in again.

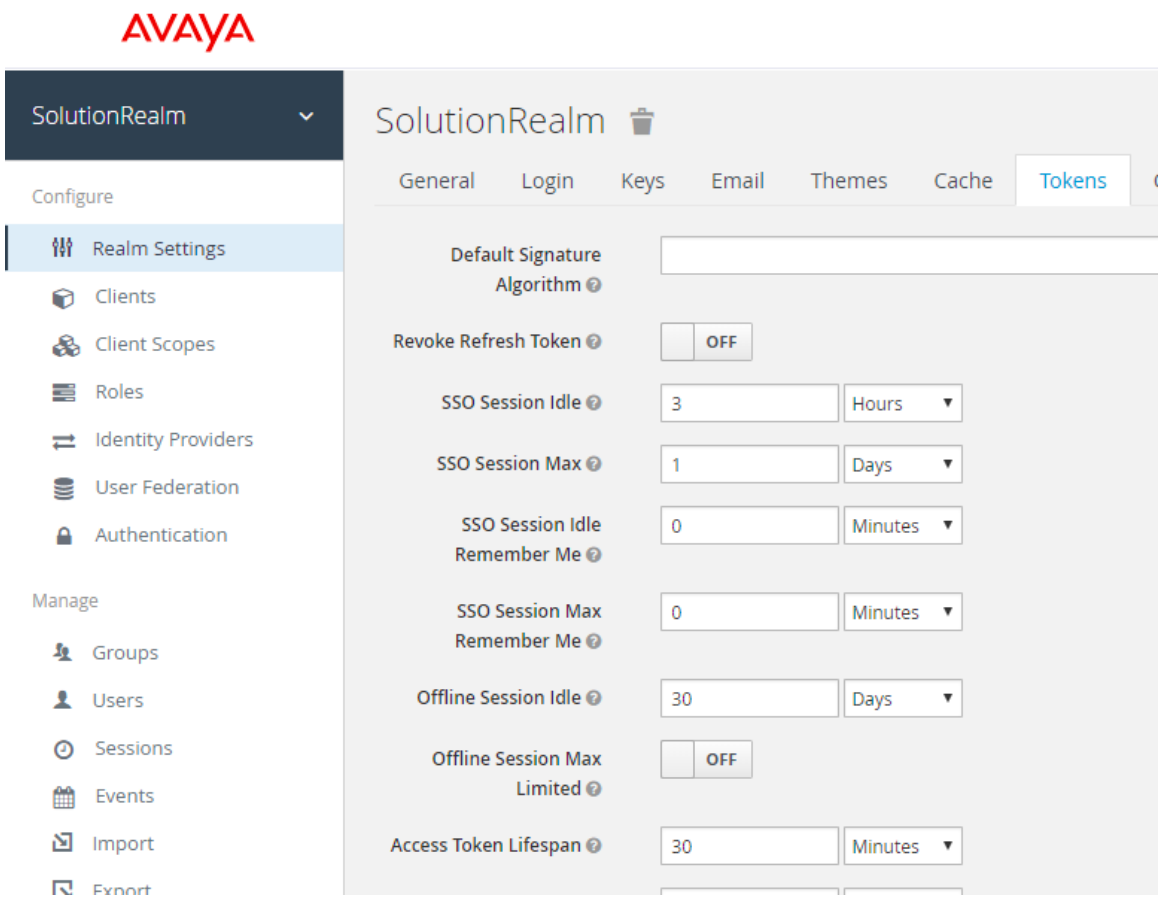
For more information and recommendations, see Access and refresh token expiry times on page 44.

Procedure

1. On the Keycloak web administration portal, navigate to **SolutionRealm** and then click **Realm Settings**.
2. In the right area, click **Tokens**.
3. Configure the expiry time for the following settings:
   - **SSO Session Idle**
   - **SSO Session Max**
   - **Access Token Lifespan**
4. Click **Save**.

Example

The following is an example of expiry times configuration:



Related links

Access and refresh token expiry times on page 44

Blocking access to the Avaya Authorization service

About this task

Use this procedure if you need to prevent a previously logged in user from logging in to Avaya Aura® Device Services using the third-party identity provider.

Procedure

1. On the Keycloak web administration interface, navigate to your realm and then click **Users**.
2. In the **Search** field, enter the user name and then click  .

   Avaya Aura® Device Services displays the list of users.
3. Click the **Edit** button located to the right of the required user name.

   Avaya Aura® Device Services displays the user profile page.
4. On the Details tab, set **User Enabled** to **OFF**.
5. Click **Save**.

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

Procedure

Perform steps 1 to 6 on the seed node first and then on all non-seed nodes.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the configuration utility using the `app configure` command.
3. Select **Enable OAuth Cluster**.
4. Select **Enable OAuth Cluster** again and then enter `y`.
5. Select **Exit**.
6. Select **Yes** and then select **Apply**.

7. On the seed node, run the `svc aads restart` command to restart Avaya Aura® Device Services and then wait until the restart process is completed.
8. On all non-seed nodes, run the `svc aads restart` command to restart Avaya Aura® Device Services.

Keycloak log management

Avaya Aura® Device Services collects Keycloak logs along with other system logs.

You can set the required detail level and collect Keycloak logs from the Log Management section of the Avaya Aura® Device Services web administration portal. For more information, see Changing a logging level on page 205 and Downloading logs on page 206.

Chapter 5: Avaya Spaces integration

Avaya Spaces is a cloud-based team collaboration and meeting platform. Avaya Spaces integrates multiple forms of communication, such as voice, video, instant messaging, and screen-sharing, into a single application that can be used on different platforms.

Using the Avaya Aura® Device Services web administration portal, you can:

- Create and register users in your enterprise on Avaya Spaces. These users do not need to perform the user self-registration sign-up process.
- Allocate licenses to users without having to wait until they log in to Avaya Spaces. You can use the Avaya Aura® Device Services web administration portal as a single administration point for managing Avaya Spaces licenses.

Checklist for configuring Avaya Spaces integration

Use this checklist to configure integration with Avaya Spaces.

No.	Task	Notes	✔
1	Set up an Avaya Spaces account.	See Avaya Spaces account configuration on page 77. Skip this step if you already have an Avaya Spaces account and you configured your company on Avaya Spaces.	
2	Obtain an Avaya Aura® Device Services API key and API key secret for your company on Avaya Spaces.	See Obtaining an API key and API key secret on page 79.	
3	Configure Avaya Spaces settings on Avaya Aura® Device Services.	See Setting up Avaya Spaces integration on page 79.	
4	Manage Avaya Spaces users and licenses.	See User and license management overview on page 84.	

Avaya Spaces account configuration

To manage Avaya Spaces users on Avaya Aura® Device Services, you must create and configure an Avaya Spaces account. This account stores the parameters required to authorize your Avaya Aura® Device Services system on Avaya Spaces.

Use the following sections to create and configure your Avaya Spaces account.

Registering an Avaya Spaces account

About this task

Use this procedure to register an Avaya Spaces account using your email address.

Procedure

1. In your web browser, enter https://accounts.avayacloud.com/.
2. In the **Email or Phone** field, type your email address.
3. Click **Yes, sign me up!**.

   Avaya Spaces sends a confirmation email to the email address you specified.
4. In your mailbox, open the confirmation email and then click the **Confirm** button.

   You are redirected to the Avaya Spaces My Account page.
5. Provide your first name, last name, password, and, optionally, a photo.
6. Click **Create an account**.

Setting up a company and domain in Avaya Spaces

About this task

You must provide the company domain associated with your Avaya Aura® Device Services system.

For more information, see the Configuring a company in *Avaya Spaces User Manual*.

Procedure

1. Log in to https://accounts.avayacloud.com/ as an administrator.
2. If you have not set up your company or want to configure a new company, do the following:
   a. Click on your user name in the top-right area of the screen and then click **Add Company**.
   b. Type a name and description for your company.
   c. Click **Save**.
3. Click **Manage Companies** and click the existing company name.

4. Click the **Domains** tab.
5. Click **Add Domain**.
6. Enter the domain name and then click **OK**.
7. To verify ownership of the domain, next to the domain name, click **Verify**.
8. Do one of the following:
   - Follow the on-screen instructions to add the verification code to your domain account and then click **Verify**.
   - At the bottom-right area of the Verify Domain window, click **Manual Verify** to have Avaya personnel verify the ownership of the domain.

Related links

Obtaining an API key and API key secret on page 79
Disabling Avaya Spaces integration on page 100

Creating an API key

About this task

To access Avaya Spaces services, you must create an API key for your company and then provide this key and associated API key secret on Avaya Aura® Device Services. An API key secret is created automatically when you create an API key.

Procedure

1. Log in to Avaya Spaces at https://accounts.avayacloud.com/ as an administrator.
2. In the left pane, click **Manage Companies**.
3. Select your company from the list.
4. Click the **API Key** tab.
5. Click **Add API key +**.
6. In the Add API key window, select **AADS** from the drop-down list and then click **Add API key**.

   You can also type `AADS` in the search field. Avaya Spaces only displays entries that contain the text you entered.

   Avaya Spaces displays the new key in the API Keys table.

Obtaining an API key and API key secret

About this task

Each company that is registered on Avaya Spaces has an associated API key and key secret. Avaya Aura® Device Services requires these values to access Avaya Spaces services.

Before you begin

- Ensure that your company and domain are configured in Avaya Spaces.
- Ensure that at least one API key with the “AADS” role is configured for your company in Avaya Spaces.

Procedure

1. Log in to Avaya Spaces at https://accounts.avayacloud.com/ as an administrator.
2. In the left pane, click **Manage Companies**.
3. Select your company from the list.
4. Click the **API Key** tab.
5. From the API Keys table, copy the API key with the “AADS” role that you want to use and save it on your computer.
6. In the API Keys table, click **View/Edit** for the API key you copied.
7. In the Secret area, click to copy the API key secret to the clipboard and save it on your computer.

Setting up Avaya Spaces integration

About this task

You can set up integration with a specific company configured on your Avaya Spaces account. When integration is set up, you can use the Avaya Aura® Device Services web administration portal to view and manage users for that company.

You can have multiple companies configured on your Avaya Spaces account. However, Avaya Aura® Device Services only supports integration with one company at a time. If you want to set up integration for another company, you must delete the existing configuration first.

Note:

As of Release 8.0.2, Avaya Aura® Device Services contains all required Avaya Spaces CA certificates in a separate public CA truststore, so you do not need to import these certificates manually.

Before you begin

- Obtain the API key and API key secret for the Avaya Spaces company that you are planning to use for integration.

- Ensure that you have at least one verified domain for the company.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Configuration**.
2. Select the **Enable Spaces Integration** check box.
3. In **Spaces URI**, enter `accounts.avayacloud.com`.

   If required, you can provide a new value later without having to set up integration again.
4. In **Spaces API Key**, enter the API key that you copied from Avaya Spaces.
5. In **Spaces API Key secret**, enter the API key secret that you copied from Avaya Spaces.
6. Click **Save**.

Result

When the integration process is completed, Avaya Aura® Device Services notifies you and automatically populates the following fields:

- **Company Name**: Shows the name of the Avaya Spaces company for which you are setting up integration.
- **Domain**: Shows all verified domain names configured for the company in Avaya Spaces.
- **Status**: Shows the connection status.
- **License Information**: Shows information about the available advanced licenses and license expiration dates.

Next steps

- Configure data synchronization between Avaya Aura® Device Services and Avaya Spaces.
- Update language and time zone databases.

Related links

Setting up a company and domain in Avaya Spaces on page 77
Obtaining an API key and API key secret on page 79
Disabling Avaya Spaces integration on page 100
Updating Avaya Spaces integration parameters on page 99
Avaya Spaces integration settings on page 100
Avaya Aura Device Services does not contain the latest Avaya Spaces CA certificate on page 280

Configuring data synchronization between Avaya Aura® Device Services and Avaya Spaces

About this task

Use this procedure to synchronize user data, licensing, and company domain information between Avaya Aura® Device Services and Avaya Spaces. You can configure automatic synchronization on a scheduled date or at a specific time interval. You can also synchronize user data manually.

When synchronization is enabled, Avaya Aura® Device Services synchronizes user data in the following cases:

- When you synchronize data manually.
- During scheduled synchronization events.

If Avaya Aura® Device Services cannot synchronize data, it displays an error message on the Configuration page. If synchronization fails because of a connection issue, Avaya Aura® Device Services also raises an alarm.

If synchronization is disabled, Avaya Aura® Device Services only stores Avaya Spaces configuration data.

Before you begin

Enable Avaya Spaces integration.

Procedure

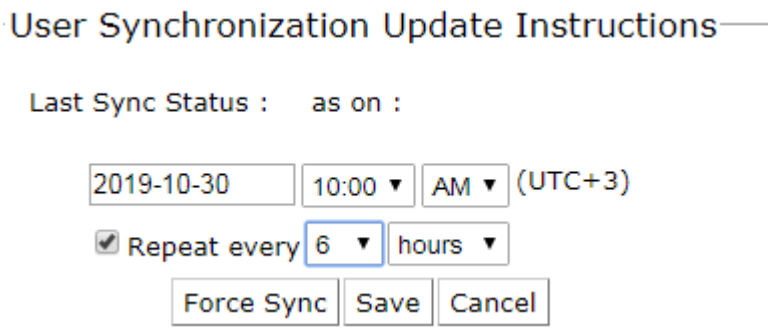
1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Configuration**.
2. Select the **Enable user license synchronization** check box.
3. In the IX Spaces Configuration area, click **Save**.
4. In the User Synchronization Update Instructions area, specify the date and time when you want to synchronize user data.
5. To configure scheduled synchronization, select the **Repeat every** check box and then specify the period between consecutive synchronization attempts.

   Scheduled synchronization starts from the time and date that you specified in the previous step.
6. **(Optional)** To immediately synchronize user data, click **Force Sync**.

   Immediate synchronization does not affect scheduled synchronization.
7. Click **Save**.

Example

The following example shows an automatic synchronization update that starts on March 5, 2020 at 10:00 a.m. and then repeats every 6 hours:



Related links

Setting up user synchronization with the LDAP server on page 116
Viewing the Avaya Spaces connection status on page 101
Avaya Aura Device Services alarms list on page 209
Avaya Spaces connectivity errors on page 280

Uploading Avaya Spaces language and time zone settings to Avaya Aura® Device Services

About this task

Avaya Aura® Device Services does not automatically receive information about languages and time zones in Avaya Spaces. You must manually upload new language and time zone settings, which are available on Avaya Spaces, using the **clitool** command.

Before you begin

- Obtain the list of Avaya Spaces languages and time zone settings from the Avaya Spaces administrator.
- Prepare text files containing information about Avaya Spaces languages and time zones. For more information about file formats, see Language file format on page 83 and Time zone file format on page 84.

Procedure

1. Use a file transfer utility, such as SFTP or SCP, to upload files with information about languages and time zones to a directory with read rights for clitool.

   For example, upload the files to `/opt/Avaya/DeviceServices/<version number>/`

2. Run the `cdto misc` command.
3. To update languages do one of the following:
   - To replace the existing languages with the languages from the file, run the following command:

     ```
     sudo ./clitool-acs.sh languageORTimeZoneUpdate
     <PATH_TO_LANGUAGES> true true
     ```

- To add the languages from the file in addition to the existing languages, run the following command:

  ```
  sudo ./clitool-acs.sh languageORTimeZoneUpdate
  <PATH_TO_LANGUAGES> true false
  ```

  In these commands, <PATH_TO_LANGUAGES> is the full path to the file containing new languages. For example, /opt/Avaya/DeviceServices/8.0.2.0.88/language.properties

4. To update time zones, do one of the following:
   - To replace the existing time zones with the time zones from the file, run the following command

     ```
     sudo ./clitool-acs.sh languageORTimeZoneUpdate
     <PATH_TO_TIMEZONES> false true
     ```
   - To add the time zones from the file in addition to the existing time zones, run the following command:

     ```
     sudo ./clitool-acs.sh languageORTimeZoneUpdate
     <PATH_TO_TIMEZONES> false false
     ```

   In these commands, <PATH_TO_TIMEZONES> is the full path to the file containing new time zones. For example, /opt/Avaya/DeviceServices/8.0.2.0.88/timezone.properties

Language file format

The UTF-8 text file containing new languages for Avaya Spaces can have any name and extension. For example, language.properties. The file contains a sequence of language=code pairs, where:

- language is the name of the language, which is displayed on the Avaya Aura® Device Services web administration portal. For example: français (Canada) - French (Canada)
- code is the language and locale code. For example, fr-CA. This code uses the LL[-CC] format where:
  - LL is a language code. The language code is represented by two lowercase letters. For example: fr. For more information about codes, see ISO 639-1.
  - CC is an optional country code. The country code is represented by two uppercase letters. For example: CA. For more information about codes, see ISO ISO 3166-1.

Each pair must be on a separate line.

The following is an example of a language file:

```
English=en-US
Deutsch - German=de-DE
español - Spanish=es-LA
français (Canada) - French (Canada)=fr-CA
français (France) - French (France)=fr-FR
```

```
italiano - Italian=it-IT
日本語 - Japanese=ja
한국어 - Korean=ko-KR
```

Time zone file format

The text file containing new Avaya Spaces time zones can have any name and extension. For example, `timezone.properties`. The file contains a sequence of time zones in the `area/location` Olson name format. For example, `America/New_York` or `Europe/Isle_of_Man`. Each time zone must be on a separate line.

The following is an example of a time zone file:

```
Africa/Addis_Ababa
Atlantic/Stanley
Atlantic/Faroe
Pacific/Fiji
Europe/Helsinki
Europe/Paris
America/Cayenne
Pacific/Gambier
```

User and license management overview

After setting up Avaya Spaces integration, you can:

- View Avaya Spaces users.
- Register users in your enterprise on Avaya Spaces.
- Allocate licenses to Avaya Spaces users.

Enterprise user registration on Avaya Spaces

You can register users that are configured in your enterprise LDAP directory on Avaya Spaces. The registration process includes the following steps:

1. Selecting users in your enterprise that you want to register on Avaya Spaces.

   You can only register users with an assigned email address.
2. Registering the selected users on Avaya Spaces.

Avaya Aura® Device Services displays the users selected for registration on the Assign License page. The selected users can have the following status:

Status	Status name	Description
To be processed	TO_BE_PROCESSED	The user is ready for registration on Avaya Spaces.
In progress	IN_PROGRESS	User registration is in progress.
Cancelled	CANCELLED	The user registration operation is cancelled.
Failed	FAILED	The user registration failed.

Avaya Aura® Device Services displays the registered users on the View and Manage page.

Avaya Spaces user licenses

All Avaya Spaces users have the Essential license by default. If a user requires additional features, you can assign a Business or Power license to them. The number of available licenses is dependent on how many Business and Power licenses your company purchased. For more information about Avaya Spaces user licenses, see “Assigning Users” and “Plans” in *Using Avaya Spaces*.

When configuring an enterprise user for registration on Avaya Spaces, you can select a license option. After registering the user on Avaya Spaces, you can allocate a different license type for that user if required.

All licenses of the same license type have the same expiration date.

Trial licenses

Avaya Spaces offers trial Business and Power licenses. Trial licenses provide access to the same features as the advanced licenses but for a limited amount of time.

Avaya Spaces assigns trial licenses automatically. If you select the Essential license when configuring an enterprise user for registration on Avaya Spaces, then, when the user logs in to Avaya Spaces for the first time, the Essential license is converted to the Business Trial license or the Power Trial license. The default trial license is the Business Trial license, even if the company does not have any purchased licenses. You *cannot* assign trial licenses manually when configuring enterprise users for registration on Avaya Spaces. Trial licenses are personal.

If you have available Business or Power licenses, you can update the user’s trial license to either Business or Power license at any time. After the trial period expires, Avaya Spaces keeps the trial license for a user until the user logs in to Avaya Spaces. When the user logs in, Avaya Spaces assigns the Essential license to this user.

Trial licenses are per-user licenses, therefore each trial license has its own expiration date.

Avaya Aura® Device Services displays trial licenses as “Business (Trial)” and “Power (Trial)”.

Avaya Spaces licensing information on Avaya Aura® Device Services

When data synchronization is enabled, Avaya Aura® Device Services retrieves information about licenses from Avaya Spaces, including the following:

- The number of available licenses.
- The license expiration date for Business, Power, and Trial licenses.

Avaya Aura® Device Services displays this information on the Configuration page. Avaya Aura® Device Services also displays information about license expiration dates on the View and Manage page.

If a license expired or will expire soon, Avaya Aura® Device Services displays a warning message when you:

- Add enterprise users for registration on Avaya Spaces.
- Review Avaya Spaces users on the Configuration page.
- Assign a different license to a Avaya Spaces user.

Adding enterprise users for registration on Avaya Spaces

About this task

Use this procedure to:

- Select users from your enterprise LDAP directory that you want to register on Avaya Spaces.
- Provide configuration details for these users, such as the appropriate Avaya Spaces license type, time zone, and language.

You can select a single user or an LDAP group. When you select an LDAP group, all users from that group are added for registration on Avaya Spaces. You cannot select an LDAP group that is configured for automatic registration of group members on Avaya Spaces. You also cannot select a user that belongs to an LDAP group that is configured for automatic registration.

After adding a user using this procedure, you can only modify the selected license type. Therefore, if you need to change other data, such as the time zone or language, you must remove and then re-add the user.

You must ensure that the domain part of the user's email address matches one of your company domains configured on Avaya Spaces. Otherwise, the registration procedure will fail.

You can only add enterprise users with an assigned email address.

Before you begin

If you are planning to assign advanced Avaya Spaces user licenses, ensure that you have enough licenses of the required type.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **Assign License**.
2. From the drop-down list, select one of the following:
   - **User**: To select a single enterprise user.
   - **Group**: To select all users from an LDAP group.
3. In **Search User/Group**, enter the following search criteria:
   - To find a user, type their name or email address.
   - To find a group, type the group name.

   Avaya Aura® Device Services displays the entries that contain the text you entered. If a user does not have an email address, the entry contains `(null)` after the user name. For example: `John Doe (null)`.
4. From **License**, select an Avaya Spaces license to assign to the user.

   You can update the license type later when you are registering the user on Avaya Spaces.
5. **(Optional)** From **Time Zone**, select a time zone for the user.

   The list contains time zones available on Avaya Spaces. If you leave this field blank, the default time zone for your Avaya Spaces company is used.

6. **(Optional)** From **Language**, select a language for the user.

   The list contains languages available on Avaya Spaces. The default language is English.

7. Click **Add**.

   If the enterprise user does not have an email address, Avaya Aura® Device Services displays an error message. Otherwise, Avaya Aura® Device Services adds the selected user to the table on the Assign License page.

Next steps

Register the selected enterprise users on Avaya Spaces.

Related links

Registering enterprise users on Avaya Spaces on page 87
Removing an unregistered user on page 88
Avaya Spaces user licenses on page 85

Registering enterprise users on Avaya Spaces

About this task

After adding enterprise users, you can start the registration process. When registration is complete, enterprise users can use Avaya Spaces services.

You can also use this procedure to re-register users with the “CANCELLED” or “FAILED” status.

After starting the registration process, you cannot start the new registration process until:

- Avaya Aura® Device Services processes all users.
- You cancel the registration process.

Before you begin

Add enterprise users as described in Adding enterprise users for registration on Avaya Spaces on page 86.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **Assign License**.

   Avaya Aura® Device Services displays the users you added for registration.

2. **(Optional)** To select another Avaya Spaces license for a user, click the **License** field for the user and then select the required license from the drop-down list.

3. Click **Assign**.

Result

Avaya Aura® Device Services starts the registration process for all users and changes their status to “TO_BE_PROCESSED”. When Avaya Aura® Device Services starts processing a user, the user status changes to “IN_PROGRESS”. When the user is registered on Avaya Spaces, Avaya Aura®

Device Services no longer displays the user on the Assign License page. Instead, the user is displayed on the View and Manage page.

Avaya Aura® Device Services displays the results of the registration process on the Assign License page.

Related links

Cannot register an enterprise user on Avaya Spaces on page 282
Cancelling user registration and license upgrade operations on page 98

Removing an unregistered user

About this task

Use this procedure to remove a user from the list of users you selected for registration on Avaya Spaces. After adding an enterprise user for registration, you cannot modify that user's time zone or language. You must remove and then re-add the user.

Note:

You can modify the user's license type.

You cannot remove with the "TO_BE_PROCESSED" or "IN_PROGRESS" status.

When you use this procedure to remove a user, that user is *not* removed from your enterprise LDAP directory.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **Assign License**.
2. Do one of the following:
   - To select a single user, select the check box next to the user's name or search for the user by typing a user name or email address in the **Search** field.
   - To select multiple users, select the check boxes for the required users.
   - To select all users in bulk, select the **Select all** check box.
3. Click **Delete**.

   Avaya Aura® Device Services removes all selected users from the list of users selected for registration.

Related links

Cannot register an enterprise user on Avaya Spaces on page 282

Automatic registration of LDAP group members on Avaya Spaces

Avaya Aura® Device Services enables you to automatically register enterprise users that belong to a specific LDAP group. When a new user is added to a group that uses automatic registration functionality, Avaya Aura® Device Services registers that user on Avaya Spaces. If a user is

removed from that group, Avaya Aura® Device Services automatically removes that user from Avaya Spaces.

Important:

Avaya Aura® Device Services receives information about the status and members of LDAP groups when synchronizing data with the enterprise LDAP server. Therefore, you must enable periodic synchronization with your LDAP server to use the automatic registration functionality. You can use manual synchronization if you need to register new LDAP group users on Avaya Spaces immediately.

User settings provided through automatic registration take priority over manual registration settings provided on the Assign License page.

When an LDAP group is configured for automatic registration, you can only manage settings for the entire group. For example, you cannot update a user's license or remove a user from Avaya Spaces if the user is a member of an LDAP group that uses automatic registration.

For users that are automatically registered on Avaya Spaces, Avaya Aura® Device Services displays the LDAP group's Distinguished Name (Group DN) on the View and Manage page in the **Registered Group DN** field.

If you delete or rename an LDAP group that is configured for automatic registration, Avaya Aura® Device Services removes all users that belong to that group from Avaya Spaces.

LDAP group priority order

If a user belongs to multiple LDAP groups that are configured for automatic registration, Avaya Aura® Device Services must choose which settings to use. There might be the following use cases:

- User belongs to multiple LDAP groups with different names.
- User belongs to multiple LDAP groups with the same name. This might occur if the same user is configured on multiple LDAP servers.

User belongs to multiple LDAP groups with different names

Avaya Aura® Device Services sorts all LDAP groups that use the automatic registration functionality in case insensitive ascending alphabetical order and assigns a unique priority number to each LDAP group based on this order. If you have multiple LDAP servers in your deployment, Avaya Aura® Device Services sorts all groups in all servers. If a user belongs to multiple LDAP groups, Avaya Aura® Device Services uses the group settings with the highest priority for that user.

Note:

Avaya Aura® Device Services sorts groups in case insensitive order.

For example, Avaya Aura® Device Services might assign priorities as follows:

LDAP group	Priority
cn=adminGroup	2
cn=AADSGroup	1
cn=SMGRGroup	4
cn=OtherGroup	3

If a user belongs to cn=OtherGroup and cn=adminGroup groups, Avaya Aura® Device Services will use settings configured for the cn=adminGroup group.

User belongs to LDAP groups with the same name

An enterprise user can be configured on multiple LDAP servers. If the user is a member of groups that have the same name on these servers, Avaya Aura® Device Services determines which settings to use based on the provenance priority configured for each LDAP server on the LDAP Configuration page on the Avaya Aura® Device Services administration portal.

Note:

For an LDAP group configured for automatic registration, Avaya Aura® Device Services displays the provenance priority and the LDAP server on the LDAP Group Auto Assign page in the **Directory** field.

For example, the user johndoe@aads.example.com is configured on two LDAP servers: Open LDAP and Active Directory 2016. This user is a member of the cn=adminGroup group on both servers. If the provenance priority is 3 for the OpenLDAP server and 2 for the Active Directory server, then Avaya Aura® Device Services uses settings configured for the cn=adminGroup on Active Directory.

Related links

Modifying the provenance priority on page 112

Enabling automatic registration for an LDAP group

About this task

When automatic registration is enabled for a group, Avaya Aura® Device Services automatically registers new group users on Avaya Spaces or removes users that are deleted from the group. Avaya Aura® Device Services registers new users with the license, time zone, and language settings that you configured for the group.

If a user that belong to an LDAP group that uses automatic registration was already registered on Avaya Spaces through the Assign License page, Avaya Aura® Device Services overwrites the existing settings with the settings configured for the LDAP group.

You cannot configure automatic registration settings while Avaya Aura® Device Services is synchronizing data with LDAP servers.

Before you begin

- Enable automatic synchronization with your enterprise LDAP server. Avaya Aura® Device Services registers new members of an LDAP group selected for automatic registration on Avaya Spaces when synchronizing data with the LDAP server. If synchronization is disabled, Avaya Aura® Device Services displays a warning message on the LDAP Group Auto Assign page.

  For more information about enabling synchronization, see Setting up user synchronization with the LDAP server on page 116.
- If you are planning to assign Business or Power Avaya Spaces user licenses, ensure that you have enough licenses of the required type.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **LDAP Group Auto Assign**.
2. In the **Search** field, start typing the name of an LDAP group and then press `Enter` to display search results.
3. Select the required LDAP group.
4. From **License**, select an Avaya Spaces license to assign to LDAP group users.

   You can select either an Essential, Power, or Business license. Business and Power licenses are only available if your company purchased these license types.
5. **(Optional)** From **Time Zone**, select a time zone for the users of the group.

   The list contains time zones available on Avaya Spaces. If you leave this field blank, the default time zone for your Avaya Spaces company is used.
6. **(Optional)** From **Language**, select a language for the users of the group.

   The list contains languages available on Avaya Spaces. The default language is English.
7. Do one of the following:
   - If you want to keep a user on Avaya Spaces after the user is deleted from the LDAP group, clear the **Delete users removed from the LDAP group from Spaces** check box.
   - If you want to remove a user from Avaya Spaces after the user is deleted from the LDAP group, select the **Delete users removed from the LDAP group from Spaces** check box.
8. Click **Register**.

   Avaya Aura® Device Services starts registering all users of the LDAP group on Avaya Spaces on the next synchronization with LDAP. Avaya Aura® Device Services displays these users on the Assign License page with the “IN_PROGRESS” status. When the registration completes, Avaya Aura® Device Services displays these users on the View and Manage page.
9. **(Optional)** To start the registration process immediately, perform manual synchronization with your LDAP server:
   a. Navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
   b. Select the appropriate LDAP server.
   c. Click **Force LDAP Sync**.

Updating the automatic registration settings for an LDAP group

About this task

You can modify the following settings that Avaya Aura® Device Services uses when automatically registering LDAP group users on Avaya Spaces:

- License
- Time Zone
- Language

Avaya Aura® Device Services applies changes to all users of the LDAP group that are currently registered on Avaya Spaces.

Before you begin

If you are planning to assign a new Avaya Spaces license type to a group, ensure that you have enough licenses of the required type.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **LDAP Group Auto Assign**.
2. From the list of LDAP groups that use automatic registration, select the check box next to the appropriate group name.
3. Click **Update**.
4. In the LDAP Group Update window, select the appropriate license type, time zone, and language.
5. Click **Update**.

   Avaya Aura® Device Services applies changes on the next synchronization with the LDAP server.
6. **(Optional)** To apply changes immediately, perform manual synchronization with the LDAP server.

Disabling automatic registration for an LDAP group

About this task

Use this procedure to disable the automatic registration of users in an LDAP group. When automatic registration is disabled for a group, Avaya Aura® Device Services stops automatically registering new users of that group on Avaya Spaces. All users of that group that are currently registered on Avaya Spaces remain registered.

If a user belongs to other LDAP groups configured for automatic registration, then Avaya Aura® Device Services uses the settings from another group. The settings Avaya Aura® Device Services uses depend on based on the LDAP group priority.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **LDAP Group Auto Assign**.

2. From the list of LDAP groups that use automatic registration, select the check box next to the appropriate group name.
3. Click **Unregister**.

   Avaya Aura® Device Services applies changes on the next synchronization with the LDAP server.
4. **(Optional)** To apply changes immediately, perform manual synchronization with the LDAP server.

Avaya Spaces user management

Avaya Aura® Device Services displays Avaya Spaces users and the licenses assigned to these users on the View and Manage page. On this page, you can:

- Assign a different license to a user.
- Deallocate an advanced license from a user.
- Delete a user from your Avaya Spaces company.

  You cannot delete an Avaya Spaces user using the Avaya Aura® Device Services web administration portal. The user's record remains on Avaya Spaces. You must submit a written request to the Avaya Spaces administrator to delete the user from Avaya Spaces.

Note:

You cannot perform any of these operations for a user that belongs to an LDAP group that is configured for automatic registration. For these users, Avaya Aura® Device Services displays the LDAP Group DN in the **Registered Group DN** field.

You cannot perform multiple management operations for the same user at the same time. For example, you cannot delete a user if you are assigning a different license for that user.

Avaya Aura® Device Services displays the status information about ongoing management operations in the Status column for each Avaya Spaces user and below the list of Avaya Spaces users. Avaya Aura® Device Services updates this status information approximately every two minutes.

Viewing user information

About this task

On the View and Manage page, the list of Avaya Spaces users contains general user information, such as the first name, last name, and email address. You can open a user entry to view more detailed information, such as the following:

- Time zone
- Language
- License type
- License expiration date
- Phone numbers

When you open a user entry, Avaya Aura® Device Services automatically synchronizes with Avaya Spaces to obtain the latest information for that user.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **View and Manage**.

   Avaya Aura® Device Services displays the list of Avaya Spaces users.

2. Navigate to the required user and double-click the user entry to open it.

   Avaya Aura® Device Services displays a separate window with the detailed user information.

Deallocating licenses

About this task

You have a limited number of advanced Business or Power licenses for Avaya Spaces. Therefore, the number of licenses might be less than the number of users in your deployment. If required, you can deallocate an advanced license from a user and reassign it to another Avaya Spaces user. When you deallocate a license from a user, Avaya Spaces assigns the Essential license to that user.

You cannot deallocate a license from a user that belongs to a LDAP group, which is configured for automatic registration of group users.

You cannot deallocate Essential and Trial licenses.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **View and Manage**.
2. Do one of the following:
   - To deallocate a license from a single user, select the check box next to the user's name.
   - To deallocate licenses from multiple users, select the check boxes for the required users.
   - To deallocate licenses from all users, select the check box in the table header.
3. Click **De-Allocate**.

Result

Avaya Aura® Device Services starts the deallocation process and displays its status in the Status column. Depending on the number of users, this process might take several minutes to complete. Avaya Aura® Device Services notifies you when the process is completed.

Related links

Avaya Spaces user management operation fails on page 282

Assigning a different license to Avaya Spaces users

About this task

Use this procedure to assign licenses of another type to Avaya Spaces users. You can assign a new license to a single user or to multiple users at the same time.

Avaya Aura® Device Services notifies you if the license that you want to assign to a user has expired or is expiring soon. You can assign a license to a user even if the license has expired. In this case, the Essential license will be assigned to the user.

If a user has a Trial license of any type assigned, you can assign either a Business or Power license to the user. You cannot assign an Essential license to a user with a Trial license.

If you assign a Business or Power license to a user with an Essential or Trial license, you can cancel this operation from the Assign License page until Avaya Aura® Device Services assigns a new license to the user. In this case, the user's status is displayed as "UDPATE_CANCELLED" on the View and Manage page.

You cannot assign a new license to a user that belongs to a LDAP group, which is configured for automatic registration of group users.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **View and Manage**.
2. Do one of the following:
   - To update a license for a single user, select the check box next to the user's name.
   - To update licenses for multiple users, select the check boxes for the required users.
   - To update licenses for all users, select the check box in the table header.
3. Select the check box for the users you want to update.
4. Click **Update**.

   Avaya Aura® Device Services displays the Update Users License window.
5. Do one of the following:
   - To assign a license to each user separately, in **Update License**, select the required license type for each user.
   - To assign the same license to all users, select the **Bulk Update** check box and then select the required license type from **Select License**.
6. Click **Save**.
7. In the Confirm Action window, click **OK**.

Result

Avaya Aura® Device Services starts the update process and displays the update status in the Status column. Depending on the number of users, the update process might take several minutes to complete.

Related links

Avaya Spaces user management operation fails on page 282

Cancelling user registration and license upgrade operations on page 98

Removing users from your Avaya Spaces company

About this task

You can remove Avaya Spaces users from your company using the Avaya Aura® Device Services web administration portal. You can remove enterprise directory users that were registered on Avaya Spaces and users that were created on Avaya Spaces.

If you delete an enterprise directory user that was registered on Avaya Spaces, this user is *not* removed from the enterprise directory. You can re-register this user on Avaya Spaces in the future.

Note:

- You cannot remove a user that belongs to an LDAP group, which is configured for automatic registration of group users.
- After you perform this procedure, the user's record remains on Avaya Spaces. To completely delete a user and all associated records from Avaya Spaces, you must send a written request to the Avaya Spaces administrator.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **View and Manage**.
2. Do one of the following:
   - To remove a single user, select the check box next to the user's name.
   - To remove multiple users, select the check boxes for the required users.
   - To remove all users, select the check box in the table header.
3. Click **Delete**.
4. In the Confirm Action window, click **OK**.

Result

Avaya Aura® Device Services starts the removal process and displays its status in the Status column. Depending on the number of users, this process might take several minutes to complete. Avaya Aura® Device Services notifies you when users are removed from your company in Avaya Spaces.

Related links

Avaya Spaces user management operation fails on page 282

Performing an Avaya Spaces user audit

About this task

In some cases, the Avaya Aura® Device Services and Avaya Spaces databases might contain different information about a user. For example, if you cancel a license assignment operation, Avaya Aura® Device Services and Avaya Spaces might contain different information about the user license. To identify and resolve these differences, you can use the audit operation.

The audit verifies the following:

- Whether the user exists on both Avaya Aura® Device Services and Avaya Spaces.
- Whether the user has the same license type on both Avaya Aura® Device Services and Avaya Spaces.

The audit does not verify other user attributes, such as the first name, last name, or email address.

To fix inconsistencies between databases, the audit process uses information from the Avaya Aura® Device Services database, unless the user exists on Avaya Spaces only. In this case, you can choose which database record to use.

The audit process does not remove users from Avaya Aura® Device Services.

You cannot perform the audit at the same time as another user management operation, such as adding or deleting a user or updating licenses.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **View and Manage**.
2. Click **Audit Scan**.

   Avaya Aura® Device Services displays the list of users whose Avaya Aura® Device Services and Avaya Spaces database records do not match. For more information about audit scan results, see Audit status on page 97.
3. From **Action for Users not in AADS**, select one of the following options to process users that exist on Avaya Spaces only:

   - **ADD on AADS**: To create these users on Avaya Aura® Device Services.
   - **DELETE from SPACES**: To remove these users from Avaya Spaces.

   Avaya Aura® Device Services displays actions that Avaya Aura® Device Services will perform to fix inconsistencies between Avaya Aura® Device Services and Avaya Spaces databases in the Post Submit Action column.
4. Click **Submit**.

   Avaya Aura® Device Services starts processing all records found during the scan process.

Audit status

The following table shows data mismatch types that Avaya Aura® Device Services can display for users found during the audit scan process.

Data mismatch type	Description	Action	Action performed automatically
USER_NOT_IN_AADS	The user exists on Avaya Spaces only and does not exist on Avaya Aura® Device Services.	The following options are available: • Add the user to Avaya Aura® Device Services. • Remove the user from Avaya Spaces.	No, you must select the action
USER_NOT_IN_SPACES	The user exists on Avaya Aura® Device Services only and does not exist on Avaya Spaces.	The user that exists on Avaya Aura® Device Services is created on Avaya Spaces.	Yes
LICENSE_MISMATCH	The user has different licenses on Avaya Aura® Device Services and Avaya Spaces.	The license information on Avaya Spaces is updated according to the license information from the Avaya Aura® Device Services database.	Yes

Cancelling user registration and license upgrade operations

About this task

You can cancel the following operations:

- Enterprise user registration on Avaya Spaces.
- Upgrade of Essential or Trial licenses to Business or Power licenses.

