Administering Avaya Aura® Device Services

Release 7.1.2
Issue 2
December 2017

© 2016-2017, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published 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. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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 7.1, Issue 1	July 2017	• Added information on managing logs, see Managing logs on page 100. • Updated information on administration tools. See Administration tools on page 14
Release 7.1.2, Issue 2	December 2017	• Updated Dynamic Configuration on page 32. • Updated Upgrading Avaya Aura Device Services on page 129. • Added a new field, **Use Additional Base Context DN**. See Enterprise LDAP Server Configuration field descriptions on page 108. • Added Configuring additional base context DNs on page 112. • Added migration information for Avaya Aura® Device Services Release 7.1.2 in the sections under Avaya Aura Device Services migration on page 133. • Added AWS-specific management options on page 120. • Added Repairing faulty users on page 145.

Chapter 2: Avaya Aura® Device Services overview

Avaya Aura® Device Services is co-resident with Session Manager, but it is delivered as a separate OVA. You can deploy Avaya Aura® Device Services through Amazon Web Services (AWS), VMware, or Solution Deployment Manager.

Avaya Aura® Device Servicesprovides the following services to the Avaya Equinox® clients:

- **Contact:** To use the contact service, a user must be provisioned on the user on LDAP Server. Using the contact service, you can:
    - Add, update, and delete a contact.
    - Perform an enterprise search for contacts.

      Avaya Aura® Device Services supports directory searches of up to 300 contacts. The number of contacts displayed in the search results varies for each client.
    - Set and retrieve information, such as, preferred names or pictures. Using the Picture service, you can create, override, delete, and update the user pictures. You can also include these picture URLs in the contact information or search results.
    - Search and retrieve information about Avaya Scopia® users and terminals.

      You can use Avaya Aura® Device Services to search for Avaya Scopia® users and terminals only when Avaya Equinox Management address is configured on Avaya Aura® Device Services.
- **Notification:** The Notification service provides a common infrastructure that allows a client or endpoint to subscribe to receive events from a number of service resources using a single connection.
- **Dynamic Configuration:** The Dynamic Configuration service provides discovery of configuration settings to UC Clients. You can customize these settings on a global, group, individual, or platform basis. The Dynamic Configuration service uses the automatic configuration feature of Avaya Equinox® to facilitate the configuration details to the UC clients. This helps the user to avoid manual configuration of their client. To log in to the client, the user needs to provide their email address or Windows user ID, along with their enterprise credentials.
- **Web Deployment:** The Web Deployment service publishes and deploys UC client updates to end user devices. The Web Deployment service is supported on the Avaya Equinox® desktop clients.

New in this release

The following is a summary of new functionality that has been added to Avaya Aura® Device Services Release 7.1.2.

Amazon Web Services deployments

Avaya Aura® Device Services now supports Amazon Web Services deployments.

Migrations

A new migration process is available for migrating from Avaya Aura® Device Services Release 7.1 to the Release 7.1.2.

RedHat support

RedHat 7.3 is now supported. The previous 6.x versions are no longer supported. This impacts Avaya Aura® Device Services migrations.

Default REST service API port change

Prior to Avaya Aura® Device Services Release 7.1.2, the default REST API port was 8443. From Avaya Aura® Device Services Release 7.1.2, the port 8443 has been changed to 443.

Note:

- For the upgrade and migration of a system using port 8443, the value of the port will be preserved after the upgrade and migration. The REST API continues to use the port 8443.
- For a new install of Avaya Aura® Device Services, the REST API will use port 443.
- If you are using dynamic configuration settings file from the previous release, ensure that any settings referring to port 8443 are changed to port 443.

Architecture topology

Avaya Aura® Device Services and Session Manager share the same Cassandra database.

Avaya Aura® Device Services is hosted in a separate Tomcat container. Whereas, the existing Session Manager services including PPM are hosted in a JBOSS container. A common contacts schema is shared between Avaya Aura® Device Services and PPM.

The DRS synchronization performs the synchronization between System Manager and the local Avaya Aura® Device Services DRS replica.

The following diagram depicts the architecture of Avaya Aura® Device Services:

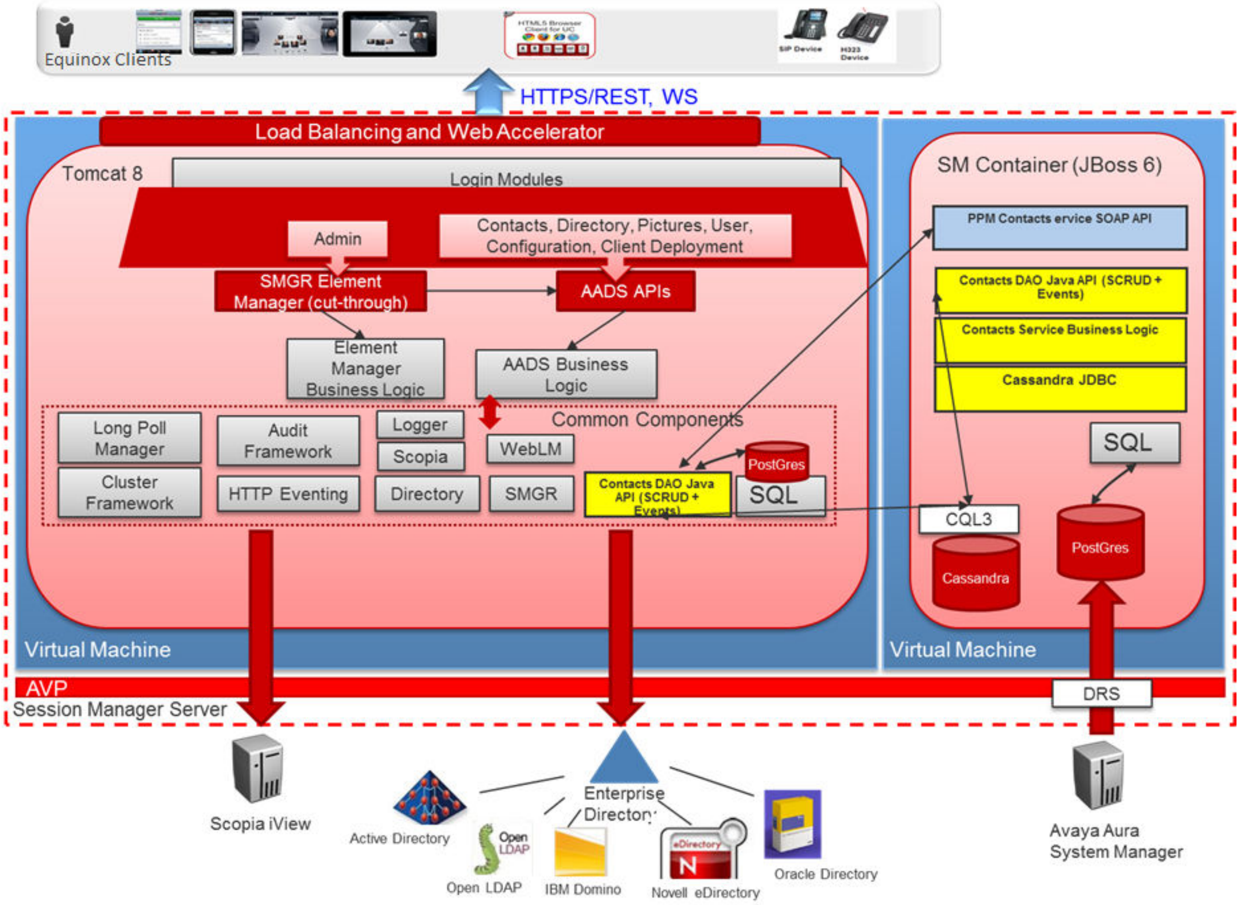

Figure 1: Avaya Aura® Device Services architecture

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

Cluster topology

When the Enable Data Storage Cluster flag is checked, all the Session Manager instances become members of a Cassandra cluster. Each Session Manager instance in the cluster can also be configured as part of a data center.

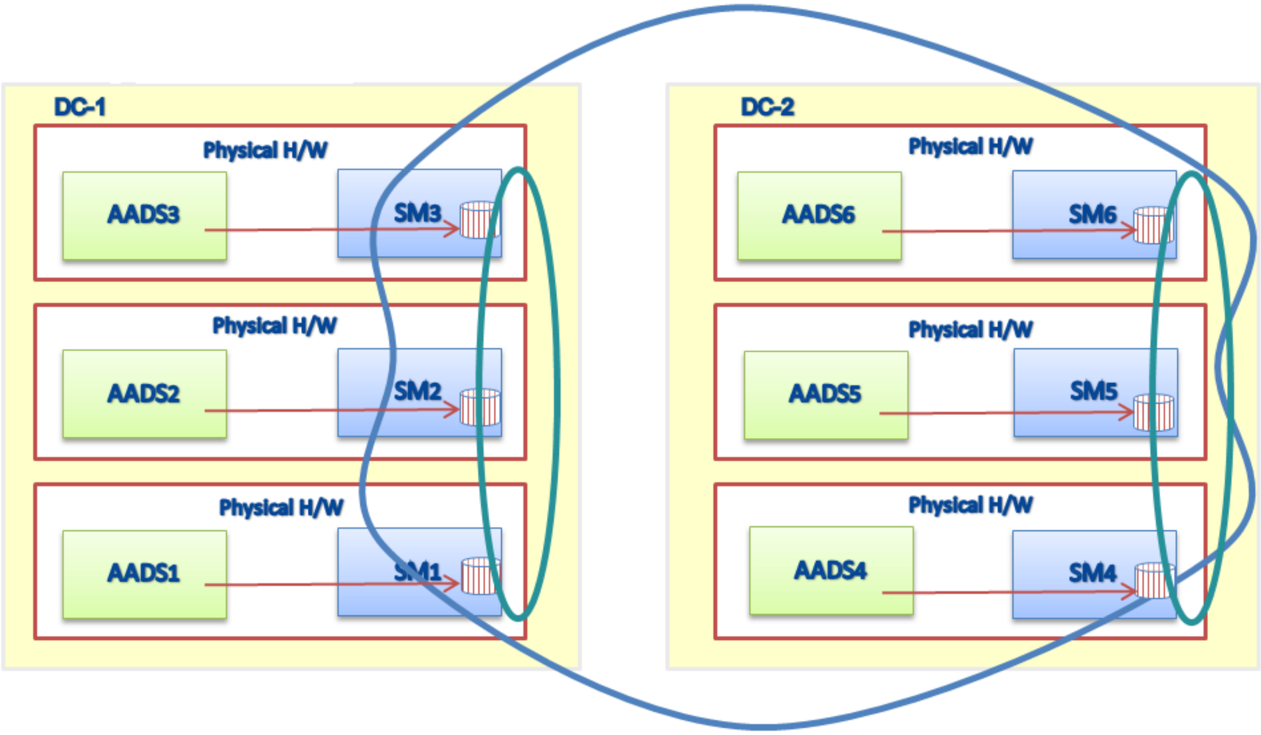

Figure 2: Cassandra Clustering Topology

Solution components

Components	Description
Avaya Aura® core	• System Manager • Session Manager • Communication Manager • Presence Services • WebLM
Enterprise Directory	The Enterprise LDAP server.
Avaya-provided server	Appliance Virtualization Platform
Endpoints	• Avaya Equinox® for Android Release 3.0 • Avaya Equinox® for iOS Release 3.0 • Avaya Equinox® for Mac Release 3.0 • Avaya Equinox® for Windows Release 3.0