You cannot cancel an operation for a user if this user belongs to a LDAP group that is configured for automatic registration.

When you cancel a user registration or license upgrade operation, Avaya Aura® Device Services keeps all users that were not processed on the Assign License page and assigns the “CANCELLED” status to these users. If Avaya Aura® Device Services processed any users before cancellation, these users are displayed on the View and Manage page.

If you cancel a user registration operation, you can repeat the registration process later.

If you cancel the license upgrade operation for a user, you can either confirm cancellation or resume the operation from the Assign License page. Until then, the user’s status is displayed as “UPDATE_CANCELLED” on the View and Manage page.

Important:

After cancelling an operation, you must perform an audit from the View and Manage page to ensure that user information is properly synchronized between Avaya Aura® Device Services and Avaya Spaces.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **Assign License**.
2. Click **Cancel** to cancel a user registration or license upgrade process.

   The **Cancel** button is only enabled if any of users on the Avaya Spaces have either the “IN_PROGRESS” or “TO_BE_PROCESSED” status.
3. If you cancelled the license upgrade operation for a user, do the following to confirm cancellation:
   a. Select the user from the table on the Assign License page.
   b. Click **Delete**.

Next steps

Perform the audit operation as described in Performing an Avaya Spaces user audit on page 96.

Related links

Registering enterprise users on Avaya Spaces on page 87
Assigning a different license to Avaya Spaces users on page 95

Updating Avaya Spaces integration parameters

About this task

After Avaya Spaces integration is configured, you can update Avaya Spaces integration parameters.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Configuration**.
2. Update the following parameters as appropriate:
   - **Spaces API Key**
   - **Spaces API Key secret**
   - **Spaces URI**
3. Click **Save**.

Related links

Avaya Spaces integration settings on page 100

Avaya Spaces integration settings

From the Configuration page, you can update the following Avaya Spaces parameters without having to reconfigure integration with Avaya Spaces:

Setting	Notes
Spaces API Key	You can use any API key and API key secret that belong to the company with which you set up integration. **Important:** If you want to set up integration for another company, you must delete the existing configuration first. If you provide an API key or API key secret for another company in the existing configuration and save the configuration, Avaya Aura® Device Services displays an error message.
Spaces API Key secret	
Spaces URI	You do not need to reconfigure integration if Avaya Spaces only changes its URI and other company data remains unchanged. For example, when Avaya Spaces migrates to another URI.

Related links

Updating Avaya Spaces integration parameters on page 99

Disabling Avaya Spaces integration

About this task

Use this procedure to disable integration with Avaya Spaces. When you disable integration, Avaya Aura® Device Services does not synchronize user data with the company you used for integration. You also cannot use the Avaya Aura® Device Services web administration portal to manage Avaya Spaces users or licenses for that company.

When integration is disabled, the Avaya Spaces configuration data remains on Avaya Aura® Device Services, so you can re-enable integration in the future.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Spaces** > **Configuration**.
2. Clear the **Enable Spaces Integration** check box.
3. In the Confirmation window, click **OK**.
4. When the process is completed, click **OK** again.

Deleting the Avaya Spaces configuration

About this task

Use this procedure to delete the Avaya Spaces configuration data from Avaya Aura® Device Services. If you want to enable integration in the future, you will need to set it up again.

You must delete the existing configuration if you want to set up integration for another company. Avaya Aura® Device Services only supports integration with one company at a time.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Spaces** > **Configuration**.
2. Click **Delete**.
3. In the Confirmation window, click **OK**
4. After the deletion process is completed, click **OK** again.

Related links

Configuring data synchronization between Avaya Aura Device Services and Avaya Spaces on page 81

Viewing the Avaya Spaces connection status

About this task

After you set up integration with Avaya Spaces, Avaya Aura® Device Services checks the connection to Avaya Spaces periodically and displays the connection status on the Configuration page. If Avaya Aura® Device Services cannot connect to Avaya Spaces, it displays an error message, which you can use to fix the connection issue.

Avaya Aura® Device Services checks the connection status every one hour. If disconnected from Avaya Spaces, Avaya Aura® Device Services checks the connection status every five minutes.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Spaces** > **Configuration**.
2. In the Status area, view the connection status.

Related links

Avaya Aura Device Services alarms list on page 209
Avaya Spaces connectivity errors on page 280

Chapter 6: LDAP server management

You must configure the enterprise LDAP server to authenticate the users and administrators of Avaya Aura® Device Services. The LDAP Configuration screen on the Avaya Aura® Device Services web administration portal displays the enterprise LDAP server that you configured during deployment.

You cannot perform all LDAP server management tasks with the configuration utility. Use the Avaya Aura® Device Services web administration portal to do the following:

- Configure multiple LDAP directories.
- Specify an order in which Avaya Aura® Device Services accesses LDAP directories.
- Select which LDAP directories are used for authentication.
- Configure multiple base context Distinguished Names (DNs).
- Set up LDAP synchronization.
- Configure attribute mappings.

Important:

- For secure connectivity to LDAP servers, you must import an LDAP certificate file to the Tomcat trust store. For more information, see Importing the secure LDAP certificate using the web administration portal on page 130.
- If FIPS is enabled on Avaya Aura® Device Services, you must use the secure LDAP (LDAPS) connection to access LDAP servers.
- After creating or updating a user in System Manager, you must force LDAP synchronization or wait 24 hours for your changes to take effect.

Related links

Updating user attributes in LDAP on page 119

Configuring the UID mapping attributes when using multiple authentication domains

About this task

If you are using multiple authentication domains, the UID mapping attribute value set for each LDAP server must be domain-qualified. Therefore, the value must include the `@domain` part. The following values are supported:

- `mail`
- `userPrincipalName`
- Any custom attribute that uses a domain-qualified value.

Note:

If you are not using multiple authentication domains, Avaya Aura® Device Services supports only the following values for the UID mapping attribute:

- `uid`, if you are using Open LDAP.
- `sAMAccountName`
- `mail`
- `userPrincipalName`

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.
2. For each LDAP server configured on Avaya Aura® Device Services, in the **UID Attribute ID** field, enter the appropriate value.

Adding a new enterprise LDAP server

About this task

Use this procedure to add a new LDAP server to Avaya Aura® Device Services. After you have added a server, you cannot modify the server URL or remove the LDAP data source.

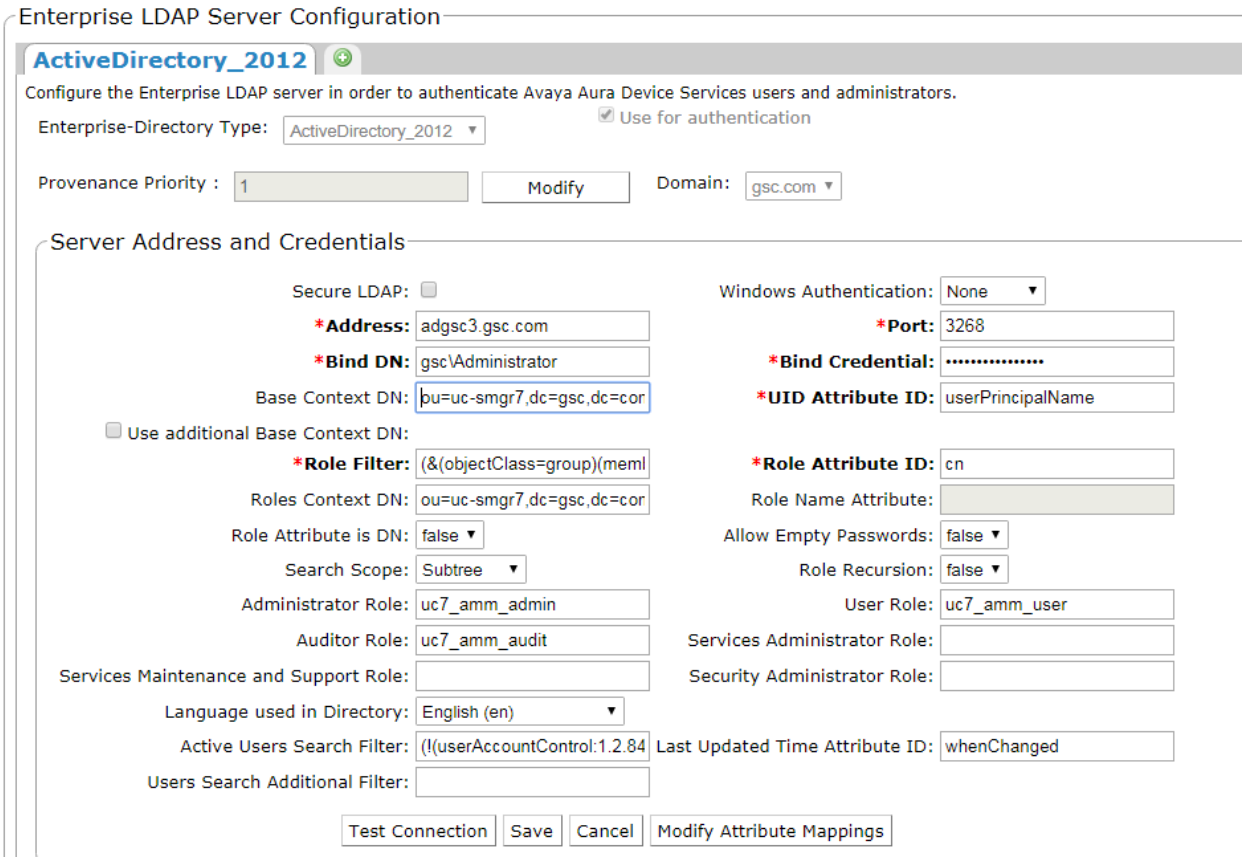
Before you begin

If you are planning to use multiple authentication domains, configure the UID mapping attributes as specified in Configuring the UID mapping attributes when using multiple authentication domains on page 103.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.



2. Click the plus (+) icon.

   Avaya Aura® Device Services displays the New Directory tab.

3. In the **Enterprise-Directory Type** field, click the LDAP server directory that you want to add.
4. In the **Provenance Priority** field, type the priority of the enterprise LDAP server directory.
5. In the Server Address and Credentials section, specify the parameters of the enterprise LDAP server directory.

   For more information about attributes, see Enterprise LDAP Server Configuration field descriptions on page 105.

6. If you want to use the new server for authentication and authorization, do the following:
   a. Select the **Use for Authentication** check box.
   b. Configure role-related attributes, such as **Role Filter**, **Role Attribute ID**, and **Role Context DN**.
7. Click **Save**.

Next steps

For each LDAP server configured on Avaya Aura® Device Services, set up a provenance priority order.

Related links

Modifying the provenance priority on page 112

Enterprise LDAP Server Configuration field descriptions

Name	Description
Enterprise-Directory Type	Specifies the name of the enterprise directory. The options are: • ActiveDirectory_2008 • ActiveDirectory_2012 • ActiveDirectory_2016 • ActiveDirectory_2019 • Novell 8.8 • Domino 7.0 or 8.5.3 • LDS_2008 • LDS_2012 • OpenLDAP 2.4.44 • OracleDirectoryServer 11.1.1
Provenance Priority	Specifies the provenance priority of the enterprise directory. Provenance priority is used while merging contacts. If a value is available in more than one directory, the value in the directory with higher provenance priority is returned. For example, if firstName is obtained from two directories, the firstName from the source with higher provenance priority is returned. You can assign a value between 2 to 10. You cannot assign Provenance priority 1 because it is always assigned to the authorization directory. Provenance priority 1 is the highest and 10 is the lowest. Provenance priority must be different for each enterprise directory or source.

Server Address and Credentials

Name	Description
Use for authentication	Specifies whether the server is used for authentication and authorization. If OAuth is enabled, you can select or clear this check box after installation. If OAuth is enabled but this check box is not selected, then you can only log in to the Avaya Aura® Device

Name	Description
	Services web administration portal using the credentials of the administrative user created during OVA installation.
Secure LDAP	Indicates whether the LDAP server connection is secure or not. If FIPS is enabled, you must use the secure LDAP connection to access LDAP servers. If you are using a secure LDAP connection, you must also import the LDAP server trusted certificate to Avaya Aura® Device Services.
Import Certificate	Specifies the LDAP server trusted certificate. This field is mandatory if you are using a secure LDAP server connection. This field is only displayed when the **Secure LDAP** check box is selected.
Windows Authentication	Specifies whether to use Windows Authentication or not. The options are: • None • Negotiate If you select the Negotiate option, the system displays the **Configuration for Windows Authentication** section. **Note:** Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.
Address	Specifies the IP address or FQDN of the LDAP server. If you are using the secure LDAP connection (LDAPS), you must use the LDAP server FQDN. IP addresses are not supported. If the LDAP server uses IPv6, use the LDAP server FQDN. This field is mandatory.
Port	Specifies the port of the LDAP server. **Important:** With the global catalog ports 3268 or 3269, 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. This field is mandatory.

Name	Description
Bind DN	Specifies 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. This field is mandatory. **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`, `user@domain`, as well as the actual DN of the user object.
Bind Credential	Specifies the password of the administrative user. The password length can be from 1 to 20 characters. The supported characters are: • Lowercase letters: a to z • Uppercase letters: A to Z • Numerics: 0 to 9 • Special characters: exclamation point (!), at sign (@), percent (%), caret (^), asterisk (*), question mark (?), underscore (_), and dot (.). Special characters are not required for the password.
Base Context DN	Specifies the complete Distinguished Name (DN) with the Organizational Unit (OU) for starting the search for users on the enterprise directory. This is the primary Base Context DN for Avaya Aura® Device Services. For example: `dc=domain, dc=company, dc=com`. If you are using multiple authorization domains, Avaya recommends including a domain component to the Base Context DN. For example: `dc=avaya, dc=com`. **Note:** Some LDAP sources, such as Domino, typically do not contain the domain component in Base Context DNs. For example: `o=MyCompany`. If Base Context DNs do not contain the domain component, Avaya Aura® Device Services considers them “empty” Base Context DNs when processing user login or search requests. If Avaya Aura® Device Services cannot find the domain specified

Name	Description
	in the request, the search continues in “empty” Base Context DNs.
Use additional Base Context DN	Enables Avaya Aura® Device Services contact search and quick search. You can add up to 10 Base Context DNs with the same value. The primary Base Context DN is used for authentication. Additional Base Context DNs are used for Avaya Aura® Device Services contact search and quick search, and can also be used for authentication. If you select this check box, you can see the **View/Edit** button. Auto-configuration will use only the primary base context DN.
View/Edit	Enables access to the Addition Base DN Configuration page, where you can add or delete additional Base Context DNs.
UID Attribute ID	Specifies the unique attribute of the user on LDAP, which is used to search for users in the LDAP server. If you are using multiple authentication domains, you must use one of the following values: • `mail` • `userPrincipalName` • Any custom attribute that uses a domain-qualified value. If you are not using multiple authentication domains, you must use one of the following values: • `uid`, if you are using Open LDAP. • `sAMAccountName` • `mail` • `userPrincipalName` This field is mandatory. **Note:** When the UID attribute is set to “mail” on 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.
Role Filter	Specifies the search filter that is used to search the roles of the user. For example: (&(objectClass=group) (member={1})
Role Attribute ID	Specifies that the user is a member of the groups defined by that attribute. For example: objectCategory

Name	Description
	This field is mandatory.
Roles Context DN	Specifies the complete Distinguished Name (DN) to search for a user role, that is, for Role Filter. For example: dc=domain,dc=company,dc=com
Role Name Attribute	Specifies the name of the role attribute. This field is mandatory only if the **Role Name Attribute Is DN** field is set to true. For example: cn if the role is stored in a DN in the form of cn=admin, ou=Users, dc=company, dc=com.
Role Attribute is DN	Indicates whether the role attribute of the user contains DN. The default value is true.
Allow Empty Passwords	Indicates whether LDAP Server acknowledges the empty password. The default value is false.
Search Scope	Specifies the level of the search in the LDAP hierarchy. The options are: • Object: For searching only for the object. • One Level: For including one level in the LDAP hierarchy in the search. • Subtree: For including subtree in the LDAP hierarchy in the search. The default value is Subtree.
Role Recursion	Specifies whether role recursion is enabled. The options are: • true • false
Administrator Role	Specifies the administrator role in which the administrative users are assigned.
Security Administrator Role	Specifies the security administrator role in which the administrative users can manage web certificates from the web administration portal.
User Role	Specifies the user role in which the common users are assigned.
Auditor Role	Specifies the auditor role in which the users can audit the system.
Services Maintenance and Support Role	Specifies the services maintenance and support role in which users can maintain and support services.
Services Administrator Role	Specifies the services administrator role.
Language used in Directory	• Simplified Chinese (zh)

Name	Description
	• German (de) • English (en) • Spanish (es) • French (fr) • Italian (it) • Japanese (ja) • Korean (ko) • Russian (ru) • Portuguese (pt)
Active Users Search Filter	Specifies whether the user is active or inactive on LDAP Server.
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. For example, if you want to search for users in the object class “user” and the object category “Person”, use the following filter: `(&(objectClass=user)(objectCategory=Person))`.
Last Updated Time Attribute ID	Specifies when the user is updated on LDAP. For example, `whenChanged` This field is mandatory.

Configuration for Windows Authentication

Name	Description
Service Principal Name (SPN)	Specifies the service principal name UIDAttributeID must be userPrincipalName.
Import keytab file	Imports the `tomcat.keytab` file and overwrites the existing file.
Kerberos Realm	Specifies the Kerberos realm.
DNS Domain	Specifies the DNS domain of the Domain Controller.
KDC FQDN	Specifies the FQDN of the Domain Controller.
KDC Port	Specifies the port number. The default KDC port is 88.

Button	Description
Test Connection	Tests the connection changes.
Save	Saves the changes made to the enterprise directory.
Modify Attribute Mappings	Modifies the attributes of the LDAP server.

Configuring additional base context DNs

About this task

Use this procedure to add additional base context DNs. Base context DNs are used to specify sections of the LDAP directory where LDAP searches for:

- Contacts, when performing LDAP lookups. The use of multiple base context DNs ensures maximum search performance.
- Groups, when configuring and publishing settings using the Dynamic Configuration service.

You can add up to 10 base context DNs for one LDAP source.

You can also use an additional base context DN for authentication. In this case, this additional base context DN uses the role context DN that is configured in the primary LDAP server.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.
2. Select the appropriate LDAP server.
3. In the Server Address and Credentials section, select the **Use additional Base Context DN** check box and then click **View/Edit**.
4. In the Additional Base Context DN Configuration window, click **+**.
5. In the table, click the **Base Context DN** field and then provide the value of the base context DN.
6. If you want to use the base context DN for authentication, select the **Use for Authentication** check box.
7. Click **Save**.
8. In the Server Address and Credentials section, click **Save**.

Testing connection to a LDAP server

About this task

Use this procedure to ensure that you configured a LDAP server correctly and Avaya Aura® Device Services can connect to the LDAP server.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. Select the appropriate LDAP server.
3. Click **Test Connection**.
4. If the test fails, check the configured LDAP address FQDN, port, and protocol and then run the test again.

Modifying the provenance priority

About this task

If you configured multiple LDAP servers , use this procedure to specify the order in which Avaya Aura® Device Services accesses LDAP directories. For example, if a givenName attribute is defined in two LDAP servers for a given user, the value that Avaya Aura® Device Services uses is based on the order you define.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.
2. Click the **Enterprise Directory** tab that you want to use to modify the provenance priority.
3. In the **Provenance Priority** field, click **Modify**.

   Avaya Aura® Device Services displays the Source Priority Configuration pop-up window.
4. In the **Provenance Priority** column, type the priority level.

   You can assign a value between 2 to 10. You cannot assign Provenance priority 1 as it is always assigned to the authorization directory. Provenance priority 1 is the highest and 10 is the lowest. Provenance priority must be different for each enterprise directory or source.
5. Click **Save**.
6. Restart Avaya Aura® Device Services to apply the new priority.

Related links

Starting or stopping Avaya Aura Device Services on page 27
LDAP group priority order on page 89

Administering the LDAP server configuration

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. Select the appropriate LDAP Server.
3. Modify the details of the enterprise directory.
4. Click **Save**.

Related links

Enterprise LDAP Server Configuration field descriptions on page 105

Enabling LDAP authentication for OAuth

About this task

Use this procedure if you want to use LDAP authentication when OAuth is enabled.

If OAuth is enabled and LDAP authentication is disabled, then you can only log in to the Avaya Aura® Device Services web administration portal using the credentials of the administrative user created during OVA installation.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
2. Select the appropriate LDAP server.
3. Select the **Use for authentication** check box.
4. Click **Save**.

Modifying enterprise directory attribute mappings

About this task

Each LDAP directory type includes a set of pre-defined attributes mappings, which map user attributes that Avaya Aura® Device Services uses to LDAP attributes defined in the default LDAP schema for the respective LDAP directory type. If you use a custom LDAP schema for your LDAP directory type, you must customize the attribute mapping accordingly.

Avaya Aura® Device Services search results do not include attributes that are not mapped to LDAP attributes.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. Select the appropriate LDAP server.
3. In the Server Address and Credentials section, click **Modify Attribute Mappings**.

   Avaya Aura® Device Services displays the Enterprise Directory Mappings page. The Modify LDAP Attribute Mappings table contains the following columns:

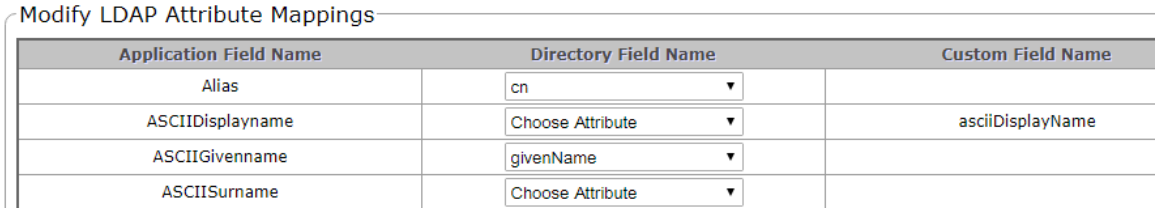
   - Application Field Name contains user attributes that Avaya Aura® Device Services uses.
   - Directory Field Name contains pre-defined attributes from the standard LDAP schema.
   - Custom Field Name enables you to enter custom attribute names.
4. In the Modify LDAP Attribute Mappings section, do one of the following for the required attribute:
   - To select one of the pre-defined LDAP attributes, click the **Directory Field Name** cell and then select the required LDAP attribute from the list.
   - To use a custom LDAP attribute, click the **Custom Field Name** cell and enter the name of the required custom LDAP attribute.
   - To un-map the attribute, clear the **Custom Field Name** value and set **Directory Field Name** to **Choose Attribute**.
5. **(Optional)** If you want to reset the attribute mapping to its default settings, click **Reset**.
6. Click **Save**.

   Avaya Aura® Device Services restarts to apply changes.

Example

The following image shows an Active Directory 2012 attribute mapping example, where:

- Alias and ASCIIGivenname attributes use default mapping.
- ASCIIDisplayname attribute is mapped to the custom asciiDisplayName LDAP attribute.
- ASCIISurname is not mapped to any LDAP attribute



Configuring Windows Authentication for Active Directory

About this task

Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.

Before you begin

Ensure that the LDAP server you use is the Domain Controller with the appropriate Active Directory version as the server type.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. In the Server Address and Credentials section, do the following:
   a. In the **Windows Authentication** field, click **Negotiate**.
   b. In the Confirm Action pop-up window, click **OK**.
   c. The **UIDAttributeID** must be userPrincipalName.
   d. Ensure that the other settings on the Server Address and Credentials page are appropriate for the LDAP configuration of your Domain Controller.
3. In the Configuration for Windows Authentication section, do the following:

   Tip:

   To complete the following fields, use the same values you entered when setting up the Windows Domain Controller.

   a. In **Service Principal Name**, type `HTTP` or `REST_FQDN`.

      For example, type `HTTP` or `aads.example.com`.

   b. To import the `tomcat.keytab` file transferred from the Windows Domain Controller, in **Import keytab file**, click **Import**.

      In cluster deployments, the file is transferred to all nodes in the cluster. An additional option is available to send the file to specific nodes in a cluster.

      You can use the following command to generate a `tomcat.keytab` file.

      ```
      ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /
      princ HTTP/<FRONT-END FQDN>@<Kerberos realm> /ptype KRB5_NT_PRINCIPAL /pass
      +rndPass /crypto all /kvno 0
      ```

      In the following example, `<Domain User Login>` is `aads_spn_user`, `<Kerberos realm>` is `EXAMPLE.COM`, and `<FRONT—END FQDN>` is `aads.example.com`.

      ```
      ktpass /out c:\tomcat.keytab /mapuser aads_spn_user@EXAMPLE.COM /princ HTTP/
      aads.example.com@EXAMPLE.COM /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto
      all /kvno 0
      ```

   c. In **Kerberos Realm**, type the Kerberos realm, which is usually in uppercase letters.

      For example, `EXAMPLE.COM`.

   d. In **DNS Domain**, type the DNS domain of the Domain Controller.

      For example, `example.com`.

e. In **KDC FQDN**, type the FQDN of the Domain Controller.

   This value also includes the DNS domain at the end.

   For example, `ad.example.com`.

f. In **KDC Port**, do not change the default setting , which is 88.

g. In a cluster deployment, click **Send Keytab File** to send the `tomcat.keytab` file to a specific node.

   This option is useful if the import to a node failed or if you add a new node to your cluster.

4. Save the settings to restart the server.

   The settings you specified are used to generate the files needed to configure the Tomcat JAASRealm and the corresponding Sun JAAS Login module for GSS Bind.

Setting up user synchronization with the LDAP server

About this task

Use this procedure to synchronize user data between Avaya Aura® Device Services and a specific LDAP server. Avaya Aura® Device Services synchronizes data that is used for number and email-to-number resolution. You can schedule the synchronization process to occur hourly, daily, or weekly.

You must enable synchronization with the LDAP server if you are planning to use automatic registration of LDAP group users for Avaya Spaces integration. Avaya Aura® Device Services registers new members of an LDAP group selected for automatic registration on Avaya Spaces when synchronizing data with the LDAP server.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. Select the appropriate LDAP server.
3. In the User Synchronization Update Instructions section, specify the date and time when you want to start synchronizing user data between Avaya Aura® Device Services and the LDAP server.
4. Select the **Repeat** check box and specify a period between consecutive synchronization attempts.
5. **(Optional)** To immediately synchronize the user data, click **Force LDAP Sync**.

   Immediate synchronization does not affect scheduled synchronizations.

6. Click **Save**.

Related links

Enabling automatic registration for an LDAP group on page 90

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**.

   Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. Configure the language setting:

Parameter	Description	Default value
Language used in Directory	The language code of one of the languages supported by Avaya Aura® Device Services.	English (en)

3. Click **Save**.
4. Click **Modify Attribute Mappings**.
5. Configure the following settings:

Parameter	Description	Default value
NativeFirstName	The attribute that stores the "given name" of the user in the language of the LDAP server.	givenName
NativeSurName	The attribute that stores the "surname" of the user in the language of the LDAP server.	sn
GivenName	This is only applicable if the language in AD is one of the non-Latin script based ones.	
SurName	This is only applicable if the language in AD is one of the non-Latin script based ones.	

   The NativeFirstName and NativeSurName parameters allow the user to identify the LDAP attributes used to store the user's native language given name and surname. These are mandatory parameters with defaults of givenName and sn.

   The GivenName and SurName parameters allows the user to identify the LDAP attributes used to store the ASCII transliteration of the user's given name and surname, respectively.

These are optional parameters and only used only if the Language used in Directory parameter is set to one of the non-Latin script languages.

The internationalization of the names must be done using the language tags specified in RFC 3866.

To configure internationalization for Microsoft Active Directory, you must configure custom attributes for the native and the ASCII transliterations of the names, if both types of names are needed.

6. Click **Save** to apply changes and restart Avaya Aura® Device Services.

Adding a trusted host

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **Trusted Hosts**.
2. Click **Add**.
3. In the new row, type the FQDN or IP address of the trusted host.

   When connecting to a cluster, add the IP address or FQDN of each node in the cluster and the virtual IP address of the cluster that you want Avaya Aura® Device Services to trust.
4. Click **Save**.

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\\`.

Updating user attributes in LDAP

About this task

In the enterprise directory, you cannot change the Distinguished Name (DN) of a user. Therefore, you cannot change other user attributes related to the DN, such as the Common Name (CN), Organization Unit (OU), and Domain Component (DC). You also cannot update the user email address. To update user attributes in LDAP, you must de-register and then re-register the user after updating the required attributes.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the `cdto misc` command.
3. Run the following command to remove the user from the enterprise directory and from the database:

   `sudo ./clitool-acs.sh runUserDiagnostics -d <email address of the user>`

   For example: `sudo ./clitool-acs.sh runUserDiagnostics -d johndoe@domain.com`.

   For more information about this command, see runUserDiagnostics tool on page 306.
4. Update the attributes in the enterprise directory as required.

   For more information, see the documentation for the LDAP server you are using.
5. Log in to Avaya IX™ Workplace Client to re-register the user on Avaya Aura® Device Services.

Open LDAP user data imports

You can upload user data to Open LDAP in bulk using the Avaya Aura® Device Services web administration portal. You can upload the following user data to Avaya Aura® Device Services:

- Given name
- Last name
- Email address
- Phone number
- User image
- Department

Users are uploaded using a ZIP archive, which contains the following:

- File in CSV format with user data.

- Directory containing user photos.

  If you are planning to upload user photos, you must specify the path to these photos in the CSV file.

  Important:

  The maximum image size is 50 KB.

For more information about the CSV file structure, see Structure of a CSV file for the bulk upload procedure on page 120.

Important:

If you are planning to upload user photos to Open LDAP, you must set the PictureURL attribute to “jpegPhoto” first. For more information, see Changing the PictureURL attribute on page 122.

Structure of a CSV file for the bulk upload procedure

For uploading user data to Open LDAP, Avaya Aura® Device Services uses files in CSV format. The following is an example of a CSV file used to uploading user data to Open LDAP:

```
Given Name,Last Name,Email Address,Phone Number,Image,Department
Aiden,Johnson,aiden_johnson@company.com,123456789,Images/aiden_johnson.jpg,Sales
James,Edwards,james_edwards@company.com,123450001,,Support
Harry,Anderson,harry_anderson@company.com,123451111,Images/harry_anderson.jpg,Support
```

In a CSV file, the first data record is a header, which is `Given Name,Last Name,Email Address,Phone Number,Image,Department` in the example. This header is not processed by Avaya Aura® Device Services and is used for informational purposes only.

Each subsequent data record in a CSV file is a sequence of comma-separated user attributes in the following order:

```
<Given Name>,<Last Name>,<Email Address>,<Phone Number>,<Image>,<Department>
```

The following table describes these attributes:

Attribute	Description	Is required	Example
Given Name	First name of the user.	Yes	Aiden
Last Name	Last name of the user.	Yes	Johnson
Email Address	Email address of the user.	Yes	aiden_johnson@company.com
Phone Number	Phone number of the user.	Yes	123456789
Image	Relative path to the user photo in the image folder.	No	Images/aiden_johnson.jpg
Department	Department of the user.	No	Sales

For example:

`Aiden,Johnson,aiden_johnson@company.com,123456789,Images/aiden_johnson.jpg,Sales`.

If you do not want to provide optional attributes, do not include these attribute values in the data record. For example, if you do not want to use user photos, provide the user attributes as follows: `James,Edwards,james_edwards@company.com,123450001,,Sales`.

To upload user photos, include a photo directory in a ZIP archive used for bulk import. The Photo attribute specifies the relative path to the user photo, starting from that directory.

For example, to upload a file called `picture.jpg`, which is located in a directory called Images, you must enter `Images/picture.jpg`.

Optional structure of a CSV file if using Microsoft Excel

If you are using Microsoft Excel to create the CSV file, you can provide each attribute in a separate column. If you do not want to provide certain attributes, leave the corresponding cells blank. For example:

	A	B	C	D	E	F
1	Given Name	Last Name	Email Address	Phone Number	Image	Department
2	Aiden	Johnson	aiden_johnson@company.com	123456789	Images/aiden_johnson.jpg	Sales
3	James	Edwards	james_edwards@company.com	123450001		Support
4	Harry	Anderson	harry_anderson@company.com	123451111	Images/harry_anderson.jpg	Support

Uploading users in bulk

About this task

Use this procedure to upload user data to Open LDAP.

- If you want to upload user photos, you must upload a ZIP archive, which contains a CSV file with user data and a directory with user photos.
- If you do not need to upload user photos, you can upload a CSV file with user data. Packaging the CSV file in a ZIP archive is not required.

In a cluster environment, you only need to upload user data to a single node. The user data will be replicated to all other nodes in the cluster.

If a user you are uploading already exists, the user data will be overwritten.

You can only perform this procedure if Open LDAP is installed on Avaya Aura® Device Services.

Before you begin

- Create a CSV file with the user data you want to upload on Avaya Aura® Device Services.

- Ensure that the PictureURL LDAP attribute is set to “jpegPhoto”. For more information, see Changing the PictureURL attribute on page 122.

Procedure

1. If you want to upload user photos, package the CSV file and the directory containing user photos into a ZIP archive with no intermediate directories.
2. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **Bulk Import Users**.
3. Click **Choose File** and select either the ZIP archive or the CSV file with user data.
4. In **Default Password for All Users**, provide a password to be used for all users you are importing.
5. Click **Upload**.

Changing the PictureURL attribute

About this task

Use this procedure if you are using onboard Open LDAP and want to upload user images.

Procedure

1. Log in to the Avaya Aura® Device Services web administration interface.
2. Navigate to **Server Connections** > **LDAP Configuration**.
3. On the Enterprise Directory page, select the onboard Open LDAP tab.
4. In Server Address and Credentials area, click **Modify Attribute Mappings**.
5. For the PictureURL attribute, enter `jpegPhoto` in the **Custom Field Name** field.
6. Click **Save**.
7. To apply the changes immediately, click **Force LDAP Sync** on the Enterprise Directory page.

Chapter 7: Certificate management

Managing certificates in the Avaya Aura® Device Services web administration portal

About this task

You can use the Avaya Aura® Device Services administration portal to review and manage certificates. The management options in the administration portal do not replace the setup that you need to complete during installation. After installation is completed, use the web administration portal for management when possible. Only use the configuration utility if the administration portal is not available or for troubleshooting purposes.

Before you begin

- You must have the Security Administrator role to access certificate management options. For more information, see the “LDAP configuration” section in *Deploying Avaya Aura® Device Services*.
- In a cluster environment, ensure that all nodes in the cluster are running.

Procedure

1. On the Avaya Aura® Device Services web administration portal, click **Certificate Management**.
2. Click the appropriate tab.

   The procedures below describe the tasks you can perform on each tab.

Managing System Manager certificates

About this task

Use this procedure to manage System Manager security identity certificates.

Procedure

1. Click the **SMGR Certificates** tab.

   The **System Manager Address**, **System Manager HTTPS Port**, and **Common Name** fields are automatically populated and cannot be modified from the Avaya Aura® Device Services web administration portal. You can use the Avaya Aura® Device Services

configuration utility to modify this information if required. The configuration utility is described in *Deploying Avaya Aura® Device Services*.

2. In the **Node Address** drop-down menu, do one of the following to generate a certificate:
   - Choose a node for a cluster configuration.

     If you choose the **All Cluster Nodes** option, certificates will be generated automatically for all cluster nodes.
   - Keep the default setting for a standalone configuration.
3. In **System Manager Enrollment Password**, type the enrollment password as defined on the System Manager web console.
4. Click **Generate Certificates** to start requesting certificates from System Manager.
5. Restart the Avaya Aura® Device Services after the certificates are generated.

   This completes all the certificate updates. For cluster environment, only the remote node is restarted.

Managing identity certificates

Procedure

1. Click the **Identity Certificates** tab.
2. Use the following subsections to manage CSRs, keystore data, and server identity certificates.
3. After performing the required task, when prompted, restart the Avaya Aura® Device Services server for the changes to take effect.

Related links

Managing CSRs on page 124
Managing keystore data on page 128

Managing CSRs

Procedure

In the Certificate Signing Requests area, do one of the following:

- To set up a new CSR, click **Create** and then follow the steps in Creating CSRs on page 125.
- To remove an existing CSR, select it and then click **Delete**.
- To process a signed CSR, click **Process Signing Request**. For more information, see Processing CA signing requests on page 127.

Related links

Managing identity certificates on page 124

Creating CSRs on page 125
Processing CA signing requests on page 127
Managing server interface certificates on page 128

Creating CSRs

About this task

This procedure provides a high-level overview of how to create CSRs.

Procedure

1. If you clicked **Create** in the Certificate Signing Requests area, complete the following settings in the Create Certificate Signing dialog box and then click **Apply**.
   a. In **Alias**, type an alias using alphanumeric characters.

      An example of an alias is `ottawacrt123`.

   b. Complete the other settings as required.

      You can use the **Show Advanced Settings** button to view additional settings information. For more information about settings, see Create Certificate Signing Request screen field descriptions on page 126.
2. Ensure that the CSR file is successfully saved on your computer.

   The generated CSR is also added to the Certificate Signing Requests area.

   In a cluster configuration, the CSR list on all nodes is identical.
3. **(Optional)** In a cluster environment, if the CSR is not available on a node, click **Propagate** to synchronize requests from the current node to the cluster.

Next steps

Provide the CSR file to the CA for signing and apply the signed CSR as described in Processing CA signing requests on page 127.

Related links

Managing CSRs on page 124
Creating a CSR for a certificate to connect Avaya Aura Device Services to the Avaya Aura Web Gateway on page 125
Create Certificate Signing Request screen field descriptions on page 126

Creating a CSR for a certificate 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, you need to use 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.

Before you begin

- When deploying a CloudFormation stack, provide the host name that is mapped directly to the Avaya Aura® Device Services nodes in the **Hostname for server-to-server** field. For more information, see “Amazon Web Services deployments” in *Deploying Avaya Aura® Device Services*.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the “Security administrator” role.
2. Navigate to **Security Settings** > **Certificate Management** > **Identity Certificates**.
3. In the Certificate Signing Requests area, click **Create**.
4. In the Create Certificate Signing Request window, click **Show Advanced Settings**.
5. Select **Specifcy SAN Manually**.
6. Select **Add FQDN** and provide the following SANs:
   - Load Balancer FQDN.
   - FQDN that is used for server-to-server communication.
   - FQDNs of all nodes in the cluster.

   For example, an Avaya Aura® Device Services cluster with three nodes uses `aads` for the stack name and `aadsrv` for the server-to-server communication host name. The domain is `aadsrv.ca.avaya.com`. In this case, the CSR must contain the following SANs:
   - `aads.ca.avaya.com` for the load balancer.
   - `aadsrv.ca.avaya.com` for server-to-server communication.
   - `aads0.ca.avaya.com` for the first node in the cluster.
   - `aads1.ca.avaya.com` for the second node in the cluster.
   - `aads2.ca.avaya.com` for the third node in the cluster.

Next steps

1. Provide the CSR file to the System Manager CA and apply the signed CSR as described in Processing CA signing requests on page 127.
2. Assign the signed certificate to the Internal server interface as described in Managing server interface certificates on page 128.

Related links

Creating CSRs on page 125

Create Certificate Signing Request screen field descriptions

Name	Description
Alias	The name of the certificate

Name	Description
Common Name	The FQDN of the node. For example, `amm.example.com` You cannot provide wildcard (*) characters in this field.
Use Existing FQDNs for SAN	Use this option to select a particular node in a cluster for which a certificate should be generated. You can also select all cluster nodes.
Specify SAN manually	Use this option to manually specify additional FQDNs or IP addresses for which the certificate should be generated.
Subject Alternative Name	An optional text field that can be used to further identify this certificate. You can provide multiple entries in this field. You cannot provide wildcard (*) characters in this field.
Key Bit Length	The certificate key length in bits.
Signature Algorithm	The hash algorithms to be used with the RSA signature algorithm.
Organizational Unit	The group within the company or organization creating the certificate.
Organization	The name of the company or organization creating the certificate.
City/Locality Name	The city where the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Country (ISO 3166)	The name of the country within which the certificate is being created in the ISO 3166 format. For more information about the format, see ISO 3166 country codes.

Related links

Creating CSRs on page 125

Processing CA signing requests

Procedure

1. Use the appropriate CA documentation to sign the signing request with the CA.
2. In the Certificate Signing Request area, select the appropriate signing request and then click **Process Signing Requests**.
3. In the Process Signing Request dialog box, click **Choose file** to add the signed certificate and then click **Apply**.

Result

The signed certificate is removed from the Certificate Signing Requests area and added to the Keystore area.

Related links

Managing CSRs on page 124

Managing keystore data

Procedure

In the Keystore area, do one of the following:

- To import keystore data, click **Import** and then import keystore data.

  For more information, see Importing keystore data on page 128.
- To export a certificate in the PKCS12 format, select a keystore file and then click **Export**.

  In the Export Certificate dialog box, you can enter a password to protect your exported file.
- To view keystore file details, click **Details**.
- To remove an existing keystore file, select it and then click **Delete**.

Related links

Managing identity certificates on page 124
Importing keystore data on page 128

Importing keystore data

Procedure

If you clicked **Import**, complete the following settings in the Import Certificate dialog box and then click **Apply**.

1. In the **Certificate Type** drop-down menu, select a format for importing the certificate.
2. From **Certificate File**, click **Choose file** to add the certificate file in the selected format.
3. If you selected the PEM format, in **Key File**, click **Choose file** to add the key file in the PEM format.
4. If you selected the PKCS12 format, in **Password**, type the password for the imported certificate.
5. In **Alias**, type an alias to be used for the imported certificate.

Related links

Managing keystore data on page 128

Managing server interface certificates

Procedure

1. Navigate to the Server Interfaces area.
2. In a cluster environment, select the node to administer from the **Node Address** list.

3. Do one of the following:
   - To assign the certificate to a specific server interface, click **Assign** and then complete the settings in the Assign Certificates dialog box as described in Certificate assignment descriptions on page 129.

     If the certificate was assigned only to a selected node, then services on that node need to be restarted to apply the change. If the assignment applies to an entire cluster, then you must restart all nodes in the cluster.
   - To view details about the certificate, click **Details**.
   - To export the certificate in the PKCS12 format, click **Export**.

Related links

Certificate assignment descriptions on page 129

Certificate assignment descriptions

Name	Description
Application	Specifies the interface for REST API to the clients.
Internal	Specifies the interface being used for server-to-server component communication.
OAM	Specifies the Operations, Administration, and Maintenance (OAM) interface.

Related links

Managing server interface certificates on page 128

Managing truststore certificates

About this task

Use this procedure to manage truststore certificates available on Avaya Aura® Device Services.

Procedure

1. Click the **Truststore** tab.
2. In the Truststore area, choose a certificate and click one of the following:
   - **Import**: To import a certificate in PEM or PKCS12 format.
   - **Details**: To view information about the certificate.
   - **Delete**: To delete the certificate from the truststore.
   - **Export**: To export the certificate in the PEM format.

- **Propagate**: To propagate the certificate to all cluster nodes.

3. Restart Avaya Aura® Device Services after importing or deleting certificates for changes to take effect. For cluster environment, restart all the nodes in the cluster for changes to take effect.

Importing the secure LDAP certificate using the web administration portal

About this task

For secure connectivity to LDAP servers, you must import an LDAP certificate file to the Tomcat trust store. The following procedure describes how to import the LDAP certificate using the Avaya Aura® Device Services web administration portal.

Before you begin

Download the CA certificate chain for the CA that signed the LDAP server identity certificate in PEM format.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
2. Select the **Secure LDAP** check box.
3. Click **Import Certificate**.
4. In the Import Certificate window, click **Choose File** and select the certificate from your computer.
5. Click **Save**.

   Avaya Aura® Device Services uploads the certificate to a secure LDAP Server. If a certificate is already uploaded, Avaya Aura® Device Services overwrites the existing certificate.

Chapter 8: Web Deployment service management

The Web Deployment service enables appcast for Avaya IX™ Workplace Client desktop applications. On the Web Deployment page, you can add, edit, or delete an appcast item from the appcast table at the bottom of the page.

The Web Deployment service supports the upload and download of the client installer, which includes software update files. Avaya Aura® Device Services creates the upload folder automatically during a deployment or upgrade. You can also store files to be downloaded later. The files can be downloaded from `https://<aads_server_address>:443/acs/resources/webdeployment/downloads/<file_name_with_extension>`. The upload service operates from the directory `https://<aads_server_address>:8445/admin/webdeployment/upload/`.

Settings for receiving the updates from a client installer

The Dynamic Configuration service has the following three settings for the Web Deployment service:

- APPCAST_ENABLED
- APPCAST_CHECK_INTERVAL
- APPCAST_URL

If the value of the APPCAST_ENABLED settings is set to true, Avaya IX™ Workplace Client will get the APPCAST_URL setting from the Dynamic Configuration service response for the Web Deployment service.

You must set the APPCAST_URL setting to `https://<IP address of the AADS Server>:443/acs/resources/webdeployment`

Web Deployment port configuration

By default, the Web Deployment service uses port 443. Optionally, you can configure Avaya Aura® Device Services to use port 8442 for the Web Deployment service. For more information, see Running a patch to allow Avaya IX Workplace Client for Windows to connect to the Web Deployment service on page 253.

Note:

For upload URLs that point to the Web Administration interface, port 8445 is used. These URLs contain `/admin` after the address and port values. For example: `https://aads.server.com:8445/admin/webdeployment/upload`

Uploading the client installer

About this task

Use this procedure to upload and download the client installer for the Web deployment service.

For Avaya IX™ Workplace Client for Windows, you can upload `.exe` or `.msi` installation files. For Avaya IX™ Workplace Client for Mac, you can upload update and installation `.dmg` files, which are packaged in a `.zip` archive.

Procedure

1. Download Avaya IX™ Workplace Client for Mac or Avaya IX™ Workplace Client for Windows installation files from the Avaya Support website.

   You must have PLDS access to download these files.

2. If you are uploading Avaya IX™ Workplace Client for Mac, pack both update and installation `.dmg` files into a `.zip` archive with no intermediate directories.

   If the `.zip` archive contains intermediate directories, re-pack the archive so that it only contains the `.dmg` files in the root directory.

   By default, the update file has the `AvayaIXWorkplaceMacOS-<version>-Sparkle.dmg` file name and the installation file has the `AvayaIXWorkplaceMacOS-<version>.dmg` file name.

   Important:

   If you change the default file names before uploading, ensure that the new file name of the update file contains the case-insensitive word “sparkle”. For example: `AEUpdSparkleLatest.dmg`. Otherwise, the upload process might not work as expected.

3. Log on to the Avaya Aura® Device Services web administration portal.
4. On the Avaya Aura® Device Services web administration portal, navigate to **Web Deployment** > **Deployment**.

   Avaya Aura® Device Services displays the Software Update Deployment page.

5. In the **Title** field, type the name of the updates or appcast for the client installer.

   When you type the name of the updates for the client installer, Avaya Aura® Device Services automatically adds `Avaya IX Workplace` before the given title.

For example, if you type the update name: *Windows Version 2.0: Critical update*

Avaya Aura® Device Services displays: `Avaya IX Workplace for Windows Version 2.0: Critical update`

6. In the **Description** field, type the description of the client installer updates.

   For more information, see the Release Notes for the new client installer.

7. In the **Version** field, type the version detail for the Avaya IX™ Workplace Client release.
8. In the **OS** field, select one of the following platforms for the Avaya IX™ Workplace Client release:
   - Windows
   - Macintosh
9. Do one of the following:
   - If you are uploading an Avaya IX™ Workplace Client for Mac client installer which requires a specific macOS version, in the **Min OS version** field, provide the minimum macOS version that is supported by the client.

     For example: `9.3.0` or `10.4.5.0`.
   - If you are uploading an Avaya IX™ Workplace Client for Mac client installer which does not require a specific macOS version, leave the **Min OS version** field blank.
   - If you are uploading an Avaya IX™ Workplace Client for Windows client installer, leave the **Min OS version** field blank.
10. In **File**, click **Choose File** and select one of the following files to upload:
    - For Avaya IX™ Workplace Client for Windows, select the `.exe` or `.msi` installation file.
    - For Avaya IX™ Workplace Client for Mac, select the `.zip` archive containing the `.dmg` installation files.

    The maximum upload size for the client installer is 100 MB. The upload service accepts alphanumeric characters, white spaces, dots, minus, and square brackets.

    After you upload the file, Avaya Aura® Device Services auto populates the **Size (in bytes)** and the **MD5 Hash** field.

11. In the **Upload URL(s)** field, choose one of the following, and then click **Upload**:
    - **Default**: To upload the client installer to the Avaya Aura® Device Services server. This is the default option. You cannot edit the value of the default URL.
    - **Custom**: To provide a URL of a different server for uploading the client installer.

    Avaya Aura® Device Services displays a pop up to specify the user credentials to upload the client installer and a confirmation dialog box to indicate the upload status.

12. In the **Download URL(s)** field, choose one of the following:
    - **Default**: To download the client installer from the Avaya Aura® Device Services server to the clients. This is the default option. You cannot edit the value of the default URL.

- **Custom**: To provide a URL of a different server for downloading the client installer.

To download the client installer, you must enter the credentials for client authentication.

13. Click **Save** to save the settings.

    Avaya Aura® Device Services populates the data in the table at the bottom of the page. For more information about fields, see Appcast items field descriptions on page 134. To edit or delete a specified setting, you can double-click to select an entry.

Appcast items field descriptions

The Appcast Items table shows the list of Avaya IX™ Workplace Client installers that you can download using the Web Deployment service.

Name	Description
Title	The name of the updates or appcast for the client installer.
Description	The description of the client installer updates or appcast.
Version	The version information for the Avaya IX™ Workplace Client release.
Publish Date	The date and time when the installer was uploaded onto the Web Deployment service.
OS	The platform of the Avaya IX™ Workplace Client installer.
Download URL	The URL that specifies the location of the Avaya IX™ Workplace Client installer.
Downloads	The number of times the appcast file has been downloaded using the download URL.
Updates	The number of times the upgrade file was applied on the already installed client using the respective appcast file download URL. This counter increases if a user does the following: • Tries to download the client from Unified Portal, and Unified Portal detects that the user already has an installed version of the client. • Updates the client using the built-in **Check for Updates** option.

Editing an appcast item

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Web Deployment** > **Deployment**.

   Avaya Aura® Device Services displays the Software Update Deployment page.

2. On the bottom of the Software Update Deployment page, double-click an entry in the table.

   Avaya Aura® Device Services displays the Edit appcast item page.

3. Edit the settings that you want to change.
4. Click **Save**.

   Avaya Aura® Device Services populates the updated data in the table at the bottom of the page.

Deleting an appcast item

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Web Deployment** > **Deployment**.

   Avaya Aura® Device Services displays the Software Update Deployment page.

2. On the bottom of the Software Update Deployment page, click an entry in the table.

   Avaya Aura® Device Services displays the Edit appcast item page.

3. Click **Delete**.

   Avaya Aura® Device Services displays the Delete item page.

4. Click **Yes**.

Reviewing download statistics

About this task

The Download statistics table shows the total number of Avaya IX™ Workplace Client installations and updates performed using the Web Deployment service. The statistic table includes data for both installers currently available for downloading and installers which have been removed from Web Deployment.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Web Deployment** > **Deployment**.
2. Navigate to the Download statistic table at the bottom of the page.

   For more information about options in the table, see Download statistics field descriptions on page 136.

Download statistics field descriptions

Name	Description
OS	The platform of the Avaya IX™ Workplace Client installer.
Fresh Install	The total number of fresh installation attempts for Avaya IX™ Workplace Client for the given OS using the Web Deployment service.
Updates	The total number of attempts to update the Avaya IX™ Workplace Client soft phones for the given OS using the Web Deployment service.
Total	The total number of fresh installation and update attempts for the Avaya IX™ Workplace Client soft phones for the given OS using the Web Deployment service.

Chapter 9: Utility Server administration

You can enable the Utility Server when you install or upgrade Avaya Aura® Device Services. The Utility Server offers the following:

- File server functionality. The Utility Server hosts various files that Avaya phones require to operate, such as firmware, configuration, or upgrade files.
- Firmware management. The Utility Server provides the option to upload new phone firmware to the file server. You can also activate or deactivate the firmware.

Important:

- You cannot enable the Utility Server using the Avaya Aura® Device Services web administration portal or configuration utility.
- Although `46xxsettings.txt` files are generated using the Dynamic Configuration service, these files are stored on the Utility Server. Therefore, you cannot generate `46xxsettings.txt` files if you do not enable the Utility Server.

Utility Server in a cluster environment

The Utility Server is not clustered. When you upload files, such as firmware packages or upgrade files, on a Utility Server node, these files are not available on other cluster nodes. You must upload these files on all other Utility Server instances manually.

Note:

Configuration files generated using the Dynamic Configuration service become available on all cluster nodes automatically.

Browser support

You can access the Utility Server functionality using the following browsers:

- Google Chrome
- Internet Explorer

Mozilla Firefox does not support certain features, such as backup and restore.

Utility Server capacity limits

Depending on the Avaya Aura® Device Services deployment method, the Utility Server has the following capacity limits for firmware files:

- If Avaya Aura® Device Services is installed on an AVP host, then the total size of firmware `.zip` files or unpacked firmware packages uploaded on the Utility Server must not exceed 6 GiB.
- If Avaya Aura® Device Services is installed on an ESXi host or AWS AMI instance, then the total size of firmware `.zip` files or unpacked firmware packages uploaded on the Utility Server must not exceed 12 GiB.

Supported and unsupported phone models

Supported phone models

The following table shows phone models and firmware types that you can use with the Avaya Aura® Device Services Utility Server.

Phone model	Supported firmware type		Notes
	SIP firmware	H.323 firmware	
Avaya 96X0 Deskphones			
9620L	✔	✔	You can only use one firmware type at a time. For example, if you want to use SIP firmware, you must deactivate H.323 firmware.
9640	✔	✔	
9640G	✔	✔	
9650	✔	✔	
Avaya 96X1 Deskphones			
9608G	✔	✔	—
9611G	✔	✔	
9621G	✔	✔	
9641G	✔	✔	
Avaya J100 Series IP Phones			
J129	✔	✖	—

Phone model	Supported firmware type		Notes
	SIP firmware	H.323 firmware	
J139	✓	✗	
J169	✓	✓	
J179	✓	✓	
Avaya Vantage™			
K155	✓	✗	—
K165	✓	✗	
K175	✓	✗	

Unsupported phone models

The Avaya Aura® Device Services Utility Server does not support the 9620 deskphones.

Setting up a DHCP server

About this task

Configure a DHCP server to allow IP phones to locate the Utility Server in the network. Avaya Aura® Device Services supports any DHCP server software as long as the software is correctly configured.

Before you begin

Contact your DHCP server software vendor to obtain server software installation and configuration instructions.

Procedure

1. Install the DHCP server software according to the server software vendor's instructions.
2. On your DHCP server, configure option 242 as follows:

```
"TLSSRVR=<Utility Server IP address or
FQDN>,TLSPORT=1543,TLSSRVRID=0,HTTPSRVR=<Utility Server IP address or
FQDN>,HTTPPORT=80,MCIPADD=<H.323 call server address list>"
```

   For example:

```
"TLSSRVR=1.2.3.4,TLSPORT=1543,TLSSRVRID=0,HTTPSRVR=1.2.3.4,HTTPPORT=80,MCIPADD=3.5
.7.9"
```

   - Only H.323 endpoints use MCIPADD.

- Firmware and custom files for SIP endpoints use HTTPS, so HTTPSRVR and HTTPPORT are not required if you are only using SIP endpoints.

3. Configure other DHCP settings, such as the available range of IP addresses, as required.

   For information about other DHCP options you can configure, see http://downloads.avaya.com/elmodocs2/one-X_Deskphone_Edition/R1.5/output/16_300698_4/admn055.html#527056.

Starting and stopping the Utility Server

Procedure

1. Log in to the Avaya Aura® Device Services as an administrator using an SSH connection.
2. Run one of the following commands:
   - `svc utilserv start` to start the Utility Server.
   - `svc utilserv stop` to stop the Utility Server.
   - `svc utilserv restart` to restart the Utility Server.

Enabling access to the Utility Server using an HTTP connection

About this task

By default, you can access files stored on the Utility Server using a secure HTTPS connection. Use this procedure if you want to access the Utility Server using an unsecure HTTP connection.

Procedure

In a cluster environment, perform this procedure on the seed node first and then on all non-seed nodes.

1. Log in to the node using an SSH connection.
2. Run the following command to navigate to the `misc` directory:

   ```
   cdto misc
   ```

3. Run the following command to enable HTTP access:

   ```
   sudo ./us-http-port.sh --enable
   ```

4. When the configuration process is complete, reload the firewall.

Result

After HTTP access to the Utility Server is enabled on all nodes, you can access Utility Server files, such as `46xxsettings.txt`, using the following URL:

`http://<Utility Server FQDN>/<file name>`

For example: `http://utilityserver.example.com/46xxsettings.txt`

Logging in to the Utility Server

Procedure

1. Open the Google Chrome or Internet Explorer browser.
2. Navigate to `https://<Utility_Server_address>:8543/admin.html`.

   In this URL, `<Utility_Server_address>` is the virtual IP address or FQDN of the Utility Server. If IPv6 support is enabled, you can use either IPv4 or IPv6 addresses.

   The following are URL examples:

   - IPv4 address example: `https://192.0.2.44:8543/admin.html`
   - IPv6 address example: `https://[2001:db8::7334]:8543/admin.html`
3. On the Login screen, enter the user name and password of the administrative user that you created during the OVA deployment.

Related links

Monitoring cluster nodes on page 203

Reviewing the disk space occupied by firmware package files

About this task

Use this procedure to ensure that the Utility Server has enough free space to store a firmware package that you want to upload or unpack.

- To check the amount of space occupied by uploaded firmware `.zip` files, run the following command:

  ```
  sudo du -hs /tmp/*.zip
  ```

  The output value must not exceed the following values:

  - 6 GiB if Avaya Aura® Device Services is installed on an AVP host.
  - 12 GiB if Avaya Aura® Device Services is installed on an AWS AMI or an ESXi host.

If the output value exceeds the listed sizes, you must remove some `.zip` files from the Utility Server before uploading new firmware packages.

- To check the amount of space occupied by unpacked firmware packages, run the following command:

```
sudo du -hs /opt/IPPhoneFirmware
```

The output value must not exceed the following values:

- 6 GiB if Avaya Aura® Device Services is installed on an AVP host.
- 12 GiB if Avaya Aura® Device Services is installed on an AWS AMI or an ESXi host.

If the output value exceeds the listed values, you must remove some unpacked firmware packages before unpacking another package.

Uploading files on the Utility Server

About this task

Use this procedure to upload files, such as firmware packages, on the Utility Server. You can upload a single file or an archive in the `.zip` format. The Utility Server stores the uploaded files in the `/tmp` directory.

Important:

In a cluster environment, you must manually upload a firmware package on each Utility Server node. Avaya Aura® Device Services does *not* automatically copy files uploaded to one node onto other cluster nodes.

Before you begin

- Configure a DHCP server. For more information, see Setting up a DHCP server on page 139.
- Ensure that you have enough free disk space to upload a firmware package. For information about reviewing disk space, see Reviewing the disk space occupied by firmware package files on page 141.

Procedure

1. On the Utility Server web interface, in the navigation pane, click **Upload Files**.
2. On the Upload File screen, click **Browse**.
3. Select the required file and click **Open**.

   The Utility Server displays the selected file name to the right of the **Browse** button.
4. Click **Upload File**.

   The uploading process can take some time depending on the file size and connection speed.

   If you upload a firmware package, it appears in the “Firmware package” table on the Manage Phone Firmware tab.

Uploading settings files to the Utility Server

About this task

When you use the Utility Server to manage settings for endpoints, you can manually upload settings files, such as `46xxsettings.txt`, to the Utility Server. If you want to use a `46xxsettings.txt` file that contains conditional statements, such as `IF` or `GOTO` commands, you must use this procedure to manually upload the settings file to the Utility Server. `46xxsettings.txt` files that you generate using the Dynamic Configuration service do not support conditionals.

The Utility Server is not clustered. Therefore, in a cluster environment, you must upload a settings file on each cluster node separately. Perform this procedure on the seed node first and then on all non-seed nodes.

Procedure

1. Run the following command to copy the settings file to the `/var/www/html` directory of an Avaya Aura® Device Services node.

   `scp <settings file> <AADS node FQDN>:/var/www/html`

   In this command, `<settings file>` is the settings file name and `<AADS node FQDN>` is the FQDN of the node where you are copying the settings file.

   For example: `scp 46xxsettings.txt aads.node1.example.com:/var/www/html`

2. Using an SSH connection, log in to the Avaya Aura® Device Services node where you copied the settings file.
3. Run the following command to navigate to the `/var/www/html` directory:

   `cd /var/www/html`

4. Run the following command to grant permission to read the setting file:

   `chmod a+r <settings file>`

   For example: `chmod a+r 46xxsettings.txt`

Result

After you upload the settings file to all Avaya Aura® Device Services nodes, you can access it from the following URL:

`https://<Utility Server FQDN>/<settings file>`

For example: `https://utilityserver.example.com/46xxsettings.txt`

Related links

Publishing the configuration settings on page 164
Administration of the Dynamic Configuration service on page 153

Uploading an IP phone custom file

About this task

Use this procedure to upload custom files or site-specific files, such as custom screen saver images, wallpaper images, or ringtones, to the Utility Server. You can upload a single file or a `.zip` archive. The files are available immediately after uploading. The Utility Server overwrites existing files.

The Utility Server stores uploaded custom files in the `/var/www/html/custom` directory.

Before you begin

Configure a DHCP server. For more information, see Setting up a DHCP server on page 139.

Procedure

1. On the Utility Server web interface, in the navigation pane, click **IP Phone Custom File Upload**.
2. On the IP Phone Custom File Upload screen, click **Browse**.
3. Select the required file and click **Open**.

   The Utility Server displays the file name to the right of the **Browse** button.
4. Click **Upload Custom Files and Activate**.

Viewing custom files uploaded on the Utility Server

Procedure

1. On the Utility Server web interface, in the navigation pane, click **IP Phone Custom File Upload**.
2. Click **Display Custom Directory**.

   The Utility Server displays a table containing the following information about the uploaded custom files:

   - The name of the custom file.
   - The file size.
   - The last modification date.

Accessing IP phone custom files

About this task

IP phones can directly access the custom files that you upload on the Utility Server

Procedure

Depending on the protocol you are using to access files, use one of the following URLs:

- To access custom files using the HTTP protocol, use the `<IP or FQDN>:80/custom/<file_name>` URL. In the URL, `<IP or FQDN>` can be one of the following:
  - Avaya Aura® Device Services server IP address
  - Utility Server virtual IP address
  - Avaya Aura® Device Services server FQDN
  - Utility Server virtual FQDN
- To access custom files using the HTTPS protocol, use the `<virtual IP or FQDN>:1543/custom/<file_name>` URL. In the URL, `<virtual IP or FQDN>` can be one of the following:
  - Utility Server virtual IP address
  - Utility Server virtual FQDN

Backing up H.323 phone settings on the Utility Server

About this task

Use this procedure to back up H.323 phone settings, such as contact list, ring volume, and ring tone settings, on the Utility Server.

Important:

The Utility Server does not support the backup of SIP phone settings.

The Utility Server stores phone settings in a text file in the `/var/www/http/PhoneBackup/` directory. The name of this file contains the extension number of the phone. In a cluster environment, phone settings are stored on the seed node. The Utility Server supports both HTTP and HTTPS authentication methods for backup operations.

When you back up the Utility Server, the backup includes phone settings.

Before you begin

Configure a DHCP server. For more information, see Setting up a DHCP server on page 139.

Procedure

1. Run the following commands to enable port 80 on the server:

   ```
   cdto misc
   sudo ./us-http-port.sh --enable
   ```

   For more information about this command, run the `sudo ./us-http-port.sh –h` command.

2. Log in to your phone and perform a manual backup.

For more information about performing a manual backup on your phone, see the documentation for your phone model.

The backup file is created on the server in the `/PhoneBackup` directory. For example: `/PhoneBackup/17774441530_96xxdata.txt`.

3. Reboot the phone.
4. Add one of the following entries to the `46xxsettings.txt` file for the phone model:
   - `SET BRURI http://<username>:<password>@<AADS_IP_OR_FQDN>/PhoneBackup`
   - `SET BRURI https://<username>:<password>@<AADS_IP_OR_FQDN>/PhoneBackup`

   In these entries, `<username>` and `<password>` are credentials of the administrative user that you created during the OVA deployment and `<AADS_IP_OR_FQDN>` is either the IP address or FQDN of Avaya Aura® Device Services. In a cluster environment, `<AADS_IP_OR_FQDN>` is either the IP address or FQDN of the seed node.

Utility Server backup and restore

Backing up data stored on the Utility Server

About this task

Use this procedure to back up data stored on the Utility Server, such as upgrade scripts or `46xxsettings.txt` files. The Utility Server backs up files that are stored on the Utility Server's web browser.

In a cluster environment, perform the backup procedure from the seed node.

Note:

- The Utility Server does *not* back up firmware files. After backing up and restoring the Utility Server, you need to manually re-upload and activate the required firmware packages.
- Backing up Avaya Aura® Device Services does *not* back up the Utility Server data.

Procedure

1. On the Utility Server web interface, in the navigation pane, click **Utility Services Backup and Restore**.
2. Click **Create Backup**.

   If the backup is completed successfully, the Utility Server displays the path to the backup file and the link to download the file.

3. Click **Download the newly created Utility Services Backup File** and save the backup file on an external storage device.
4. Click **Continue**.

Restoring the Utility Server data

About this task

Use this procedure to restore the Utility Server data from the backup file. The following rules apply when restoring the Utility Server data:

- All binaries that were activated before the backup procedure will be activated during the restore procedure.
- `46xxsettings.txt` files, which were generated using the Dynamic Configuration service and stored in folders with groupIDs, will be restored in the same folders.

Procedure

1. Log in to the Utility Server.
2. On the Utility Server web interface, in the navigation pane, click **Utility Services Backup and Restore**.
3. From the **Upload and Restore Utility Server Backup File** field, select **Browse** and navigate to the backup file.
4. Click **Upload Backup**.

   When the restore procedure is complete, the Utility Server displays the procedure status.
5. In a cluster environment, repeat the steps above for all other nodes in the cluster.

Backup and restore of phone model to group ID mapping

When you back up the Utility Server data, phone model to group ID mapping is not backed up. Phone model to group ID mapping is maintained in the database. Therefore, to back up and restore this mapping, you must back up the Cassandra database as part of the Avaya Aura® Device Services backup procedure.

If the Avaya Aura® Device Services backup does not include the database backup, but the Utility Server was backed up and restored, then the restored system will not have phone model to group ID mapping. `46xxsettings.txt` files will still be stored in group ID folders, but these folders will not be mapped to the correct phone models. In this case, you must manually assign group IDs to the phone models as described in Assigning a group identifier to a phone model on page 156. Otherwise, phones cannot download `46xxsettings.txt` files from the Utility Server.

Firmware management

The following sections describe the firmware management operations available on the Utility Server.

Viewing firmware packages available on the Utility Server

Procedure

1. On the Utility Server web interface, in the navigation pane, click **Manage phone Firmware**.

   Firmware packages available on the Utility Server are listed in the “Firmware Package” table. The table also contains package status information:

   - Packed: Package is uploaded on the Utility Server.
   - Unpacked: Package content is extracted and ready to be activated.
   - Active: Phones can download the package content.

   For more information about package statuses, see Firmware package statuses on page 148.
2. To review the firmware package information, select the required package and click **View**.

Firmware package statuses

Status	Description
Packed	The firmware package is uploaded on the Utility Server. When the firmware package has this status, you can perform the following actions: • View information about the package. • Unpack the package. • Remove the `.zip` archive with the package from the Utility Server.

Status	Description
Unpacked	The firmware package files are extracted but cannot be downloaded by the phones. The Utility Server places the unpacked files in the `/opt/IPPhoneFirmware/<package_name>` directory. For example, if the package name is `96x1-IPT-H323-R6_6_4_01-102616`, it will be placed in the `/opt/IPPhoneFirmware/96x1-IPT-H323-R6_6_4_01-102616` directory. When the firmware package has this status, you can perform the following actions: • View information about the package. • Activate the package. • Remove the extracted files from the `/opt/IPPhoneFirmware/<package_name>` directory. The `.zip` archive with the firmware package will still be available on the Utility Server.
Active	Phones can download content from a package with this status. When the package is active, the Utility Server creates symbolic links to all package files and also copies the upgrade script from the package into the `/var/www/html` directory. When the firmware package has this status, you can perform the following actions: • View information about the package. • Deactivate the package. The package content is no longer available for phones to download, but the extracted files are still stored on the Utility Server. **Note:** You cannot remove firmware package files from the Utility Server if the package is active.

Unpacking a firmware package

About this task

Before making the uploaded firmware available for phones to download, you must unpack the firmware package content. The Utility Server stores uploaded firmware packages in the `/tmp` directory. When you unpack the package, the Utility Server places the firmware files into the `/opt/IPPhoneFirmware/<package_name>` directory. For example, if you unpack the `96x1-IPT-H323-R6_6_4_01-102616.zip` package, the Utility Server places its content into the `/opt/IPPhoneFirmware/96x1-IPT-H323-R6_6_4_01-102616` directory.

During the unpacking procedure, the Utility Server checks the signatures of firmware files. If the signatures are not valid, then the files will not be unpacked and the Utility Server will display an

error message. You can skip the signature check by selecting the **Forcibly Unpack** option, but it is not recommended.

Before you begin

Upload the firmware package onto the Utility Server.

Procedure

1. On the Utility Server web interface, in the navigation pane, click **Manage Phone Firmware**.
2. From the **Firmware Package** table, select the required package with the “Packed” status.
3. Unpack the firmware package using one of the following options:
   - **SHA256 Unpack**: Extracts files from a SHA256 signed firmware package.
   - **SHA1 Unpack**: Extracts files from a SHA1 signed firmware package.
   - **Forcibly Unpack**: Extracts files from a firmware package without signature checking.

   Note:

   - Avaya recommends that you use an SHA256 signed firmware package and always check the signatures of firmware files.
   - You cannot unpack a SHA256 signed firmware package using the **SHA1 Unpack** option or SHA1 signed firmware package using the **SHA256 Unpack** option.

   After the unpacking procedure is completed, the Utility Server displays the procedure status.
4. Click **Continue**.

   The firmware now has the “Unpacked” status in the “Firmware Package” table.

Activating a firmware package

About this task

Use this procedure to make an unpacked firmware package available for phones to download. During this procedure, the Utility Server creates symbolic links for all files in the `/opt/IPPhoneFirmware/<package_name>` directory and also copies the upgrade file from the package directory into the web server root directory, `/var/www/html`.

Before you begin

Unpack the required firmware package.

Procedure

1. On the Utility Server web interface, in the navigation pane, click **Manage Phone Firmware**.
2. Select the required firmware package that has the “Unpacked” status.

3. Click **Activate**.
4. Click **Continue**.

   The firmware package version has the “Active” status in the “Firmware package” table.

Next steps

Update the path to the `46xxsettings.txt` file in the upgrade file.

Related links

Updating the path to the 46xxsettings.txt file in an upgrade file on page 151

Updating the path to the 46xxsettings.txt file in an upgrade file

About this task

Phones start the upgrade procedure by downloading and interpreting the content of the upgrade file. This file contains upgrade instructions, including information about downloading the `46xxsettings.txt` file. You must update the default path to the `46xxsettings.txt` file, which is specified in the upgrade file. This enables the phone to download the `46xxsettings.txt` file generated by Avaya Aura® Device Services and stored on the Utility Server.

Note:

The file name of the upgrade model is based on the phone model. For example, 96x1 phones use the `96x1Hupgrade.txt` file name.

Before you begin

- Activate the firmware package for the phone model.
- Assign the group identifier to the phone model on the Avaya Aura® Device Services web administration portal.

Procedure

1. Log in to the Avaya Aura® Device Services as an administrator using an SSH connection.
2. Run the `cd /var/www/html` command to navigate to the directory where the Utility Server stores upgrade files for activated firmware packages.
3. Open the required upgrade file in a text editor, such as vi.

   For example, to open the upgrade file for 96x1 series phones in vi, use the `vi 96x1Hupgrade.txt` command.
4. In the upgrade file, replace the `GET 46xxsettings.txt` entry with `GET <GrouID>/46xxsettings.txt`, where `<GroupID>` is the group identifier assigned to the phone model.

   For example, if you assigned `123` to the 96x1 phone model, the updated entry must look as follows: `GET 123/46xxsettings.txt`.
5. Save the upgrade file.

Related links

Activating a firmware package on page 150
Assigning a group identifier to a phone model on page 156

Deactivating a firmware package

About this task

Use this procedure if you no longer need a certain firmware package to be available for phones to download. For example, you can use this procedure when a new firmware version is available.

Procedure

1. On the Utility Server web interface, in the navigation pane, click **Manage Phone Firmware**.
2. From the “Firmware package” table, select the required version with the “Active” status.
3. Click **Deactivate**.
4. Click **Continue**.

   The firmware package version has the “Unpacked” status.

Removing a firmware package

About this task

Use this procedure if you want to remove a certain firmware package form the Utility Server.

You cannot remove a firmware package with the “Active” status.

Procedure

1. On the Utility Server web interface, in the navigation pane, click **Manage Phone Firmware**.
2. From the **Firmware Package** table, select the firmware package you want to remove.
3. Click **Remove**.

   Depending on the current status of the firmware package, removing the package results in one of the following:

   - If the firmware package status is “Unpacked”, the firmware package status becomes “Packed”. The Utility Server removes all package files from the `/opt/IPPhoneFirmware/<package_name>` directory. The archive file still exists in the `/tmp` directory and is available for unpacking.
   - If the firmware package status is “Packed”, the Utility Server removes the package from the system. If you want to use this package again, you must re-upload this file onto the Utility Server.

Chapter 10: Administration of the Dynamic Configuration service

With the Dynamic Configuration service, Avaya Aura® Device Services can dynamically retrieve and deploy automatic configuration settings on Avaya IX™ Workplace Client. You can also use the Dynamic Configuration service to manage configuration settings and generate `46xxsettings.txt` files for the following endpoints:

- Avaya Vantage™.
- Avaya J100 Series IP Phones.
- 9600 Series IP Deskphones.

Avaya Aura® Device Services generates a separate `46xxsettings.txt` file for each endpoint category. The generated `46xxsettings.txt` files are stored on the Utility Server.

Dynamic configuration provides a centralized place to administer user, group, platform, global, and exception settings. You can set up automatic configuration on Avaya IX™ Workplace Client using one of the following methods:

- DNS-based discovery if you want to use an email address for automatic configuration.
- Web address, which requires a URL for automatic configuration.

  For example: `https://<IP address>:443/acs/resources/configurations`.

For more information about setting up automatic configuration on Avaya IX™ Workplace Client, see *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*.

Using the Dynamic Configuration service, you can publish configuration settings for the following:

- **Global:** Any other settings category can override global settings. Global settings are used for both Avaya IX™ Workplace Client and desk phones.
- **Group:** User, platform, exception, and System Manager settings can override group settings. Group settings are only used for Avaya IX™ Workplace Client.

  When a client requests automatic configuration, Avaya Aura® Device Services searches for user groups only in the configured contexts on the LDAP server containing the user. For example, Avaya Aura® Device Services uses two LDAP servers configured as follows:

  - LDAP 1 has the primary base context DN set to PrimaryBase1 and two additional base contexts, Base 2 and Base 3.
  - LDAP 2 has the primary base context DN set to PrimaryBase2 and two additional base contexts, Base 4 and Base 5.

In this case, for a user that is in LDAP 1, Avaya Aura® Device Services only searches for groups in PrimaryBase1, Base 2, and Base 3.

Note:

The authentication domain is an enterprise directory with the **Use for authentication** check box selected. If a user belongs to an authentication domain and a group that is not in the authentication domain, the Dynamic Configuration service still works correctly.

- **User:** Platform, exception, and System Manager settings can override user settings. These settings are only used for Avaya IX™ Workplace Client.
- **Platform:** Exception and System Manager settings can override platform settings. These settings are only used for Avaya IX™ Workplace Client.
- **Exception:** Exception settings are specific to the System Manager Home location. These settings are only used for Avaya IX™ Workplace Client.
- **Phone model:** The phone model settings are specific to Avaya Vantage™ endpoints, Avaya J100 Series IP Phones, and 9600 Series IP Deskphones.

Conflicting group names

Do not publish group settings to LDAP groups if there are users that belong to more than one group. Otherwise, a conflict occurs where the same setting is in two different groups with different values. In this case, Avaya Aura® Device Services must choose one value to return and the mechanism used is based on the ASCII ordering of group names, which could result in users getting the wrong value assigned to them for conflicting settings.

When there is a conflict between two group names, Avaya Aura® Device Services does the following to determine which group name to choose:

1. Finds the first character in the group names that differ.

   This check is case-sensitive.

2. Determines the unicode decimal representation of the characters.

   Avaya Aura® Device Services chooses the group name where the character with a unicode decimal representation is the smallest.

When there is a conflict with more than two groups, Avaya Aura® Device Services uses the same algorithm, but it looks at additional characters.

For example, a company has the following LDAP groups:

- All Users
- HR
- Payroll
- atlanta
- 101_department

In this example, PHNLDLENGTH is published to both the 101_department and Payroll groups with a value of 7 and 11 respectively. Avaya Aura® Device Services returns the value 11 from the 101_department group. This is because the unicode decimal representation for the number 1 is 49, and the decimal representation for the capital letter P is 80.

The typical unicode representation flow is numbers (0 to 9) > capital letters > lowercase letters.

Conferencing settings

Avaya Aura® Device Services automatically discovers the following settings from the Avaya Equinox® Conferencing during Avaya IX™ Workplace Client deployment:

- CONFERENCE_FACTORY_URI
- CONFERENCE_PORTAL_URI
- UNIFIEDPORTALENABLED

You can override the values for these settings from the Avaya Aura® Device Services web administration portal with any fixed user, group, phone model, or platform value.

Related links

Adding a new enterprise LDAP server on page 103
Dynamic configuration setting priorities on page 155

Viewing the Home location in System Manager

About this task

When a user moves from one geographical location to another, the Home location settings help to identify the location of the user. When the IP address of the calling phone does not match the IP address pattern of any location, Session Manager uses the dial plan rules and Home location settings to complete the call. For more information about creating locations and dial patterns, see *Administering Avaya Aura® Session Manager*.

Use this procedure to find the Home location for a user.

Procedure

1. On the Home page of the System Manager web console, navigate to **User Management** > **Manage Users**.
2. Select a user and click **View**.
3. In the Communication Profile tab, click the arrow next to the **Session Manager Profile** section.

   The Home location is displayed in the Call Routing Settings section.

Dynamic configuration setting priorities

With dynamic configuration, different settings that are common at the user, group, platform, global, phone model, and exceptions levels have different priorities.

Avaya IX™ Workplace Client

For Avaya IX™ Workplace Client, if the same settings from different levels are applied to a user, the system overrides the settings in the following order:

- System Manager
- Exceptions
- Platform
- User
- Group
- Global
- Custom

For example, if a setting is specified at both the platform and group levels, the system overrides the value with the platform level settings.

Other endpoints and phones

For Avaya J100 Series IP Phones, 9600 Series IP Deskphones, and Avaya Vantage™ endpoints, if the same settings from different levels are applied to a user, the system overrides the settings in the following order:

- Phone Model
- Global

Assigning a group identifier to a phone model

About this task

You must assign a group identifier to each supported phone model so that phones can use Avaya Aura® Device Services automatic configuration functionality. The group identifier is used as a path parameter in a request a phone sends to Avaya Aura® Device Services or the Utility Server hosted on Avaya Aura® Device Services to obtain the `46xxsettings.txt` file. For example if you assign `123` to a phone model, then Avaya Aura® Device Services will generate `46xxsettings.txt` files for that model in the `/var/www/html/123/` directory.