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 5.5. Appliance Virtualization Platform supports ESXi 5.5 and 6.0. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.
Solution Deployment Manager	The centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
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 AADS if you have any of the following:

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

Chapter 3: 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 (aka 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.

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.

For example:

```
[admin@aads-dev-114 ~]$ sudo /opt/Avaya/DeviceServices/7.1.0.0.243/CAS/7.0.1.0.2804/
misc/
Usage:
clitool-acs.sh listClusterNodes
clitool-acs.sh applicationInterface <start|stop>
clitool-acs.sh removeClusterNode <serverUUID> [force]
clitool-acs.sh clusterVirtualIp [<virtual IP address> master|backup]|[clear <node IP
address>]
clitool-acs.sh systemManagerUPM [<recommended System Manager UPM user and password>]
clitool-acs.sh pushKeytab
clitool-acs.sh registerClusterNode <serverUUID> <IP address> [force]
clitool-acs.sh longpollTimeout [<longpoll timeout duration>]
clitool-acs.sh ldapConfiguration [<ldap properties filename> <ldap user's password>] |
--current
clitool-acs.sh corsConfiguration [<cors propeties filename>]
clitool-acs.sh certWarningPeriod [<number of days>]
clitool-acs.sh notificationFrontend [http|websocket|schemeHTTP|schemeWebsocket|host|
port|<schemeWSS> <schemeHTTP> <host IP or name> <port>
clitool-acs.sh checkVersions
clitool-acs.sh clientCertificateVerificationConfig [<service_name> <off|optional|on>]
clitool-acs.sh restFrontend [scheme|host|port|<scheme> <host IP or name> <port>]
```

```
clitool-acs.sh licenseServerUrl <ip/fqdn> <port>
clitool-acs.sh drsSyncDuration [<recommended DRS sync duration timeout>]
clitool-acs.sh microsoftExchangeServer [<recommended Microsoft Exchange Server Details>]
```

collectLogs

The **`collectLogs`** utility copies the logs from an Avaya Aura® Device Services node to a file or to a directory specified as parameters in the command.

Usage example

- **`$ sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/bin/collectLogs.sh -n 2`**: creates an archive with a log history to a count of two.
- **`$ sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/bin/collectLogs.sh -d /tmp/ -n 2 -nt`** : copies the log files to the `/tmp` directory with a log history to a count of two. The -nt option indicates no tar so that the log files are collected in the specific directory but not combined in to a single archive.
- **`$ sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/bin/collectLogs.sh -d /tmp/ -name <archive_name>`**: creates an archive of the log files that prefixes <archive_name> to the filename in the `/tmp` directory with each of the log files to the maximum log history depth of twenty.

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 `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin`.

```
[avaya@AWSDev-14 /]$ sudo /opt/Avaya/DeviceServices/7.1.x.x.243/CAS/7.1.x.x.243/bin/
statusAADS.sh
[sudo] password for avaya:
2016-06-23_11:00:04 Displaying status for Avaya Aura Device Services Application
2016-06-23_11:00:04 ulimit file count ...................  [  OK  ]
2016-06-23_11:00:04 ulimit process count ................  [  OK  ]
2016-06-23_11:00:04 iptables status .....................  [  OK  ]
2016-06-23_11:00:04 RecoveryManager Watchdog status .....  [  OK  ]
2016-06-23_11:00:04 RecoveryManager Service status ......  [  OK  ]
2016-06-23_11:00:05 net-SNMP status .....................  [  OK  ]
2016-06-23_11:00:05 RecoveryManager status ..............  [  OK  ]
2016-06-23_11:00:05 AADSKeepalived status ................. [INACTIVE]
2016-06-23_11:00:05 AADSTomcat status .....................  [  OK  ]
2016-06-23_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 `sudo service AADSService 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:

   ```
   sudo service AADSService stop
   ```

Chapter 4: 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.

Procedure

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

   In the DNS, add an entry to map IP address with the FQDN.

   If the FQDN does not resolve through DNS, you must add the IP address and FQDN of Avaya Aura® Device Services in the `etc/hosts` file of the system from where 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`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, the system 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.

6. Click **Log on**.

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. In the Navigation pane, click **Service Control** > **Application Management**.
2. In the Application Properties area, complete the required settings, which are described in Application Properties field descriptions on page 19.
3. Click **Save**.

Related links

Application Properties field descriptions on page 19

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.

Name	Description
	You can enter a value between 3 and 15 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 100. The default value is 50.

Related links

Managing application sessions on page 19

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

About this task

You can use the 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.
- In a cluster environment, ensure that all nodes in the cluster are running.

Procedure

1. On the 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.

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 22.

- 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 22.

Creating 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. In **Subject Alternative Name**, type a node name.
   c. Complete the other settings as required.

      You can use the **Show Advanced Settings** button to view additional settings information.
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 22.

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.

Managing keystore data

Procedure

In the Keystore area, do one of the following:

- To import keystore data, click **Import** and then perform Importing keystore data on page 23.

- 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 details about a keystore file, click **Details**.
- To remove an existing keystore file, select it and then click **Delete**.

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.

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 23.

     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**.

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.

Name	Description
OAM	Specifies the Operations, Administration, and Maintenance (OAM) interface.

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.
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.

Chapter 5: 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 AADS API using a preexisting authentication to a Windows domain. AADS 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 AADS and Active Directory servers. Errors in the setup might cause the authentication to fail. You can enable debug logs to assist with troubleshooting.

Related links

Authentication prerequisites on page 25
Setting up the Windows Domain Controller on page 26
Setting up IWA on the Avaya Aura Device Services administration portal on page 28

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.
- A Windows client on the Active Directory domain.
- An AADS server that is resolvable by the DNS.
- A domain user that will be mapped to the Service Principal Name (SPN) of the AADS server.
- Domain users for all individual users.

Important:

The Active Directory, Windows client, and AADS server must resolve each other's FQDNs. However, they do not need to use the same DNS server or to belong to the same zone.

Note:

For information about setting up the DNS server, see *Administering Avaya Communicator for Android, iPad, and Windows*.

Related links

Integrated Windows Authentication administration and management on page 25

Setting up the Windows Domain Controller

About this task

Use this procedure to add the AADS 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 HTTP/<FRONT-END FQDN> <Domain user login>
   ```

   In the following example, “<FRONT-END FQDN>” is `aads.example.com` and “<Domain user login>” is `aads_user`:

   ```
   setspn -S HTTP/aads.example.com aads_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 27.

3. **(Optional)** To remove a duplicated SPN from another user, run the following command:

```
setspn -d <SPN> <old user>
```

4. 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> /pass +rndPass /crypto all /kvno 0
```

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

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

The `tomcat.keytab` file enables AADS to authenticate against the Kerberos Key Distribution Center (KDC). This file assigns a random password to the user.

5. Transfer the generated `tomcat.keytab` file to the AADS 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 AADS server. You can generate and re-import a new `tomcat.keytab` file anytime.

Related links

Integrated Windows Authentication administration and management on page 25
Windows Domain Controller command descriptions on page 27

Windows Domain Controller command descriptions

Setting up the Windows Domain Controller on page 26 uses the following command values:

Command	Description	Example value
<FRONT—END FQDN>	The REST front host FQDN of the AADS 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_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`

Related links

Setting up the Windows Domain Controller on page 26

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 28 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.

Related links

Integrated Windows Authentication administration and management on page 25

Chapter 6: Administration of client and user services and settings

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

Procedure

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

   The system 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, the certificate allows all key usages.

3. To set the client certificate policy for the Admin 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 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

Name	Description
	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.

Configuring the client certificate policy using the command line interface

About this task

Use this procedure if you accidentally changed the admin interface (OAMP) client certificate policy and are no longer able to access the system interface. To change the certificate, you must access the Avaya Aura® Device Services seed node. Use this procedure to change the setting through the command line interface (CLI).

Procedure

1. On the SSH terminal, log in as an administrator.
2. Run one of the following commands:
   - To change the setting to **None**:

     ```
     sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-acs.sh
     clientCertificateVerificationConfig oampGuiClient off
     ```
   - To change the setting to **Optional**:

     ```
     type sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-
     acs.sh clientCertificateVerificationConfig oampGuiClient optional
     ```
   - To change the setting to **Required**:

     ```
     sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-acs.sh
     clientCertificateVerificationConfig oampGuiClient on
     ```

   After you run the appropriate command, it will take few minutes for the changes to take effect.

Dynamic Configuration

With the Dynamic Configuration service, the system can dynamically retrieve and deploy the device configuration settings to the Avaya Equinox® clients.

Dynamic Configuration provides a centralized place to administer user, group, platform, global, and exception settings. You can configure the Device Configuration settings on the Avaya Equinox® clients using one of the following methods:

- DNS-based auto discovery.
- Web address: On the Avaya Equinox® clients, type the Auto Configuration or Device Configuration URL.

  For example: `https://<IP address>:443/acs/resources/configurations`

For information about how to configure DNS-based auto discovery and other settings on the Avaya Equinox® clients, see *Planning for and administering Avaya Equinox® for Android, iOS, Mac, and Windows*.

Note:

Authentication domain is an enterprise directory with provenance priority 1. 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.

Using the Dynamic Configuration service, you can configure and publish the configuration settings for the following:

- **User:** The User specific settings can be overridden by platform, exception, and System Manager settings.
- **Group:** The Group specific settings can be overridden by user, platform, exception, and System Manager settings. The LDAP groups are ordered alphabetically.

  If a user belongs to more than one group on LDAP Server, the settings are applied on the basis of the alphabetical order of the group.

  Note:

  The Dynamic Configuration service uses the `memberof` attribute to find the user group. By default, the Microsoft Active directory uses these settings. To find the user group for:

  - LDS_2012, LDS_2008, OpenLDAP, and OracleDirectoryServer directories, enable the `memberof` attribute.
  - Novell directory, use the `groupMembership` attribute.
  - Domino directory, use the `dominoAccessGroups` attribute.

  For information about these attributes, see the product documentation for these directories. For enabling the `memberof` attribute for OpenLDAP, see the *OpenLDAP Software Administrator's Guide* at http://www.openldap.org/.
- **Platform:** The Platform settings can be overridden by exception and System Manager settings.
- **Global:** The Global settings can be overridden by any other settings category.
- **Exceptions:** The Exceptions settings are specific to the System Manager Home location.

Home location settings

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.

On the System Manager web console, you can configure:

- Dial plan rules from **Routing** > **Dial Patterns**.
- Home location of a user from **Routing** > **Locations**.

For information about creating location and dial patterns, see *Administering Avaya Aura® Session Manager*.

ESMSRVR setting

The ESMSRVR setting is retrieved from the **IM Gateway SIP Entity** field from the Presence profile on System Manager. Therefore, if the Presence profile is assigned to a user on System Manager, then the system overrides the value from Presence profile to any locally configured ESMSRVR value at Group and Global levels. So the system uses the Presence profile value for configuration.

Conferencing setting

Avaya Aura® Device Services auto discovers the following settings from the Avaya Equinox® Conferencing Management during Avaya Equinox® deployment:

- CONFERENCE_FACTORY_URI
- CONFERENCE_PORTAL_URI
- UNIFIEDPORTALENABLED

As an administrator you can override the values for these settings from the Avaya Aura® Device Services administration portal with any fixed user, group, or platform value.

Viewing Home location

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 system displays the Home location in the Call Routing Settings section.

Implementation of the Dynamic Configuration settings

In Dynamic Configuration, different settings that are common at the user, group, platform, global, and exceptions levels have different priorities. The administrator must take this into account while creating Dynamic Configurations.

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.

Example

If administrators have users in two LDAP groups, the users in Group 1 use Avaya Multimedia Messaging, but users in Group 2 cannot use Avaya Multimedia Messaging. To configure this, the administrator must set the ESMENABLED setting for each group. This setting is available at the user, group, platform, and global levels.

Solution

This setting is specific to the LDAP group, so the ESMENABLED setting must be configured on the group level. The configuration for users is as follows:

- Group 1 must be set to ESMENABLED =1
- Group 2 must be set to ESMENABLED =0

After creating the configuration, publish the settings for users in Group 1 and Group 2.

✱ **Note:**

In this case, do not configure the ESMENABLED setting at the platform level.

Creating a new configuration

About this task

Use this procedure to create a new configuration for a user, a group, a platform, and all users. 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, 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 templates.

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.

Related links

Configuration settings on page 37
Configuration field descriptions on page 36

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.
Platform	Specifies a platform to retrieve the data. • iOS • Android • Windows • Mac
USER, **Group**, **Platform**, **Global**, 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.
Settings configured on SMGR	The system displays this section for the users. Displays the read-only settings. To edit the values, go to the SMGR configuration.
Category	Specifies the category for the group settings.

Button	Description
Retrieve	Retrieves the settings based on the search criteria.
Save	Saves a new test configuration. Overwrites an existing configuration.

Button	Description
Test	Provides a test URL to test the configuration settings.
Publish	Publishes the configuration settings.
Upload settings	Uploads dynamic settings through the additional parameter settings file downloaded from the PLDS.

Link	Description
View Published Settings	Displays all the published settings for Global, Group, User, Platform, 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, take the mouse over the ℹ icon that is beside the setting name.

Avaya Equinox® does not support the following settings, but can be used by other clients:

- CONFIG_SERVER
- CONFIG_SERVER_SECURE_MODE
- ENABLE_PRESENCE

System parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
MODEL	A string of maximum 10 characters that identifies the endpoint platform and version. This value is built into the application as an identifier for the endpoint or release to allow the value to be used in conditional statements. The platform names are abbreviated.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	For Release 3.2: • aca.3.2 is the value for Avaya Equinox® for Android. • aci.3.2 is the value for Avaya Equinox® for iOS. • acm.3.2 is the value for Avaya Equinox® for Mac. • acw.3.2 is the value for Avaya Equinox® for Windows.		
MODEL4	A string of maximum 4 characters that identifies the endpoint platform. This value is built into the application as an identifier for the endpoint or release to allow the value to be used in conditional statements. For example:. • aca is the value for Avaya Equinox® for Android. • aci is the value for Avaya Equinox® for iOS. • acm is the value for Avaya Equinox® for Mac. • acw is the value for Avaya Equinox® for Windows.	Not Applicable	Supported on all platforms.

SIP parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
SIPENABLED	The parameter that indicates whether the SIP service is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **Services** > **Phone Service** > **Phone Service**	Supported on all platforms.
SIP_CONTROLLER_LIST	The parameter that consolidates SIP controller parameters for IP address, port, and transport protocol into a single configuration parameter. The parameter setting must be a list of SIP controller designators, separated by commas without any intervening spaces. Each controller designator must have the following format: `host[:port][;transport=xxx]` For example, `proxy1:5061;transport=tls,proxy2:5061;transport=tls`. **Note:** • The parameter value can be an FQDN or an IP address. • If you use this parameter with LOCKED_PREFERENCES and OBSCURE_PREFERENCES, all three associated UI fields are locked. The SIP fields are Server Address, Server Port, and Use TLS.	• **Settings** > **Services** > **Phone Service** > **Server Address** • **Settings** > **Services** > **Phone Service** > **Server Port** • **Settings** > **Services** > **Phone Service** > **Use TLS**	Supported on all platforms.
SIPDOMAIN	The SIP domain.	**Settings** > **Services** > **Phone Service** > **Domain**	Supported on all platforms.
SIPSSO	The parameter that indicates whether unified login is enabled for the SIP service.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.		
SIPUSERNAME	The SIP account name.	**Settings** > **Accounts** > **Phone Service** > **Extension**	Supported on all platforms.
SIPPASSWORD	The SIP account password.	**Settings** > **Accounts** > **Phone Service** > **Password**	Supported on all platforms.
ENABLE_MDA_JOIN	The parameter to enable MDA Join if you are using a version of Communication Manager later than 6.3. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value. On Communication Manager 6.3 and earlier versions, Communication Manager gets reset if a user attempts to bridge into an active call from their MDA extension. Hence, by default, the remote line appearance Join button is disabled.	Not Applicable	Supported on all platforms.
ENFORCE_SIPS_URI	The parameter to enable SIPS in URI. The options are: • 1: Indicates enabled. This is the default value. • 0: Indicates disabled.	Not Applicable	Supported on Avaya Equinox® for Windows
ENABLE_PPM_CALL_JOURNALING	The parameter that indicates whether Session Manager stores the history of the 100 most recent calls for each user. This is irrespective of whether the endpoint registers to Session Manager. The options are: • 1: Indicates enabled. This is the default value.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	• 0: Indicates disabled. If the user logs in to the Avaya Equinox® client on an endpoint, the endpoint downloads the latest 100 call history records from Session Manager. Subsequently, the endpoint maintains its local call history, while Session Manager continues to maintain its call history independently. With this feature, active synchronization of call history between Session Manager and the endpoints is minimal after the initial login or download. However, when a user attempts to delete a call history from an endpoint, the endpoint sends a PPM request to delete the corresponding call history from the central repository of Session Manager. Call history download is initiated by the client when the client: • Recovers from a network outage or outage due to a network change. • Registers with Session Manager.		
COMM_ADDR_HANDLE_TYPE	A virtual configuration setting that defines 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. The system 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.		Supported only on Avaya Aura® Device Services.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	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.		
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. Accepted values are 1 to 255.		Supported only on Avaya Aura® Device Services.

Unified login parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
SSOENABLED	The parameter that indicates whether unified login is enabled. The options are: • 1: Indicates enabled. This is the default value. • 0: Indicates disabled.	**Settings** > **Services** > **Unified Login** > **Unified Login**	Supported on all platforms.
SSOUSERID	The unified login user ID.	**Settings** > **Accounts** > **Equinox** > **Username**	Supported on all platforms.
SSOPASSWORD	The unified login password.	**Settings** > **Accounts** > **Equinox** > **Password**	Supported on all platforms.

Automatic configuration parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
AUTOCONFIG_USESSO	The parameter that indicates whether the endpoint uses the unified login credentials during the retrieval of the `46xxsettings` file. Else, the assumption is that the automatic configuration credentials are unique. The options are: • 1: Indicates that the automatic configuration credentials are the same as the unified login credentials. This is the default value. • 0: Indicates that the automatic configuration credentials are unique.	Not Applicable	Supported on all platforms.
SETTINGS_CHECK_INTERVAL	The interval used to define how often endpoints will check for settings file changes. The range for this parameter is 0 to 30 days. Avaya recommends that your deployment must include this setting with a non-zero value. • A value of 1 indicates daily. This is the default value for mobile clients. • A value of 7 indicates weekly. • A value of 0 indicates that configuration updates are not performed. This is the default value for desktop clients.	Not Applicable	Supported on all platforms.
SETTINGS_FILE_URL	The URL to move settings files from one server to another. This URL is used during the next check interval if defined. For example, `SET SETTINGS_FILE_URL`	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	`"https://acquirerofexample.com/mysettingsfile.txt"`.		