Avaya Aura® Device Services does not generate `46xxsettings.txt` files for phone models that have no assigned group identifiers.

Note:

If you change the group identifier for a specific phone model, Avaya Aura® Device Services automatically does the following:

- Creates a new `46xxsettings.txt` file for that phone model in the new directory.
- Removes the `46xxsettings.txt` file from the previous directory.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Device Settings**.
2. In the **Group ID** filed, provide a unique identifier for each phone model.

   A group identifier must be an integer between 0 to 999.
3. Click **Save**.

Adding a new platform

About this task

Avaya Aura® Device Services provides the following pre-defined platform types for which you can publish configuration settings:

- Android
- iOS
- Mac
- Avaya Vantage™
- Windows

If you want to use the dynamic configuration service for clients on another platform, use this procedure to add the platform to Avaya Aura® Device Services.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Configure Platforms**.

   Avaya Aura® Device Services displays a list of available platforms.
2. Click **Add**.
3. In **Platform Name**, provide a name for your platform.
4. In **User Agent Identifier**, provide an entry that Avaya Aura® Device Services will use to identify the client platform.

   The entry must comply with the following requirements:

   - The entry must be part of the User Agent request header that the client platform sends to Avaya Aura® Device Services using Auto Config API.
   - The entry must be unique.
   - The entry must not be part of a User Agent request header of any other client.
   - The entry must not be part or must not contain **User Agent Identifier** configured for any other platform.

- The entry must not be part or must not contain the name of a pre-defined platform.

If you leave **User Agent Identifier** blank, Avaya Aura® Device Services will use the value that you provided in **Platform Name** as the user agent identifier.

5. Click **Save**.

Deleting a platform

About this task

Use this procedure to delete a platform that you added. You cannot delete pre-defined platforms.

When you delete a custom platform, Avaya Aura® Device Services also deletes all settings published for this platform.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Configure Platforms**.
2. Navigate to the platform you want to delete.
3. Select the check box to the left of the platform name.
4. Click **Delete**.

Creating a new configuration

About this task

Use this procedure to create a new configuration for users, groups, phone models, or platforms. You can also create a new configuration for exceptions, such as settings specific to System Manager.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Configuration**.
2. In the User, Group, Platform, Global, Phone Model, and Exceptions sections, specify the required settings.

   In the Global section, you can use the **New**, **Edit**, and **Remove** buttons to define custom attributes with a default value, description, and validation template.
3. Click **Save**.
4. In the Save Configuration window, select **Create new configuration** and type a name for the specified configuration.
5. Click **Save**.

You can view the saved configuration from the **Configuration** drop-down list.

Configuration field descriptions

Name	Description
Search Criteria	
Configuration	Displays the **USER**, **Group**, **Platform**, **Global**, and **Exceptions** settings for the selected configuration.
User	Displays the **Settings configured on SMGR**, **USER**, **Group**, **Platform**, **Global**, and **Exceptions** settings for the user.
Group	Displays the **Group**, **Platform**, and **Global** settings for the selected group.
Phone Model	Displays the **Phone Model** and **Global** settings for the selected phone model.
Platform	Specifies a platform to retrieve the data. • ACML • Android • iOS • Mac • Vantage • Windows • Other platforms defined by you
USER, **Group**, **Platform**, **Global**, **Phone Model**, and **Exceptions**	
Search	Searches the setting name from the list of settings for the typed search string.
Include	Includes or excludes the setting.
Setting	Displays a list of settings.
Value	Specifies the value that is assigned to a setting.
Discovered	The system displays this section for the users. Displays the read-only settings. To edit the values, go to the SMGR configuration.

Button	Description
Retrieve	Retrieves the settings based on the search criteria.
Save	Saves a new configuration and overwrites an existing configuration.
Test	Provides a test URL to test the configuration settings.

Button	Description
Publish	Publishes the configuration settings.
Reset	Discards any changes made on the page.
Delete	Deletes the existing configuration settings.
Import	Uploads configuration settings. You can: • Import a `46xxsettings.txt` file. • Perform a bulk import. • Import dynamic configuration settings.

Link	Description
View Published Settings	Displays all the published settings for Global, Group, User, Platform, Phone Model, and Exceptions.

Configuration settings

The System Manager specific settings, such as, SIP_CONTROLLER_LIST, SIPDOMAIN, ESMSRVR, and PRESENCE_SERVER that are available in the **User**, **Group**, and **Global** settings sections are only for testing the Configuration settings.

Tip:

To view the details and associated values of each setting, hover your mouse over the icon that is beside the setting name.

Avaya IX™ Workplace Client does not support the following settings, but they can be used by other clients:

- CONFIG_SERVER
- CONFIG_SERVER_SECURE_MODE
- ENABLE_PRESENCE

For detailed information about configuration settings, see *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*.

Password masking

For security reasons, Avaya Aura® Device Services does not display the actual values for configuration settings that represent passwords. Avaya Aura® Device Services hides the values for the following settings:

- SIPPASSWORD
- SSOPASSWORD

- ESMPASSWORD
- ACSPASSWORD
- CESPASSWORD
- DIRPASSWORD
- PKCS12PASSWORD
- SCEPPASSWORD
- EWSPASSWORD
- UNIFIED_PORTAL_PASSWORD
- ADMIN_PASSWORD
- AGENT_PASSWORD
- FORCE_SIP_PASSWORD
- SIPHA1
- CESVMPIN
- Any custom parameters that are used as passwords.

After you set the values for these settings and save the configuration, Avaya Aura® Device Services displays the special value ********** both on the web administration portal and in the browser developer or inspect view.

In search results, Avaya Aura® Device Services displays password type settings as follows:

- If a setting is editable, then Avaya Aura® Device Services does not display a specific value. If you want to save or publish a configuration, you must set the actual values for the required password type settings. Avaya Aura® Device Services notifies you about this by displaying a warning message at the top of the Configuration page.
- If a setting is not editable, then Avaya Aura® Device Services displays the special value **********. Non-editable settings are auto-discovered from other sources. Avaya Aura® Device Services displays these settings on the Discovered tab when you search settings for a user.

Avaya Aura® Device Services specific parameters

The following table lists Avaya Aura® Device Services specific configuration parameters. For detailed information about other configuration settings, see *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*.

SIP parameters

Name	Description	Avaya IX™ Workplace Client platform support
COMM_ADDR_HANDLE_TYPE	A virtual configuration setting that defines the SIP handle subtype for the user. The SIP handle subtype setting is used to select the correct SIP handle for the Avaya Aura® System Manager users. Avaya Aura® Device Services does not send virtual settings to endpoints, and these settings are for the Dynamic Configuration service internal usage only. AutoConfig Service does not respond with SIPUSERNAME and SIPDOMAIN if COMM_ADDR_HANDLE_TYPE is not configured. The options are: • Avaya SIP: Only numeric SIP handles of subtype Avaya SIP are retrieved from System Manager. The system ignores all other alphanumeric SIP handles of Avaya SIP subtype. • Avaya E.164: Maximum 15 digits and a plus (+) prefix are retrieved from System Manager. • Blank: The system rejects the blank value.	Supported only on Avaya Aura® Device Services.
COMM_ADDR_HANDLE_LENGTH	The parameter that indicates the required length of the Avaya SIP handle for the user. This field is mandatory if you select Avaya SIP for COMM_ADDR_HANDLE_TYPE. The valid value is a positive integer number that contains up to 255 digits. For example, 2000 is a valid value because it contains four digits, which is less than 255.	Supported only on Avaya Aura® Device Services.

Overwriting an existing configuration

About this task

You can overwrite an existing configuration that can be applied to the following: a user, a group, a platform, a phone model, exceptions, and all users.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Configuration**.
2. In the **User**, **Group**, **Platform**, **Global**, **Phone Model**, or **Exceptions** fields, specify the settings.

   Note:

   You cannot set the special value `**********` for password type configuration settings when overwriting an existing configuration. If you enter `**********`, Avaya Aura® Device Services does *not* consider the value changed.
3. Click **Save**.
4. In the Save Configuration window, select **Overwrite existing configuration** and select an existing configuration.
5. Click **Save**.

   Avaya Aura® Device Services overwrites the configuration settings to an existing configuration.

Testing configuration settings

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Configuration**.
2. In the **Configuration** field, select a saved configuration.
3. Click **Test**.

   Avaya Aura® Device Services displays the Test Settings window.
4. Copy the URL from the **Test URL** field and paste in a browser to view the changed settings.

   You must use the administrator credentials to view the settings.

   Avaya Aura® Device Services does *not* hide values of configuration settings that represent passwords.
5. Click **OK** to close the Test Settings window.

Publishing the configuration settings

About this task

Publish the configuration settings to override the user settings for the specified user, the group settings for the specified group, the platform settings for the specified platform, the phone model settings for the specified model, or all global settings specified.

After publishing the endpoint settings, Avaya Aura® Device Services generates a new `46xxsettings.txt` file for the selected endpoint series and stores this file on the Utility Server. The file is stored in the `/var/www/html/<endpoint group ID>/` directory, where `<endpoint group ID>` is the group identifier assigned to the endpoint model. If you publish Global settings, then Avaya Aura® Device Services generates new `46xxsettings.txt` files for all supported endpoint series.

If you change the group identifier assigned to an endpoint model, Avaya Aura® Device Services automatically generates a new `46xxsettings.txt` file in the `/var/www/html/<new endpoint group ID>/` directory.

Important:

- If the Utility Server is disabled, Avaya Aura® Device Services will not generate `46xxsettings.txt` files after publishing Global or Phone Model settings.
- Avaya Aura® Device Services cannot generate `46xxsettings.txt` files that contain conditionals, such as `IF` or `GOTO` commands. If you want to use a `46xxsettings.txt` file that contains conditionals, you must manually upload it to the Utility Server. For more information, see Uploading settings files to the Utility Server on page 143.
- If you change the Default Configuration parameters, such as Lock settings, Obscure lock settings, or Split Horizon DNS mapping, you need to republish the Global and Phone Model settings to include these changes to `46xxsettings.txt` files.

Before you begin

- If you are publishing Phone Model endpoint settings, make sure that a group identifier is assigned to the required endpoint series on the Device Settings page. Otherwise, Avaya Aura® Device Services does not generate the `46xxsettings.txt` file for the selected endpoint series and displays an error message.

  Note:

  If you are publishing Global settings, Avaya Aura® Device Services generates `46xxsettings.txt` files for endpoints with assigned group identifiers only, but does not display any warning messages.

- Test configuration settings before publishing them. For more information, see Testing configuration settings on page 163.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Configuration**.
2. In the **Configuration** field, select a saved configuration.

3. At the bottom of the page, click **Publish**.

   Avaya Aura® Device Services displays the Publish/Delete Settings window.

4. To apply the user settings to a user, select the **User settings will be applied to user** check box and type the name of the user.
5. To apply the group settings to a group, select the **Group settings will be applied to group** check box and from the drop-down list, select the name of the group.
6. To apply the platform settings to a platform, select the **Platform settings will be applied to** check box and from the drop-down list, select the name of the platform.
7. To apply the exception settings, select the **Exceptions will be applied to** check box and from the **Condition** field, click **Home Location**, and from the adjacent field select the location.
8. To apply the endpoint settings to specific endpoint series, select the **Phone model settings will be applied to** check box and from the drop-down list, select the required endpoint series.
9. To apply the global settings to all users, select the **Global settings will be applied to all users** check box.
10. Click **Publish**.

    Based on the publishing settings, Avaya Aura® Device Services applies the settings.

Related links

Uploading settings files to the Utility Server on page 143
Administration of the Dynamic Configuration service on page 153

Viewing published settings

About this task

Use this procedure to view all the published settings for Global, Group, User, Platform, Phone Model, and Exceptions. You can also delete these settings from the View Published Settings page.

For password type configuration settings, Avaya Aura® Device Services displays the special value **********.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Configuration**.
2. Click **View Published Settings**.
3. On the View Published Settings page, from the **Select a Category** list, click one of the following options:
   - All

- Group
- User
- Platform
- Phone Model
- Exceptions

4. To view published settings for a specific group, user, platform, phone model, and exception, select the required value from the list.

   For example, select **Group Name** to view the published settings for a specific group.

   You can see the setting name, value of the setting, category, and category value for the selected criteria.

5. To unpublish settings, select the published setting you want to unpublish, and click **Delete Settings**.

Retrieving configuration settings for a user

About this task

Use this procedure to retrieve the configuration settings of a user using the Avaya Aura® Device Services configuration options. If the settings of that user were never changed or published, Avaya Aura® Device Services displays a message `Settings not found` in the **Group**, **Platform**, and **Global** settings sections. But you can change the settings of that user by editing and publishing the user settings of another configured user or another Test Configuration.

For example: user1@xyz.com is configured and the administrator wants to update all usernames of user2@xyz.com and publish these settings for user2@xyz.com. The administrator can select the configuration settings of user1@xyz.com and publish these settings for user2@xyz.com.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration** > **Configuration**.
2. In the **Search Criteria** section, do the following:
   a. Click the **User** check box, and type the name of the user.
   b. In the **Platform** field, click the appropriate platform.
   c. Click **Retrieve**.

      Avaya Aura® Device Services displays the configuration settings of the user.

Import of dynamic configuration settings

Importing dynamic configuration settings using a file in the JSON format

About this task

Use the following procedures to import configuration settings that are not currently available in Avaya Aura® Device Services. You can perform this task if you need Avaya IX™ Workplace Client client features with new configuration parameters.

Before you begin

- Download and use the additional parameter settings file from PLDS. Ensure that the settings file has the `.txt` extension and that it is in the JSON format. For example, `dynamicConfigUpload.txt`.
- If you are planning to import configuration settings that represent passwords, ensure that you:
  - Set the data type to “String” for all these settings. Settings that belong to the “PASSWORD” category do not support other data types.
  - Set the “category” attribute to “PASSWORD” for all these settings.

    Note:

    The “category” attribute is only required for settings that represent passwords. “PASSWORD” is the only supported value for this attribute.

For more information about the JSON file structure, see JSON file structure on page 167.

Procedure

1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, click **Dynamic Configuration** > **Configuration**.
2. On the Configuration page, click **Import**.
3. On the Import dynamic configuration settings page, in the **Select type of import** field, select **Import dynamic settings**.
4. Click **Browse** and select the settings file that you want to import.
5. Click **Import**.

   The new setting is added to the existing test configuration at all levels. You can now publish the setting to the required category (Group, User, Platform, Global, Phone Model, or Exception).

JSON file structure

The following table shows attributes that are used in a JSON file to describe dynamic configuration settings:

Attribute	Description
name	The name of the setting.
description	The description of the setting. Avaya Aura® Device Services displays the description when you hover your mouse over the setting name. If you do not want to provide a description for the setting, set description to "".
type	The data type of the setting. Settings that represent passwords must have the “String” type.
default_value	The default value of the setting. If you do not want to provide a default value, set default_value to "".
version	The version of the setting. The default version for settings available on Avaya Aura® Device Services. Therefore, you must set the version value for any setting that you import to Avaya Aura® Device Services as follows: • Less than 100 if the setting is introduced as a new setting. • More that 100 if the setting overwrites any existing setting. The version value must be higher than the values used in previous imports.
category	The attribute that indicates that the setting represents a password. Avaya Aura® Device Services hides the actual values of these settings on the Avaya Aura® Device Services web administration portal. For settings that represent passwords, you must include this attribute and set it to “PASSWORD”. Do not use this attribute for other settings.

The following example shows a JSON file containing the following two settings:

- DYNAMIC_SETTING_PASSWORD: Configuration setting that represents a password.
- DYNAMIC_SETTING_NON_PASSWORD: Non-password configuration settings.

```
{
    "settings": [
    {
        "name": "DYNAMIC_SETTING_PASSWORD",
        "description": "This is a setting that is used as a password.",
        "type": "String",
        "default_value": "password12345",
        "version": "2",
        "category":"PASSWORD"
    },
    {
        "name": "DYNAMIC_SETTING_NON_PASSWORD",
        "description": "This is a non-password setting of integrer type.",
        "type": "Integer",
```

```
        "default_value": "8443",
        "version": "50",
    }
    ]
}
```

Importing parameter values from a 46xxsettings.txt file

About this task

Use this procedure to update the dynamic configuration parameter values stored on Avaya Aura® Device Services with the values from the imported `46xxsettings.txt` file. You can choose the settings category that will use these values.

Procedure

1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, navigate to **Dynamic Configuration** > **Configuration** .
2. On the Configuration page, click **Import**.
3. On the Import dynamic configuration settings page, in the **Select type of import** field, select **Import 46xxsettings file**.
4. Click **Browse** and select the file that you want to import.
5. Click **Import**.

   Avaya Aura® Device Services imports the values and displays the results of the import. You can then save or publish the imported values.

Bulk imports

You can add dynamic configuration settings in bulk. You can either import a file from the local system or specify the settings manually. Each setting must be added as a separate line and must be in the following format: `{CATEGORY};{SUB-CATEGORY};{SETTING_NAME};{SETTING_VALUE}`.

The following table describes bulk settings that you can use:

Settings	Description
CATEGORY	The high-level category to which the particular setting belongs. The categories are: • USER • GLOBAL • GROUP • PLATFORM

Settings	Description
	• PHONEMODEL • EXCEPTION
{SUB-CATEGORY}	The name or ID of the particular object (user ID, group name, or platform name) for which the setting value will be inserted, updated, or deleted. • For the GROUP category, the subcategory is a group name. You can retrieve the group name from LDAP Server. For example: `GROUP;Group 1;SUPPORTEMAIL;admin@mysite.com` • For the USER category, the subcategory is a user name. The setting name is `ESMUSERNAME`. For example: `USER;user1@mysite.com;CESUSERNAME;user1@mysite.com` • For the PLATFORM category, the subcategory is a platform name. The options are Mac, Windows, Android, and iOS. For example: `PLATFORM;Windows;APPCAST_URL;https://appcast.mysite.com` • For the PHONEMODEL category, the subcategory is a phone model. The options are J1XX, Vantage, and 96XX. For example: `PHONEMODEL;J1XX;ADMIN_CHOICE_RINGTONE;Default` • For the GLOBAL category, there is no subcategory. The format is: `{CATEGORY};{SETTING_NAME};{SETTING_VALUE}` For example: `GLOBAL;CESSECURE;1` • For the EXCEPTION category, the format is: `{CATEGORY};{SOURCE};{EXCEPTION_CONDITION_NAME};{EXCEPTION_CONDITION_VALUE};{SETTING_NAME};{SETTING_VALUE}`. Where: - `{SOURCE}` is System Manager. - `{EXCEPTION_CONDITION_NAME}` is the Home location. - `{EXCEPTION_CONDITION_VALUE}` is the location name. - `{SETTING_NAME}` is the name of the setting. - `{SETTING_VALUE}` is the value of the setting. For example: `EXCEPTION;SMGR;Home Location;location 1;PHNLDLENGTH;5`
Tip: To delete a setting from the configuration service, append `DELETE` instead of `{SETTING_VALUE}`.	

Settings	Description
For example: `USER;user1@mysite.com;CESUSERNAME;DELETE`	

Supported characters for bulk import

In the bulk import file, you can use the majority of special characters as is. The following are the exceptions:

- To use a semicolon (;), enclose the entire attribute containing a semicolon with quotation marks.

  For example, if you have a group with the name `SEMICOLON;GROUP`, use the following: `GROUP;"SEMICOLON;GROUP";PARAMETER_NAME;parameter_value`

- To use a backslash (\), prepend it with three backslash characters as follows: `\\\\`

  For example, if you have a group with the name `BACKSLASH\`, use the following: `GROUP;BACKSLASH\\\\;PARAMETER_NAME;parameter_value`

- To use quotation marks ("), prepend them with three backslash characters as follows: `\\\"`

  For example, if you have a group with the name `QUOTATION_MARKS"`, use the following: `GROUP;QUOTATION_MARKS\\\";PARAMETER_NAME;parameter_value`

- To use the pound sign (#), prepend it with two backslash characters as follows: `\\#`

  For example, if you have a group with the name `GROUP_WITH_NUMBER_SIGN#`, use the following:

  `GROUP;GROUP_WITH_NUMBER_SIGN\\#;PARAMETER_NAME;parameter_value`

Importing configuration settings using the bulk import process

Before you begin

If you are importing a `.csv` file created using Microsoft Excel, ensure that the file does not contain any additional characters. To do so, open the file in any other text editor. For example, if you add the string `GROUP;ADMINISTRATORS;SIP_CONTROLLER_LIST;"127.0.0.1:5061;transport=TLS"` using Microsoft Excel and then open the file in a text editor, you will see that the string now contains some additional quotation marks: `"GROUP;ADMINISTRATORS;SIP_CONTROLLER_LIST;""10.255.249.144:5061;transport=TLS"""`. You must remove any additional characters. Otherwise, bulk import will fail.

Procedure

1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, navigate to **Dynamic Configuration** > **Configuration**.
2. On the Import dynamic configuration settings page, in the **Select type of import** field, select **Bulk Import**.

3. To import the settings, do one of the following:
   - In the text box, type the required entry on each line in the following format and click **Import**.

     ```
     {CATEGORY}
     ;
     {SUB-CATEGORY}
     ;
     {SETTING_NAME}
     ;
     {SETTING_VALUE}
     ```

   - Click **Browse** to select a file from the local system and click **Import**.

     The file must be in either the `.csv` or `.txt` format.

   Avaya Aura® Device Services displays the import status at the top of the page.

   When the import is successful, Avaya Aura® Device Services displays a message with the date and time of starting and completing the import. For example: `Bulk Import is completed. Started at 2015-12-30 01:01:48. Completed at 2015 -12-30 01:01:49`

   When the import fails, Avaya Aura® Device Services displays a message with the reason of the import failure and the List of errors table that has the String number, String, and Error description columns. For example: `Bulk Import failed. Reason: Input data validation failed.`

Bulk Import field descriptions

Name	Description
Bulk Import Text Box	Specifies the dynamic configuration settings in each line. You can either import a file from the local system by using the **Browse** button or specify the settings manually in this text box. This text box is expandable to add multiple configuration settings.

Button	Description
Browse	Enables you to select a file in the `.csv` format for importing the bulk configuration settings.
Import	Imports the added entry or the file and displays the status at the top of the page. When an import action is already in progress and you try to attempt a new bulk import, the system displays the message: `Bulk Import is already in progress.`
Status	Displays the bulk import status.
Reset	Resets the added entry and clears the text box.

Managing automatic logging in to Avaya clients

About this task

Use this procedure to allow or disallow users to log in to their devices using passwords stored on Avaya Aura® Device Services.

If this feature is enabled, then the following settings are sent in Dynamic Configuration responses:

- SIPHA1
- SIPPASSWORD
- AGENT_PASSWORD

Avaya clients use these SIP credentials for unified login.

Note:

This feature does not apply to other password settings.

Before you begin

If you are planning to send SIPHA1, SIPPASSWORD, or AGENT_PASSWORD in Dynamic Configuration responses, ensure that these settings are published. Dynamic Configuration responses do not contain not published settings. For more information, see Publishing the configuration settings on page 164.

Procedure

1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, navigate to **Dynamic Configuration** > **Default** .
2. Do one of the following:
   - Select the **Allow passwords** check box to send the settings in Dynamic Configuration responses.
   - Clear the **Allow passwords** check box to disable sending the settings in Dynamic Configuration responses.
3. Click **Save**.

Administering the default configuration

About this task

You can maintain internal Dynamic Configuration parameters using the Default page.

Note:

If you are using automatic configuration to provide `46xxsettings.txt` files to endpoints, you must republish the Group and Phone Model settings after updating the default

configuration settings. Otherwise, `46xxsettings.txt` files will not contain the updated configuration parameters.

Procedure

1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, navigate to **Dynamic Configuration** > **Default**.
2. Modify the default configuration settings.
3. Click **Save**.

Defaults field descriptions

Name	Description
Allow passwords	Specifies that the user can log in to the device with the stored password on the server. • If you select the check box, the Dynamic Configuration response contains the SIPHA1, SIPPASSWORD, and AGENT_PASSWORD settings. Avaya clients use these SIP credentials for unified login. **Note:** If the **Allow passwords** check box is selected but the settings are not published, then the Dynamic Configuration response will not contain these settings. For more information about publishing settings, see Publishing the configuration settings on page 164. • If you clear the check box, the Dynamic Configuration response does not contain the SIPHA1, SIPPASSWORD, and AGENT_PASSWORD settings.
Lock Settings	Specifies that the administrator can lock the attributes. The system displays the locked attributes on the client, but the user cannot edit locked attributes. In the Dynamic Configuration response, the system always displays the LOCKED_PREFERENCES settings that contain the settings that are specified for the user. When you select the **Lock Settings** check box, the system displays the **Obscure locked settings** check box.

Name	Description
Obscure locked settings	Specifies that the all log setting will also be included in the OBSCURE_PREFERENCES setting in the Dynamic Configuration service output. • If you select the check box, you can view the obscured settings (OBSCURE_PREFERENCES) in the Dynamic Configuration response. The value of OBSCURE_PREFERENCES and LOCKED_PREFERENCES are the same. • If you clear the check box, the system hides the obscured settings (OBSCURE_PREFERENCES) in the Dynamic Configuration response.

Button	Description
Save	Saves the default configuration settings.
Cancel	Resets any changes made on the page.

Split Horizon DNS mapping

With Split Horizon DNS mapping, clients can be supported inside and outside the firewall of an enterprise.

The Dynamic Configuration service output contains different settings, such as, ESMSRVR, CESSRVR, DIRSRVR, SIP_CONTROLLER_LIST, CONFERENCE_PARTICIPANT_URL, APPCAST_URL. These settings can contain IP addresses. To replace the IP addresses with appropriate FQDNs for these settings in the Dynamic Configuration service output, enable the Split Horizon DNS mapping feature.

Note:

If you are using automatic configuration to provide `46xxsettings.txt` files to endpoints, you must republish the Group and Phone Model settings after updating Split Horizon DNS mapping. Otherwise, `46xxsettings.txt` files will not contain the updated configuration parameters.

Example

For example, a Presence server is located internally in an enterprise network and also has Network Address Translation (NAT) access from outside the enterprise using the internet. In this case, there will be two Presence server IP addresses for the clients.

For the Presence server, the internal IP address is 190.160.10.1 and external IP address is 90.165.14.11:

- On the Configurations page, you can use any of these two IP addresses as the value for the PRESENCE_SERVER setting.

- FQDN of the Presence server is *pserver1.avaya.com*.

To configure Split Horizon DNS mapping, you need to map the Presence server IP address to the Presence server FQDN. When you enable Split Horizon DNS mapping, the internal and external clients receive the PRESENCE_SERVER setting with the same value (FQDN): pserver1.avaya.com.

Mapping the IP address to the FQDN

About this task

Use this procedure to map the IP address to the FQDN so that the client can connect with the servers or URLs inside and outside the enterprise firewall.

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Dynamic Configuration** > **DNS Mapping**.

   Avaya Aura® Device Services displays the Split Horizon DNS Mapping page.
3. Click **Add**.

   Avaya Aura® Device Services displays a new row to add the IP address and FQDN.
4. In the **IP address** field, type the IP address of the server or URL to which the client will connect.
5. In the **Fully Qualified Domain Name** field, type the FQDN of the server or URL to which the client will connect.
6. Click **Save**.

Enabling Split Horizon DNS mapping

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Dynamic Configuration** > **DNS Mapping**.

   Avaya Aura® Device Services displays the Split Horizon DNS Mapping page.
3. Select the **Enable Split Horizon DNS Mappings** check box.

Split Horizon DNS Mapping field descriptions

Name	Description
Search	Searches the values from the list of entries for the typed search string.

Name	Description
IP Address	Specifies the IP address of the different servers or URLs to which the client will connect.
Fully Qualified Domain Name	Specifies the fully qualified domain name of the different servers or URLs to which the client will connect.

Button	Description
Add	Displays a row to specify the IP address and FQDN of the different servers or URLs to which the client will connect.
Save	Saves the added row entry.
Cancel	Discards any changes made on the page.

Chapter 11: Integrated Windows Authentication administration and management

Integrated Windows Authentication (IWA) enables you to log in to different services with the same credentials. To support IWA, some Avaya Aura® Device Services server administration is required. Users must be able to authenticate to the Avaya Aura® Device Services API using a preexisting authentication to a Windows domain. Avaya Aura® Device Services uses SPNEGO to negotiate authentication with the client and Kerberos to validate the authentication of the client user. User roles are retrieved normally through LDAP.

Use the following sections to complete IWA configuration on the Avaya Aura® Device Services and Active Directory servers. Errors in the setup might cause the authentication to fail. You can enable debug logs to assist with troubleshooting.

Note:

IWA is only supported if you are using a single authentication directory. The domain of the User Principal Name (UPN) and the authentication domain must be the same as the root domain of the directory. If you are using multiple authentication directories, IWA is disabled.

Authentication prerequisites

You must have the following to set up IWA:

- An Active Directory server.
- A DNS server for the DNS domain of Active Directory.

  For information about setting up the DNS server, see *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*.
- A Windows client on the Active Directory domain.
- An Avaya Aura® Device Services server that is resolvable by the DNS.
- A domain user that will be mapped to the Service Principal Name (SPN) of the Avaya Aura® Device Services server.
- Domain users for all individual users.

- Only a single authentication domain is supported and all users must be in the same domain.
- The sAMAccountName attribute must match the user name part of the userPrincipalName attribute.

  For example, if the sAMAccountName is jdoe, then the userPrincipalName must use the following format: jdoe@<*domain.name*>.
- To log in to a computer, the user must enter the user name part of the userPrincipalName configured for that user. The domain must also match the domain part of that user userPrincipalName. The user login name format is `<user name>\<domain>`.

  For example, if the user has the “jdoe@avaya.com” userPrincipalName, where “avaya” is the domain and “jdoe” is the user name, then the user logs in to a computer using the “avaya \jdoe” account.

Important:

- Do not change the userPrincipalName attribute configured for the user. If you change the userPrincipalName after IWA is configured, IWA will not work.
- The Active Directory, Windows client, and Avaya Aura® Device Services server must resolve each other’s FQDNs. However, they do not need to use the same DNS server or belong to the same zone.

Setting up the Windows Domain Controller

About this task

Use this procedure to add the Avaya Aura® Device Services SPN to a domain user on the Windows Domain Controller or the Active Directory server. The SPN must be unique across the domain. To avoid issues with duplicated SPNs, keep track of any SPNs assigned to users.

For detailed information about Domain Controller users, see https://technet.microsoft.com/en-us/library/cc786438(v=ws.10).aspx.

Important:

Enter all commands exactly as shown in this procedure, and use the following guidelines:

- The host name used to access the Tomcat server must match the host name in the SPN exactly. Otherwise, authentication will fail.
- The server must be part of the local trusted intranet for the client.
- The SPN must be formatted as `HTTP/<host name>` and must be exactly the same everywhere.
- The port number must not be included in the SPN.
- Only one SPN must be mapped to a domain user.
- The Kerberos realm is always the uppercase equivalent of the DNS domain name. For example, `EXAMPLE.COM`.

Procedure

1. Create a new IWA service account.

   Do not select an account associated with an existing user.

2. If you are using Active Directory 2008 or higher, run the following command to attach the SPN to the domain name:

   `setspn -S HTTPS/<FRONT-END FQDN> <Domain user login>`

   In the following example, `<FRONT-END FQDN>` is `aads.example.com` and `<Domain user login>` is `aads_spn_user`:

   ```
   setspn -S HTTP/aads.example.com aads_spn_user
   ```

   Important:

   - If you are using Active Directory 2003, you must use `setspn -A` instead of `setspn -S`.
   - When you use `setspn -S`, the Active Directory server searches for other users with the same SPN assigned. If the server finds a duplicated SPN, see step 3 on page 180.

3. **(Optional)** To remove a duplicated SPN from another user, run the following command:

   `setspn -d <SPN> <old user>`

4. Run one of the following commands to generate a `tomcat.keytab` file:

   - If FIPS is disabled on Avaya Aura® Device Services, run the following command:

     `ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /princ HTTP/<FRONT-END FQDN>@<Kerberos realm> /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto all /kvno 0`

   - If FIPS is enabled on Avaya Aura® Device Services, run the following command:

     `ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /princ HTTP/<FRONT-END FQDN>@<Kerberos realm> /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto <Encryption Type> /kvno 0`

     Where *<Encryption Type>* can be one of the following:

     - `AES256-SHA1`: If you want to use the AES256-SHA1 encryption type.
     - `AES128-SHA1`: If you want to use the AES128-SHA1 encryption type.

     The encryption type must correspond the encryption type configured for the domain user that is mapped to the Avaya Aura® Device Services SPN. For more information, see Enabling encryption for the domain user on page 182.

     AES256–SHA1 is the preferred encryption type.

The following example displays the command for generating a keytab file in FIPS mode. In this example, `<Domain User Login>` is `aads_spn_user`, `<Kerberos realm>` is `EXAMPLE.COM`, and `<FRONT—END FQDN>` is `aads.example.com`.

```
ktpass /out c:\tomcat.keytab /mapuser aads_spn_user@EXAMPLE.COM /princ HTTP/
aads.example.com@EXAMPLE.COM /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto
AES256-SHA1 /kvno 0
```

5. Transfer the generated `tomcat.keytab` file to the Avaya Aura® Device Services server using the OAMP administration portal.

   Since this is a credentials file, handle it securely and delete the original file after this file is imported into the Avaya Aura® Device Services server. You can generate and re-import a new `tomcat.keytab` file anytime.

Next steps

- If you are using FIPS, enable AES encryption for the domain user as described in Enabling encryption for the domain user on page 182.
- Set up IWA on Avaya Aura® Device Services as described in Setting up IWA on the Avaya Aura Device Services administration portal on page 182.

Related links

Enabling encryption for the domain user on page 182

Windows Domain Controller command descriptions

Setting up the Windows Domain Controller on page 179 uses the following command values:

Command	Description	Example value
<FRONT—END FQDN>	The REST front host FQDN of the Avaya Aura® Device Services server. This is either the FQDN of the Virtual IP assigned to the cluster (if internal load balancing is used) or the FQDN of the external load balancer, if it is used.	`aads.example.com`
<Domain user login>	The Windows login ID for the domain user you created.	`aads_spn_user`
<Kerberos realm>	The domain name for the Kerberos realm. The Kerberos realm is always the uppercase equivalent of the DNS domain name.	`EXAMPLE.COM`

Enabling encryption for the domain user

About this task

In FIPS mode, Kerberos uses Advanced Encryption Standard (AES). By default, support for Kerberos AES authentication is disabled for Active Directory users. Use this procedure to enable encryption support for the domain user that is mapped to the Avaya Aura® Device Services SPN.

This procedure is only required if FIPS is enabled on Avaya Aura® Device Services.

Before you begin

Generate a keytab file as described in Setting up the Windows Domain Controller on page 179.

Procedure

1. In Active Directory, select the domain user that is mapped to the Avaya Aura® Device Services SPN.

   For example: aads_spn_user.

2. Open the domain user properties.
3. Click the **Account** tab.
4. In the Account options area, do one of the following:
   - If you used the AES256–SHA1 encryption type when generating a keytab file, select the **This account supports Kerberos AES 256 bit encryption** check box.
   - If you used the AES128–SHA1 encryption type when generating a keytab file, select the **This account supports Kerberos AES 128 bit encryption** check box.
5. Click **OK**.

Related links

Setting up the Windows Domain Controller on page 179

Setting up IWA on the Avaya Aura® Device Services administration portal

About this task

This procedure describes the changes you must perform on the Avaya Aura® Device Services administration portal to configure IWA.

Procedure

1. On the Avaya Aura® Device Services administration portal, click **LDAP Configuration**.
2. In the Server Address and Credentials area, do the following:
   a. In the **Windows Authentication** drop-down menu, select **Negotiate**.

b. In the Confirm Action dialog box, click **OK**.

c. In **UID Attribute ID**, type `userPrincipalName`.

   If this field is not set to `userPrincipalName`, you might encounter license issues and other unpredictable behavior.

d. Ensure that the other settings are appropriate for the LDAP configuration of your Domain Controller.

   Important:

   The LDAP server that you use must be the domain controller with the appropriate Active Directory version as the server type.

3. In the Configuration for Windows Authentication area, complete the following information using the same values you provided when setting up the Windows Domain Controller:

   a. In **Service Principal Name (SPN)**, type `HTTP/<FRONT—END FQDN>`.

      For example, `HTTP/aads.example.com`.

   b. Click **Import** to import the `tomcat.keytab` file transferred from the Windows Domain Controller.

      In cluster deployments, the file is transferred to all nodes in the cluster. An additional option is available to send the file to specific nodes in a cluster.

   c. In **Kerberos Realm**, type the Kerberos realm, which is usually in all uppercase letters. For example, `EXAMPLE.COM`.

   d. In **DNS Domain**, type the DNS domain of the Domain Controller.

      For example, `example.com`.

   e. **(Optional)** Select the **Use SRV Record** check box.

   f. **(Optional)** If **Use SRV Record** is not selected, in **KDC FQDN**, type the FQDN of the Domain Controller.

      This value also includes the DNS domain at the end. For example, `ad.example.com`.

   g. **(Optional)** In **KDC Port**, retain the default value of 88.

      This field is only visible if **Use SRV Record** is not selected.

   h. **(Optional)** In a cluster deployment, click **Send Keytab File** to send the `tomcat.keytab` file you imported in step 3.b on page 183 to a specific node.

      This option is useful if the import to a node failed or if you add a new node to your cluster.

4. Click **Save** to retain the settings and restart the server.

   The settings that you updated are used to generate the files needed to configure the Tomcat JAASRealm and the corresponding Sun JAAS Login module for GSS Bind.

Chapter 12: AWS-specific management options

If you deployed Avaya Aura® Device Services in an Amazon Web Services (AWS) environment, use the following sections to perform AWS-specific management operations. You can perform these management operations anytime.

Updating an existing stack with a new CloudFormation template

About this task

You can apply changes to an existing CloudFormation stack by updating the stack with a newer CloudFormation template. Changes to the stack can include additional nodes, new resources, and new port configuration. The system updates all the objects contained in the stack to match the new settings. Existing EBS volumes and S3 buckets are preserved.

To update an existing single-node stack you must use a new single-node stack template. To update an existing cluster you must use a new multi-node stack template. If you are expanding a cluster, you must already have a cluster with two or more nodes. You cannot expand a single AWS node into an AWS cluster

Before you begin

Generate a new CloudFormation template that matches the application and profile of the existing system but includes the additional resources required. For more information, see the “Creating CloudFormation templates” section in *Deploying Avaya Aura® Device Services*.

Procedure

1. Sign in to the AWS console.
2. Navigate to **Services** > **Management Tools** > **CloudFormation**.
3. Select the stack to update.
4. Click **Actions** > **Update Stacks**.
5. Update the stack using the Update Stack pages.

   You can add an additional CIDR block when going from two to three subnets. Do not change the value of any other stack parameters.

Chapter 13: Security options

Configuring the data retention period

About this task

Log files and the Avaya Aura® Device Services Cassandra database contain private and sensitive user data. To maximize data privacy and security, you can specify how long you want to keep user data on Avaya Aura® Device Services. The default data retention period is 1 day.

Avaya Aura® Device Services encrypts log files that are older than the configured retention period, but it does not delete these logs.

When a user is deleted from data sources, such as the enterprise LDAP directory, iView, or System Manager, Avaya Aura® Device Services deletes the corresponding records for that user from the Cassandra database within the last hour before the configured retention period elapses. For example, if the retention period is one day and the user is just deleted from the LDAP directory, then Avaya Aura® Device Services removes the user information from the Cassandra database within the time range between 23 and 24 hours after the user is deleted from the LDAP directory.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Data Security** > **Data Retention**.
2. In **Retention time (days)**, set the period for which you want to keep user data on Avaya Aura® Device Services.

   The range is 1 to 30 days.
3. Click **Save**.

Related links

Data retention on page 24
Log management on page 204

Data encryption management

When you deploy the Avaya Aura® Device Services OVA, you can enable data encryption and configure basic settings, such as providing a passphrase or enabling the local key store. After

deploying the Avaya Aura® Device Services OVA, you can use system layer commands to perform additional data encryption management operations, such as the following:

- Enabling a remote key server.
- Managing encryption passphrases.
- Reviewing data encryption status.

Important:

In AWS deployments, you enable data encryption on AWS itself. Therefore, you cannot use the system layer commands for disk encryption management in AWS deployments.

Related links

Data encryption commands on page 304

Remote key server management

When configuring data encryption during the OVA deployment, if you choose not to enter a passhrapse after every reboot, Avaya Aura® Device Services stores encryption keys in a local key store. To enhance security, you can set up a remote key server. You can add multiple remote key servers.

Enabling a remote key server

About this task

Use this procedure to use a remote key sever to store encryption keys.

When adding a remote key server for the first time, you can choose either to continue using the local key store or to disable it. When both the local key store and the remote key server are enabled at the same time, Avaya Aura® Device Services uses the local key store to decrypt the encrypted disks at boot time.

If you already have a remote key server enabled, you can use this procedure to add another remote key server.

Before you begin

Configure your remote key server. The exact configuration procedure depends on the key server you are using.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

   `sys encryptionRemoteKey add <server address> <port>`

   In this command:

   - `<server address>` is the IP address or FQDN of the remote key server.
   - `<port>` is a port that the remote key server uses to connect to Avaya Aura® Device Services. This is an optional value. If you do not enter a port number, the remote key server uses port 80 by default.

3. When prompted, enter the existing passphrase.
4. When prompted to remove the local key store, do one of the following:
   - To disable the local key store, enter `y`.
   - To continue using the local key store, enter `n`.

Disabling a remote key server

About this task

Use this procedure if you do not want to use a remote key server to store encryption keys. If you have multiple remote key stores, Avaya Aura® Device Services will continue using other remote key stores until you disable them.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

   `sys encryptionRemoteKey remove <server address>`

   In this command, `<server address>` is the IP address or FQDN of the remote key server you want to disable. You must use the same IP address or FQDN that you used when enabling the remote key server.

Passphrase management

Avaya Aura® Device Services requires an encryption passphrase to access encrypted partitions.

When enabling data encryption during the Avaya Aura® Device Services OVA deployment, you set up a single passhprase. After the OVA is deployed, you can use system layer commands to:

- Configure up to seven additional passhprases.
- Change existing passphrases.
- Remove a passphrase.
- View status of passphrases.

Adding a passphrase

About this task

Use this procedure to set up additonal passphrases. You can have up to seven passphrases in total. If you have multiple passphrases, you can use any of them to access encrypted disk partitions.

A passphrase you add must comply with the passphrase complexity rules.

Before you begin

Ensure that you have a passphrase slot available. For more information, see Reviewing the passphrase status on page 188.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionPassphrase add
   ```

3. When prompted, type one of the existing passphrases.
4. When prompted, type a new passphrase.
5. Type the new passphrase again to confirm it.

Passphrase complexity rules

All encryption passphrases you add to Avaya Aura® Device Services must contain at least:

- Eight characters.
- One character from each of the following character sets:
  - Uppercase letters: A to Z
  - Lowercase letters: a to z
  - Numerics: 0 to 9
  - Special characters

Related links

passwdrules command on page 303

Removing a passphrase

About this task

Use this task to remove an existing encryption passphrase.

Avaya Aura® Device Services requires at least one encryption passphrase. If you have only one passphrase, you cannot remove it.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionPassphrase remove
   ```

3. When prompted, type the encryption passphrase you want to remove.

Reviewing the passphrase status

About this task

Use this procedure to view information about the number of passphrases you have on Avaya Aura® Device Services.

Tip:

You can use this procedure before adding a new passphrase to see if Avaya Aura® Device Services has a free slot for a new passphrase.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionPassphrase list
   ```

   Avaya Aura® Device Services displays passphrase and slot assignment information.

   ```
   Slot        Status      Passphrase/Remote Server
   ------------------------------------------------
   Key Slot 0: ENABLED     Passphrase
   Key Slot 1: ENABLED     Passphrase
   Key Slot 2: ENABLED     Passphrase
   Key Slot 3: DISABLED    empty
   Key Slot 4: DISABLED    empty
   Key Slot 5: DISABLED    empty
   Key Slot 6: DISABLED    empty
   Key Slot 7: DISABLED    empty
   ```

Viewing data encryption status

About this task

Use this procedure to view information about data encryption, including the following:

- Whether data encryption is enabled.
- Whether the local key store is enabled.
- Whether the encryption passphrase must be entered after every reboot.
- Information about configured remote key servers.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the `sys encryptionStatus` command.

Local key store management

Enabling the local key store

About this task

If you do not want to enter an encryption passphrase after every Avaya Aura® Device Services reboot and you do not have a remote key server, you can enable the local key store. However, the local key store is less secure than a remote key store or entering a passphrase after every reboot.

You can enable the local key store even if a remote key server is enabled. When both the local key store and the remote key server are enabled at the same time, Avaya Aura® Device Services uses the local key store to decrypt the encrypted disks at boot time.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionLocalKey enable
   ```

3. When prompted, enter the encryption passphrase.

Disabling the local key store

About this task

When you disable the local key store and do not have a remote key server, you will need to enter your passphrase after every Avaya Aura® Device Services reboot. If at least one remote key server is confgured, then Avaya Aura® Device Services will use this remote key server to store encryption keys.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionLocalKey disable
   ```

Advanced Intrusion Detection Environment tool management

Advanced Intrusion Detection Environment (AIDE) is a tool for monitoring file system changes. AIDE creates a baseline database of system layer files and then verifies the integrity of the files by comparing the database to the actual state of the system layer files. AIDE only performs file integrity checks and does not provide other checks, such as rootkit searches.

On Avaya Aura® Device Services, you can manage AIDE using the **`fsit.sh`** system layer script, which is located in the `/opt/Avaya/bin` directory. The **`fsit.sh`** script is available after you deploy the Avaya Aura® Device Services OVA.

Avaya recommends that you run AIDE scanning at least once a week.

Creating a baseline database

About this task

Use this procedure to create a baseline database of operational system and Avaya Aura® Device Services files. AIDE uses this database as a reference when performing file system integrity scans.

You must create a database before you start running AIDE scans. Do *not* create a new database before each scan. Create a new baseline after you installed Avaya Aura® Device Services and then create a new baseline each time after you upgraded Avaya Aura® Device Services.

The database creation process can take up to 50 minutes depending on the system data.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **`fsit.sh`** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to create an AIDE database as a background process:

   ```
   sudo ./fsit.sh -updateDB &
   ```

   Creating the database as a background process enables you to perform other tasks at the same time.

Result

AIDE creates the baseline database and records the results in the `/var/log/aide/aide_update_status.log` file. If the database is created successfully, the log contains the `Completed` entry and a time stamp. Otherwise, the log contains the `Failed` entry. You can view the log file content using the **`cat`** command.

The following is an example of the **`cat`** command output when the baseline database is created successfully.

```
[admin@aads68 bin]$ sudo cat /var/log/aide/aide_update_status.log
Completed (Wed Dec 11 15:27:24 IST 2019)
[admin@aads68 bin]$
```

AIDE scanning

During the scanning process, AIDE compares the actual state of the file system with the reference values stored in the baseline database and informs you if there are any differences. You can either run AIDE scanning manually or configure automatic scanning. AIDE scanning can take up to 50 minutes depending on the system data. AIDE records the scanning results to the `/var/log/aide/aide_scan_status.log` file.

You must run AIDE scans on a regular basis.

Excluding files and directories from AIDE scanning

About this task

By default, AIDE checks the integrity of all Avaya Aura® Device Services files and directories, except for the following:

- `/opt/spirit/LogTail*`
- `/opt/spirit/logging/`
- `/opt/spirit/persist/persisted_ids.properties`

Avaya Aura® Device Services regularly updates certain files and directories, such as `/opt/Avaya/DeviceServices/<version>/logs/`. AIDE includes all changed files in the scanning report, regardless of the reason for the change. This might result in false positive alarms in the scan report. You can add certain files and directories you want to exclude from scanning to the `/etc/aide.conf` AIDE configuration file. AIDE will not include these files and directories in scanning reports.

Warning:

Be cautions when excluding a file or directory from scanning because an intruder might place a malicious file in a place that AIDE does not check.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Open the `/etc/aide.conf` file in a text editor.

   For example, to open the file in vi, run the `vi /etc/aide.conf` command.
3. For each file or directory you want to exclude from scanning, add an entry in the following format:

   `!<path to file or directory>`

   In this entry, `<path to file or directory>` is the absolute path to the file or directory you want to exclude. For example, enter `!/opt/Avaya/DeviceServices/8.0.1.0001/logs/` to exclude the entire directory from the report.

   If you want to exclude a single file, add the `$` character at the end of the entry. For example: `!/opt/Avaya/DeviceServices/8.0.1.0001/logs/File.log$`

   The entry format supports regular expressions. For example, you can enter `!/opt/Avaya/DeviceServices/8.0.1.0001/logs/File*` to exclude only files and directories that have names starting with `File`.
4. Save the `/etc/aide.conf` file.

Running AIDE scanning manually

About this task

Use this procedure to run AIDE scanning manually. Scanning can take up to 50 minutes, depending on the system data. Avaya recommends that you run AIDE scanning at least once a week.

Do not run or schedule AIDE scanning, ClamAV virus scanning, and ClamAV database updates at the same time. Run AIDE scanning during the least busy periods to minimize the impact on Avaya Aura® Device Services performance.

Before you begin

Ensure that you created a baseline database for your current Avaya Aura® Device Services release.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **`fsit.sh`** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to run AIDE scanning as a background process:

   ```
   sudo ./fsit.sh -scanNow &
   ```

Result

AIDE checks the file system integrity and records the results of the scan to the `/var/log/aide/aide_scan_report.log` file.

Next steps

Review the scanning results.

Related links

Creating a baseline database on page 191

Configuring automatic scanning

About this task

Use this procedure to configure automatic AIDE scanning. Automatic scanning is performed once a day. Scanning can take up to 50 minutes, depending on the system data.

Do not run or schedule AIDE scanning, ClamAV virus scanning, and ClamAV database updates at the same time. Schedule AIDE scanning for the least busy periods to minimize the impact on Avaya Aura® Device Services performance.

Before you begin

Ensure that you created a baseline database for your current Avaya Aura® Device Services release.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **fsit.sh** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to configure automatic scanning:

   ```
   sudo ./fsit.sh -enableScan <hour> <minute>
   ```

   Replace `<hour>` and `<minute>` with the time when you want to run the scan process. Use the 24–hour time format. For 12 a.m., enter `0`.

   For example, enter `sudo ./fsit.sh -enableScan 16 00` to run scanning at 4:00 p.m.

Result

AIDE checks the file system integrity once a day and records the results of the scan to the `/var/log/aide/aide_scan_report.log` file.

Next steps

Review the scanning results.

Related links

Creating a baseline database on page 191

Disabling automatic scanning

About this task

Use this procedure to disable automatic AIDE scanning.

Procedure

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

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command:

   ```
   sudo ./fsit.sh -disableScan
   ```

Reviewing the AIDE scanning report

About this task

Use this procedure to review the results of the latest AIDE scan. The report contains the following:

- The baseline database status.

- Information about the automatic scanning configuration.
- The last database update and scan dates.
- The number of scanned files and directories.
- The number of added, removed, or changed files.
- Information about added, removed, or changed files.
- Detailed Information about changes.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **fsit.sh** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command:

   ```
   sudo ./fsit.sh -status
   ```

   The scan results are displayed in the terminal window.

Example

The following example shows a scan report with differences between the baseline database and the actual system state found:

```
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2019-12-11 15:26:52

Summary:
  Total number of files:        55724
  Added files:                  0
  Removed files:                0
  Changed files:                1


---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /opt/Avaya/bin/fsit.sh

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


File: /opt/Avaya/bin/fsit.sh
 SHA512   : 7v0sOtK9erPSw8dw8GLTCacbvdHO28qj , bdxUm2J38kb/1yfDVO/KiA+55CeJ1hfX
```

The following example shows a scan report with no differences found:

```
AIDE, version 0.15.1

### All files match AIDE database. Looks okay!
```

ClamAV antivirus software management

ClamAV is an open-source antivirus tool for Linux. It can detect viruses, malware, trojans, and other malicious software on Avaya Aura® Device Services.

On Avaya Aura® Device Services, you can manage the ClamAV antivirus tool using the **avScan.sh** system layer script, which is located in the `/opt/Avaya/bin` directory. The **avScan.sh** script is available after the Avaya Aura® Device Services OVA is deployed. You can do the following:

- Update the ClamAV virus databases either manually or automatically.
- Scan Avaya Aura® Device Services for malicious software either manually or automatically.
- Review the scan results.

ClamAV antivirus database updates

To address new malware threats, you must keep the ClamAV antivirus databases up-to-date. You can either update the databases manually or configure automatic updates.

Updating the ClamAV antivirus databases manually

About this task

To address new malware treats you must keep the ClamAV antivirus databases up-to-date. Use this procedure to update the antivirus databases manually.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **avScan.sh** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to update the ClamAV databases:

   ```
   sudo ./avScan.sh -updateNow
   ```

Configuring automatic update of antivirus databases

About this task

To address new malware treats, you must keep the ClamAV antivirus databases up-to-date. Use this procedure to configure automatic ClamAV antivirus database updates. An automatic update is performed on a daily basis at the time you specify.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **avScan.sh** script location:

```
cd /opt/Avaya/bin
```

3. Run the following command to configure automatic update of ClamAV databases:

   ```
   sudo ./avScan.sh -enableUpdate <hour> <minute>
   ```

   Replace `<hour>` and `<minute>` with the time when you want to run the update process. Use the 24-hour time format. For 12 a.m., use `0`.

   For example, enter `sudo ./avScan.sh -enableUpdate 16 00` command to run the update process every day at 4:00 p.m.

ClamAV antivirus scanning

During the scanning process, ClamAV checks the file system for trojans, viruses, and other malicious threats. Avaya Aura® Device Services performs virus scanning as a background process, so you can perform other tasks at the same time. You can either run antivirus scans manually or configure automatic scanning.

Avaya recommends that you run antivirus scans on a regular basis.

Running ClamAV antivirus scanning manually

About this task

Use this procedure to run ClamAV antivirus scanning manually.

Do not run or schedule AIDE scanning, ClamAV virus scanning, and ClamAV database updates at the same time. Run ClamAV virus scanning during the least busy periods to minimize the impact on Avaya Aura® Device Services performance.

Before you begin

Update the ClamAV antivirus databases.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **`avScan.sh`** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to start virus scanning:

   ```
   sudo ./avScan.sh -scanNow
   ```

   Scanning continues even if the terminal session ends or times out.

Next steps

Review the scanning results.

Related links

Reviewing the antivirus scan report on page 198

Configuring automatic ClamAV antivirus scanning

About this task

Use this procedure to configure automatic ClamAV antivirus scanning. Automatic scans are performed on a daily basis at the time you specify. Avaya Aura® Device Services performs antivirus scanning as a background process, so you can perform other tasks at the same time.

Do not run or schedule AIDE scanning, ClamAV virus scanning, and ClamAV database updates at the same time. Schedule ClamAV scanning for the least busy periods to minimize the impact on Avaya Aura® Device Services performance.

Before you begin

Update the ClamAV antivirus databases.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **`avScan.sh`** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to configure automatic antivirus scanning:

   ```
   sudo ./avScan.sh -enableScan <hour> <minute>
   ```

   Replace `<hour>` and `<minute>` with the time when you want to run the virus scanning. Use the 24-hour time format. For 12 a.m., use `0`.

   For example, enter `sudo ./avScan.sh -enableScan 17 00` to start virus scanning every day at 5:00 p.m.

Next steps

Review the scanning results.

Related links

Reviewing the antivirus scan report on page 198

Reviewing the antivirus scan report

About this task

Use this procedure to review the results of the latest ClamAV antivirus scan. The report contains the following:

- Information about automatic updates and scanning configuration.
- The last update and scan dates.
- The ClamAV version.
- The number of scanned files and directories.

- The number of infected files found.
- The amount of data read and scanned in megabytes.
- The amount of time spent on scanning.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **avScan.sh** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command:

   ```
   sudo ./avScan.sh -status
   ```

   The scan results are listed in the terminal window.

Example

The following is an example of a status report with the malware found:

```
[root@aads68 bin]# ./avScan.sh -status


Daily Update: Disabled
Last Update : Completed (Mon Dec 16 12:25:30 IST 2019)
Daily Scan  : 12:27
Last Scan   : Completed (Mon Dec 16 12:45:23 IST 2019)


----------------------------------------------------------------------------

WARNING: Can't open file /etc/gshadow: Permission denied
WARNING: Can't open file /etc/shadow: Permission denied
WARNING: Can't open file /etc/gshadow-: Permission denied
WARNING: Can't open file /etc/shadow-: Permission denied
/etc/dummy_vir.txt: Eicar-Test-Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 6610635
Engine version: 0.101.4
Scanned directories: 6131
Scanned files: 39386
Infected files: 1
Total errors: 4
Data scanned: 2833.87 MB
Data read: 3647.60 MB (ratio 0.78:1)
Time: 368.627 sec (6 m 8 s)
```

Disabling automatic antivirus database updates

About this task

Use this procedure to disable automatic updates of ClamAV database updates.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **avScan.sh** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command:

   ```
   sudo ./avScan.sh -disableUpdate
   ```

Disabling automatic antivirus scanning

About this task

Use this procedure to disable automatic ClamAV antivirus scans.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the **avScan.sh** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command:

   ```
   sudo ./avScan.sh -disableScan
   ```

Enabling additional STIG hardening

About this task

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

Procedure

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

   ```
   sys secconfig --stig --enable
   ```

3. When prompted, press `c` to apply new password rules.

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

```
sys secconfig --stig --query
```

Disabling additional STIG hardening

About this task

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

Procedure

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

```
sys secconfig --stig --disable
```

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

```
sys secconfig --stig --query
```

Configuring the SameSite cookie attribute

About this task

When you use the CORS technology, Avaya Aura® Device Services might receive cross-origin HTTP requests from a different domain. To prevent cross-site request forgery attacks, you can use the SameSite attribute to specify when Avaya Aura® Device Services sends cookies in response to cross-origin requests. The SameSite attribute can have one of the following values:

- **Strict**: Avaya Aura® Device Services only sends cookies to the domain that sent the HTTP request. Avaya Aura® Device Services does not send cookies to third-party domains. It also does not send cookies for cross-origin requests.

  Avaya Aura® Device Services uses this values after a fresh installation of Release 8.0.2.
- **Lax**: Avaya Aura® Device Services sends cookies when performing top-level navigations, but does not send cookies for cross-origin requests.

  Avaya Aura® Device Services uses this value after upgrading to Release 8.0.2.
- **None**: Avaya Aura® Device Services sends cookies in response to all requests, including cross-origin requests.

You can set the SameSite attribute for the following interface levels.

- Service interface, which is used for REST API and Utility Server cookies.
- Administrator interface, which is used for Avaya Aura® Device Services and Utility Server administration portal cookies.

Avaya Aura® Device Services retains the configured values after an upgrade.

Before you begin

Enable cross-origin resource sharing.

Procedure

1. Do the following to configure the SameSite attribute for the Service interface:
    a. On the Avaya Aura® Device Services web administration portal, navigate to **Service Connections** > **CORS Configuration** > **Service Interface**.
    b. From **SameSite cookie attribute value**, select **Strict**, **Lax**, or **None**.
    c. Click **Save**.
2. Do the following to configure the SameSite attribute for the Administrator interface:
    a. On the Avaya Aura® Device Services web administration portal, navigate to **Service Connections** > **CORS Configuration** > **Admin Interface**.
    b. From **SameSite cookie attribute value**, select **Strict**, **Lax**, or **None**.
    c. Click **Save**.

Related links

Cross-origin resource sharing on page 36
Enabling Cross-origin resource sharing for the Service Interface on page 37
Enabling Cross-origin resource sharing for the Administrator Interface on page 37

Chapter 14: Monitoring options

Monitoring cluster nodes

About this task

Use this procedure to check network issues with your server and to ensure that all clustered nodes are running properly.

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Cluster Configuration** > **Cluster Nodes**.

   Avaya Aura® Device Services displays the Cluster Monitoring and Management page.
3. Check the status of the Avaya Aura® Device Services nodes in the table.

   The table has the following column headers to display the status:

   - **Node Address**
   - **Status**
   - **Service Status**
   - **Singleton Services**

   Audits that run only on a single node are called singleton services.

Cluster Nodes field descriptions

Name	Description
Virtual IP	Displays the virtual IP address and FQDN if a virtual IP address is configured. This is used as a load balancer node.
Virtual IP Master	Displays the virtual IP and FQDN of the master node if a virtual IP address is configured.
Virtual IP Backup	Displays the virtual IP and FQDN of the backup node if a virtual IP address is configured.
Seed Node IP	Displays the IP address and FQDN of the seed node of the cluster.
Virtual IP Utility Server	Displays the virtual IP address and FQDN of the Utility Server.

Logs and alarms

Log management

Avaya Aura® Device Services stores the common log at `/opt/Avaya/DeviceServices/<version>/logs/AADS.log`.

If a log file exceeds the log size limit, Avaya Aura® Device Services creates a new log file and keeps the old file on the system. When the number of log files exceeds 20, Avaya Aura® Device Services deletes the oldest log file. Avaya Aura® Device Services encrypts all log files that contain private information if they are older than the configured retention period.

You can view additional messages at `/opt/Avaya/DeviceServices/<version>/tomcat/<version>/logs/catalina`. For example, these messages can include the logs generated during the start of Avaya Aura® Device Services.

Related links

Configuring the data retention period on page 185

Configuring remote logging

About this task

You can configure Avaya Aura® Device Services to copy all log files onto a remote logging server. When remote logging is enabled, Avaya Aura® Device Services writes log files onto both the local and remote servers at the same time.

To maximize data privacy and security, you can use Kerberos to transfer logs to a remote logging server over a secure connection. For authentication, Kerberos uses a keytab file, which contains pairs of Kerberos principals and encrypted keys. Kerberos Distribution Center (KDC) generates the keytab file.

Before you begin

- Set up a remote logging server. The exact configuration process depends on the server that you use to store log files. You can use a Linux or Unix server.
- For a secure connection between Avaya Aura® Device Services and your remote logging server, configure the KDC on the remote logging server. The exact configuration process depends on the server that you use to store log files.
- If you want to use Kerberos authentication, obtain the keytab file from the KDC and upload it to Avaya Aura® Device Services using any file transfer program. You can upload the keytab file to the `/home` directory.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
sys secconfig --stig --remote_audit
```

3. When you see the `Remote logging active?` prompt, type `yes`.
4. When you see the `Remote server FQDN?` prompt, type the FQDN of the remote storage server.

   You must enter the FQDN. IP addresses are not supported.
5. When you see the `Remote logging port?` prompt, type `60`.

   This is the default logging port value.
6. When you see the `Remote logging enable krb5?` prompt, type of the following:
   - `yes`, if you want to use Kerberos to encrypt log files that Avaya Aura® Device Services off-loads to the remote server.
   - `no`, if you want to use an unencrypted connection to send log files to the remote server.
7. When you see the `Remote logging krb5_key_file?` prompt, do one of the following:
   - If Avaya Aura® Device Services displays the existing keytab file, press `Enter`.
   - If Avaya Aura® Device Services does not display an existing keytab file, provide the full path to the keytab file that you uploaded on Avaya Aura® Device Services and then press `Enter`.

     The following is an example of the keytab file location: `/home/krb5.keytab`.

   Avaya Aura® Device Services checks the keytab file and copies it to the `/etc` directory.

Monitoring Avaya Aura® Device Services logs

About this task

You can monitor the `AADS.log` file in run time using the **`tail`** command.

Procedure

1. On the SAT terminal, log on to Avaya Aura® Device Services.
2. Run the following command:

   `tail -f /opt/Avaya/DeviceServices/<version>/logs/AADS.log`

   Avaya Aura® Device Services displays the logs generated during run time.

Changing a logging level

About this task

The logging level that you select determines which system events Avaya Aura® Device Services includes in log files. Avaya support personnel can use these log files for troubleshooting purposes. If the log files that you provide do not contain enough information, support personnel will ask you to select another logging level.

Unless you are told to change the logging level, use the WARNING level for all logging categories.

After selecting a new logging level, you must wait until the issue reoccurs before you can send updated logs to support personnel. When the issue is resolved, you *must* switch back to the recommended logging level.

Important:

Increasing logging details results in larger log files and might also decrease the system performance.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Log Management** > **Log Level**.
2. In the **Logger** field, select the category for which you want to set up the logging level:
   - Avaya Aura® Device Services Logs: Collects the logs generated by the Avaya Aura® Device Services server.
   - System Logs: Collects all the system logs, including Keycloak logs.
   - All Logs: Collects all server and system logs.
3. In the **Current logging level** field, select one of the following options:
   - ERROR: Provides critical server errors.
   - WARNING (Recommended): Provides important but non-critical server messages to understand the current function of the server.
   - INFO: Provides information about internal server events and messages.
   - FINE: Provides detailed logs. The dynamic configuration and web deployment services use this information for debugging purposes.
   - FINEST: Provides very detailed logs on frequent events.

     Warning:

     The FINE and FINEST logging levels can affect system performance. Do not use these options if they are not required.
4. Click **Save**.

   In cluster deployments, Avaya Aura® Device Services applies changes to all nodes in the cluster.

Downloading logs

About this task

Use this procedure to download Avaya Aura® Device Services logs to your computer. Support personnel can use the log files you collect for troubleshooting purposes.

You can only collect and download logs for one node at a time. You cannot download logs for an entire cluster at once.

To protect personal data, Avaya Aura® Device Services supports log anonymization for the logs you download. If you choose to anonymize logs, Avaya Aura® Device Services replaces all private or sensitive information with asterisk (*) symbols. Log files on Avaya Aura® Device Services remain unchanged.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Log Management** > **Log Level**.
2. In the Collect Logs area, in **Number of rotated log files to collect (1–20)**, enter the number of logs you want to download.

   This setting specifies the number of files from the log file history to include in the log collection. The range is 1 to 20. If you leave this field empty, Avaya Aura® Device Services collects all available logs.

3. To collect logs for a node, click **Collect** in the corresponding row.
4. Wait until Avaya Aura® Device Services collects the logs and then click **OK**.
5. To download the logs you collected for a node, click **Download**.
6. When Avaya Aura® Device Services prompts you to anonymize logs, do one of the following:
   - Click **Yes** to anonymize logs.

     The anonymization process might take several minutes depending on the number of logs and the size of log files.
   - Click **No** to just decrypt and download log files unchanged.

Related links

collectlogs on page 291
Logs collected using the collectlogs command are encrypted on page 283

Alarms

The alarms that Avaya Aura® Device Services triggers are visible in System Manager.

You must set up serviceability agents to receive Avaya Aura® Device Services alarms in System Manager. To configure serviceability agents, set up an SNMPv3 user profile and an SNMP target profile. Then assign the SNMPv3 user profile to the SNMP target profile.

If FIPS is enabled, only SNMPv3 profiles are supported.

For more information, see *Administering Avaya Aura® System Manager*.

Related links

System Manager does not show Avaya Aura Device Services alarms on page 265

Alarms configuration on System Manager

Setting up an SNMPv3 user profile

About this task

An SNMPv3 user profile enables you to define privileges so serviceability agents can read and write data in SNMP Management Information Bases (MIBs).

Procedure

1. On the System Manager web console, navigate to **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
2. In the User Details section, click **Edit**.
3. In the **User Name** field, type `initial`.
4. In the **Authentication Protocol** field, select **SHA**.

   The **MD5** setting is not supported.
5. In the **Authentication Password** field, type the authentication password.

   The default authentication password is `avaya123`.
6. In the **Confirm Authentication Password** field, confirm the password.
7. In the **Privacy Protocol** field, select **AES**.
8. In the **Privacy Password** field, type the privacy password.

   The default privacy password is `avaya123`.
9. In the **Confirm Privacy Password** field, confirm the password.
10. In the **Privileges** field, select **Read/Write**.
11. Click **Commit**.

Setting up an SNMP target profile

About this task

An SNMP target profile contains settings for sending alarms from Avaya Aura® Device Services to System Manager.

Procedure

1. On the System Manager web console, navigate to **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMP Target Profiles**.
2. On the Target Details tab, click **Edit**.
3. In the **Name** field, type the name of the profile.
4. In the **Description** field, type a description for the profile.
5. In the **IP Address** field, type the System Manager IP address.
6. In the **Port** field, type `10162`.

7. In the **Notification Type** field, select **Trap**.
8. In the **Protocol** field, select **V3**.
9. Click **Commit**.

Assigning the SNMPv3 user profile

About this task

You must assign the SNMPv3 user profile to the target profile so System Manager can receive alarms from Avaya Aura® Device Services.

Before you begin

Associate the Avaya Aura® Device Services server with the configured Session Manager.

Set up an SNMPv3 user profile and an SNMP target profile.

Procedure

1. On the System Manager web console, navigate to **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Select the Avaya Aura® Device Services host name, and click **Manage Profiles**.
3. Click the **SNMP Target Profiles** tab.
4. In the Assignable Profiles section, click the SNMP target profile you created, and click **Assign**.
5. Click the **SNMPv3 User Profiles** tab.
6. In the Assignable Profiles section, select the SNMPv3 profile you created, and click **Assign**.
7. Click **Commit**.

Avaya Aura® Device Services alarms list

The following table shows alarms that Avaya Aura® Device Services can trigger. You can view these alarms in System Manager.

Alarm description	Severity	Event code	SNMP OID
AADS Disk space usage is below critical threshold	critical	OP_AADS-00099	.1.3.6.1.4.1.6889.2.89.0.99
AADS Disk space usage has reached critical threshold	critical	OP_AADS-00098	.1.3.6.1.4.1.6889.2.89.0.98
AADS Disk space usage is below warning threshold	minor	OP_AADS-00097	.1.3.6.1.4.1.6889.2.89.0.97
AADS Disk space usage has reached warning threshold	minor	OP_AADS-00096	.1.3.6.1.4.1.6889.2.89.0.96

Alarm description	Severity	Event code	SNMP OID
AADS Restore process is successful	major	OP_AADS-00095	.1.3.6.1.4.1.6889.2.89.0.95
AADS Restore process failed	major	OP_AADS-00094	.1.3.6.1.4.1.6889.2.89.0.94
AADS Backup process is successful	major	OP_AADS-00093	.1.3.6.1.4.1.6889.2.89.0.93
AADS Backup process failed	major	OP_AADS-00092	.1.3.6.1.4.1.6889.2.89.0.92
The associated SM is back up and successfully reachable	critical	OP_AADS-00091	.1.3.6.1.4.1.6889.2.89.0.91
The associated SM is down and hence not reachable for SMGR	critical	OP_AADS-00090	.1.3.6.1.4.1.6889.2.89.0.90
AADS Server Node Licenses Threshold cleared	minor	OP_AADS-00089	.1.3.6.1.4.1.6889.2.89.0.89
AADS Server Node Licenses Threshold reached	minor	OP_AADS-00088	.1.3.6.1.4.1.6889.2.89.0.88
AADS Server Node Licenses Available	major	OP_AADS-00087	.1.3.6.1.4.1.6889.2.89.0.87
AADS Server Node Licenses Unavailable	major	OP_AADS-00086	.1.3.6.1.4.1.6889.2.89.0.86
AADS Multisite Adapter Successfully connected to remote site(s)	major	OP_AADS-00085	.1.3.6.1.4.1.6889.2.89.0.85
AADS Multisite Adapter Cannot connect to remote site(s)	major	OP_AADS-00084	.1.3.6.1.4.1.6889.2.89.0.84
DRS is up clearing the alarm	major	OP_AADS-00083	.1.3.6.1.4.1.6889.2.89.0.83
DRS is failed may be because postgres is down or error in DRS eventing , check if postgres is up and repair the node from SMGR GUI	major	OP_AADS-00082	.1.3.6.1.4.1.6889.2.89.0.82
Successfully connected to Exchange EWS service using delegate account	major	OP_AADS-00081	.1.3.6.1.4.1.6889.2.89.0.81
Not able to connect Exchange EWS service using delegate account	major	OP_AADS-00080	.1.3.6.1.4.1.6889.2.89.0.80

Alarm description	Severity	Event code	SNMP OID
Successfully connected to PPM Web service	major	OP_AADS-00079	.1.3.6.1.4.1.6889.2.89.0.79
Not able to connect to PPM Web service	major	OP_AADS-00078	.1.3.6.1.4.1.6889.2.89.0.78
AADS Node Certificate is valid	major	OP_AADS-00077	.1.3.6.1.4.1.6889.2.89.0.77
AADS Node Certificate is expiring, has expired, or cannot be read	major	OP_AADS-00076	.1.3.6.1.4.1.6889.2.89.0.76
Synchronized with time server	major	OP_AADS-00075	.1.3.6.1.4.1.6889.2.89.0.75
Synchronization with time server lost	major	OP_AADS-00074	.1.3.6.1.4.1.6889.2.89.0.74
AADS Media storage is below critical threshold	critical	OP_AADS-00073	.1.3.6.1.4.1.6889.2.89.0.73
AADS Media storage has exceeded critical threshold	critical	OP_AADS-00072	.1.3.6.1.4.1.6889.2.89.0.72
AADS Media storage is below warning threshold	minor	OP_AADS-00071	.1.3.6.1.4.1.6889.2.89.0.71
AADS Media storage has exceeded warning threshold	minor	OP_AADS-00070	.1.3.6.1.4.1.6889.2.89.0.70
AADS Connection to System Manager LDAP server was restored	major	OP_AADS-00069	.1.3.6.1.4.1.6889.2.89.0.69
AADS Connection to System Manager LDAP server was lost	major	OP_AADS-00068	.1.3.6.1.4.1.6889.2.89.0.68
AADS Backup Node released Virtual IP back to Primary	major	OP_AADS-00067	.1.3.6.1.4.1.6889.2.89.0.67
AADS Backup Node acquired Virtual IP from Primary	major	OP_AADS-00066	.1.3.6.1.4.1.6889.2.89.0.66
AADS Connection to Remote Domain was restored	major	OP_AADS-00065	.1.3.6.1.4.1.6889.2.89.0.65
AADS Connection to Remote Domain was lost	major	OP_AADS-00064	.1.3.6.1.4.1.6889.2.89.0.64
AADS is not operating in License Restricted Mode	critical	OP_AADS-00063	.1.3.6.1.4.1.6889.2.89.0.63
AADS is operating in License Restricted Mode	critical	OP_AADS-00062	.1.3.6.1.4.1.6889.2.89.0.62

Alarm description	Severity	Event code	SNMP OID
AADS is not operating in License Error Mode	major	OP_AADS-00061	.1.3.6.1.4.1.6889.2.89.0.61
AADS is operating in License Error Mode	major	OP_AADS-00060	.1.3.6.1.4.1.6889.2.89.0.60
AADS JBoss Backend Certificate is valid	major	OP_AADS-00057	.1.3.6.1.4.1.6889.2.89.0.57
AADS JBoss Backend Certificate is expiring, has expired, or cannot be read	major	OP_AADS-00056	.1.3.6.1.4.1.6889.2.89.0.56
AADS OAM Certificate is valid	major	OP_AADS-00055	.1.3.6.1.4.1.6889.2.89.0.55
AADS OAM Certificate is expiring, has expired, or cannot be read	major	OP_AADS-00054	.1.3.6.1.4.1.6889.2.89.0.54
AADS REST Certificate is valid	major	OP_AADS-00053	.1.3.6.1.4.1.6889.2.89.0.53
AADS REST Certificate is expiring, has expired, or cannot be read	major	OP_AADS-00052	.1.3.6.1.4.1.6889.2.89.0.52
AADS Web Service has passed internal testing	major	OP_AADS-00051	.1.3.6.1.4.1.6889.2.89.0.51
AADS Web Service has failed internal testing	major	OP_AADS-00050	.1.3.6.1.4.1.6889.2.89.0.50
AADS HTTP or SIP error code count is below threshold within time period	major	OP_AADS-00049	.1.3.6.1.4.1.6889.2.89.0.49
AADS HTTP or SIP error code count has exceeded threshold within time period	major	OP_AADS-00048	.1.3.6.1.4.1.6889.2.89.0.48
AADS Database storage is below critical threshold	critical	OP_AADS-00047	.1.3.6.1.4.1.6889.2.89.0.47
AADS Database storage has exceeded critical threshold	critical	OP_AADS-00046	.1.3.6.1.4.1.6889.2.89.0.46
AADS Database storage is below warning threshold	minor	OP_AADS-00045	.1.3.6.1.4.1.6889.2.89.0.45
AADS Database storage has exceeded warning threshold	minor	OP_AADS-00044	.1.3.6.1.4.1.6889.2.89.0.44
AADS System memory is below threshold	major	OP_AADS-00043	.1.3.6.1.4.1.6889.2.89.0.43
AADS System memory is exceeding threshold	major	OP_AADS-00042	.1.3.6.1.4.1.6889.2.89.0.42

Alarm description	Severity	Event code	SNMP OID
AADS System log level is no longer set to debug, which will improve performance	minor	OP_AADS-00041	.1.3.6.1.4.1.6889.2.89.0.41
AADS System log level is set to debug, which will degrade performance	minor	OP_AADS-00040	.1.3.6.1.4.1.6889.2.89.0.40
AADS System load average is below threshold	major	OP_AADS-00037	.1.3.6.1.4.1.6889.2.89.0.37
AADS System load average is exceeding threshold	major	OP_AADS-00036	.1.3.6.1.4.1.6889.2.89.0.36
AADS total created accounts is below maximum	major	OP_AADS-00035	.1.3.6.1.4.1.6889.2.89.0.35
AADS total created accounts has reached maximum	major	OP_AADS-00034	.1.3.6.1.4.1.6889.2.89.0.34
AADS number of concurrent sessions is below maximum threshold	major	OP_AADS-00033	.1.3.6.1.4.1.6889.2.89.0.33
AADS number of concurrent sessions is exceeding maximum threshold	major	OP_AADS-00032	.1.3.6.1.4.1.6889.2.89.0.32
AADS rate of requests/ responses went below maximum threshold	major	OP_AADS-00031	.1.3.6.1.4.1.6889.2.89.0.31
AADS is exceeding the maximum rate of requests/ responses within time period	major	OP_AADS-00030	.1.3.6.1.4.1.6889.2.89.0.30
AADS Connection to Session Manager was restored	major	OP_AADS-00029	.1.3.6.1.4.1.6889.2.89.0.29
AADS Connection to Session Manager was lost	major	OP_AADS-00028	.1.3.6.1.4.1.6889.2.89.0.28
AADS Connection to its Media Store was restored	major	OP_AADS-00027	.1.3.6.1.4.1.6889.2.89.0.27
AADS Connection to its Media Store was lost	major	OP_AADS-00026	.1.3.6.1.4.1.6889.2.89.0.26
AADS Connection to its Data Store was restored	major	OP_AADS-00025	.1.3.6.1.4.1.6889.2.89.0.25
AADS Connection to its Data Store was lost	major	OP_AADS-00024	.1.3.6.1.4.1.6889.2.89.0.24
AADS Connection to LDAP/ Active Directory server was restored	major	OP_AADS-00021	.1.3.6.1.4.1.6889.2.89.0.21

Alarm description	Severity	Event code	SNMP OID
AADS Connection to LDAP/ Active Directory server was lost	major	OP_AADS-00020	.1.3.6.1.4.1.6889.2.89.0.20
Clear alarm	minor	OP_AADS-00002	.1.3.6.1.4.1.6889.2.89.0.2
An AADS Core Component was restarted successfully	major	OP_AADS-00011	.1.3.6.1.4.1.6889.2.89.0.11
An AADS Core Component has stopped functioning	major	OP_AADS-00010	.1.3.6.1.4.1.6889.2.89.0.10
Test alarm	minor	OP_AADS-00001	.1.3.6.1.4.1.6889.2.89.0.1
Avaya Spaces alarms			
AADS Spaces connection lost	critical	OP_AADS-00172	.1.3.6.1.4.1.6889.2.89.0.172
AADS Spaces connection restored	critical	OP_AADS-00173	.1.3.6.1.4.1.6889.2.89.0.173
AADS Spaces certificate expired	critical	OP_AADS-00174	.1.3.6.1.4.1.6889.2.89.0.174
AADS Spaces certificate restored	critical	OP_AADS-00175	.1.3.6.1.4.1.6889.2.89.0.175
AADS Spaces Host unreachable	critical	OP_AADS-00176	.1.3.6.1.4.1.6889.2.89.0.176
AADS Spaces Host reachable and connected	critical	OP_AADS-00177	.1.3.6.1.4.1.6889.2.89.0.177

Enhanced Access Security Gateway for real time support

Enabling the Enhanced Access Security Gateway after Avaya-provided OVA deployment

About this task

Use this procedure to enable Enhanced Access Security Gateway (EASG) functionality in Avaya Aura® Device Services. Avaya support engineers can use this functionality to access your computer and resolve product issues in real time.