Conferencing parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
CONFERENCE_FACTORY_URI	The URL that defines the adhoc conference resource to be used by the endpoint. This is an optional parameter. Hence, the value can be null. • Avaya Equinox® Conferencing: This parameter is the advanced parameter vnex.vcms.core.conference.factoryURI provisioned in Avaya Equinox® Management. • Avaya Aura® Conferencing: This parameter is the adhoc URI entered in the provisioning client. If this parameter is not provisioned, Communication Manager adhoc conferencing is used. For example, `SET CONFERENCE_FACTORY_URI +15552220881@yourenterprise.com`.	• On mobile clients: **Settings** > **Services** > **My Meeting Room** > **Adhoc Conference Address** • On desktop clients: **Settings** > **Services** > **Phone Service** > **Adhoc Conference Address**	Supported on all platforms.
CONFERENCE_ACCESS_NUMBER	The primary conference access number. This parameter populates the meeting invitation dial-in number for participants. • Avaya Equinox® Conferencing: This parameter is the Auto-Attendant number found on the Avaya Equinox® Management settings pane. This parameter is required only for Avaya Equinox® Conferencing 9.0.1 and earlier versions.	On desktop clients: **Settings** > **Services** > **My Meeting Room** > **Conference Access Number**	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	• Avaya Aura® Conferencing: This parameter is the Service URI in the provisioning client. The conference access numbers are found in My Meeting Resources on the Avaya Aura® Conferencing portal. For example, `SET CONFERENCE_ACCESS_NUMBER +15552221000`.		
ADDITIONAL_CONFERENCE_ACCESS_NUMBER_LIST	The additional PSTN conference access numbers. This parameter provides alternate dial-in numbers in the meeting invite. Available on Avaya Equinox® Conferencing and Avaya Aura® Conferencing. For example, `SET ADDITIONAL_CONFERENCE_ACCESS_NUMBER_LIST Label1:Number1,Label2:Number2,...,LabelN:NumberN`.	Not Applicable	Supported on all platforms.
UNIFIEDPORTALENABLED	The parameter that determines whether the Avaya Equinox® Conferencing meeting account is enabled for a user. This parameter is mandatory for MeetMe conferences. The options are: • 1: Indicates that the Avaya Equinox® Conferencing meeting account is enabled. • 0: Indicates that the Avaya Equinox® Conferencing meeting account is disabled. This is the default value.	**Settings** > **Services** > **My Meeting Room** > **My Meeting Room**	Supported on all platforms.
CONFERENCE_PORTAL_URI	The Conference Portal address for the user. This parameter is used to: • Populate the meeting invitation location field with	**Settings** > **My Services** > **My Meeting Room** > **Meeting Address**	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	the URL for participants to join the meeting. - Connect to the portal to retrieve the meeting invitation template. Available on Avaya Equinox® Conferencing and Avaya Aura® Conferencing. This parameter is mandatory for MeetMe conferences. For example, `SET CONFERENCE_PORTAL_URI https://conferencing.yourenterprise.com:8443/portal/tenants/default/?ID=17111552226080`.		
UNIFIED_PORTAL_SSO	The parameter that indicates whether Unified Portal uses unified login. The options are: - 1: Indicates that Unified Portal uses unified login. This is the default value. - 0: Indicates that Unified Portal does not use unified login.	**Settings** > **Services** > **Unified Login** > **My Meeting Room**	Supported on all platforms.
UNIFIED_PORTAL_USERNAME	The Unified Portal user name.	**Settings** > **Accounts** > **My Meeting Room** > **Username**	Supported on all platforms.
UNIFIED_PORTAL_PASSWORD	The Unified Portal password.	**Settings** > **Accounts** > **My Meeting Room** > **Password**	Supported on all platforms.
CONFERENCE_MODERATOR_CODE	The conference moderator code. Use this parameter to start your own meetings. Users can click to join their own bridge by using a UC client. Only available in Avaya Aura® Conferencing. You can find the moderator code in My Meeting Resources	**Settings** > **Services** > **My Meeting Room** > **Moderator Code**	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	on the Avaya Aura® Conferencing portal. For example, `SET CONFERENCE_MODERATOR_CODE 683044`.		
CONFERENCE_PARTICIPANT_CODE	The conference participant code. This parameter populates the meeting template with the code for participants to join meetings. Users can share their participant code with other users in Calendar invites by using the Share My Bridge feature. Only available in Avaya Aura® Conferencing. You can find the participant code in My Meeting Resources on the Avaya Aura® Conferencing portal. For example, `SET CONFERENCE_PARTICIPANT_CODE 03974587`.	**Settings** > **Services** > **My Meeting Room** > **Participant Code**	Supported on all platforms.
CONFERENCE_PARTICIPANT_URL	The conference participant URL. This parameter populates the meeting template and the location field with the URL to join the meeting. This parameter is applicable only to Avaya Aura® Conferencing.	On desktop clients: **Settings** > **Services** > **My Meeting Room** > **Participant URL**	Supported on Avaya Equinox® for Mac and Windows
CONFERENCE_VIRTUAL_ROOM	The Scopia Virtual Room ID of the virtual room owner. When Avaya Aura® Device Services is integrated with Avaya Equinox® Management, the Virtual Room of the user is provided as configuration data. Only available in Avaya Equinox® Conferencing.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	You can find the Virtual Room number in the user settings on Equinox Conference Portal. This property is provided in the Avaya Equinox® client to facilitate the user to provision the value into the Equinox Outlook Add-on. For example, `SET CONFERENCE_VIRTUAL_ROOM +171115552224545`.		
CONFERENCE_FQDN_SIP_DIAL_LIST	A list of Scopia conference bridges that can support SIP Enhanced Conference Experience. Top-of-Mind requires this auto-configuration setting to have all the Scopia or Equinox portal domains that you use so that Top-of-Mind click to call can work. For example, `SET CONFERENCE_FQDN_SIP_DIAL_LIST Scopia.slav.com,Alphascopia.slav.com,lab.slav.com,scopia.partner.com`.	Not Applicable	Supported on all platforms.
UCCPENABLED	The parameter to enable or disable the UCCP Conferencing protocol in the client. Only available in Avaya Equinox® Conferencing. This parameter is mandatory for MeetMe conferences. The options are: • 1: Indicates that the UCCP Conferencing protocol is enabled in the client. This is the default value. • 0: Indicates that the UCCP Conferencing protocol is disabled in the client. SIP CCMP is used for conferencing.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	You must enable this parameter only: • When the Equinox Conference Control element is accessible for all Avaya Equinox® clients. • In enterprise networks that support WebSockets. For example, `SET UCCPENABLED 1`.		
OUTLOOK_ADDON_HOST_URI	The JavaScript source for the deployments that do not want to access the centrally cloud-hosted Outlook Add-on.	Not Applicable	Supported on all platforms.
SHOW_EQUINOX_MEETING_PANEL_IN_TOM	The parameter that determines whether the My Meeting Portal panel is displayed on the Top of Mind screen. The options are: • 1: Indicates that the My Meeting Portal panel is displayed on the Top of Mind screen. This is the default value. • 0: Indicates that the My Meeting Portal panel is not displayed on the Top of Mind screen.	Select the **Top of Mind** filter, and in the Equinox Meetings area, select **Hide**.	Supported on all platforms.

Automatic software updates parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
APPCAST_ENABLED	The parameter that indicates whether the service is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.
APPCAST_URL	The URL that defines the appcast feed used by the endpoints.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.

Name	Description	Client UI setting name	Avaya Equinox® platform support
APPCAST_CHECK_INTERVAL	The interval at which endpoints check for software updates. The range for this parameter is 0 to 30 days. The default is 1 day. The value 0 indicates that automatic checking is disabled.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.

Avaya Multimedia Messaging parameters

Use the following automatic configuration parameters if you configured the Avaya Equinox® clients to interwork with Avaya Multimedia Messaging:

Name	Description	Client UI setting name	Avaya Equinox® platform support
ESMENABLED	The parameter that indicates whether Avaya Multimedia Messaging is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **Services** > **Multimedia Messaging** > **Multimedia Messaging**	Supported on all platforms.
ESMSSO	The parameter that indicates whether the Avaya Multimedia Messaging service uses unified login. The options are: • 1: Indicates that Avaya Multimedia Messaging uses unified login. This is the default value. • 0: Indicates that Avaya Multimedia Messaging does not use unified login.	**Settings** > **Services** > **Unified Login** > **Multimedia Messaging**	Supported on all platforms.
ESMUSERNAME	The Avaya Multimedia Messaging account user name.	**Settings** > **Accounts** > **Multimedia Messaging** > **Username**	Supported on all platforms.
ESMPASSWORD	The Avaya Multimedia Messaging account password.	**Settings** > **Accounts** > **Multimedia Messaging** > **Password**	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
ESMSRVR	The IP address or fully qualified domain name of the Avaya Multimedia Messaging server.	**Settings** > **Services** > **Multimedia Messaging** > **Server Address**	Supported on all platforms.
ESMPORT	The port of the Avaya Multimedia Messaging server. The default value is 8443.	**Settings** > **Services** > **Multimedia Messaging** > **Server Port**	Supported on all platforms.
ESMSECURE	The parameter that indicates whether TLS is being used. The options are: • 1: Indicates that TLS is used. This is the default value. • 0: Indicates that TLS is not used.	Not Applicable	Supported on all platforms.
ESMREFRESH	The parameter that indicates the Avaya Multimedia Messaging refresh interval in minutes. Valid values are 0, 10, 30, and 60. The default value is 0, which indicates continuous mode. **Note:** The manual mode option is no longer supported.	**Settings** > **Services** > **Multimedia Messaging** > **Polling Interval**	Supported on all platforms.
ESMHIDEONDISCONNECT	The parameter to hide Avaya Multimedia Messaging conversations and message details in the Messages screen and Messaging area of the Top Of Mind screen when not connected to Avaya Multimedia Messaging. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.