The EASG is installed automatically when you deploy the Avaya Aura® Device Services OVA on a VMware standalone host or on vCenter.

Procedure

1. Open the SSH console as an administrator.

2. Run the following command to check the EASG status:

   ```
   EASGStatus
   ```

   By default, the EASG status is disabled.

3. Run the following command to enable EASG:

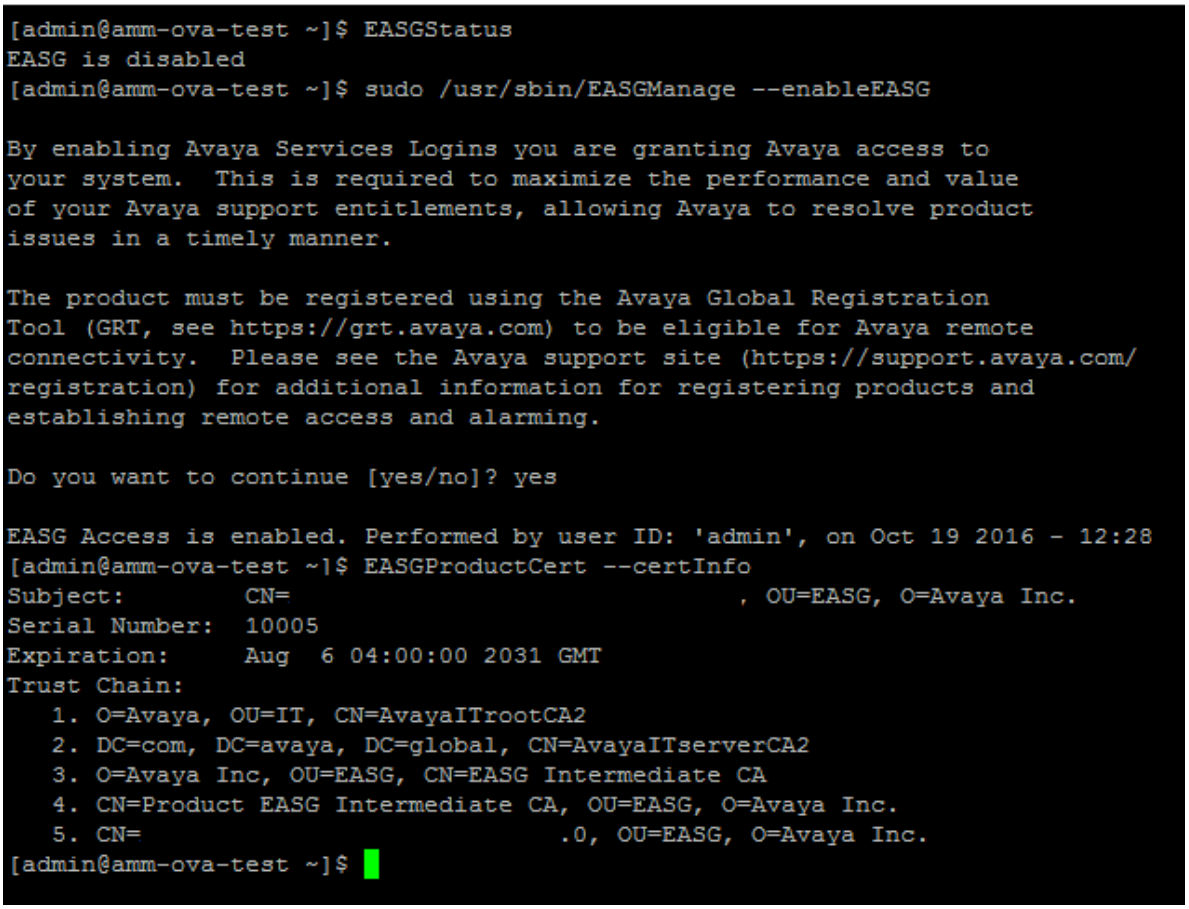
   ```
   sudo /usr/sbin/EASGManage --enableEASG
   ```

4. Run the following command to verify the product certificate:

   ```
   sudo EASGProductCert --certInfo
   ```

   Avaya Aura® Device Services displays the product certificate details.

   For example:



   If the certificate expires within 360, 180, 30, or 0 days, Avaya Aura® Device Services writes a certificate expiry notification to the `/var/log/messages` log file.

Removing EASG

About this task

Use this procedure to remove EASG permanently. You can use the Avaya-provided OVA deployment process to reinstall EASG.

Procedure

In the SSH console, run the following command to remove EASG:

```
sudo /opt/Avaya/permanentEASGRemoval.sh
```

Chapter 15: Backup and restore

You can perform backups in a standalone or cluster environment. In case of a system malfunction where one or more Avaya Aura® Device Services nodes must be reinstalled and reconfigured, you can restore the data that was present when you made the backup. The backup and restore procedures are the same, regardless of the deployment method.

The restore procedure must be performed on the same Avaya Aura® Device Services build version from which the backup was made. Patches can cause changes to the format and content of the data that is stored when a backup is taken. Before you restore the data, patch the build to the same patch level that the build was on at the time that the backup was taken.

The backup procedure requires significant resources, so do not perform the backup during busy periods.

Backing up Avaya Aura® Device Services

About this task

Use this procedure to back up Avaya Aura® Device Services configuration files and user data. This procedure applies to both standalone and cluster environments. In a cluster environment, you can perform the backup procedure from any node.

Note:

Backing up Avaya Aura® Device Services does not back up the Utility Server data. For more information about backing up data stored on the Utility Server, see Backing up data stored on the Utility Server on page 146.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. To create a backup, run one of the following commands:
   - `app backup -t` To create a backup in a `.tar.zip` file.
   - `app backup` To create a backup in a directory.
3. If you created your backup in a `.tar.zip` file, provide a password when prompted and then re-enter the password to confirm.

   If the password does not comply with the password complexity rules, Avaya Aura® Device Services prompts you to enter a new password. For more information about the password complexity rules, see passwdrules command on page 303.

4. When prompted with `Yes for proceed, all else for cancel`, type `Yes` and then press `Enter`.

   Avaya Aura® Device Services creates a backup file in the administrator's home directory. In a cluster environment, backup files are created on each cluster node.
5. Ensure that the administrator's home directory contains the backup file or backup directory.
6. Copy the backup files to an external storage using a file transfer program, such as SFTP or SCP.
7. In a cluster environment, repeat steps 5 and 6 on all remaining nodes in the cluster.

Restoring options for standalone and cluster environments

Restoring Avaya Aura® Device Services in a standalone environment

About this task

Use this procedure to restore a standalone Avaya Aura® Device Services node.

Before you begin

- Ensure that the application installation binary required to install Avaya Aura® Device Services is available.

  Note:

  The application installer must be the same version as the Avaya Aura® Device Services version that was used to create the backup.
- If the virtual machine needs to be re-created, ensure that the OVA required to deploy the virtual machine is available.
- Ensure that the required Avaya Aura® Device Services backup file is available.
- Determine if the Utility Server was enabled on the system that you are restoring.

Procedure

1. Reinstall the same version of Avaya Aura® Device Services that was backed up:
   a. Redeploy the OVA if the node needs to be re-imaged.

      For more information about deploying OVAs, see the "Initial setup" section in *Deploying Avaya Aura® Device Services*.

b. Log in to the Avaya Aura® Device Services CLI as an administrator and run the following command:

```
app install
```

c. If the Utility Server was enabled on the system that you are restoring, enable the Utility Server from the **Utility Server** menu.

d. In the **Front-end host, System Manager and Certificate Configuration** menu, configure the following settings:

- **System Manager FQDN**
- **System Manager Enrollment Password**
- **Keystore password**

e. In the **Session Manager Configuration** menu, configure the following settings:

- **Session Manager Management IP**
- **Session Manager Asset IP**

f. After the initial setup is completed, run the Configuration Utility using the `app configure` command.

g. If the Utility Server was enabled on the system that you are restoring, in the **Utility Server Configuration** menu, configure the following settings:

- **Utility Server VIP**
- **Utility Server FQDN**

2. On System Manager, verify that DRS replication is working.

   For more information, see Checking for DRS synchronization on page 257.

3. On the Avaya Aura® Device Services web administration portal, force LDAP synchronization and ensure that Avaya Aura® Device Services does not display the `503 Service Unavailable` error.

   For more information, see Setting up user synchronization with the LDAP server on page 116.

4. Copy the backup file or backup directory to the home directory of the administrative user using a file transfer utility, such as SFTP or SCP.

5. To restore the backed-up configuration files, run the following command:

```
app restore <path>
```

   In this command, `<path>` is the absolute path to the backup file in `.tar.zip` format or to the backup directory.

6. When prompted, enter the password you used to create the backup.

   If the password is wrong, Avaya Aura® Device Services prompts you to re-enter the password. After three failed attempts, Avaya Aura® Device Services aborts the restore process. In this case, you will need to run the `app restore` command again.

Next steps

If the Utility Server is enabled on the system and you need to restore Utility Server data, see Restoring the Utility Server data on page 147.

Restoring an Avaya Aura® Device Services cluster

About this task

Use this procedure to restore an entire cluster. Restoring a cluster is useful if a failure occurs that results in the loss of all nodes.

To restore an Avaya Aura® Device Services node, you must install the Avaya Aura® Device Services software, then restore the configuration and data files from a previous backup.

Before you begin

- Ensure that the application installation binary required to install Avaya Aura® Device Services is available.

  Note:

  The application installer must be the same version as the Avaya Aura® Device Services version that was used to create the backup.
- If the virtual machine needs to be re-created, ensure that the OVA required to deploy the virtual machine is available.
- Ensure that the required Avaya Aura® Device Services backup files are available for the nodes that are restored. Each node has its own specific backup file or backup directory. When restoring an Avaya Aura® Device Services node, you must use the correct backup file or directory for that node.
- Determine if the Utility Server was enabled on the system that you are restoring.

Procedure

Perform step 1 on the seed node first, and then on all non-seed nodes.

1. Reinstall the same version of Avaya Aura® Device Services that was backed up:
   a. Redeploy the OVA if the node needs to be re-imaged.

      For more information about deploying OVAs, see the “Initial setup” section in *Deploying Avaya Aura® Device Services*.
   b. Log in to the Avaya Aura® Device Services CLI as an administrator and run the following command:

      ```
      app install
      ```
   c. If the Utility Server was enabled on the system that you are restoring, enable the Utility Server from the **Utility Server** menu.
   d. If you are reinstalling a non-seed node, in the **Cluster Configuration** menu, set **Initial cluster node** to `n`.
   e. If you are reinstalling a non-seed node, in the **Cluster Configuration** menu, set **Cluster seed node** to the IP address of the seed node.

f. In the **Front-end host, System Manager and Certificate Configuration** menu, configure the following settings:
   - **System Manager FQDN**
   - **System Manager Enrollment Password**
   - **Keystore password**

g. In the **Session Manager Configuration** menu, configure the following settings:
   - **Session Manager Management IP**
   - **Session Manager Asset IP**

h. After the initial setup is completed, run the Configuration Utility using the `app configure` command.

i. If you enabled the Utility Server, configure the settings in the **Clustering Configuration** menu.

j. If the Utility Server was enabled on the system that you are restoring, in the **Utility Server Configuration** menu, configure the following settings:
   - **Utility Server VIP**
   - **Utility Server FQDN**

2. On the seed node, configure SSH/RSA public and private keys.

   For more information, see “Configuring RSA public and private keys for SSH connections in a cluster” in *Deploying Avaya Aura® Device Services*.

3. If OAuth was enabled on the system that you are restoring, enable OAuth database replication on all nodes in the cluster.

   For more information, see Enabling OAuth database replication in a cluster environment on page 74.

4. If onboard Open LDAP was enabled on the system that you are restoring, enable Open LDAP replication on all nodes in the cluster.

   For more information, see Enabling Open LDAP replication on page 255.

5. On System Manager, verify that DRS replication is working for all nodes.

   For more information, see Checking for DRS synchronization on page 257.

6. On the Avaya Aura® Device Services web administration portal, force LDAP synchronization and ensure that Avaya Aura® Device Services does not display the `503 Service Unavailable` error.

   Perform this step on each node in the cluster.

   For more information, see Setting up user synchronization with the LDAP server on page 116.

Perform steps 7 to 9 on the seed node first and then on all non-seed nodes.

7. Copy the backup file or backup directory to the home directory of the administrative user using a file transfer utility, such as SFTP or SCP.

   Ensure that you are using the backup file or backup directory created for the current node.

8. To restore the backed-up configuration files, run the following command:

   ```
   app restore <path>
   ```

   In this command, `<path>` is the absolute path to the backup file or backup directory.

9. When prompted, enter the password you used to create the backup.

   If the password is wrong, Avaya Aura® Device Services prompts you to re-enter the password. After three failed attempts, Avaya Aura® Device Services aborts the restore process. In this case, you will need to run the `app restore` command again.

10. Repeat steps 7 to 9 on the non-seed nodes.

11. From the seed node, run the following command to repair the Cassandra database:

    ```
    sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/cassandra/
    cassandraRepair.sh -M
    ```

    If prompted, enter the Cassandra database user name and password. The default Cassandra database user name and password are `aem_system` and `avaya123` respectively.

Next steps

If the Utility Server is enabled on the system and you need to restore Utility Server data, see Restoring the Utility Server data on page 147.

Chapter 16: Avaya Aura® Device Services upgrade and migration operations

The upgrade path can flow through one or more prior releases, depending on the currently installed release. The following table shows the specific release upgrades along the upgrade path.

Upgrade path number	From	To
1	7.1	7.1.2
2	7.1.2	7.1.3
3	7.1.2	7.1.3 SP1
4	7.1.3	7.1.3 SP1
5	7.1.3 SP1	7.1.3 SP2
6	7.1.3 SP2	7.1.5
7	7.1.5	7.1.6
8	7.1.6	8.0
9	8.0	8.0.1
10	8.0.1	8.0.2

Depending on the release you are currently using, you might need to perform several upgrade procedures. For example, if you want to upgrade Avaya Aura® Device Services Release 7.1.6 to Release 8.0.2, follow upgrade paths 8, 9, and 10.

This document focuses on the upgrade and migration process for path 10. For information about migration and upgrade processes for previous releases, see the following documents:

- For Release 7.1, see “Upgrading Avaya Aura® Device Services” in Deploying Avaya Aura Device Services.
- For Release 7.1.2, see “Upgrades and migrations” in Administering Avaya Aura Device Services.
- For Release 7.1.3.x, see see “Avaya Aura® Device Services upgrade operations” in Administering Avaya Aura Device Services.
- For Release 7.1.5, see “Avaya Aura® Device Services upgrade and migration operations” in Administering Avaya Aura Device Services.
- For Release 7.1.6, see “Avaya Aura® Device Services upgrade operations” in Administering Avaya Aura Device Services.

- For Release 8.0, see “Avaya Aura® Device Services upgrade operations” in Administering Avaya Aura Device Services.
- For Release 8.0.1, see Avaya Aura® Device Services upgrade and migration operations.

Important:

- Perform the system layer update before you upgrade Avaya Aura® Device Services.
- As of Release 8.0, Avaya Aura® Device Services is FIPS 140-2 compliant. You can install Avaya Aura® Device Services in either FIPS or non-FIPS mode. You *cannot* enable FIPS mode when you are upgrading or migrating your Avaya Aura® Device Services to the latest release. If you need to enable FIPS, you must uninstall Avaya Aura® Device Services first, enable FIPS at the system layer, and then install the latest Avaya Aura® Device Services version.

Disk encryption

As of Release 8.0.1, Avaya Aura® Device Services supports disk encryption.

AVP deployments

For AVP deployments, you can use the existing upgrade procedures to enable disk encryption. You can enable disk encryption when you deploy a new Avaya Aura® Device Services Release 8.0.2 OVA. You cannot perform a rollback when disk encryption is enabled.

ESXi deployments

For ESXi deployments, you *cannot* enable disk encryption when you are upgrading from Avaya Aura® Device Services Release 8.0.1 to Release 8.0.2. If you need to enable disk encryption, you must perform a migration. If you do not need disk encryption or disk encryption is already enabled in Release 8.0.1, you can upgrade from Release 8.0.1 to Release 8.0.2.

Avaya Aura® Device Services only supports rollback to Release 8.0.1 when you perform an upgrade. Rollback is *not* supported with the migration process.

AWS deployments

For AWS deployments, you *cannot* enable disk encryption on Avaya Aura® Device Services. You must enable disk encryption on AWS. For more information, see How to Protect Data at Rest with Amazon EC2 Instance Store Encryption.

Related links

Upgrading Avaya Aura Device Services on AVP on page 229
Migrating Avaya Aura Device Services on ESXi on page 244

System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs

Each VMware or AWS virtual machine that is created by deploying the Avaya Aura® Device Services OVA file has a system layer (operating system). The system later is updated with system layer updates provided by Avaya.

Important:

Do not apply updates obtained from sources other than Avaya to the system layer of Avaya Aura® Device Services virtual machines. Only use update artifacts provided by Avaya.

Checklist for updating the system layer

Use this checklist to update the system layer.

No.	Task	Notes	✔
1	Determine if the system layer update is applicable to the given virtual machine.	See Determining if a system update is applicable on page 225. Skip the remaining steps if the update is not applicable.	
2	Download, extract, and stage the update.	See Downloading, extracting, and staging a system layer update on page 226.	
3	Change SELinux mode to “permissive”.	See Changing the SELinux mode to permissive on page 227.	
4	Install the update during a maintenance window.	See Installing a staged system layer update on page 228.	

Determining if a system update is applicable

About this task

Before installing a system update for a virtual machine, query the version of the currently installed system. Use the current version to determine if the system layer requires an update. The virtual machine might be installed using an OVA that was already built with the latest system layer version.

Procedure

1. Log in to the virtual machine using the administrative user ID.
2. Query the version number of the system version by running the `sys versions` command.

Note:

Ignore the patch level reported by the above command.

Next steps

- If the above system version is already on the recommended system update, then no further action is required.
- If the system version is lower than the recommended system update version, then continue with the process to download and stage the update.

Downloading, extracting, and staging a system layer update

About this task

Before installing a system layer update, you must first download the update from the Avaya Support website, and then extract and stage the update on the system. The staging process places the update into a system area, which prepares the system for the installation of the update.

Tip:

Avaya recommends cleaning up the downloaded and extracted artifacts after staging. The staging operation copies the content to an internal system area. The downloaded and extracted content are no longer required.

Procedure

1. Download the update from the Avaya Support website.

   `ucapp-system-3.4.3.0.7.tgz` is an example of a system layer update artifact.

2. Transfer the update to the administrative account of the server to be updated, using standard file transfer methods, such as SFTP or SCP.
3. Log in to the administrative account of the server using SSH.
4. To extract the update, run the following command:

   ```
   tar -zxf ucapp-system-<version>.tgz
   ```

   For example:

   ```
   tar -zxf ucapp-system-3.4.3.0.7.tgz
   ```

5. To stage the update, change to the required directory and perform the following staging command:

   ```
   cd ucapp-system-<version>
   sudo ./update.sh --stage
   ```

   For example:

   ```
   cd ucapp-system-3.4.3.0.7
   sudo ./update.sh --stage
   ```

6. **(Optional)** To free up disk space, clean up the downloaded and extracted files using the following commands:

   ```
   cd..
   rm ucapp-system-<version>.tgz
   rm -rf ucapp-system-<version>
   ```

   For example:

   ```
   rm ucapp-system-3.4.3.0.7.tgz
   rm -rf ucapp-system-3.4.3.0.7
   ```

7. To verify that the update has been staged, query the status:

   ```
   sysUpdate --status
   ```

   The **sysUpdate** command is added to the system the first time a system update is staged. After staging, if the command is not recognized, you must exit the current session and establish a new session. Establishing a new session creates the **sysUpdate** command (alias) for the new session.

8. **(Optional)** If a system update is staged in error, run the following command to delete this staged update:

   ```
   sysUpdate --delete
   ```

   You cannot delete a staged update once the installation of the update has started.

9. **(Optional)** For more information about the **sysUpdate** command, run one of the following commands:

   ```
   sysUpdate --help
   sysUpdate --hhelp
   ```

   The **--help** option provides the command line syntax. The **--hhelp** option provides verbose help.

Next steps

Install the staged update during a maintenance window.

Changing the SELinux mode to “permissive”

About this task

Before installing the system layer update for Avaya Aura® Device Services, you must ensure that the SELinux kernel security module operates in the “permissive” mode.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Open the SELinux configuration file `/etc/selinux/config` in a text editor with sudo privileges.

   For example, to open the file in vi, run the `sudo vi /etc/selinux/config` command.

3. Set the value of the `SELINUX` parameter to `permissive`.

   ```
   SELINUX=permissive
   ```

   Warning:

   Ensure that `permissive` is properly spelled. Misspelling the setting value can case kernel panic issues.

4. Save the file.
5. Run the `sudo reboot` command to reboot Avaya Aura® Device Services:
6. Do the following to verify the SELinux configuration:
   a. Log in to the Avaya Aura® Device Services CLI as an administrator.
   b. Run the following command:

      ```
      sestatus
      ```

   c. Ensure that Avaya Aura® Device Services displays `permissive` in the command output.

Next steps

Install the staged system layer update.

Installing a staged system layer update

About this task

After a system update is staged, you can install it. The installation runs in the background in order to minimize the possibility of interference, such as the loss of an SSH session. The background installation process follows these steps:

- A login warning message is created so users logging into the system know that a system update is in progress.
- If the application is running, it is shut down.
- The update is installed onto the system.
- The server is rebooted.
- Post-reboot cleanup actions are performed.
- The application is started.
- The login warning message is removed.

Important:

Do not perform any system maintenance actions, such as starting, stopping, or upgrading the application, while the system update is in progress.

Before you begin

Change SELinux mode to “permissive” as described in Changing the SELinux mode to permissive on page 227.

Procedure

1. Log in to the administrative account using SSH.
2. Type `sysUpdate --install` to start the installation.

   Avaya Aura® Device Services reboots after the installation process completes.
3. **(Optional)** Run one of the following commands to monitor the progress of the update:

   ```
   sysUpdate --monitor
   sysUpdate --monitor less
   ```

   The **`--monitor`** option uses the Linux tail browser. The **`-- monitor less`** option uses the Linux less browser.
4. **(Optional)** Run the following command to review the status of the update:

   ```
   sysUpdate --status
   ```
5. **(Optional)** Run the following command to obtain logs of the current and previous system layer update installations:

   ```
   sysUpdate --logs
   ```

   This command gathers log files into an archive in ZIP format and places this archive in the current working directory.
6. After Avaya Aura® Device Services reboots, log in to the administrative account using SSH.
7. Run the following command:

   ```
   sudo /opt/Avaya/bin/selinux app
   ```

   Avaya Aura® Device Services requires this command to run various services, such as httpd, openldap, or keycloak.
8. Run the following command to restart Avaya Aura® Device Services:

   ```
   svc aads restart
   ```

Next steps

If your organization requires stricter STIG compliance, re-enable additional STIG hardening after you finish installing the system layer update. For more information, see Enabling additional STIG hardening on page 200.

Upgrading Avaya Aura® Device Services on AVP

About this task

The following are the high-level steps for upgrading Avaya Aura® Device Services to Release 8.0.2 when Avaya Aura® Device Services is installed on an Appliance Virtualization Platform (AVP) host.

The following procedures reference clusters. If you are working with a standalone Avaya Aura® Device Services server, ignore the references to other cluster nodes.

Important:

- You must use the original host name and IP address from the currently installed cluster when deploying OVAs.
- The upgrade procedure backs up Session Manager Data Storage and restores this data when you perform the rollback procedure. Any Session Manager data that is changed between these two points in time will be lost when you restore this data as part of the rollback procedure. Therefore, Avaya recommends that you avoid configuring or performing any maintenance activities on Session Manager until the completion of either the Avaya Aura® Device Services upgrade procedure or the rollback procedure.

Procedure

1. Prepare for the upgrade:
   a. Record the currently installed version of the Avaya Aura® Device Services application.
   b. Obtain a copy of that application installer and copy of the OVA for the currently installed release.
   c. Obtain a copy of the latest system layer update file, application installer file, and OVA.
   d. Back up the Session Manager User Data Storage. This backup is used if you need to abort the upgrade procedure and roll back to the currently installed release.
   e. Back up each node of the Avaya Aura® Device Services cluster. These backups are used if you need to abort the upgrade procedure an roll back to the currently installed release.
   f. Record configuration values from the existing Avaya Aura® Device Services system.
   g. Copy logs, home directory content, and backup files to an external storage.

   Important:

   Complete the upgrade preparation steps before the maintenance window, so you can start the upgrade as soon as the maintenance window starts.
2. Upgrade the existing virtual machines:
   a. Upgrade the system layer.
   b. Upgrade the application.
   c. Back up each node of the Avaya Aura® Device Services cluster. These backups are used in the upgrade procedure.
3. Deploy new virtual machines:
   a. Delete the existing virtual machines of the cluster.
   b. Deploy the new Avaya Aura® Device Services Release 8.0.2 OVA to create new virtual machines for each node in the cluster.
4. Restore the Avaya Aura® Device Services Release 8.0.2 application using the backups created in step 2.

You can also enable the Utility Server.

5. **(Optional)** Migrate the Utility Server data:
   a. Create “no firmware” backups on a legacy 7.1 Utility Services server.
   b. Restore the backup on the Utility Server embedded within the Avaya Aura® Device Services on each cluster node.
6. **(Optional)** If required, you can abort the upgrade procedure and roll back to the previously installed release:
   a. Delete the newly deployed machines of the cluster.
   b. Restore the Session Manager User Data Storage, which was backed up in step 1.
   c. Restore the cluster.

Important:

You *cannot* rollback to Release 8.0.1 if you enabled disk encryption when deploying Release 8.0.2 OVAs in step 3.

Related links

Disk encryption on page 224

Preparing for an AVP upgrade

About this task

Use this procedure to download the latest installation files required for the upgrade and to collect data from the existing Avaya Aura® Device Services servers to upgrade to the new Avaya Aura® Device Services release.

Perform the upgrade preparation procedure before the maintenance window so you can start the upgrade as soon as the maintenance window starts. This procedure does not alter the system and Avaya Aura® Device Services remains available.

Before you begin

Determine the keystore password you want to use when installing Avaya Aura® Device Services Release 8.0.2.

Procedure

1. Record the currently installed version of the Avaya Aura® Device Services application.

   To upgrade to Release 8.0.2, you must have Avaya Aura® Device Services Release 8.0.1.

2. Back up the cluster as described in Backing up Avaya Aura Device Services on page 217.

   When you create backup files for cluster nodes, you can specify a name for each backup file to keep the backup files organized. For example, if the server host name is server1.example.com, then the `app backup –t –d /home/admin recover` command creates the `/home/admin/recover_server1.tar` backup file.

3. Download the application installer file and the OVA file of the same version that is used in the currently installed release.

   You can use these files in case the upgrade is aborted and you need to revert Avaya Aura® Device Services back to the currently installed version.

4. Download the latest versions of the following files:

   - System layer update file.
   - Application installer file.
   - OVA file.

   For more information about system layer updates, see Preparing for an AVP upgrade on page 231.

5. Log in to Avaya Aura® Device Services as an administrative user using an SSH connection.

6. Run the following command to collect the current system logs:

   ```
   app collectlogs collect
   ```

   Avaya Aura® Device Services creates a `.zip` file containing the logs in the `/var/log/Avaya/collected-logs` directory.

   Support teams can resolve issues that might occur on the new system by comparing the collected logs to the logs on the new system.

7. Do the following to record server information and then save the output in a safe location:

   a. To obtain the fully qualified host name, run the following command:

      ```
      hostname -f
      ```

   b. To obtain the IP address and the network mask, run the following command:

      ```
      ifconfig -a | grep inet | grep -v 127.0.0.1
      ```

   c. To obtain the IP address of the default gateway, run the following command:

      ```
      netstat -nrv | grep '^0.0.0.0'
      ```

   d. To obtain the DNS search list and DNS server IP address, run the following command:

      ```
      cat /etc/resolv.conf
      ```

   e. To obtain the NTP server IP address, run the following command:

      ```
      cat /etc/ntp.conf | grep "^server"
      ```

   f. Log in as the administrator and run the following commands to display the user name and primary group for the administrative account:

      ```
      id --user --name
      id --group --name
      ```

   g. If you want to use the same keystore password, obtain the existing keystore password by referencing notes from the original installation.

If you do not want to use the same keystore password, record a new keystore password.

h. Record the current System Manager enrollment password by referencing notes from the original installation.

8. Copy the following files to an off-board storage location using a file transfer program, such as SFTP or SCP:
   - The `.zip` archive containing the logs.
   - Any other desired content from the `/home` directory.
9. For each virtual machine in the cluster, record the network to which the virtual machine is attached, and use the original installation notes to record the OVA profile used while deploying the original OVA.
10. Repeat steps 5 to 9 for all remaining nodes in the cluster.

Next steps

Upgrade the existing AVP virtual machines.

Upgrading the existing AVP virtual machines

About this task

Use this procedure to upgrade the Avaya Aura® Device Services system layer and application on the existing cluster nodes. This procedure prepares the servers for creating backup files that are later used to restore into newly deployed virtual machines that are deployed using Release 8.0.1 OVAs.

Before you begin

- Ensure that you have created system backups and saved the required server information by completing the upgrade preparation procedure. For more information, see Preparing for an AVP upgrade on page 231.
- Ensure that you have the latest system layer update file and latest binary installer file.
- Upgrade to the latest system layer release on all nodes. For more information, see System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs on page 225.

  Important:

  You must apply the system layer update to all nodes in the cluster before starting the upgrade process. Otherwise, the upgrade will fail.
- Determine whether you need to enable the Utility Server.
- To use OAuth, contact Avaya product management to obtain an activation code. For more information, see *Avaya Aura® Device Services Release Notes* for Release 8.0.1. The OAuth feature is currently restricted, so you need a code to enable it.

Procedure

In a cluster environment, repeat steps 1 to 11 on the seed node first, then on the backup node, and then on all other non-seed nodes in the cluster.

1. Log in to a node as an administrator using an SSH connection.
2. **(Optional)** To enable IPv6 support, run the following command to enable IPv6 at the system layer:

   ```
   sys ipv6config set
   ```

   Tip:

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

   ```
   sys ipv6config -h
   ```

3. Run the following command to remove the inactive Avaya Aura® Device Services version:

   ```
   app removeinactive
   ```

4. Transfer the binary file to the administrator's home directory on the Avaya Aura® Device Services server by using a file transfer tool of your choice.
5. Run the following command to make the file executable:

   ```
   sudo chmod 755 aads-<version>.bin
   ```

   For example:

   ```
   sudo chmod 755 aads-8.0.2.0.16.bin
   ```

6. Run the following command to start the upgrade:

   ```
   sudo ./aads-<version>.bin
   ```

   For example:

   ```
   sudo ./aads-8.0.2.0.16.bin
   ```

7. When the system prompts you to enable the Utility Server, do one of the following:
   - If you want to enable the Utility Server, select **Yes**.
   - If you do not want to enable the Utility Server, select **No**.

   Important:

   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.

8. When the system prompts you to enable onboard OpenLDAP, do one of the following:
   - If you want to enable onboard OpenLDAP, select **Yes** .
   - If you do not want to enable onboard OpenLDAP, select **No**.
9. When the system prompts you to enable OAuth, do one of the following:
   - If you want to enable OAuth, select **Yes** and then enter the activation code.

- If you do not want to enable OAuth, select **No**.

10. **(Optional)** When the system prompts you to enable IPv6, do the following:
    - If you want to enable IPv6, select **Yes** and then provide virtual IPv6 addresses of your choice for Avaya Aura® Device Services and the Utility Server, if it is enabled.
    - If you do not want to enable IPv6, select **No**.

    This step is only applicable if you enabled IPv6 at the system layer in step 2.
11. Follow the system prompts to complete the upgrade procedure.
12. Repeat the steps above on the backup node first, and then on all other non-seed nodes in the cluster.
13. If you enabled OAuth, on the seed node, configure Keycloak settings as described in "Configuring Keycloak settings" in *Deploying Avaya Aura® Device Services*.
14. If you enabled IPv6, on all nodes, configure the virtual IPv6 address and Utility Server virtual IPv6 address using the Avaya Aura® Device Services configuration utility.
15. In a cluster environment, if you enabled OAuth, enable OAuth database replication.

    For more information, see Enabling OAuth database replication in a cluster environment on page 74.
16. If onboard Open LDAP was enabled on the system that you are restoring, enable Open LDAP replication on all nodes in the cluster.

    For more information, see Enabling Open LDAP replication on page 255.
17. Log in to the seed node as an administrative user using an SSH connection.
18. Run the `svc aads start` command to start Avaya Aura® Device Services.
19. Repeat steps 17 and 18 on all other cluster nodes.
20. Verify that DRS replication is working for all nodes on System Manager.

    For more information, see Checking for DRS synchronization on page 257.
21. Log in to the seed node as an administrative user using an SSH connection.
22. Run the following command to create a backup:

    ```
    app backup -t -d <home-directory-of-admin-user> upgrade
    ```

    The system creates a file with the `upgrade_<hostname>.tar` name in the administrative user's home directory.
23. Run the following command to add permissions to the backup file:

    ```
    sudo chown admin:admingrp upgrade_<hostname>.tar
    ```
24. Transfer the backup file to an off-board storage location using a file transfer program, such as SFTP or SCP.
25. Repeat steps 23 to 24 for all other cluster nodes.

Next steps

Deploy new AVP virtual machines.

Deploying new AVP virtual machines

About this task

Use this procedure to deploy and prepare Release 8.0.2 virtual machines to complete the upgrade. To improve efficiency, you can perform multiple steps simultaneously across all nodes in the cluster.

Before you begin

- Upgrade the existing AVP virtual machines.
- Ensure that you have the latest Avaya Aura® Device Services installer and OVA.

Procedure

1. Log in to the seed node of the existing cluster as an administrative user using an SSH connection.
2. Run the following command on each node in the cluster to stop Avaya Aura® Device Services and verify that the services are stopped:

   ```
   svc aads stop
   svc aads status
   ```

3. Run the following command to shut down the Avaya Aura® Device Services Release 8.0.2 virtual machine and turn off the power:

   ```
   sudo shutdown -hP now
   ```

4. Repeat the steps above for all other cluster nodes.
5. Do the following to deploy the Avaya Aura® Device Services Release 8.0.2 OVA:
   a. Delete the existing virtual machine for the seed node.
   b. Deploy the Avaya Aura® Device Services OVA for the seed node.
   c. Configure the new server with the server configuration information you saved from the node.

      For more information, see Preparing for an AVP upgrade on page 231.

   d. Attach the new virtual machine to the network recorded for the node in Preparing for an AVP upgrade on page 231.
   e. Repeat substeps a to d for other cluster nodes.
6. If you have an installer that is newer than the one staged in `/opt/Avaya/` within the virtual machine, do the following for each node in the cluster:
   a. Copy the installer to the administrative user's home directory using a file transfer program, such as SFTP or SCP.

b. Run the following commands to move the installer to the standard staging location:

```
sudo mv aads-<new-release>.bin /opt/Avaya
sudo chown ucapp:ucgrp /opt/Avaya/aads-<new-release>.bin
sudo chmod 750 /opt/Avaya/aads-<new-release>.bin
```

c. Run the following command to remove the older installer file staged in the virtual machine:

```
sudo rm /opt/Avaya/aads-<version-to-be-deleted>.bin
```

Next steps

Complete the upgrade.

Completing the upgrade

About this task

Use this procedure to complete the upgrade of Avaya Aura® Device Services to Release 8.0.2.

Before you begin

- Deploy the new AVP virtual machines.
- Ensure that the required Session Manager and System Manager servers are running and reachable.
- Ensure that you are using the same Avaya Aura® Device Services installer that was used for upgrading the existing AVP virtual machines.

Procedure

1. For each node in the cluster, transfer the backup file that you created when performing Upgrading the existing AVP virtual machines on page 233 to the administrative user's home directory.

   Use a file transfer program, such as SFTP or SCP.

2. For each node in the cluster, transfer the Avaya Aura® Device Services installer, which was used for upgrading the existing AVP virtual machines, to the administrative user's home directory.
3. Restore the cluster as described in Restoring an Avaya Aura Device Services cluster on page 220.
4. Verify that DRS replication is working for all nodes on System Manager.

   For more information, see Checking for DRS synchronization on page 257.

5. From the seed node, run the following commands to generate personal information metadata:

```
cdto misc
sudo ./clearPhoneNumberLastSync.sh
```

6. From the Avaya Aura® Device Services web administration portal, perform synchronization with LDAP.

For more information, see Setting up user synchronization with the LDAP server on page 116.

Next steps

- If the Utility Server is enabled on the system, and if you need to migrate the data from a legacy 7.1 Utility Services machine, complete Migrating Utility Server data on page 252.
- Configure AIDE scanning and ClamAV antivirus security tools as described in Security options on page 190.

Rolling back the AVP upgrade

About this task

Use this procedure to abort the upgrade procedure and roll back from Avaya Aura® Device Services Release 8.0.2 to Release 8.0.1.

Important:

Rollback is *not* supported if you enabled disk encryption when you deployed new Release 8.0.2 OVAs.

Based on the state of the system at the time when you decided to roll back, some steps in this procedure might not apply. For example, if the Avaya Aura® Device Services application is not running on a node, then the instructions to stop the node do not apply.

Before you begin

- Complete Preparing for an AVP upgrade on page 231.
- Ensure that the required Session Manager and System Manager servers are running and reachable.

Procedure

1. Log in to the seed node as an administrative user using an SSH connection.
2. Run the following command to stop Avaya Aura® Device Services Release 8.0.2 and verify that the services are stopped:

   ```
   svc aads stop
   svc aads status
   ```

3. Run the following command to shut down the Avaya Aura® Device Services Release 8.0.2 virtual machine and turn off the power:

   ```
   sudo shutdown -hP now
   ```

4. Repeat the steps above for all other cluster nodes.
5. Do the following to deploy the Avaya Aura® Device Services OVA for the previously installed release:
   a. Delete the existing virtual machine for the seed node.
   b. Deploy the Avaya Aura® Device Services OVA for the seed node.

c. Configure the new server with the server configuration information you saved from the node while performing Preparing for an AVP upgrade on page 231.

d. Attach the new virtual machine to the network recorded for the node.

   You obtained this information while performing Preparing for an AVP upgrade on page 231.

e. Repeat steps a to d for other cluster nodes.