Avaya Aura® Device Services parameters

Use the following automatic configuration parameters if you configured the Avaya Equinox® clients to interwork with Avaya Aura® Device Services:

Name	Description	Client UI setting name	Avaya Equinox® platform support
ACSENABLED	The parameter that indicates whether Avaya Aura® Device Services is enabled. The options are: • 1: Indicates that Avaya Aura® Device Services is enabled. • 0: Indicates that Avaya Aura® Device Services is disabled. This is the default value.	**Settings** > **Services** > **Device Services** > **Device Services**	Supported on all platforms.
ACSSRVR	The Avaya Aura® Device Services IP address or FQDN.	**Settings** > **Services** > **Device Services** > **Server Address**	Supported on all platforms.
ACSPORT	The Avaya Aura® Device Services port. The default value is 443.	**Settings** > **Services** > **Device Services** > **Server Port**	Supported on all platforms.
ACSSECURE	The parameter that indicates whether TLS is being used. The options are: • 1: Indicates that TLS is used. This is the default value. • 0: Indicates that TLS is not used.	Not Applicable	Supported on all platforms.
ACSSSO	The parameter that indicates whether Avaya Aura® Device Services uses unified login. The options are: • 1: Indicates that Avaya Aura® Device Services uses unified login. This is the default value. • 0: Indicates that Avaya Aura® Device Services does not use unified login.	**Settings** > **Services** > **Unified Login** > **Device Services**	Supported on all platforms.
ACSUSERNAME	The Avaya Aura® Device Services user name.	**Settings** > **Accounts** > **Device Services** > **Username**	Supported on all platforms.
ACSPASSWORD	The Avaya Aura® Device Services password.	**Settings** > **Accounts** > **Device Services** > **Password**	Supported on all platforms.
CONTACT_MATCHING_SEARCH_LOCATION	The parameter that determines whether Avaya Equinox® performs contact resolution using	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	the local contact cache or by searching Avaya Aura® Device Services or both. The options are: • 1: All. This is the default value. • 2: Local. • 3: Avaya Aura® Device Services.		

Client Enablement Services parameters

Use the following parameters if Avaya Equinox® for Android and iOS are configured to interwork with Client Enablement Services. Client Enablement Services is not supported on Avaya Equinox® for Mac and Windows.

Note:

Avaya Equinox® for Android on Avaya Vantage™ does not support Client Enablement Services.

Name	Description	Client UI setting name	Avaya Equinox® platform support
CESENABLED	The parameter that indicates whether Client Enablement Services is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **Services** > **Client Enablement (CES)**: • On Avaya Equinox® for Android: **CES** • On Avaya Equinox® for iOS: **Client Enablement Services**	Supported on Avaya Equinox® for Android and iOS.
CESSSO	The parameter that indicates whether Client Enablement Services uses unified login. The options are: • 1: Indicates that Client Enablement Services uses unified login. This is the default value. • 0: Indicates that Client Enablement Services does not use unified login.	**Settings** > **Services** > **Unified Login** > **Client Enablement (CES)**	Supported on Avaya Equinox® for Android and iOS.

Name	Description	Client UI setting name	Avaya Equinox® platform support
CESUSERNAME	The Client Enablement Services account name.	**Settings** > **Accounts** > **Client Enablement Services** > **Username**	Supported on Avaya Equinox® for Android and iOS.
CESPASSWORD	The Client Enablement Services account password.	**Settings** > **Accounts** > **Client Enablement Services** > **Password**	Supported on Avaya Equinox® for Android and iOS.
CESSRVR	The IP address or fully qualified domain name of the Client Enablement Services server.	**Settings** > **Services** > **Client Enablement (CES)** > **Server Address**	Supported on Avaya Equinox® for Android and iOS.
CESPORT	The Client Enablement Services server port. The default value is 7777.	**Settings** > **Services** > **Client Enablement (CES)** > **Server Port**	Supported on Avaya Equinox® for Android and iOS.
CESSECURE	The parameter that indicates whether TLS is being used. The options are: • 1: Indicates that TLS is used. This is the default value. • 0: Indicates that TLS is not used. **Note:** Avaya Equinox® only supports TLS connections to Client Enablement Services. The user cannot change this value from the Settings menu in the application.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.
CESVMPIN	The voice mail PIN required for visual voice mail.	**Settings** > **Services** > **Voicemail** > **PIN**	Supported on Avaya Equinox® for Android and iOS.

Desktop parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
DESKTOP_HTTP_APPLICATION_INTEGRATION	The parameter to control Desktop HTTP Application Integration. The options are: • 1: Indicates that Desktop HTTP	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	Application Integration is enabled. This is the default value. • 0: Indicates that Desktop HTTP Application Integration is disabled. The External Application API controls features such as Headset API integration with Plantronics Hub and Jabra Direct. It does not control Equinox native (Out-of-the-box) support for Plantronics headsets.		
ENABLE_OUTLOOK_ADDON	The parameter to enable or disable the Outlook Add-on functionality. The options are: • 1: Indicates that the Outlook Add-on functionality is enabled. This is the default value in the UC and OTT signed-in user modes. • 0: Indicates that the Outlook Add-on functionality is disabled.	**Settings** > **Desktop Integration** > **Outlook Add-in** > **Enable Outlook Add-In**	Supported on Avaya Equinox® for Windows.
OUTLOOK_CALL_CONTACT	The parameter to enable or disable the Outlook Add-on Call Contact functionality by deployment or user preference. The options are: • 1: Indicates that the Outlook Add-on Call Contact functionality is enabled. This is the default value. • 0: Indicates that the Outlook Add-on Call	**Settings** > **Desktop Integration** > **Outlook Add-in** > **Allow calls from Outlook contacts**	Supported on Avaya Equinox® for Windows.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	Contact functionality is disabled.		
OUTLOOK_ADDON_HOST_URI	The parameter that indicates the HTTP location of the JavaScript Outlook Add-on.	Not Applicable	Supported on Avaya Equinox® for Windows.
ENABLE_BROWSER_EXTENSION	The parameter to enable or disable the browser extension functionality. The options are: • 1: Indicates that the browser extension functionality is enabled. This is the default value in the UC and OTT signed-in user modes. • 0: Indicates that the browser extension functionality is disabled.	**Settings** > **Desktop Integration** > **Browser Add-in** > **Enable Browser Add-In**	Supported on Avaya Equinox® for Windows.

EC500 parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
EC500ENABLED	The parameter that indicates whether EC500 is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **Services** > **EC500 Calling** > **EC500 Calling**	Supported on Avaya Equinox® for Android and iOS.
EC500VOICEMAILNUMBER	The voice mail system access number. Endpoints can retrieve this value from multiple sources. A summary of this logic is: • With SIP, the number comes from the PPM protocol, which pulls the configuration from Avaya Aura®.	**Settings** > **Services** > **Voicemail** > **PIN**	Supported on Avaya Equinox® for Android and iOS.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	• With Client Enablement Services, the number comes from the Client Enablement Services server. • In other situations, the number comes from this parameter.		
FNUIDLEAPPEARANCESELECT	The number to dial for the Idle Appearance Select feature. This number is used to identify an idle line on your extension when you make a call.	**Settings** > **Services** > **EC500 Calling** > **Idle Appearance Select**	Supported on Avaya Equinox® for Android and iOS.
FNUSIMRINGENABLE or FNUOFFPBXCALLENABLE	The number to dial for enabling Off-PBX calls. This number is used to enable your mobile phone to ring when you receive a call on your deskphone.	**Settings** > **Services** > **EC500 Calling** > **Off PBX Call Enable**	Supported on Avaya Equinox® for Android and iOS.
FNUSIMRINGDISABLE or FNUOFFPBXCALLDISABLE	The number to dial for disabling Off-PBX calls. This number is used to disable your mobile phone from ringing when you receive a call on your deskphone.	**Settings** > **Services** > **EC500 Calling** > **Off PBX Call Disable**	Supported on Avaya Equinox® for Android and iOS.
FNUCFWDENABLE or FNUCFWDALL	The number to dial for enabling call forwarding for all calls.	**Settings** > **Services** > **EC500 Calling** > **Call Forward All Enable**	Supported on Avaya Equinox® for Android and iOS.
FNUCFWDDISABLE or FNUCFWDCANCEL	The number to dial for canceling call forwarding.	**Settings** > **Services** > **EC500 Calling** > **Call Forward All Disable**	Supported on Avaya Equinox® for Android and iOS.
FNUACTIVEAPPEARANCESELECT	The number to dial for the Active Appearance Select feature. This number is used to join an active call on your deskphone using your mobile phone.	**Settings** > **Services** > **EC500 Calling** > **Active Appearance Select**	Supported on Avaya Equinox® for Android and iOS.
FNUSACENABLE	The number to dial for enabling the Send All Calls feature. This number is used to send all calls to a predefined number set on the server by the administrator.	**Settings** > **Services** > **EC500 Calling** > **Send All Calls Enable**	Supported on Avaya Equinox® for Android and iOS.

Name	Description	Client UI setting name	Avaya Equinox® platform support
FNUSACCANCEL	The number to dial for disabling the Send All Calls feature. This number is used to disable the sending of all calls to a predefined number set on the server by the administrator.	**Settings** > **Services** > **EC500 Calling** > **Send All Calls Disable**	Supported on Avaya Equinox® for Android and iOS.
FNE_SETUP_DELAY	The parameter that indicates the delay in seconds between the EC500 call being placed and the transmission of the digits for EC500. The default value is 3 seconds. The purpose of this setting is to address call setup delays with specific regions and trunk providers.	**Settings** > **Advanced** > **FNE Setup Delay**	Supported on Avaya Equinox® for Android and iOS.
STATION_SECURITY_ENABLED	The parameter that indicates whether EC500 station security is enabled. The station security code reduces the risk of toll fraud. The options are: • 1: Indicates that EC500 station security is enabled. • 0: Indicates that EC500 station security is disabled. This is the default value.	**Settings** > **Services** > **EC500 Calling** > **Station Security**	Supported on Avaya Equinox® for Android and iOS.

Exchange Web Services parameters

Use the following parameters if Avaya Equinox® is configured to interwork with Exchange Web Services (EWS):

Name	Description	Client UI setting name	Avaya Equinox® platform support
EWSENABLED	The parameter that indicates whether EWS is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **Services** > **Exchange Calendar** > **Exchange Calendar**	Supported on all platforms.
EWSSSO	The parameter that indicates whether EWS uses unified login.	**Settings** > **Services** > **Unified Login** > **Exchange Calendar**	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	The options are: • 1: Indicates that EWS uses unified login. This is the default value. • 0: Indicates that EWS does not use unified login.		
EWSSERVERADDRESS	The server address that can be used to connect to EWS directly. For example, usmail.slav.com. If you configure this parameter, Avaya Equinox® tries to establish a connection to EWS directly using the server address and avoids the Auto-discover process.	**Settings** > **Services** > **Exchange Calendar** > **Server Address**	Supported on all platforms.
EWSDOMAIN	The Exchange server domain. For example, avaya.com. The Auto-discover process uses EWSDOMAIN to find an EWS endpoint.	**Settings** > **Services** > **Exchange Calendar** > **Domain**	Supported on all platforms.
EWSUSERNAME	The Exchange account user name. This parameter must have the user name portion of a user's Exchange email address. For example, for an Exchange email address username@avaya.com, EWSUSERNAME = username. • If EWS uses Unified Login, this parameter is ignored and SSOUSERID is used. • If EWS does not use Unified Login, this parameter is used. • If EWS does not use Unified Login and this parameter is not specified in the auto-configuration file, the user can view the EWS user name setting in the Auto-configuration wizard.	**Settings** > **Accounts** > **Exchange Calendar** > **Username**	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
EWSPASSWORD	The EWS account password. • If EWS uses Unified Login, this parameter is ignored and SSOPASSWORD is used. • If EWS does not use Unified Login, this parameter is used. • If EWS does not use Unified Login and this parameter is not specified in the auto-configuration file, the user can view the EWS password setting in the Auto-configuration wizard.	**Settings** > **Accounts** > **Exchange Calendar** > **Password**	Supported on all platforms.

Dialing rule parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
ENHDIALSTAT	The parameter that indicates whether dialing rules are enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **Advanced** > **Dialing Rules** > **Dialing Rules**	Supported on all platforms.
PHNOL	The number to dial to access an external line.	**Settings** > **Advanced** > **Dialing Rules** > **Number to dial to access an outside line**	Supported on all platforms.
PHNCC	The country code.	**Settings** > **Advanced** > **Dialing Rules** > **Your country code**	Supported on all platforms.
SP_AC or DIALPLANAREACODE	The area or city code.	**Settings** > **Advanced** > **Dialing Rules** > **Your area/city code**	Supported on all platforms.
PHNPBXMAINPREFIX or DIALPLANPBXPREFIX	The PBX main prefix.	**Settings** > **Advanced** > **Dialing Rules** > **PBX main prefix**	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
PHNLD	The number to dial for long distance calls.	**Settings** > **Advanced** > **Dialing Rules** > **Number to dial for long distance calls**	Supported on all platforms.
PHNIC	The number to dial for international calls.	**Settings** > **Advanced** > **Dialing Rules** > **Number to dial for international calls**	Supported on all platforms.
PHNDPLENGTH	The internal extension length.	**Settings** > **Advanced** > **Dialing Rules** > **Length of internal extensions**	Supported on all platforms.
DIALPLANEXTENSIONLENGTHLIST	A list of PHNDPLENGTH values separated by commas. This parameter takes precedence over PHNDPLENGTH.	**Settings** > **Advanced** > **Dialing Rules** > **Length of internal extensions**	Supported on all platforms.
PHNLDLENGTH	The length of national phone numbers.	**Settings** > **Advanced** > **Dialing Rules** > **Length of national phone numbers**	Supported on all platforms.
DIALPLANNATIONALPHONENUMLENGTHLIST	A list of PHNLDLENGTH values separated by commas. This parameter takes precedence over PHNLDLENGTH.	**Settings** > **Advanced** > **Dialing Rules** > **Length of national phone numbers**	Supported on all platforms.
PHNREMOVEAREACODE or DIALPLANLOCALCALLPREFIX	The parameter that indicates whether the area code must be removed for local calls. The options are: • 1: Indicates enabled. Area code is removed for local calls. • 0: Indicates disabled. Area code is not removed for local calls. This is the default value.	**Settings** > **Advanced** > **Dialing Rules** > **Remove area/city code for local calls**	Supported on all platforms.
AUTOAPPLY_ARS_TO_SHORTNUMBERS	The parameter to disable the dialing rule logic that automatically appends the ARS code to numbers that are shorter than the shortest extension length.	Not applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	The options are: • 1: Indicates enabled. This is the default value. • 0: Indicates disabled.		
APPLY_DIALINGRULES_TO_PLUS_NUMBERS	The parameter to replace the plus sign (+) with dial plan digits. When possible, configure the plus (+) dialing option in Session Manager instead of enabling this parameter. The options are: • 1: Indicates true. • 0: Indicates false. This is the default value.	**Settings** > **Advanced** > **Dialing Rules** > **Apply dialing rules to '+' numbers**	Supported on all platforms.

Presence parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
DND_SAC_LINK	The parameter that activates the Send All Calls feature when the user sets the presence status to Do Not Disturb. The options are: • 1: Indicates that the Send All Calls feature is activated. • 0: Indicates that the Send All Calls feature is not activated. This is the default value.	**Settings** > **User Preferences** > **General** > **Activate SAC When DND Is Set**	Supported on all platforms.
WINDOWS_IMPROVIDER	The parameter that indicates whether an UC client is the IM provider for Windows clients. The options are: • 1: Indicates that an UC client is the IM provider for Windows clients. This is the default value.	**Settings** > **Desktop Integration** > **IM Provider** > **Set as default IM Provider**	Supported on Avaya Equinox® for Windows.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	• 0: Indicates that an UC client is not the IM provider for Windows clients. IM provider enables Microsoft Outlook to: • Use Avaya Equinox® for any initiated IM or a call from a contact card. • Display presence of Avaya Equinox® contacts. **Note:** You must perform a separate integration from MS Exchange to Avaya Aura® Presence Services. This is to get the presence information into the Avaya Presence system and therefore Avaya Equinox® clients.		

LDAP parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
DIRENABLED	The parameter that indicates whether LDAP is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **Services** > **Enterprise Directory** > **Enterprise Directory**	Supported on Avaya Equinox® for Mac and Windows.
DIRSSO	The parameter that indicates whether to use unified login. The options are: • 1: Indicates Yes. This is the default value.	**Settings** > **Services** > **Unified Login** > **Enterprise Directory**	Supported on Avaya Equinox® for Mac and Windows.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	• 0: Indicates No.		
DIRSRVR	The IP address or fully qualified domain name of the LDAP server.	**Settings** > **Services** > **Enterprise Directory** > **Server Address**	Supported on Avaya Equinox® for Mac and Windows.
DIRSRVRPRT	The port number of the LDAP server. The default value is 636.	**Settings** > **Services** > **Enterprise Directory** > **Server Port**	Supported on Avaya Equinox® for Mac and Windows.
DIRUSERNAME	The LDAP authentication user name.	**Settings** > **Accounts** > **Enterprise Directory** > **Username**	Supported on Avaya Equinox® for Mac and Windows.
DIRPASSWORD	The LDAP authentication password.	**Settings** > **Accounts** > **Enterprise Directory** > **Password**	Supported on Avaya Equinox® for Mac and Windows.
DIRTOPDN	The LDAP search base. For example, OU=Global Users,DC=global,DC=avaya,DC =com.	**Settings** > **Services** > **Enterprise Directory** > **LDAP Search Base**	Supported on Avaya Equinox® for Mac and Windows.
DIRSECURE	The parameter that indicates whether to use TLS or TCP for LDAP. The options are: • 1: Indicates TLS. This is the default value. • 0: Indicates TCP.	**Settings** > **Services** > **Enterprise Directory** > **Use TLS**	Supported on Avaya Equinox® for Mac and Windows.
DIRIMATTRIBUTE	The client provides access to the enterprise directory search using a direct LDAP connection. While processing the results, the client can process the attribute, such as telephoneNumber, specified in this parameter as an instant messaging address. For example, telephoneNumber, as often the administrator provisions users with Presence Server instant messaging	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	addresses that correspond to the telephone number of the user. The default value is mail. **Note:** If LDAP search is used, then the user’s LDAP profile must have the same attribute configured which is specified in this parameter.		
DIRUSEIMDOMAIN	The parameter that indicates whether the client must perform a mapping to the IM domain. The options are: • 1: Indicates enabled. This is the default value. • 0: Indicates disabled. In this parameter, the telephone number of the user is mapped into the IM domain. Example: 16135551212 becomes `16135551212@presence.example.com` if the IM domain is presence.example.com. This parameter is also used if an email address field is used. For example, alice@example.com becomes `alice@presence.example.com`. This parameter is only enabled in single domain deployments. You must not use domain mapping if any form of messaging federation is in place. Instead, ensure that the correct IM address is stored in an LDAP attribute.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.
DIRTYPE	The type of LDAP directory to which the endpoint connects.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	Valid values are: • ACTIVEDIRECTORY: This is the default value. • DOMINO • NOVELL		
DIRSCOPE	The parameter that defines the scope of the LDAP search. Valid values are: • LDAP_SCOPE_BASE • LDAP_SCOPE_ONELEVEL • LDAP_SCOPE_SUBTREE: This is the default value.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.
DIRTIMEOUT	The search time-out interval in seconds. The range is 10 to 200 and the default value is 100.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.
DIRMAXENTRIES	The maximum number of matching entries to display. The range is 10 to 100 and the default value is 50.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.