6. If the application installer for the previously installed release is older than the one embedded in the OVA that you used to deploy the virtual machine, do the following for each node in the cluster:

   a. Copy the installer to the administrative user's home directory using a file transfer program, such as SFTP or SCP.

   b. Run the following commands to move the installer to the standard staging location:

   ```
   sudo mv aads-<new-release>.bin /opt/Avaya
   sudo chown ucapp:ucgrp /opt/Avaya/aads-<new-release>.bin
   sudo chmod 750 /opt/Avaya/aads-<new-release>.bin
   ```

   c. Run the following command to remove the older installer file staged in the virtual machine:

   ```
   sudo rm /opt/Avaya/aads-<version-to-be-deleted>.bin
   ```

7. On the Home page of the System Manager web console, navigate to **Elements** > **Session Manager** > **System Status** > **User Data Storage**.
8. Click **Backup and Restore**.
9. Select the Session Manager on which you want to run the restore operation.
10. Click **Restore**.
11. From the "Restore File" column, select the backup that you created while performing Preparing for an AVP upgrade on page 231.
12. Do one of the following:
    - Click **Commit** to accept the selection.
    - Click **Reset** to reload the Restore File selection list.
    - Click **Cancel** to cancel the restore request and return to the User Data Storage screen.
13. Click **Confirm** to send a request to each Session Manager to begin the restore operation using the selected file.

    To cancel the restore request, click **Cancel**.
14. Restore the Avaya Aura® Device Services cluster as described in Restoring an Avaya Aura Device Services cluster on page 220.

Upgrading Avaya Aura® Device Services on ESXi or AWS

About this task

This procedure provides the high-level steps for upgrading Avaya Aura® Device Services to Release 8.0.2 when Avaya Aura® Device Services is installed on an ESXi host or an Amazon Machine Image (AMI) in the AWS cloud environment.

Use this procedure if you do not need disk encryption for ESXi or if disk encryption is already enabled in Release 8.0.1. If you need to enable disk encryption for ESXi, see Migrating Avaya Aura Device Services on ESXi on page 244. On AWS deployments, you cannot enable disk encryption on Avaya Aura® Device Services, so use this procedure for all AWS deployments.

This procedure also describes cluster deployments. If you have a standalone Avaya Aura® Device Services deployment, ignore the references to other cluster nodes.

Note:

If required, you can abort the upgrade procedure and roll back to the previously installed release.

Procedure

1. Obtain a copy of the latest system layer update file and application installer file.

   For more information about system layer updates, see System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs on page 225.

2. Perform a full system backup.

   These backups are used if you need to abort the upgrade procedure and roll back to the currently installed Release 8.0.1.

3. Upgrade the virtual machines:
   a. Upgrade the system layer.
   b. Upgrade the Avaya Aura® Device Services application.

4. **(Optional)** Migrate Utility Services data:
   a. Create “no firmware” backups on the legacy 7.1 Utility Services server.
   b. Restore the backup onto each Avaya Aura® Device Services node.

Creating a full system backup

About this task

Create a full Avaya Aura® Device Services backup before performing complex maintenance procedures, such as upgrades. If Avaya Aura® Device Services is backed up, you can abort the upgrade procedure and roll back to the previously installed release if required.

Before you begin

Ensure that you are using Avaya Aura® Device Services Release 8.0.1.

Procedure

Complete Backing up Avaya Aura Device Services on page 217.

Next steps

Upgrade ESXi and AWS virtual machines.

Upgrading ESXi or AWS virtual machines

About this task

Use this procedure to upgrade the Avaya Aura® Device Services system and application layers on the existing servers.

Before you begin

- Back up your Avaya Aura® Device Services Release 8.0.1 system.
- Download the system layer update file and the latest binary installer file.
- Upgrade to the latest system layer release on all nodes. For more information, see System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs on page 225.

  Important:

  You must apply the system layer update to all nodes in the cluster before starting the upgrade process. Otherwise, the upgrade will fail.
- Determine whether you need to enable the Utility Server.
- To use OAuth, contact Avaya product management to obtain an activation code. For more information, see *Avaya Aura® Device Services Release Notes* for Release 8.0.1. The OAuth feature is currently restricted, so you need a code to enable it.

Procedure

In a cluster environment, repeat steps 1 to 11 on the seed node first, then on the backup node, and then on all other non-seed nodes in the cluster.

1. Log in to a node as an administrator using an SSH connection.
2. **(Optional)** To enable IPv6 support for ESXi deployments, run the following command to enable IPv6 at the system layer:

   ```
   sys ipv6config set
   ```

   Tip:

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

   ```
   sys ipv6config -h
   ```

   Important:

   AWS deployments *do not* support IPv6.

3. Run the following command to remove the inactive Avaya Aura® Device Services version:

   ```
   app removeinactive
   ```

4. Transfer the binary file to the administrator home folder on Avaya Aura® Device Services by using a file transfer tool of your choice.
5. Run the following command to make the file executable:

   ```
   sudo chmod 755 aads-<version>.bin
   ```

   For example:

   ```
   sudo chmod 755 aads-8.0.2.0.16.bin
   ```

6. Run the following command to start the upgrade:

   ```
   sudo ./aads-<version>.bin
   ```

   For example:

   ```
   sudo ./aads-8.0.2.0.16.bin
   ```

7. When the system prompts you to enable the Utility Server, do one of the following:
   - If want to enable the Utility Server, select **Yes** and then enter the activation code.
   - If you do not want to enable the Utility Server, select **No**.

   Important:

   You must either enable the Utility Server on all nodes or disable it on all nodes. You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.

8. When the system prompts you to enable onboard OpenLDAP, do one of the following:
   - If you want to enable onboard OpenLDAP, select **Yes** .
   - If you do not want to enable onboard OpenLDAP, select **No**.
9. When the system prompts you to enable OAuth, do one of the following:
   - If want to enable OAuth, select **Yes** and then enter the activation code.
   - If you do not want to enable OAuth, select **No**.
10. **(Optional)** When the system prompts you to enable IPv6, do the following:
    - If you want to enable IPv6, select **Yes** and then provide virtual IPv6 addresses of your choice for Avaya Aura® Device Services and the Utility Server, if it is enabled.
    - If you do not want to enable IPv6, select **No**.

    This step is only applicable if you enabled IPv6 at the system layer in step 2.
11. Follow the system prompts to complete the upgrade procedure.
12. Repeat the steps above on the backup node first and then on all other non-seed cluster nodes.
13. If you enabled OAuth, on the seed node, configure Keycloak settings as described in “Configuring Keycloak settings” in *Deploying Avaya Aura® Device Services*.

14. If you enabled IPv6, on all nodes, configure the virtual IPv6 address and Utility Server virtual IPv6 address using the Avaya Aura® Device Services configuration utility.
15. In a cluster environment, if OAuth was enabled on the system you are upgrading, enable OAuth database replication on all nodes in the cluster.

    For more information, see Enabling OAuth database replication in a cluster environment on page 74.
16. If onboard Open LDAP was enabled on the system that you are restoring, enable Open LDAP replication on all nodes in the cluster.

    For more information, see Enabling Open LDAP replication on page 255.
17. Log in to the seed node as an administrative user using an SSH connection.
18. Run the `svc aads restart` command to restart Avaya Aura® Device Services.
19. Repeat steps 16 and 17 on all other cluster nodes.
20. Verify that DRS replication is working for all nodes on System Manager.

    For more information, see Checking for DRS synchronization on page 257.
21. From the seed node, run the following commands to generate personal information metadata:

    ```
    cdto misc
    sudo ./clearPhoneNumberLastSync.sh
    ```
22. From the Avaya Aura® Device Services web administration portal, perform synchronization with LDAP.

    For more information, see Setting up user synchronization with the LDAP server on page 116.

Next steps

- If you enabled the Utility Server and you need to migrate data from a legacy 7.1 Utility Services machine, complete Migrating Utility Server data on page 252.
- Configure AIDE scanning and ClamAV antivirus security tools as described in Security options on page 190.

Rolling back the ESXi or AWS upgrade

About this task

Use this procedure to abort the upgrade procedure and roll back to the previously installed Avaya Aura® Device Services release. You can roll back to a previously installed release if that release is still present on the server.

In a cluster environment, the order for rolling back nodes is the reverse of the order used for upgrading Avaya Aura® Device Services.

You cannot use Avaya Aura® Device Services during a rollback. In a cluster environment, services are started after all nodes are rolled back.

Before you begin

Complete Upgrading ESXi or AWS virtual machines on page 241.

Procedure

1. Using an SSH connection, log in as an administrator to the node that you last upgraded.
2. Run the following commands to perform the rollback for this node:

```
cd
app rollback
```

3. Repeat the previous steps for all other nodes in the reverse order to the one you used for upgrading Avaya Aura® Device Services.

   The seed node must be the last node that you roll back.
4. Log in to the seed node as an administrator using an SSH connection.
5. Run the `svc aads start` command to start Avaya Aura® Device Services.
6. Repeat steps 4 to 5 for the backup node first and then for all other non-seed nodes.

Next steps

If OAuth was enabled on the system that you are restoring, enable OAuth replication on all nodes in the cluster. For more information, see “Enabling OAuth database replication in a cluster environment” in *Deploying Avaya Aura® Device Services*.

Migrating Avaya Aura® Device Services on ESXi

About this task

This procedure provides the high-level steps for migrating Avaya Aura® Device Services to Release 8.0.2 when Avaya Aura® Device Services is installed on an ESXi host. This procedure does not apply to AWS deployments.

You only need to perform the migration if you need to enable disk encryption on Release 8.0.2. Otherwise, upgrade Avaya Aura® Device Services as described in Upgrading Avaya Aura Device Services on ESXi or AWS on page 240.

This procedure also describes cluster deployments. If you have a standalone Avaya Aura® Device Services deployment, ignore the references to other cluster nodes.

Important:

- You must use the original host name and IP address from the currently installed cluster when deploying OVAs.
- You *cannot* roll back when performing procedures. You can only rollback when performing an upgrade.

Procedure

1. Obtain a copy of the latest system layer update file and application installer file.

For more information about system layer updates, see System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs on page 225.

2. Upgrade the virtual machines:
   a. Upgrade the system layer.
   b. Upgrade the Avaya Aura® Device Services application.
3. Prepare for the migration:
   a. Back up each node of your Avaya Aura® Device Services deployment. These backups are used in the migration procedure.
   b. Record configuration values from the existing Avaya Aura® Device Services system.
   c. Copy logs, home directory content, and backup files to an external storage.

   For more information, see Preparing for migration on page 248.
4. Deploy new virtual machines:
   a. Delete the existing virtual machines.
   b. Deploy the new Avaya Aura® Device Services Release 8.0.2 OVA to create new virtual machines.

   For more information, see Deploying new ESXi virtual machines on page 250.
5. Restore the Avaya Aura® Device Services Release 8.0.2 application using the backups created in step 3.

   For more information, see Completing the migration on page 251.
6. **(Optional)** Migrate Utility Services data:
   a. Create “no firmware” backups on the legacy 7.1 Utility Services server.
   b. Restore the backup onto each Avaya Aura® Device Services node.

Related links

Disk encryption on page 224

Creating a full system backup

About this task

Create a full Avaya Aura® Device Services backup before performing complex maintenance procedures, such as upgrades. If Avaya Aura® Device Services is backed up, you can abort the upgrade procedure and roll back to the previously installed release if required.

Before you begin

Ensure that you are using Avaya Aura® Device Services Release 8.0.1.

Procedure

Complete Backing up Avaya Aura Device Services on page 217.

Next steps

Upgrade ESXi and AWS virtual machines.

Upgrading ESXi virtual machines

About this task

Use this procedure to upgrade the Avaya Aura® Device Services application to the Release 8.0.2 on the existing servers. You will use this Avaya Aura® Device Services system to create backup files, which you will restore on the newly deployed servers.

Before you begin

- Back up your Avaya Aura® Device Services Release 8.0.1 system.
- Download the system layer update file and the latest binary installer file.
- Upgrade to the latest system layer release on all nodes. For more information, see System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs on page 225.

  Important:

  You must apply the system layer update to all nodes in the cluster before starting the upgrade process. Otherwise, the upgrade will fail.
- Determine whether you need to enable the Utility Server.
- To use OAuth, contact Avaya product management to obtain an activation code. For more information, see *Avaya Aura® Device Services Release Notes* for Release 8.0.1. The OAuth feature is currently restricted, so you need a code to enable it.

Procedure

In a cluster environment, repeat steps 1 to 11 on the seed node first, then on the backup node, and then on all other non-seed nodes in the cluster.

1. Log in to a node as an administrator using an SSH connection.
2. **(Optional)** To enable IPv6 support for ESXi deployments, run the following command to enable IPv6 at the system layer:

   ```
   sys ipv6config set
   ```

   Tip:

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

   ```
   sys ipv6config -h
   ```

   Important:

   AWS deployments *do not* support IPv6.
3. Run the following command to remove the inactive Avaya Aura® Device Services version:

   ```
   app removeinactive
   ```

4. Transfer the binary file to the administrator home folder on Avaya Aura® Device Services by using a file transfer tool of your choice.
5. Run the following command to make the file executable:

   ```
   sudo chmod 755 aads-<version>.bin
   ```

   For example:

   ```
   sudo chmod 755 aads-8.0.2.0.16.bin
   ```

6. Run the following command to start the upgrade:

   ```
   sudo ./aads-<version>.bin
   ```

   For example:

   ```
   sudo ./aads-8.0.2.0.16.bin
   ```

7. When the system prompts you to enable the Utility Server, do one of the following:
   - If want to enable the Utility Server, select **Yes** and then enter the activation code.
   - If you do not want to enable the Utility Server, select **No**.

   Important:

   You must either enable the Utility Server on all nodes or disable it on all nodes. You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.
8. When the system prompts you to enable onboard OpenLDAP, do one of the following:
   - If you want to enable onboard OpenLDAP, select **Yes** .
   - If you do not want to enable onboard OpenLDAP, select **No**.
9. When the system prompts you to enable OAuth, do one of the following:
   - If want to enable OAuth, select **Yes** and then enter the activation code.
   - If you do not want to enable OAuth, select **No**.
10. **(Optional)** When the system prompts you to enable IPv6, do the following:
    - If you want to enable IPv6, select **Yes** and then provide virtual IPv6 addresses of your choice for Avaya Aura® Device Services and the Utility Server, if it is enabled.
    - If you do not want to enable IPv6, select **No**.

    This step is only applicable if you enabled IPv6 at the system layer in step 2.
11. Follow the system prompts to complete the upgrade procedure.
12. Repeat the steps above on the backup node first and then on all other non-seed cluster nodes.
13. If you enabled OAuth, on the seed node, configure Keycloak settings as described in “Configuring Keycloak settings” in *Deploying Avaya Aura® Device Services*.
14. If you enabled IPv6, on all nodes, configure the virtual IPv6 address and Utility Server virtual IPv6 address using the Avaya Aura® Device Services configuration utility.
15. In a cluster environment, if OAuth was enabled on the system you are upgrading, enable OAuth database replication on all nodes in the cluster.

For more information, see Enabling OAuth database replication in a cluster environment on page 74.

16. If onboard Open LDAP was enabled on the system that you are restoring, enable Open LDAP replication on all nodes in the cluster.

    For more information, see Enabling Open LDAP replication on page 255.

17. Log in to the seed node as an administrative user using an SSH connection.
18. Run the `svc aads restart` command to restart Avaya Aura® Device Services.
19. Repeat steps 16 and 17 on all other cluster nodes.
20. Verify that DRS replication is working for all nodes on System Manager.

    For more information, see Checking for DRS synchronization on page 257.

Next steps

Prepare for migration.

Preparing for migration

About this task

Use this procedure to record server information and back up your upgraded Avaya Aura® Device Services Release 8.0.2 system. This information and backup files are required when you deploy new Avaya Aura® Device Services Release 8.0.2 OVAs.

Before you begin

- Determine the keystore password you want to use when installing Avaya Aura® Device Services Release 8.0.2.
- Upgrade the system layer and the Avaya Aura® Device Services application to Release 8.0.2 as described in Upgrading ESXi or AWS virtual machines on page 241.

Procedure

1. Record the currently installed version of the Avaya Aura® Device Services application.
2. Back up the cluster as described in Backing up Avaya Aura Device Services on page 217.

   When you create backup files for cluster nodes, you can specify a name for each backup file to keep the backup files organized. For example, if the server host name is server1.example.com, then the `app backup –t –d /home/admin recover` command creates the `/home/admin/recover_server1.tar` backup file.

In cluster deployments, repeat steps 4 to 7 on all nodes starting from the seed node.

3. Run the following command to add permissions to the backup file:

   ```
   sudo chown admin:admingrp upgrade_<hostname>.tar
   ```

4. Log in to Avaya Aura® Device Services as an administrative user using an SSH connection.

5. Run the following command to collect the current system logs:

   ```
   app collectlogs collect
   ```

   Avaya Aura® Device Services creates a `.zip` file containing the logs in the `/var/log/Avaya/collected-logs` directory.

   Support teams can resolve issues that might occur on the new system by comparing the collected logs to the logs on the new system.

6. Do the following to record server information and then save the output in a safe location:

   a. To obtain the fully qualified host name, run the following command:

      ```
      hostname -f
      ```

   b. To obtain the IP address and the network mask, run the following command:

      ```
      ifconfig -a | grep inet | grep -v 127.0.0.1
      ```

   c. To obtain the IP address of the default gateway, run the following command:

      ```
      netstat -nrv | grep '^0.0.0.0'
      ```

   d. To obtain the DNS search list and DNS server IP address, run the following command:

      ```
      cat /etc/resolv.conf
      ```

   e. To obtain the NTP server IP address, run the following command:

      ```
      cat /etc/ntp.conf | grep "^server"
      ```

   f. Log in as the administrator and run the following commands to display the user name and primary group for the administrative account:

      ```
      id --user --name
      id --group --name
      ```

   g. If you want to use the same keystore password, obtain the existing keystore password by referencing notes from the original installation.

      If you do not want to use the same keystore password, record a new keystore password.

   h. Record the current System Manager enrollment password by referencing notes from the original installation.

7. Copy the following files to an off-board storage location using a file transfer program, such as SFTP or SCP:

   - The `.zip` archive containing the logs.
   - Any other desired content from the `/home` directory.

8. In cluster deployments, repeat steps 3 to 6 on all nodes.

9. On each node in the cluster, run the following commands to stop Avaya Aura® Device Services and to verify that the services are stopped:

   ```
   svc aads stop
   svc aads status
   ```

10. On each node in the cluster, run the following command to shut down the Avaya Aura® Device Services virtual machine and turn off the power:

    ```
    sudo shutdown -h now
    ```

    If the virtual machine stays powered on, shut down the virtual machine using the vSphere client interface.

11. For each virtual machine in the cluster, record the network to which the virtual machine is attached, and use the original installation notes to record the OVA profile used while deploying the original OVA.

Next steps

Deploy new ESXi virtual machines.

Deploying new ESXi virtual machines

About this task

Use this procedure to deploy and prepare new Release 8.0.2 virtual machines for the migration.

In cluster deployments, perform this procedure on each cluster node. To improve efficiency, you can perform multiple steps simultaneously across all nodes in the cluster.

Before you begin

- Created system backups and save the required server information by completing the migration preparation procedure. For more information, see Preparing for migration on page 248.
- Upgrade the existing ESXi virtual machines.
- Ensure that you have the latest Avaya Aura® Device Services Release 8.0.2 installer and OVA.

Procedure

1. Delete the existing virtual machine for the node.
2. Deploy the Avaya Aura® Device Services 8.0.2 OVA for the node using the server configuration information you gathered for your upgraded Release 8.0.2 Avaya Aura® Device Services.

   For more information about OVA deployment procedures, see the “VMware deployment options” section in the “Initial setup” chapter in *Deploying Avaya Aura® Device Services*.

3. Attach the new virtual machine to the network recorded for the node in Preparing for migration on page 248.
4. If you have an installer that is newer than the one staged in `/opt/Avaya/` within the virtual machine, do the following for each node in the cluster:
   a. Copy the installer to the administrative user’s home directory using a file transfer program, such as SFTP or SCP.

b. Run the following commands to move the installer to the standard staging location:

```
sudo mv aads-<new-release>.bin /opt/Avaya
sudo chown ucapp:ucgrp /opt/Avaya/aads-<new-release>.bin
sudo chmod 750 /opt/Avaya/aads-<new-release>.bin
```

c. Run the following command to remove the older installer file staged in the virtual machine:

```
sudo rm /opt/Avaya/aads-<version-to-be-deleted>.bin
```

Next steps

Complete the migration.

Completing the migration

About this task

To complete the migration to Release 8.0.2, deploy the Avaya Aura® Device Services application on a new virtual machines and then restore backup files.

Before you begin

- Deploy the new ESXi virtual machines.
- Ensure that the required Session Manager and System Manager servers are running and reachable.
- Ensure that you are using the same Avaya Aura® Device Services installer that was used to upgrade the existing ESXi virtual machines to Release 8.0.2.

Procedure

1. For each node in the cluster, transfer the backup file that you created when performing Upgrading the existing AVP virtual machines on page 233 to the administrative user's home directory.

   In cluster deployments, ensure that you transfer each backup file to a node with the corresponding host name.

   To transfer backup files, use a file transfer program, such as SFTP or SCP.

2. For each node in the cluster, transfer the Avaya Aura® Device Services application installer that you used to update the existing ESXi virtual machines to the administrative user's home directory.
3. Do one of the following:
   - If you are migrating a standalone system, perform the steps in Restoring Avaya Aura Device Services in a standalone environment on page 218.
   - If you are migrating a cluster, perform the steps in Restoring an Avaya Aura Device Services cluster on page 220.
4. Verify that DRS replication is working for all nodes on System Manager.

   For more information, see Checking for DRS synchronization on page 257.

5. From the seed node, run the following command to generate personal metadata:

```
cdto misc
sudo ./clearPhoneNumberLastSync.sh
```

6. From the Avaya Aura® Device Services web administration portal, perform synchronization with LDAP.

   For more information, see Setting up user synchronization with the LDAP server on page 116.

Next steps

- If the Utility Server is enabled on the system, and if you need to migrate the data from a legacy 7.1 Utility Services machine, complete Migrating Utility Server data on page 252.
- Configure AIDE scanning and ClamAV security tools as described in Security options on page 190.

Migrating Utility Server data

About this task

Use this procedure to migrate data from the legacy Avaya Aura® Utility Services to the Utility Server embedded within Avaya Aura® Device Services. This process restores a backup, which was created on the Utility Services server, into the Utility Server embedded within Avaya Aura® Device Services. Since the Utility Server uses only a subset of data from the Avaya Aura® Utility Services server, this procedure only extracts the required subset of data.

Important:

- In a cluster environment, perform this procedure on all cluster nodes, starting from the seed node.
- Any active firmware packages are deactivated during this procedure.

Procedure

1. Create a “no firmware” backup on the legacy Avaya Aura® Utility Services machine and then store the backup file on the machine that you use to access the web administration portal.

   Important:

   Ensure that the **No firmware** backup option is used for this procedure. The legacy Avaya Aura® Utility Services servers allow you to choose whether the backup file will contain phone firmware. For disk space considerations, the Utility Server embedded within Avaya Aura® Device Services only supports backups that do not include phone firmware. You must manually upload phone firmware on the Utility Server and then unpack and activate the firmware.

2. Log in to web administration portal for the Utility Server using the following URL:

   `https://<Utility_Server_address>:8543/admin.html`

Replace `Utility_Server_address` with the virtual IP address or FQDN of the Utility Server.

Note:

Use the user name and password of the administrative user that you created while deploying the OVA.

3. Navigate to **Miscellaneous** > **Utility Services Backup and Restore**
4. Click **Browse** and navigate to the backup file created in step 1.
5. Select the backup file and click **Open**.
6. Click **Upload Backup**.
7. Repeat the previous steps for all other cluster nodes.

Upgrading existing test configurations

About this task

Upgrading Avaya Aura® Device Services may sometimes introduce new auto-configuration settings. In such a scenario, all existing auto-config test configurations must be upgraded to reflect newly introduced settings. For this, you must perform the following task.

Procedure

1. Log on to the Avaya Aura® Device Services server as an administrator.
2. Run the following commands:

```
cdto misc
sudo ./clitool-acs.sh upgradeAutoConfigTestConfigurations
```

This command automatically upgrades the existing test configurations.

Running a patch to allow Avaya IX™ Workplace Client for Windows to connect to the Web Deployment service

About this task

For software updates through Avaya IX™ Workplace Client for Windows clients, you must apply a patch by following the instructions in this section. The patch opens port 8442 for the Web deployment service and sets up port 8442 to pass web deployment requests without certificate validation.

Important:

You must use this procedure only if you have Avaya IX™ Workplace Client for Windows clients and ESG servers in your environment.

If you have only Avaya Aura® Device Services and Avaya IX™ Workplace Client for Windows clients in the network, you must set the REST and OAMP fields on the **Client Administration** > **Client Settings** screen to None.

You can use the patch with the following arguments:

- enable: To apply the workaround to allow Avaya IX™ Workplace Client for Windows to reach the Web Deployment service.
- disable: To revert the workaround to allow Avaya IX™ Workplace Client for Windows to reach the Web Deployment service.

If the disable argument is used, the patch removes port 8442 from nginx and iptables. In this procedure, the enable argument is used to apply the workaround.

You must run this patch after every upgrade or rollback of Avaya Aura® Device Services so that the Web deployment service works for the Windows client.

Procedure

1. Go to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/`.
2. Run the following command:

   ```
   sudo ./webdeployment-patch.sh enable
   ```

   For example, the **`sudo ./webdeployment-patch.sh enable`** command displays the following messages:

   ```
   grep acs-nginx-webdeployment-8442.conf /opt/Avaya/DeviceServices/
   7.1.0.0.243/nginx/1.8.0-1/conf/nginx.conf
   acs-nginx-webdeployment-8442.conf will be added now
   iptables rule will be added now
   iptables: Saving firewall rules to /etc/sysconfig/iptables:
   [  OK  ]
   2017-01-24_12:17:36 Reloading Nginx .....................
   [  OK  ]
   ```

   After running the patch, you must download URL and appcast URL to use port 8442.
3. Log on to the Avaya Aura® Device Services web administration portal.
4. In the navigation pane, click **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.
5. On the Software Update Deployment page, change the Download URL port for Appcast to 8442.

   For example, `https://<AADS FQDN or IP Address>:8442/acs/resources/webdeployment/downloads/Avaya Equinox Setup 3.0.0.136.msi`.
6. Change the APPCAST URL port in Dynamic Configurations to 8442.

For example, `https://<AADS FQDN or IP Address>:8442/acs/resources/webdeployment`.

Running a patch to allow the Avaya Aura® Web Gateway to connect to the Avaya Aura® Device Services automatic configuration service

About this task

You can perform this task only if you have the Avaya Aura® Web Gateway server set up in the Avaya Aura® Device Services environment and if the REST certificate policy is set to NONE on the Avaya Aura® Device Services web administration portal.

You must run the `dynamicconfigurations-patch.sh` script to allow the connection between the Avaya Aura® Web Gateway and Avaya Aura® Device Services automatic configuration service using the certificate policy. This patch opens the port 8440 for auto-configuration service and the Avaya Aura® Device Services provides the auto-configuration service on port 8440.

You must run this patch after every upgrade or rollback or migration of Avaya Aura® Device Services to allow the Avaya Aura® Web Gateway to reach Avaya Aura® Device Services automatic configuration service.

You can use the patch with the following arguments:

- enable: To open port 8440 to allow Avaya Aura® Device Services to communicate with the Avaya Aura® Web Gateway.
- disable: To close port 8440 from nginx and iptables.

Procedure

Run the following commands:

```
cdto misc
sudo ./dynamicconfigurations-patch.sh enable
```

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/openldap.log` file.

   The following is an example of a `/var/log/Avaya/openldap/openldap.log` file entry indicating that data replication is enabled:

   ```
   Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 fd=17 ACCEPT from IP=1.2.3.5:63930
   (IP=1.2.3.4:3268)
   Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 BIND
   dn="cn=administrator,dc=company,dc=com" method=12
   Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 BIND
   dn="cn=administrator,dc=company,dc=com" mech=SIMPLE ssf=0
   Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 RESULT tag=97 err=0 text=
   ```

   If `/var/log/Avaya/openldap/openldap.log` contains error messages, such as `ldap_sasl_bind_s failed rc -1`, then some nodes are not accessible. In this case, you must make these nodes accessible from other nodes and then repeat the data replication procedure.
9. Repeat steps 1 to 8 on all remaining nodes on the cluster.

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.

Checking for DRS synchronization

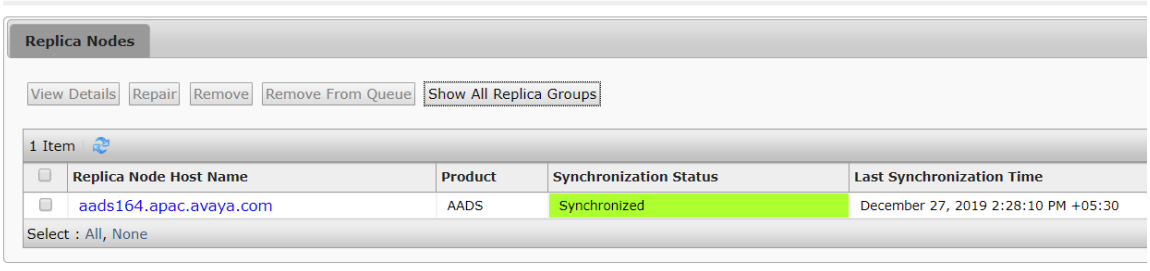
About this task

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.

   The following is an example of a synchronized Avaya Aura® Device Services system.



Chapter 17: Troubleshooting

DRS remains in Ready to Repair state

Cause

Tomcat must restart to register the DRS URL.

Solution

Restart Tomcat.

The DRS state changes to repairing, synchronizing, and then synchronized.

DRS remains in repairing state for a long time

Cause

When Avaya Aura® Device Services logs are set to the FINEST level, large nginx logs are created during the DRS process. Writing these logs on the disk affects system performance, which causes connection timeouts.

Solution

1. Change the log level to WARN.
2. From System Manager, synchronize the node.

   After the node is synchronized, you can change the log level back to FINEST.

Related links

Changing a logging level on page 205
Checking for DRS synchronization on page 257

DRS remains in not polling state

Condition

A DRS polling error occurs.

Cause

System Manager and Avaya Aura® Device Services are not in the same DNS or the `/etc/hosts` file for System Manager does not include the Avaya Aura® Device Services IP addresses and FQDN.

Solution

1. Update the System Manager `/etc/hosts` file to include the Avaya Aura® Device Services IP addresses and FQDNs.
2. Update the Avaya Aura® Device Services `/etc/hosts` file to include the System Manager IP addresses and FQDNs.
3. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
4. Reconfigure System Manager details again and wait until the DRS configuration process is complete.

DRS fails with constraint error

Cause

DRS replication fails with a constraint error.

Solution

1. Perform a manual repair from the System Manager web interface.
2. If the above step fails, do the following to re-register DRS:
   a. Go to the `/opt/Avaya/DeviceServices/<build>/CAS/<build>/drs` directory.
   b. Run the following commands in sequence:

```
removeReplicationEntry.sh
drsInstall.sh
drsStart.sh
```

Services are not working properly after an installation or upgrade

Condition

After installing or upgrading Avaya Aura® Device Services in a cluster, services are not working properly. Log files contains an error, such as the following:

```
2017-11-10 14:34:38 ERROR datastore:191 - (ConfigurationStore.java:2166) Decryption
failed for server bind credentials, setting it to original
 2017-11-10 14:34:38 ERROR impl:191 - (SecurityServiceImpl.java:117) Exception occurred
while decrypting data
 2017-11-10 14:34:38 FINE impl:245 - (SecurityServiceImpl.java:117) Exception stack
```

```
trace
 javax.crypto.IllegalBlockSizeException: Input length must be multiple of 16 when
decrypting with padded cipher
 at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:922)
 at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:833)
 at com.sun.crypto.provider.AESCipher.engineDoFinal(AESCipher.java:446)
 at javax.crypto.Cipher.doFinal(Cipher.java:2165)
 at
com.avaya.cas.security.impl.SecurityServiceImpl.apoKruptos(SecurityServiceImpl.java:107)
 at
com.avaya.cas.security.impl.SecurityServiceAdapter.apoKruptos(SecurityServiceAdapter.jav
a:57)
 at
com.avaya.cas.datastore.ConfigurationStore.getServerConfigParamFromRow(ConfigurationStor
e.java:2164)
 at
com.avaya.cas.datastore.ConfigurationStore.getAllServerConfigurations(ConfigurationStore
.java:2062)
 at
com.avaya.acs.cli.AadsCryptoToolCliApp.encryptLdapPasswords(AadsCryptoToolCliApp.java:17
0)
 at com.avaya.acs.cli.AadsCryptoToolCliApp.main(AadsCryptoToolCliApp.java:104)
```

Solution

1. Navigate to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/config` and check the `install.properties` file.

   The files at both the nodes should have the same value for SEED_NODE.
2. If the values are different, uninstall Avaya Aura® Device Services from all nodes.
3. Run the Avaya Aura® Device Services binary installer as described in *Deploying Avaya Aura® Device Services*.

EASG login using craft username results in an Access Denied error

Cause

You can only paste 99 characters in PuTTY versions earlier than 0.63. Therefore, you might get an Access Denied error if you exceed the character limit.

Solution

Update PuTTY to the latest version.

ESG cannot connect to Avaya Aura® Device Services

Condition

ESG cannot connect to Avaya Aura® Device Services when the REST certificate policy is set to None. This occurs in deployments with Avaya Aura® Device Services and Avaya Aura® Web Gateway, if the following features are being used:

- Avaya Aura® Device Services web deployment feature for desktops.
- WebRTC call feature with Avaya Aura® Web Gateway.

Solution

Set the certificate validation policy in the Avaya Aura® Device Services web administration portal to Optional. Do not set the certificate validation policy to None.

Web deployment binaries for Avaya IX™ Workplace Client for Windows and Avaya IX™ Workplace Client for Mac must be moved to another web server or to the Avaya Aura® Device Services web server on a unchallenged web port.

Note:

The Web deployment service is only accessible within the enterprise network or through VPN.

A new private key failed to generate

Condition

The Avaya Aura® Device Services configuration utility closes abruptly while configuring the SSH/RSA Public/Private keys.

Cause

The `/home` directory is full. Therefore, Avaya Aura® Device Services cannot create the `/authorized_keys` file. The log file displays a disk space warning.

Solution

Clean up the `/home` directory.

Check for Updates feature is not working

Condition

The Check for Updates feature on Avaya IX™ Workplace Client for Windows does not work and an error is displayed.

Solution

1. On the Windows computer where Avaya IX™ Workplace Client is installed, navigate to `C:\Windows\System32\drivers\etc\` and add the virtual FQDN of System Manager to the `hosts` file in the following format:

   ```
   <IP Address> <virtual FQDN of System Manager>
   ```

2. Close Avaya IX™ Workplace Client and ensure that the client is not running in Windows Task Manager.
3. Run the following command as an administrator:

   ```
   ipconfig /flushdns
   ```

4. Restart Avaya IX™ Workplace Client.
5. If the Check for Updates feature is still not working, go to **Client Settings** > **Support**.
6. Click **Reset Application**.
7. Configure Avaya IX™ Workplace Client and then log in to the client.

   You can configure the client settings using the Automatic Configuration service.

Slow Avaya Aura® Device Services performance

Condition

Performance is slow.

Cause

The network latency between all Avaya Aura® Device Services servers and their respective Session Manager servers is more than 5 ms.

Solution

The network latency must be less than 5 ms.

Primary System Manager fails

Condition

The primary System Manager fails. Geographic redundancy is enabled in System Manager.

Cause

Avaya Aura® Device Services does not support the System Manager geographic redundancy mode. Therefore, Avaya Aura® Device Services cannot switch to the secondary System Manager automatically.

Solution

If the primary System Manager fails and you need to use Avaya Aura® Device Services before it is restored, perform the following steps to enroll Avaya Aura® Device Services against the secondary System Manager. In a cluster environment, perform these steps on each cluster node.

Important:

After the primary System Manager is back online, you must re-enroll against the primary System Manager.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the `app configure` command.
3. Select **Front-end host, System Manager and Certificate Configuration**.
4. Select **System Manager FQDN** and provide the FQDN of the secondary System Manager.
5. Select **System Manager Enrollment Password** and provide the enrollment password of the secondary System Manager.
6. Click **Apply**.
7. When the primary System Manager is back online, repeat this procedure and provide the FQDN and the enrollment password of the primary System Manager.

Unable to access the web administration portal when the primary node Session Manager is non-operational

Condition

In a cluster, if the Session Manager associated with the primary Avaya Aura® Device Services node is non-operational, the Avaya Aura® Device Services web administration portal is unavailable.

Solution

Use the FQDN for the other nodes to access the Avaya Aura® Device Services web administration portal when the primary node is non-operational.

PPM certificate error

Condition

If you upgrade Session Manager from a release earlier than release 6.2 FP4 to Release 7.0.1 or later before installing Avaya Aura® Device Services, the system displays a PPM certificate error while adding contacts.

Cause

The error occurs because Session Manager expects a SIP CA certificate.

Solution

1. Log in to Avaya Aura® Device Services as an administrator.
2. Go to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin`.
3. Run the following command:

   ```
   sudo ./demo_certs.sh -I
   ```

   The system displays the message `Certificate was added to keystore.`.
4. Restart Avaya Aura® Device Services.

Repairing faulty users

About this task

The Contact Integrity Audit generates a list of faulty users, which cannot be repaired automatically. You can repair faulty users manually by de-registering or re-registering users in Avaya Aura® Device Services.

Procedure

1. Log in to Avaya Aura® Device Services as an administrator.
2. Run the `cdto misc` command.
3. Run the following command to get the list of faulty users:

   ```
   sudo ./clitool-acs.sh dataIntegrityAuditDiagnostics fetchFaultyUsers
   ```
4. For any faulty user you want to repair, do the following:
   a. Run the following command to de-register the user from Avaya Aura® Device Services:

      ```
      sudo ./clitool-acs.sh runUserDiagnostics -d <email address of the user>
      ```
   b. After the user is de-registered, log out and log back in to the Avaya Aura® Device Services client for the user.
5. If the faulty users are not yet repaired, investigate the user's contact data.

Exception in the AADS.log file

Condition

When running a command in Avaya Aura® Device Services, the `AADS.log` file shows an exception error, such as the following:

```
ERROR 04 Dec 2017 10:00:23,846 main com.avaya.cas.management.logging -
(Log4jPropertiesConfig.java:123) IOException while reading config file /opt/Avaya/
DeviceServices/7.1.2.0.557/CAS/7.1.2.0.557/tomcat/8.0.24/lib/log4j.properties:
java.io.FileNotFoundException: /opt/Avaya/DeviceServices/7.1.2.0.557/CAS/7.1.2.0.557/
tomcat/8.0.24/lib/log4j.properties (No such file or directory)
```

Solution

Ignore the exception error.

The AADS.log file contains contact integrity data

Condition

The `AADS.log` file contains the following type of data:

```
WARN 11 Dec 2017 03:00:05,426 Audit Manager scheduling pool-3
com.avaya.acs.services.drs.core - (DataIntegrityService.java:157) Contact Integrity
audit is disabled, so no further processing will happen...
 WARN 11 Dec 2017 03:00:15,430 Audit Manager scheduling pool-0
com.avaya.acs.services.drs.core - (DataIntegrityService.java:157) Contact Integrity
audit is disabled, so no further processing will happen...
 WARN 11 Dec 2017 03:00:25,434 Audit Manager scheduling pool-0
com.avaya.acs.services.drs.core - (DataIntegrityService.java:157) Contact Integrity
audit is disabled, so no further processing will happen...
 WARN 11 Dec 2017 03:00:35,444 Audit Manager scheduling pool-1
com.avaya.acs.services.drs.core - (DataIntegrityService.java:157) Contact Integrity
audit is disabled, so no further processing will happen...
```

Solution

None. If a Contact Integrity Audit is not run, then the system resources are not burdened.

System Manager does not show Avaya Aura® Device Services alarms

Condition

Alarms are generated on Avaya Aura® Device Services and user profiles are properly created and assigned, but System Manager does not show these alarms.