Media parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
DTMF_PAYLOAD_TYPE	The RTP payload type to be used for RFC 2833 signaling. Valid values are 96 through 127. The default value is 120.	Not Applicable	Supported on all platforms.
RTP_PORT_LOW	The lower limit of the UDP port range to be used by RTP/RTCP or SRTP/SRTCP connections. Valid values are 1024 through 65503. The default value is 5004.	Not Applicable	Supported on all platforms.
RTP_PORT_RANGE	The range or number of UDP ports available for RTP/RTCP or SRTP/SRTCP connections.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	This value is added to RTP_PORT_LOW to determine the upper limit of the UDP port range. Valid values are 32 through 64511. The default value is 200.		
ECHO_CANCELLATION	The echo cancellation algorithm. Echo cancellation is a process that removes echo from a voice communication to improve voice quality on a telephone call. The supported values are: • aec: This is the default value. • aecm • off	Not Applicable	Supported on Avaya Equinox® for Android.
ENABLE_OPUS	The parameter to enable or disable the Opus codec capability. The supported values are: • 0: The parameter is disabled. • 1: ENABLE_OPUS_WIDEBAND_20K. This is the default value. • 2: ENABLE_OPUS_NARROWBAND_16K. • 3: ENABLE_OPUS_NARROWBAND_12K.	Not Applicable	Supported on all platforms.
OPUS_PAYLOAD_TYPE	The RTP dynamic payload type used for the Opus codec. This parameter is used when the media offer is sent to the farend in an INVITE or 200 OK when INVITE with no SDP is received. Valid values are 96 through 127. The default value is 116.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
DSCPAUD	The parameter that indicates the DSCP marking for audio frames that the endpoint generates. This parameter is used only in OTT deployments. In TE deployments, DSCP values are obtained from PPM as Avaya Aura® is available. Valid values are 0 through 63. The default value is 46.	Not Applicable	Supported on all platforms.
DSCPSIG	The parameter that indicates the DSCP marking for signaling frames that the endpoint generates. This parameter is used only in OTT deployments. In TE deployments, DSCP values are obtained from PPM as Avaya Aura® is available. Valid values are 0 through 63. The default value is 24.	Not Applicable	Supported on all platforms.
DSCPVID	The parameter that indicates the DSCP marking for video frames that the endpoint generates. This parameter is used only in OTT deployments. In TE deployments, DSCP values are obtained from PPM as Avaya Aura® is available. Valid values are 0 through 63. The default value is 34.	Not Applicable	Supported on all platforms.
MEDIAENCRYPTION	The parameter to specify the media encryption ciphers. The default value is 1,2,9. Value: • 1: Indicates aescm128-hmac80 • 2: Indicates aescm128-hmac32 • 9: Indicates none • 10: Indicates aescm256-hmac80	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	• 11: Indicates aescm256-hmac32 Avaya Equinox® supports any combinations of 1, 2, 10, 11, and 9, such as 1,9 or 2,9 or 1,2,9 or 10,9 or 11,9 or 10,11,9 or 1,2,10,11,9. The ordering of these digits does not affect the functionality of Avaya Equinox®. To support the Best Effort SRTP negotiation, the parameter must contain 9 and at least one other value of 1, 2, 10, and 11. If the parameter does not contain 9, Avaya Equinox® automatically adds 9. For interoperability with Avaya Aura®: • For the Avaya Aura® 6.x environment, the recommended value for this parameter is 1,9. • For the Avaya Aura® 7.x environment, the recommended value for this parameter is 10,1,9.		
ENCRYPT_SRTCP	The parameter to enable SRTCP encryption. The options are: • 1: Indicates that SRTCP encryption is enabled. • 0: Indicates that SRTCP encryption is disabled. This is the default value.	Not Applicable	Supported on all platforms.
ENABLE_MEDIA_HTTP_TUNNEL	The parameter to enable the Media HTTP Tunneling feature. The options are: • 1: Indicates that the Media HTTP Tunneling feature is enabled. This is the default value.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	• 0: Indicates that the Media HTTP Tunneling feature is disabled. This parameter is applicable only to Avaya Equinox® Conferencing.		

Video parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
ENABLE_VIDEO	The parameter that indicates whether video is enabled. The options are: • 1: Indicates that video is enabled. This is the default value. • 0: Indicates that video is disabled.	• On mobile clients: **Settings** > **Services** > **Phone Service** > **Video Calling** • On desktop clients: **Settings** > **User Preferences** > **Audio / Video** > **Video Calling**	Supported on all platforms.
VIDEO_MAX_BANDWIDTH_ANY_NETWORK	The parameter that indicates the video bandwidth on any network. The supported values in kilobits per second (kbps) are: • 1792 • 1280: The default value for Windows clients. • 1024: The default value for MacOS clients. • 768 • 512: The default value for mobile clients. • 384 • 256 • 128 • 0: The value to indicate that video is blocked. You can also specify a custom value between 0 to 10000.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
VIDEO_MAX_BANDWIDTH_CELLULAR_DATA	The parameter that indicates the video bandwidth on the cellular data network. The supported values are the same as for VIDEO_MAX_BANDWIDTH_ANY_NETWORK. The default value is 512 kbps to limit video resolution.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.
BFCP_TRANSPORT	The parameter to enable or disable Binary Floor Control Protocol (BFCP) and set the Transport mode. The options are: • 1: Indicates UDP only. This is the default value for Avaya Equinox® clients as there is no way to enable this parameter for Meet-Me clients if the default value is 0. • 0: Indicates that BFCP is disabled. This is the default value for Avaya Aura® Device Services.	Not Applicable	Supported on all platforms.
BFCP_UDP_MINIMUM_PORT	The parameter that specifies the lower limit of the UDP port range to be used by the BFCP signalling channel. The range is 1024 to 65503. The default value is 5204. Usually, the BFCP minimum port value is equal to the RTP UDP port maximum value + 1.	Not Applicable	Supported on all platforms.
BFCP_UDP_MAXIMUM_PORT	The parameter that specifies the upper limit of the UDP port range to be used by the BFCP signalling channel. The range is 1024 to 65503. The default value is 5224.	Not Applicable	Supported on all platforms.
ENABLE_MSS_VIDEO	The parameter to enable or disable the Multi-stream	Not Applicable	Supported on Avaya Equinox® for Mac and Windows

Name	Description	Client UI setting name	Avaya Equinox® platform support
	Switching (MSS) video feature. The options are: • 1: Indicates that the video feature is enabled for MSS v1. This is the default value. • 0: Indicates that the MSS video feature is disabled.		

Voice mail parameter

Name	Description	Client UI setting name	Avaya Equinox® platform support
AAM_PORTAL_URI	The URI of Avaya Aura® Messaging Web Portal. This parameter allows users to start the voice mail portal on their client for advanced interactions, such as downloading voice mail or adjusting settings.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.

Administration parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
SUPPORTEMAIL	The default email address to send diagnostic logs.	On Avaya Equinox® for Android: **Settings** > **Support** > **Report a Problem** > **Support Email Address**	Supported on all platforms.
SUPPORTURL	The default URL to get support.	Not Applicable	Supported on all platforms.
LOG_VERBOSITY	The parameter that indicates whether verbose logging is enabled in the local client. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **Support** > **Enable Diagnostics**	Supported on all platforms.
ANALYTICSENABLED	The parameter that allows administrators to stop collecting	**Settings** > **Support** > **Quality Improvement**	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	data on behalf of their user community. The options are: • 1: Indicates enabled. This is the default value. • 0: Indicates disabled.		
ISO_SYSTEM_LANGUAGE	The parameter that indicates the system language if silent installation is used. The default language is the same as the language of the operating system if supported. Else, the default language is set to en_US.	**Settings** > **User Preferences** > **Display** > **Languages**	Supported on Avaya Equinox® for Mac and Windows.
CELLULAR_DIRECT_ENABLED	The parameter that indicates whether the Cellular Direct feature is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value. Avaya Equinox® starts a call by using the cellular network if both the following conditions are met: • The value of this parameter is set to 1. • The dialed number matches any number specified in the CELLULAR_DIRECT_NUMBER_LIST parameter. For example, if you set the value of this parameter to 1 and if the user dials 911, which is specified in CELLULAR_DIRECT_NUMBER_LIST, Avaya Equinox® starts the call by using the cellular network.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.
CELLULAR_DIRECT_NUMBER_LIST	A multivalue parameter that is a number of phone numbers that are sent directly to the native phone client on iOS or Android.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	The numbers can contain any digits or characters that can be dialed from the client UI or the native dialer, including: • Special characters, such as plus (+), asterisk (*), and hash (#). • Any alphanumeric character, such as A-Z, a-z, or 0-9. **Note:** iOS does not support numbers containing an asterisk (*) or a hash (#).		

Security settings parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
REVOCATIONCHECKENABLED	The parameter that indicates whether certificate revocation is checked. Supported values are: • 0: Disabled. • 1: Best effort. The default value for checking certificate revocation. The revocation checking failures, such as no response and no revocation authority, are not fatal. • 2: Mandatory. Certificate revocation is checked. Revocation checking failures are fatal.	Not Applicable	Supported on Avaya Equinox® for Mac and Windows.
TLSSRVRID	The parameter that defines the actions to be taken when the server	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	identity validation fails. Supported values are: • 0: Allow the connection to continue. This is the default value. • 1: Abort the connection. This parameter applies to all protocols for all configured services on the endpoint. **Note:** If you correct the Subject Alternative Name value in the System Manager certificate after a server identity validation failure, you must inform the user to log in again to Avaya Equinox®.		
SUPPORTWINDOWSAUTHENTICATION	The parameter that indicates whether Windows Authentication is used when challenged for authentication on a device that is logged in to the domain. Supported values are: • 1: Enabled. • 0: Disabled. This is the default value.	Not Applicable	Supported on Avaya Equinox® for Windows.
PKCS12URL	The parameter that indicates the URL to be used to download a PKCS #12 file containing a client identity certificate and its private key. Avaya Aura® Device Services validates the	Not Applicable	Supported on Avaya Equinox® for Android and iOS.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	entry for standard URL format.		
PKCS12PASSWORD	The parameter that indicates the password for the PKCS#12 certificate, which you specified in PKCS12URL. This parameter is optional and must only be used in cases where you want to ensure that access to the settings file is protected appropriately. If the password is absent, but is required to install the certificate, the user is prompted in the application to enter the PKCS12PASSWORD as required.	**Certificate Password**	Supported on Avaya Equinox® for Android and iOS.
MYCERTURL	The parameter that indicates the URL of the SCEP server from which the client must obtain an identity certificate. This is needed if the client does not already have an identity certificate from that server. The default value is empty, which means that the client does not attempt to retrieve an identity certificate using SCEP.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.
MYCERTCN	The parameter that indicates the Common Name (CN) that is used in the subject of an SCEP certificate request. If you keep this parameter value blank,	Not Applicable	Supported on Avaya Equinox® for Android and iOS.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	Avaya Equinox® prompts the user to enter a value before starting SCEP enrollment.		
SCEPPASSWORD	The parameter that indicates the password to be included in the challengePassword attribute of an SCEP certificate request. If you keep this parameter value blank, Avaya Equinox® prompts the user to enter a value before starting SCEP enrollment.	**Password**	Supported on Avaya Equinox® for Android and iOS.
SCEP_USESSO	The parameter that indicates whether SCEP uses unified login. The options are: • 0: Indicates that SCEP does not use unified login. This is the default value. • 1: Indicates that SCEP uses unified login.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.
MYCERTDN	The parameter that indicates the part of the certificate subject that is common to all clients. The value must begin with a forward slash "/" and might include the OU, O, L, ST, and C values. The default value is an empty string. Avaya recommends that a forward-slash character "/" be used as a separator between components because commas do not work with some servers.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	If the value includes spaces, ensure that you enter the entire value. For example, `SET MYCERTDN /C=US/ST=NJ/L=MyTown/O=MyCompany`.		
MYCERTCAID	The parameter that indicates an identifier for the CA certificate with which the certificate request must be signed if the server hosts multiple certificate authorities. The default value is CAIdentifier.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.
MYCERTKEYLEN	The parameter that indicates the bit length of the public and private keys generated for the SCEP certificate request. The range is 1024 to 2048. The default value is 2048.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.
MYCERTRENEW	The parameter that indicates the percentage of the identity certificate's validity interval after which renewal procedures must be started. The range is 1 to 99. The default value is 90. When the client certificate passes this interval, a visual warning is presented to the user stating that the certificate will expire shortly and must be renewed.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.