Solution

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

2. Go to the `/var/net-snmp` directory.
3. Memorize the timestamp of the `snmpd.conf` file.
4. Log in to the System Manager web console and navigate to **Home** > **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
5. From the agents list, select the Avaya Aura® Device Services node for which alarms are not displayed on System Manager.
6. On the Serviceability Agents page, select Avaya Aura® Device Services and click **Manage Profiles**.
7. On the next page, click **Commit**.

   The timestamp of the `snmpd.conf` file should be updated.
8. If the timestamp of the `snmpd.conf` file was not updated, perform the remaining steps.

   If the timestamp was updated, then you do not need to do anything else.
9. Log in to System Manager as the root user using SSH.
10. Run the `locate recoverAgent.sh` command to obtain the full path to the `recoverAgent.sh` script.

    For example:

    ```
    >locate recoverAgent.sh
    >/opt/Avaya/Mgmt/7.1.11/remoteSnmpConfig/utility/recoverAgent.sh
    ```
11. Run the following command to remove the Avaya Aura® Device Services entry from System Manager:

    ```
    sh <path_to_recoverAgent.sh> <AADS_IP_address>
    ```

    In this command, `<path_to_recoverAgent.sh>` is the full path to `recoverAgent.sh` and `<AADS_IP_address>` is the IP address of Avaya Aura® Device Services.
12. Log in to the Avaya Aura® Device Services CLI as the root user.
13. Run the following command:

    ```
    $SPIRIT_HOME/scripts/utils/reinitilizeSnmpdConfiguration.sh
    ```

    Note:

    The command might fail when restarting snmpd. This is the expected behavior.

    ```
    Stopping existing snmpd service...
    Stopping snmpd (via systemctl): [ OK ]
    Restarting snmpd (via systemctl): Job for snmpd.service failed because the
    control process exited with error code. See "systemctl status snmpd.service"
    and "journalctl -xe" for details.
     [FAILED]
    Setting the reinitialized property to true
    ```
14. Run the following command:

    ```
    systemctl restart AADSSpiritAgent.service
    ```

Firmware upgrade fails for certain endpoints

Condition

When using the Utility Server, the firmware upgrade fails for certain endpoints, such as 9611, 9621, or 9640 phones.

Cause

DHCP option 242 does not have the TLSSRVRID parameter set to 0. In this case, some endpoints cannot:

- Fetch settings files and firmware from the Utility Server using HTTPS.
- Generate a certificate file that uses the Utility Server IP address as the Common Name (CN).

Solution

On your DHCP server, set TLSSRVRID to 0 for DHCP option 242.

The following is an example of the DHCP option 242 configuration: `TLSSRVR=10.103.1.39, TLSPORT=1543, TLSSRVRID=0`.

Open LDAP replication fails

Condition

Open LDAP replication fails. The `/var/log/Avaya/openldap/openldap.log` file contains entries such as the following:

- `Server unwilling to perform`
- `ldap bind failed`
- `syncrepl: consumer state is newer than provider`

Solution

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

   ```
   sudo systemctl restart slapd
   ```

3. Repeat the steps above on all remaining nodes in the cluster.
4. Review the `/var/log/Avaya/openldap/openldap.log` file and ensure that it does not contain any error messages.

If the `/var/log/Avaya/openldap/openldap.log` file still contains error messages, do the following:

5. On all nodes in the cluster, run the following commands:

   ```
   cdto openldap
   sudo ./recover_openldap.sh
   ```

6. Enable Open LDAP replication again.

Open LDAP replication fails if Avaya Aura® Device Services uses a custom identity certificate for server interfaces

Condition

When you use a custom identity certificate for an Avaya Aura® Device Services service interface, Open LDAP replication might fail. The `/var/log/Avaya/openldap/openldap.log` file contains the `TLS negotiation failure` entry.

Cause

The custom identity certificate is applied to a single node and not to the entire cluster.

Solution

Re-import the custom certificate as described in Managing server interface certificates on page 128. Ensure that you select **Apply For Cluster** when importing the certificate.

Response delay from Open LDAP

Condition

Open LDAP performance is slow.

Cause

Avaya Aura® Device Services writes Open LDAP logs into the `/var/log/Avaya/openldap/openldap.log` file. If the log file size becomes too large, Open LDAP performance might decrease.

Solution

Avaya recommends to truncate the `/var/log/Avaya/openldap/openldap.log` file when the file size exceeds 30 MB.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command to check the `/var/log/Avaya/openldap/openldap.log` file size:

   ```
   ls -lh /var/log/Avaya/openldap/openldap.log
   ```

3. If the file size is more than 30 MB, run the following command to clear the file content:

   ```
   sudo truncate -s 0 /var/log/Avaya/openldap/openldap.log
   ```

Allocating unused disk space to logical volumes

About this task

In rare circumstances, you might need to allocate free disk space to a specific disk volume to address unexpected disk engineering issues. Only use this procedure in these circumstances. For additional assistance, contact Avaya support.

Important:

You can only allocate free disk space to disk volumes if data encryption is disabled on Avaya Aura® Device Services. If data encryption is enabled, you *cannot* allocate free disk space.

Before you begin

- Increase the size of the disk that hosts logical volumes. For example, if a logical volume requires an additional 20.0 GiB of space and the host disk is currently 50.0 GiB, then you must change the disk size to 70.0 GiB. For more information, see Increasing the virtual disk size of ESXi virtual machines on page 271 and Increasing the virtual disk size of AWS virtual machines on page 273.
- Since the allocation of disk space to a volume cannot be undone at the operating system level, create a snapshot of the virtual machine before performing the allocation procedure. If an error occurs during the procedure, reverting to the snapshot will restore the system to the point prior to where allocations were performed. After reverting to the snapshot, you can try to perform the allocation procedure again.

  Tip:

  To save system resources and maintain the performance of the virtual machine, delete the snapshot after the allocation procedure is completed successfully.

  On VMware ESXi, you can choose to exclude the virtual memory of the virtual machine from the snapshot. Therefore, the snapshot creation process will take less time. However, if the virtual memory is excluded from the snapshot, the state of the running application processes and other system processes is not preserved in the snapshot. Therefore, any runtime data will be lost when you revert to that snapshot. Avaya recommends that you shut down the application using the `svc aads stop` command before taking the snapshot. After you allocate disk space and delete the snapshot, start the application using the `svc aads start` command.

Procedure

1. Log in to the virtual machine as an administrative user using an SSH connection.
2. Run the following command to scan the disks on the virtual machine to detect available free space:

   ```
   sys volmgt --scan
   ```

   This command scans the virtual disks of the system to detect a size increase. Then the command displays the file system summary, which includes the size and amount of free storage for each virtual disk, and the size and usage of the volumes hosted on these disks.

In the following example, 50.00 GiB of free storage is available to be allocated to the volumes on disk 1.

```
                          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 |
+------------------------------+-----------------------------------------------+
```

Tip:

- You can run the `sys volmgt –h` command to get basic information on command line syntax, and the `sys volmgt –hh` command for verbose help.
- You can review summaries, such as the one above, at any time by running the `sys volmgt --summary` command. This command does not scan disks for newly available unallocated storage. Use this command if you know that disk sizes have not been increased since the last summary was displayed.

3. Run the following commands to allocate a specific amount of disk space to a volume:

```
sys volmgt --extend <volume> <x>[m|g|t]
```

In this command:

- `<volume>` specifies the name of the volume that is displayed when you run either the `sys volmgt --summary` or `sys volmgt --scan` command.
- `<x>` specifies amount of space. `<x>` is a decimal number.
- `m` means megabytes.
- `g` means gigabytes.
- `t` means terabytes.

For example, the following command allocates 10.5 GiB to the `/var/log` volume:

```
sys volmgt --extend /var/log 10.5g
```

4. Run the following command to allocate all remaining disk space to a volume on the disk:

```
sys volmgt --extend <volume> --remaining
```

All `--extend` operations are run as background tasks.

a. To monitor the status of the operation in progress or of the last completed operation, run one of the following commands:

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

The first command uses the `tail` browser to display the results. The second command uses the `less` browser to display the results.

b. To gather all volume management logs into a `.zip` file in the current working directory, run the following command:

```
sys volmgt --logs
```

c. If you suspect that the reported size of a file system is not correct, check if the operation is still in progress by running the following command:

```
sys volmgt --status
```

d. If the status is reported as “Complete”, you can correct the situation by running `--extend` without an increment value:

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

This operation does not add more space to the volume that hosts the file system. Instead, it reissues the command to make full use of the volume space. The file system expansion process is part of the original `--extend` operation, which is used to increase the volume size. However, in some cases, this operation might be interrupted and require the above command to re-initiate the expansion.

ESXi virtual hardware adjustments

The following sections describe how to perform virtual hardware adjustments on ESXi virtual machines. These adjustments are external to the guest operating system of the virtual machine.

These virtual hardware adjustment procedures only apply to virtual machines hosted on VMware ESXi hosts.

Important:

If you are using Appliance Virtualization Platform (AVP), avoid adjusting virtual hardware parameters because your adjustments could affect other applications hosted on the same AVP instance.

Increasing the virtual disk size of ESXi virtual machines

About this task

Use this procedure to increase the size of virtual disks on existing Avaya Aura® Device Services virtual machines.

An Avaya Aura® Device Services virtual machine has three virtual disks. VMware vSphere emulates the physical environment very closely. Therefore, virtual disks of a virtual machine can be referred to as “hard disks”.

Disk number	Description
Hard disk 1	Operating system and application software.
Hard disk 2	Application logs.
Hard disk 3	Application data.

Note:

You cannot reduce the disk size.

Procedure

1. Log in to the virtual machine as an administrative user using an SSH connection.
2. Run the following command to perform a graceful shutdown of the virtual machine operating system and to power off the virtual machine:

   ```
   sudo shutdown -hP now
   ```
3. Using the vSphere client, log in to either the vCenter server or ESXi host.
4. Delete all virtual machine snapshots.

   Note:

   You cannot modify the size of virtual disks when snapshots exist on the system.
5. In the vSphere client inventory, right-click the required virtual machine and then select **Edit Settings**.
6. Navigate to the Virtual Hardware tab.
7. Select the desired unit size, such as GB, TB, or MB, and enter the new value for the disk size.

   Important:

   Perform this step with caution because updating the disk size cannot be undone. Make sure you use the desired units and the disk size value. Otherwise, you might need to delete the virtual machine and deploy a new OVA.
8. Click **OK**.
9. Repeat steps 5 to 8 if you need to increase the disk size of any other virtual disks.

Next steps

Distribute the allocated free space between the logical volumes as described in Allocating unused disk space to logical volumes on page 269.

Adjusting the CPU and memory resources of the Avaya Aura® Device Services virtual machine

About this task

Use this procedure only in a VMware virtualized environment.

Before you begin

Install VMware with an Enterprise Plus license.

Procedure

1. Shut down the Avaya Aura® Device Services virtual machine.
2. In the vSphere client inventory, right-click the Avaya Aura® Device Services virtual machine and select **Edit Settings**.
3. In the Virtual Machine Properties window, in the Hardware tab, click **Memory** or **CPUs**.
4. Do one of the following:
   - Change the memory configuration.
   - Change the CPU settings.
5. Click **OK** to exit the window.
6. Restart the Avaya Aura® Device Services virtual machine.

Increasing the virtual disk size of AWS virtual machines

About this task

Use this procedure to increase the size of on an existing Avaya Aura® Device Services virtual machine deployed on AWS.

The following table shows the three virtual disks and the block devices of these disks, which are used by Avaya Aura® Device Services virtual machines on AWS.

Disk number	Block device	Desciption
Disk 1	`/dev/sda1`	Stores operating system and application software.
Disk 2	`/dev/xvdb`	Stores application logs.
Disk 3	`/dev/xvdc`	Stores application data.

Note:

You cannot reduce the disk size.

Procedure

1. On the AWS console, navigate to **Services** > **Compute**, and then click **EC2**.
2. On the EC2 Management Console page, click **Instances**.

3. Select the instance to which you want to add storage.

   AWS displays instance details.
4. Click the **Description** tab.
5. In the **Block devices** field, select a disk for which you want to increase the size.

   The options are:

   - disk1
   - disk2
   - disk3

   Note:

   Avaya Aura® Device Services restart is required when you change the size of disk1. If you do not modify disk1, Avaya Aura® Device Services restart is not required.
6. In the **EBS ID** field, click the ID.

   AWS displays the Volumes page with only the selected device.
7. To update the storage on the EBS disk volume, click **Actions** > **Modify Volume**.
8. In the Modify Volume window, in the **Size** field, enter the required disk size.
9. Click **Modify**.
10. In the Confirmation window, click **Yes**.
11. In the Status window, click **Close**.
12. If you updated disk1, do the following to restart the system for the changes to take effect:
    a. Log in to the virtual machine as an administrative user using an SSH connection.
    b. Run the `sudo reboot` command.

       If Avaya Aura® Device Services is running when you run this command, then Avaya Aura® Device Services will be gracefully shut down.

    Note:

    The process of increasing the disk size might take some time to complete. Monitor the size of the virtual disks and only proceed with any other disk-related activities after the size changes take effect.

Next steps

Distribute the allocated free space between the logical volumes as described in Allocating unused disk space to logical volumes on page 269.

Cannot reinstall a non-seed node due to Cassandra startup error

Condition

When reinstalling a non-seed node, Avaya Aura® Device Services becomes unresponsive while trying to start the Cassandra database.

Cause

If the non-seed node was not uninstalled from the cluster properly, then it remains as a registered cluster node in the Cassandra database.

Solution

1. On the non-seed node, run the following command to uninstall the node:

   ```
   sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/uninstaller/
   uninstallAADS.sh
   ```

2. On the seed node, run the following command to restart services:

   ```
   svc aads restart
   ```

3. Reinstall the non-seed node.

Troubleshooting for OAuth2 authorization

OAuth2 authentication does not work as expected

Condition

Keycloak is not properly configured. As a result, OAuth2 authentication is not working as expected.

Solution

Verify the initial Keycloak configuration in the Avaya Aura® Device Services configuration utility and the Keycloak web administration portal. For more information about using the Keycloak web administration portal, see Avaya Aura Device Services OAuth2 management on page 39.

Keycloak documentation is available at Keycloak documentation.

Login page for the third-party identity provider is not displayed

Condition

The user cannot reach the login page for the third-party identity provider when trying to log in to Avaya IX™ Workplace Client.

Solution

- If the issue happens during the automatic configuration phase of the client, ensure that you configured DNS records on your DNS server to return an Avaya Aura® Device Services URL with the following parameter: `?preferredAuth=bearer`.
- Ensure that the machine where the client is running can connect to the address that is provided in the IDPSSODescriptor file as the SSO service URL.

An error page is displayed instead of the Login page

Condition

When the user tries to log in to Avaya IX™ Workplace Client, the user is redirected to the third-party identity provider, but an error page is displayed instead of the Login page.

Cause

The following are possible causes:

- Avaya Aura® Device Services, the third-party identity provider, and the machine where the client is running use different time synchronization services.
- The IDPSSODescriptor metadata file contains parameters that are not compatible with Avaya Aura® Device Services.
- The third-party identity provider is configured incorrectly.

Solution

- Ensure that the machine where the client is running uses the same network time synchronization service as Avaya Aura® Device Services and the third-party identity provider.
- Ensure that the IDPSSODescriptor metadata file contains only compatible parameters.
- Contact your third-party identity provider to verify configuration.

Related links

Interoperability issues between Avaya Aura Device Services and the third-party identity provider on page 279

Login credentials do not work

Condition

When the user tries to log in to Avaya IX™ Workplace Client, the user is directed to the third-party identity provider's Login page, but the user's login credentials do not work. The Login page displays information about an incorrect user name and password even though user entered the correct credentials.

Cause

Incorrect configuration of the identity provider on Keycloak.

Solution

Verify the third-party identity provider configuration on Keycloak.

Avaya IX™ Workplace Client displays an authentication error

Condition

The user can log in on the identity provider's Login page, but Avaya IX™ Workplace Client displays an authentication error.

Solution

- Verify that the mapping of the identity provider attributes are correct.
- Verify that the user record created on Keycloak contains the correct attribute values.

Related links

Verifying the mapping of the identity provider's attributes on page 278
Verifying the attributes imported for a user on page 277

Verifying the attributes imported for a user

Procedure

1. In a web browser, enter the following URL:

   `https://<AADS IP or FQDN>:<AADS PORT>/auth/admin`

2. Enter the user name and the password that you created when configuring the Keycloak settings.
3. In the left area, click **Users**.
4. In the **Search** field, type the user's name and then click the magnifying glass icon.
5. Click the link in the ID column for the user to open user's properties.
6. Click the **Attributes** tab.
7. Ensure that Keycloak displays correct values for all attributes that the third-party identity provider releases.
8. If an attribute is missing or no value is set for attribute, ensure that the attribute mapping for the identity provider contains all attributes that the third-party identity provider releases.
9. Click the **Role Mappings** tab.
10. From **Client Roles**, select **aads**.
11. Ensure that the **Assigned Roles** and **Effective Roles** fields contain the correct Avaya Aura® Device Services user role for the user.
12. If the user has no user role assigned, do the following:
    a. Ensure that the role mapping attribute in the identity provider mapping is correct.

b. Ensure that the identity provider's SAMLResponse contains the correct information for the role mapping attribute.

Verifying the mapping of the identity provider's attributes

Procedure

1. In a web browser, enter the following URL:

   `https://<AADS IP or FQDN>:<AADS PORT>/auth/admin`

2. Enter the user name and the password that you created when configuring the Keycloak settings.
3. In the left area, click **Identity Providers**.

   Currently, the identity provider is automatically imported with the name "Shibboleth".

4. Click the **Shibboleth** link.
5. Click the **Mappers** tab.
6. Verify that the attribute mapping uses correct names for attributes that are released by the identity provider.

   Tip:

   You can open a a decrypted SAMLResponse returned from the identity provider in a new browser window and then compare the attribute names from the SAMLResponse with attriubte names that are used in the Keycloak attribute mapping.

A test user cannot log in to the identity provider

Condition

When setting up the connection between the third-party identity provider and Avaya Aura® Device Services, a test user is typically used to verify that configuration of the third-party provider and Avaya Aura® Device Services. When testing the connection, the user logs in to the identity provider, but the login fails.

Cause

The identity provider might not be correctly configured. This results in the Keycloak service storing incorrect user information. Therefore, the login fails.

Solution

Delete the user record from the Keycloak database.

1. Log in to the Keycloak web administration interface.
2. In the left area, click **Users**.
3. In the **Search** field, type the user's name and then click the magnifying glass icon.
4. In the Actions column, click **Delete** for the user to delete the user's record.

When the user log in again, Keycloak creates a new database entry with the correct user information.

Interoperability issues between Avaya Aura® Device Services and the third-party identity provider

Condition

Avaya Aura® Device Services cannot communicate with the third-party identity provider. Avaya IX™ Workplace Client cannot use SSO capabilities.

Solution

To communicate with a third-party SAML v2.0 identity provider, Avaya Aura® Device Services must negotiate certain SAML v2.0 parameters with the identity provider. To prevent issues, upload the identity provider's IDPSSODescriptor metadata file to Avaya Aura® Device Services when you enable OAuth2 authentication support on Avaya Aura® Device Services. The IDPSSODescriptor file automatically populates many identity provider settings on Avaya Aura® Device Services.

After you configure the identity provider on Keycloak, it generates the SPSSODescriptor metadata file. You can provide this file to the identity provider. You can find this file at the following location:

`https://<AADS FQDN>/auth/realms/SolutionRealm/broker/<SAML ALIAS>/endpoint/descriptor`. In this URL, `<AADS FQDN>` is the Avaya Aura® Device Services front-end FQDN, and `<SAML ALIAS>` is the alias of the identity provider.

You can prevent many issues by exchanging the IDPSSODescriptor and SPSSODescriptor files. However, if the metadata files contain information that is incorrect or not supported by Avaya Aura® Device Services, interoperability issues might still occur.

If you continue to experience problems, verify the following settings on the third-party identity provider and Avaya Aura® Device Services Keycloak.

- The identity provider that you use must support the Service Provider-initiated (SP-initiated) SAML v2.0 flow.
- The NameID format option must be set to emailAddress.
- The identity provider must support the HTTP POST binding.
- The identity provider and Avaya Aura® Device Services must use the same time synchronization service.
- Ensure that no network firewalls must block access from Avaya Aura® Device Services to the identity provider.
- The certificates specified in the identity provider's IDPSSODescription file must be valid.
- For attribute mapping, Keycloak must use the same spelling for attribute names as the identity provider. These attribute names are case-sensitive.
- The attribute names that the identity provider releases must be correctly mapped as friendly names or attribute names on Keycloak.

  By default, Keycloak maps the friendly name of the attribute.
- Role information must be correctly released to Avaya Aura® Device Services, so that the correct user role can be assigned to each user.

Avaya Spaces integration

Avaya Spaces connectivity errors

The following table shows the errors that Avaya Aura® Device Services can display when it cannot connect to Avaya Spaces.

Error	Description	Solution
Avaya Spaces Host unreachable	Avaya Spaces is down.	Verify that Avaya Spaces is accessible.
	An incorrect Avaya Spaces URL is used to set up integration.	Navigate to **Spaces** > **Configuration** and ensure that **Spaces URI** is set to `accounts.avayacloud.com`.
Avaya Spaces configuration error, Either certificate expired OR invalid API key and secret	Avaya Spaces integration settings are incorrectly configured on Avaya Aura® Device Services.	Re-configure Avaya Spaces integration.
	An Avaya Spaces CA certificate is not valid or has expired.	Re-upload the Avaya Spaces CA certificate in the web browser you use to log in to the Avaya Aura® Device Services web administration portal.
Avaya Spaces connection failed	Network connectivity issues.	• Verify your network setup. • Gather logs and contact Avaya support personnel.

Related links

Setting up Avaya Spaces integration on page 79

Avaya Aura® Device Services does not contain the latest Avaya Spaces CA certificate

Condition

Avaya Aura® Device Services displays the OFFLINE status for Avaya Spaces on the Configuration page. The error message contains the following text:

```
Status: OFFLINE
failed on processing exception javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to
find valid certification path to requested target.
```

System Managerraises the “AADS Spaces certificate expired” error.

Cause

Avaya Aura® Device Services does not contain the latest Avaya Spaces CA certificate in the public CA truststore.

Solution

You must manually download the latest Avaya Spaces CA certificate and import it to the Avaya Aura® Device Services public CA truststore using the **keytool** command.

This procedure is for the Google Chrome browser. For other browsers, perform a search on documentation for exporting an SSL certificate from a website for that browser.

1. In the Google Chorme browser, navigate to https://accounts.avayacloud.com.
2. Press F12 to open Developer Tools.
3. Click the **Security** tab.
4. In the Security overview section, click **View certificate**.
5. In the Certificate window, click the **Certification Path** tab.
6. Select the root CA and click **View Certificate**.
7. In the new Certificate window that is opened, click the **Details** tab.
8. Click **Copy to File**.
9. In the Certificate Export Wizard, click **Next**.
10. In the Export File Format window, select **Base-64 encoded X.509 (.CER)** and then click **Next**.
11. Select a location where you want to store the certificate and then click **Next**.
12. Click **Finish**.
13. Copy the certificate to the home directory of the administrative user on Avaya Aura® Device Services.

    You can use any file transfer program, such as SFTP or SCP.
14. Log in to the Avaya Aura® Device Services CLI.
15. Run the following command:

```
sudo keytool -importcert -noprompt -alias <ALIAS_NAME> -file
<PATH_TO_CERTIFICATE> -keystore /opt/Avaya/DeviceServices/<VERSION>/CAS/<VERSION>/
cert/publicCA-ts.jks -storepass <KEYSTORE_PASSWORD>
```

    In this command:

    - <ALIAS> is a name of your choice that the public CA truststore will use for the Avaya Spaces CA certificate.
    - <PATH_TO_CERTIFICATE> is the full path to the Avaya Spaces CA certificate.
    - <KEYSTORE_PASSWORD> is the Keystore password created during Avaya Aura® Device Services deployment.

Cannot register an enterprise user on Avaya Spaces

Condition

Avaya Aura® Device Services cannot register an enterprise user on Avaya Spaces. On the Assign License page, Avaya Aura® Device Services displays the FAILED status for that user.

Cause

- Temporary connection issues between Avaya Spaces and Avaya Aura® Device Services.
- Settings configured for a user in the enterprise LDAP directory do not meet Avaya Spaces requirements.

  For example, the registration process fails if the domain part of the user's email address does not match any of the domains configured for your company on Avaya Spaces.

Solution

1. Perform the registration procedure for the user again.
2. If the enterprise user is not correctly configured in your enterprise directory, do the following:
   a. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces** > **Users and License** > **Assign License**.
   b. Select the user and then click **Delete**.
   c. Update settings for the user in your enterprise LDAP directory.
   d. Re-add the user for registration.
   e. Register the user on Avaya Spaces.

Related links

Adding enterprise users for registration on Avaya Spaces on page 86
Registering enterprise users on Avaya Spaces on page 87
Removing an unregistered user on page 88

Avaya Spaces user management operation fails

Condition

Avaya Aura® Device Services cannot:

- Update or deallocate a license for an Avaya Spaces user.
- Delete an Avaya Spaces user.

Avaya Aura® Device Services displays the FAILED status for that user in the list of Avaya Spaces users on the View and Manage page.

Solution

1. Review the error message.

2. Ensure that the connection to Avaya Spaces is up.
3. Ensure that the System Manager does not display any Avaya Spaces-related alarms.
4. Repeat the required management operation for the user.

   You must resolve any alarms related to Avaya Spaces connection before repeating the required management operation.

Related links

Deallocating licenses on page 94
Assigning a different license to Avaya Spaces users on page 95
Removing users from your Avaya Spaces company on page 96

Logs collected using the collectlogs command are encrypted

Condition

When data encryption is enabled on Avaya Aura® Device Services, log files that you collect using the **collectlogs** command are encrypted.

Cause

The **collectlogs** command only collects Avaya Aura® Device Services logs. If logs are encrypted, this command does not provide an option to decrypt logs. To collect and encrypt decrypted logs, you must use the **collectAndDecryptLogs.sh** script.

Solution

The **collectAndDecryptLogs.sh** script allows you to collect all logs from a single node.

1. As an administrator, log in to the CLI of the Avaya Aura® Device Services node from which you want to collect logs.
2. Run the following commands:

   ```
   cdto misc
   sudo ./collectAndDecryptLogs.sh
   ```

   Avaya Aura® Device Services collects all logs from the node, decrypts them, and stores the decrypted logs in a TAR archive in the following directory:

   `/opt/Avaya/DeviceServices/<AADS VERSION>/CAS/<AADS VERSION>/log-collection/collected-logs/`
3. **(Optional)** Download the archive with log files to your machine using a file transfer program, such as SFTP or SCP.
4. If you need to collect logs from other nodes, repeat the steps above for the required nodes in the cluster.

Related links

collectlogs on page 291

Chapter 18: 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 IX™ Workplace Client for Android, iOS, Mac, and Windows	Perform system planning and configuration for: • Avaya IX™ Workplace Client for Android • Avaya IX™ Workplace Client for iOS • Avaya IX™ Workplace Client for Mac • Avaya IX™ Workplace Client for Windows	System administrators, support personnel
Using Avaya Spaces	Administer Avaya Spaces.	System administrators, support personnel

Title	Use this document to:	Audience
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
Other		
Avaya Aura® Device Services Data Privacy Controls Addendum	Understand how Avaya Aura® Device Services processes user's personal data.	Customers, service providers, system administrators, support personnel
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 the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
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 only displays the documents for the selected category.
7. Click **Enter**.

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in**Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- 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 **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics 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 collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable **Include in email notification** to receive email alerts.
  - 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 website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log on to the website. 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.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

  Note:

  Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to 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: Additional administration tools

You can use the following tools for Avaya Aura® Device Services administration:

- The JConsole java tool

  JConsole uses the extensive instrumentation of the Java Virtual Machine (Java VM) to provide information about the performance and resource consumption of applications running on the Java platform.

  You can use jconsole to monitor the following components:

  - Tomcat
  - Serviceability Agent (also known as spiritAgent)

  For more information about using the jconsole utility, see the Oracle documentation.

  Important:

  JConsole is a graphical tool and can be run locally from an Avaya Aura® Device Services node that has a graphical desktop environment installed.

- Avaya Aura® Device Services tools such as clitool-acs, and collectLogs.
  - clitool-acs

    A tool that has multiple usage possibilities. The parameters specified in the command determine the usage of the clitool-acs utility.
  - collectLogs

    Enables you to collect and download the logs from an Avaya Aura® Device Services node.
  - statusAADS

    A tool that displays the status of the Avaya Aura® Device Services server and of the related services.

    The statusAADS.sh script is located in the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin` directory.
- Linux tools such as ping, nslookup, ip, ethtool, wget, and curl
  - ping

Sends an ICMP ECHO_REQUEST to network hosts.

- nslookup

  Queries the internet servers interactively.

- ip

  Displays and manages routing devices, policy routing and tunnels.

  You can use this command to identify nodes that have a virtual IP address.

- ethtool

  Queries and manages network driver and hardware settings.

  You can use this command to confirm that the physical network adaptor is enabled and available.

- wget

  Downloads files from the Web.

  You can use this tool to perform resource discovery for a user.

- curl

  Transfers a URL.

clitool-acs

The **clitool-acs** utility provides multiple usage possibilities, depending on which parameters the utility receives in the command line.

The utility is located in the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc` directory.

Usage example

Run the **clitool-acs.sh** utility with the appropriate parameters. To view the command options, run the clitool-acs.sh utiltity without any parameters. You must run this utility with the sudo privileges.

Note:

The **clitool-acs** utility does not create report directories automatically. Before running the utility, you must run the following commands to create a report directory and set the read, write, and execute permissions to this directory:

```
mkdir <report_directory>
sudo chmod 777 <report_directory>
```

collectlogs

The **app collectlogs** command enables you to collect and download the logs from an Avaya Aura® Device Services node. For example, if you run the following command, two logs will be downloaded from the 10.10.10.1 node:

```
$ app collectlogs collect -n 2 -ip 10.10.10.1
```

By default, if details are not specified, the system will download all 20 logs from the local node.

For more information about the available options, run the following command:

```
$ app collectlogs h
```

Note:

Avaya recommends that you collect and download logs using the web administration portal. For more information, see Changing a logging level on page 205 and Downloading logs on page 206.

Related links

Logs collected using the collectlogs command are encrypted on page 283

statusAADS utility

The **statusAADS.sh** utility displays the status of the Avaya Aura® Device Services server and of the related services.

Usage example

Run the `statusAADS.sh` script from the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin` directory.

Note:

You can also run the **app status** command.

```
[avaya@AWSDev-14 /]$ sudo /opt/Avaya/DeviceServices/8.0.1.0.243/CAS/8.0.1.0.243/bin/
statusAADS.sh
[sudo] password for avaya:
2020-01-09_11:00:04 Displaying status for Avaya Aura Device Services Application
2020-01-09_11:00:04 ulimit file count ..................  [  OK  ]
2020-01-09_11:00:04 ulimit process count ..............  [  OK  ]
2020-01-09_11:00:04 iptables status ....................  [  OK  ]
2020-01-09_11:00:04 RecoveryManager Watchdog status .....  [  OK  ]
2020-01-09_11:00:04 RecoveryManager Service status ......  [  OK  ]
2020-01-09_11:00:05 net-SNMP status ....................  [  OK  ]
2020-01-09_11:00:05 RecoveryManager status .............  [  OK  ]
2020-01-09_11:00:05 AADSKeepalived status ................. [INACTIVE]
2020-01-09_11:00:05 AADSTomcat status ....................  [  OK  ]
2020-01-09_11:00:05 AADSNginx status .....................  [  OK  ]
```

Checking Avaya Aura® Device Services status

Procedure

1. Log in to the Avaya Aura® Device Services CLI.
2. Type `svc aads status`.

   The system displays the current status of Avaya Aura® Device Services

Shutting down Avaya Aura® Device Services gracefully

Procedure

1. Log in to the Avaya Aura® Device Services CLI.
2. Run the following command:

```
svc aads stop
```

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

    Command invocation syntax:
        sys <command> <arguments>

    Command syntax:
        sys <command> -h
```

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

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.

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

ipv6config
    Manages configuration of server-level IPv6.

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

passwdrules
    Manages the configuration of password rules.

encryptionStatus
    Show the status of disk encryption.

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

encryptionLocalKey
    Enables and disables disk encryption local key.

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

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

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

sys secconfig command

sys secconfig provides access to the **secconfig** command, which existed in previous releases. The following is an example of this command:

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

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

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

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

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

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

[admin@server4950aads ~]$
```

sys versions command

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

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

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

[admin@server4889aads ~]$
```

sys volmgt command

Syntax help: sys volmgt --help

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

Important:

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

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 smcvemgt usage examples

Command for querying current tunable settings

The following command queries the current tunable settings for the next boot, as well as the current runtime. This command also indicates whether there is hardware support for Variant #2/Spectre.

```
sys smcvemgt --query
```

Command for enabling patches with default settings

The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is configured for default mode. In default mode, the kernel selects the Variant #2/Spectre mitigation mechanism based on the CPU architecture of the host machine.

```
sys smcvemgt --set enabled
```

Commands for enabling patches with specific settings

- The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is set to kernel space only.

  ```
  sys smcvemgt --set v2=kernel v3=enabled
  ```

- The following command enables patches for Variant #2/Spectre, which are configured for user space with “Retpoline”, or “return trampoline”. Variant#3/Meltdown retains its current settings.

  ```
  sys smcvemgt --set v2=user+retp
  ```

Command for disabling patches

The following command disables patches for Variant #2/Spectre and Variant #3/Meltdown.

```
sys smcvemgt --set disabled
```

Command for disabling patches for a specific vulnerability

The following command disables patches for Variant #3/Meltdown. Variant #2/Spectre retains its current settings.

```
sys smcvemgt --set v3=disabled
```

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
```

passwdrules command

Description

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

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

Syntax

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

show	Shows the server password rule configuration, including default, minimum, and maximum values.
set	Sets server password rules. If you do not specify any options, then Avaya Aura® Device Services prompts you to configure each option separately. If you do not specify a certain option, Avaya Aura® Device Services continues to use the existing rule for this option.
set-default	Sets server password rules to their default values.

Syntax help

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

Options

Option	Description
`--diff=`*INTEGER*	Number of characters in the new password that must not be present in the old password.
`--min-len=`*INTEGER*	Minimum length of the password.
`--min-digs=`*INTEGER*	Minimum number of digits in the password.
`-min-upper=`*INTEGER*	Minimum number of uppercase characters in the password.
`--min-lower=`*INTEGER*	Minimum number of lowercase characters in the password.

Option	Description
`--min-other=`*`INTEGER`*	Minimum number of special characters, such as `!`, `@`, `_`, or *****, in the password.
`--min-class=`*`INTEGER`*	Minimum number of character classes that must be present in the password. The character classes are: • Digits • Uppercase characters • Lowercase characters • Special characters
`--max-repeat=`*`INTEGER`*	Maximum allowed number of consecutively repeated characters. For example, if you set this parameter to 3, then the following password is invalid: `paaassword`, because `a` is repeated three times.
`--max-class-repeat=`*`INTEGER`*	Maximum allowed number of consecutively repeated characters of the same class. For example, if you set this parameter to 3, then the `pas1sw2or3d` password is invalid, because the first three characters, which are `p`, `a`, and `s`, belong to the same character class.
`--history=`*`INTEGER`*	Number of previous passwords that must not match the new password.

Example

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

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

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

Data encryption commands

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

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

Important:

In AWS deployments, you enable data encryption on AWS itself. Therefore, you cannot use the system layer commands for disk encryption management in AWS deployments.

encryptionPassphrase command

Description

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

Syntax

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

add	Enables you to set up an encryption passphrase.
change	Enables you to change the existing encryption passphrase.
remove	Removes the encryption passphrase.
list	Displays information about passphrases and slot assignments.

encryptionStatus command

Description

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

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

Syntax

```
sys encryptionStatus
```

encryptionRemoteKey command

Description

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

Syntax

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

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

encryptionLocalKey command

Description

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

Syntax

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

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

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`

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, Avaya Aura® Device Services 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, Avaya Aura® Device Services 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, Avaya Aura® Device Services displays the available subcommands. For example, the following commands give the same results: • `cd /opt/Avaya/DeviceSerivces/<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`
`cdto logs`	`/opt/Avaya/DeviceServices/<version>/logs`
`cdto ilogs`	`/opt/Avaya/DeviceServices/.AADSInstallLogs`
`cdto tlogs`	`/opt/Avaya/DeviceServices/<version>/tomcat/<Tomcat version>/logs`
`cdto cassandra`	`/opt/Avaya/DeviceServices/<version>/cassandra/<Cassandra version>`
`cdto openldap`	`/opt/Avaya/DeviceServices/<version>/CAS/<version>/openldap`

Appendix B: Managing DNS and NTP addresses

Updating DNS addresses and search domains

About this task

DNS addresses and search domains are configured when you deploy the Avaya Aura® Device Services OVA. Avaya Aura® Device Services stores information about DNS server in the `/etc/resolv.conf` configuration file. Use this procedure if you want to configure additional DNS addresses and search domains after Avaya Aura® Device Services installation. For example, if you use primary and secondary DNS servers and you only configured the primary DNS server during the Avaya Aura® Device Services OVA deployment, you can use this procedure to configure the secondary DNS server.

Procedure

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

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

3. Open the `resolv.conf` file in a text editor.

   For example, to open the file in vi, run the `vi ./resolv.conf` command.

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>...` For example: `search example.com local.test`.

   You can add one DNS name server on each line, as per the following format:

   `nameserver <ipv4-address>` For example, `nameserver 192.0.2.1`.

5. Save the changes and close the text editor.
6. To verify the changes, run the `diff ./resolv.conf.orig ./resolv.conf` command.
7. To replace the system file, run the `sudo cp ./resolv.conf /etc/resolv.conf` command.

8. To inspect the updated system copy, run the `cat /etc/resolv.conf` command.
9. To clean up local copies, run the `rm ./resolv.conf ./resolv.conf.orig` command.

Updating NTP addresses

About this task

Your NTP address is configured when you deploy the Avaya Aura® Device Services OVA. Avaya Aura® Device Services stores information about NTP addresses in the `/etc/ntp.conf` configuration file. Use this procedure if you want to configure additional NTP addresses after Avaya Aura® Device Services installation. For example, if you use primary and secondary NTP servers and you only configured the primary NTP server during the Avaya Aura® Device Services OVA deployment, you can use this procedure to configure the secondary NTP server.

Procedure

1. Log in to the Avaya Aura® Device Services CLI 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. Open the `ntp.conf` file in a text editor.

   For example, to open the file in vi, run the `vi ./ntp.conf` command.

   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. Save the changes and close the text editor.
6. To verify your changes, run the `diff ./ntp.conf.orig ./ntp.conf` command.
7. To replace the system file, run the `sudo cp ./ntp.conf /etc/ntp.conf` command.
8. To inspect the system file, run the `cat /etc/ntp.conf` command.
9. To clean up the local files, run the `rm ./ntp.conf ./ntp.conf.orig` command.

10. To apply the changes, run the `sudo reboot` command to restart Avaya Aura® Device Services.

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 IX™ Workplace Client softphones are referenced separately in this document.
Fully Qualified Domain Name (FQDN)	A domain name that specifies the exact location of the domain in the tree hierarchy of the Domain Name System (DNS).
Network Time Protocol (NTP)	A protocol used to synchronize the real-time clock in a computer.
Secure Shell (SSH)	Secure Shell (SSH) is a group of standards and an associated network protocol that the system can use to establish a secure channel between a local and a remote computer. SSH uses public-key cryptography to mutually authenticate a user and a remote computer. SSH uses encryption and message authentication codes to protect the confidentiality and integrity of the data that is exchanged between the two computers.
Simple Network Management Protocol (SNMP)	A protocol for managing devices on IP networks.
SSL (Secure Sockets Layer) Protocol	The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.
TCP	Transmission Control Protocol.
TLS	Transport Layer Security

UDP	User Datagram Protocol. This is a communication method, similar to TCP.

Index

A

B

C

D

E

F

I

J

K

L

M

N

O

P

R

S

T

U

V

W