User policy settings parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
LOCKED_PREFERENCES	The list of locked preferences. For example, `SET LOCKED_PREFERENCES "CESSRVR","CESPORT","CESENABLED"`. The user cannot modify the values of the locked preferences in the client as locked preferences appear as read-only. To reset locked preferences, use `SET LOCKED_PREFERENCES ""`. The name of a setting must be the same across all clients. The default value is Not locked.	Not Applicable	Supported on all platforms.
OBSCURE_PREFERENCES	The list of obscured preferences. The default value is Not obscured. If you specify any parameters in this attribute, Avaya Equinox® makes the value read-only. Also, the data itself is hidden from end-users.	Not Applicable	Supported on all platforms.
VOIPCALLINGENABLED	The parameter that indicates whether VoIP is used to make calls. The supported values are: • 0: Never. • 1: Always. This is the default value. • 2: Wifi only.	**Settings** > **Services** > **Phone Service** > **Phone Service** > **Use VoIP for calls**	Supported on Avaya Equinox® for Android and iOS.
TRUSTCERTS	The list of URLs, absolute or relative, to CA certificates that will be stored in the private trust store and used to validate certificates of various servers. Set a blank value to clear the private trust store and go back to the platform trust store.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	Certificates stored in binary DER form, commonly known as `.cer`, `.crt`, or `.der` files, and Base64-encoded DER form, commonly known as `.pem` files, are supported.		
TRUST_STORE	The parameter to enable the trust stores in the server certificate chain validation. The options are: • 0: Indicates that only private trust store is used for all CSDK HTTPS and TLS connections. • 1: Indicates that both platform and private trust stores are used for all CSDK HTTPS and TLS connections. This is the default value. **Note:** If you disable the private trust store in the TRUSTCERTS setting, then all HTTPS and TLS connections use the platform trust store and this setting does not apply.	Not Applicable	Supported on all platforms.
DISABLE_PASSWORD_STORAGE	The parameter that stops the client from storing passwords locally. The options are: • 1: Indicates TRUE. • 0: Indicates FALSE. This is the default value. When the parameter is enabled, the client can continue to cache the credentials in RAM only. The client does not store passwords in persistent storage. This implies that each time the client starts, users are prompted to enter their password.	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
FORCE_LOGOUT_AFTER	The parameter that represents the number of days before the client automatically logs out. It forces users to enter their credentials to log in again. The range is from 0 to 365 days. The options are: • 1: Indicates that the parameter is enabled. • 0: Indicates that the parameter is disabled. This is the default value.	Not Applicable	Supported on Avaya Equinox® for Android and iOS.

User preferences parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
AUTO_AWAY_TIME	The parameter that indicates the idle time in minutes after which the presence status of the user automatically changes to **Away**. The value is normalized to 0, 5, 10, 15, 30, 60, 90, or 120. A value of 0 disables the feature. The default value is 10 minutes. **Note:** The value of 5 minutes is only supported on desktop clients.	**Settings** > **User Preferences** > **General** > **Auto Set to Away**	Supported on all platforms.
ADDRESS_VALIDATION	The parameter that indicates whether messaging address validation is enabled. The options are: • 1: Indicates enabled. • 0: Indicates disabled. This is the default value.	**Settings** > **User Preferences** > **Contacts** > **Messaging Address Validation**	Supported on all platforms.
PHONE_NUMBER_PRIORITY	The parameter that indicates the default phone number priority. The value is a list of comma-separated strings, which are listed from left to right to indicate	Not Applicable	Supported on all platforms.

Name	Description	Client UI setting name	Avaya Equinox® platform support
	the order in which the phone numbers will be used. If the PHONE_NUMBER_PRIORITY parameter is not defined, then the default order is used, which is Work, Mobile, Home.		
NAME_SORT_ORDER	The parameter that indicates how names are sorted in the UI. The value is a comma-separated list of the following strings: • last • first By default, names are sorted according to last name.	**Settings** > **User Preferences** > **Contacts** > **Name Sort Preferences**	Supported on Avaya Equinox® for Android and Windows.
NAME_DISPLAY_ORDER	The parameter that indicates how names are displayed in the UI. The value is a comma-separated list of the following strings: • last • first By default, the first name is displayed first.	**Settings** > **User Preferences** > **Contacts** > **Name Display Preferences**	Supported on Avaya Equinox® for Android and Windows.
HOMESCREENLAYOUT	The parameter that defines which Home screen layout to show. The options are: • 0: Displays Top of Mind. This is the default value. The user can change the preference on the mobile device. • 1: Displays the Top of Mind layout on the mobile device. • 2: Displays the Top of Mind Lite layout on the mobile device. This is the dialpad view. You can lock options 1 and 2 to prevent the user from changing them.	On the home screen, select the **Top of Mind** filter, and then select the **Top of Mind** switch.	Supported on Avaya Equinox® for Android and iOS.

Name	Description	Client UI setting name	Avaya Equinox® platform support
APPLICATION_AUTO_START	The parameter that indicates whether to start the client automatically. The values are: • 1: Yes. This is the default value for desktop clients. • 0: No. This is the default value for mobile clients.	**Settings** > **User Preferences** > **General** > **Auto Start/Login**	Supported on Avaya Equinox® for Android, Mac, and Windows.
APPLICATION_CLOSE_WINDOW	The parameter that indicates how the client functions when the user clicks **X** in the main application window. The supported values are: • 0: Minimize the client to the task bar or dock bar. This is the default value. • 1: Minimize the client to the notification area. • 2: Exit the client.	**Settings** > **User Preferences** > **Display** > **Main Window X Preferences**	Supported on Avaya Equinox® for Mac and Windows.

iOS 10 CallKit parameters

Name	Description	Client UI setting name	Avaya Equinox® platform support
IOS10CALLKIT_ENABLED	The parameter that determines whether iOS 10 CallKit is enabled in the Avaya Equinox® for iOS client. The options are: • 1: Indicates enabled. This is the default value. • 0: Indicates disabled. Introduced in iOS 10, CallKit is a new framework developed by Apple that enables VoIP applications on iOS to adopt the native phone interface for calls. The aim is to give *first-party experience to third-party applications*. Avaya Equinox® for iOS supports the CallKit framework on iOS 10 and later versions.	**Settings** > **Services** > **Phone Service** > **Integrated Calls**	Supported on Avaya Equinox® for iOS.

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, 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**, or **Exceptions** fields, specify the settings.
3. Click **Save**.
4. In the Save Configuration window, select **Overwrite existing configuration** and select an existing configuration.
5. Click **Save**.

   The system 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**.

   The system 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 admin credentials to view the settings.
5. Click **OK** to close the Test Settings window.

Publishing the 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. At the bottom of the page, click **Publish**.

   The system 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 global settings to all users, select the **Global settings will be applied to all users** check box.
9. Click **Publish**.

   Based on the publishing settings, the system applies the settings.

Viewing published settings

About this task

Use this procedure to view all the published settings for Global, Group, User, Platform and Exceptions. You can also delete these settings from the View Published Settings page.

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
   - Exceptions
4. To view published settings for a specific group, user, platform, and exception, select the required value from the list, for example, Group Name, to view 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 **Unpublish 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, the system 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 the 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**.

    The system displays the configuration settings of the user.

Supported characters for LDAP password

The characters supported for LDAP password are:

- a to z
- A to Z
- 0 to 9
- Other supported characters include, exclamation point (!), at symbol (@), hash (#), percent sign (%), caret (^), star (*), question mark (?), underscore (_), dot (.)

Importing Dynamic Configuration settings

Importing dynamic configuration settings

About this task

Use this procedure to import dynamic configuration settings.

Before you begin

Download the additional parameter settings file from the PLDS. Ensure that the settings file has the `.txt` extension and it is in json format. For example, `dynamicConfigUpload.txt`.

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 in all the existing test configuration at all levels. You can now publish the setting to the required category (Group/User/Platform/Global/Exception).

Importing 46xxsettings file

About this task

Use this procedure to import a 46xxsettings file.

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 46xxsettings file that you want to import.
5. Click **Import**.

   The system 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 • EXCEPTION

Settings	Description
{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 sub-category 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 GLOBAL category, there is no sub-category. 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}`.

For example: `USER;user1@mysite.com;CESUSERNAME;DELETE`

Importing configuration settings using the bulk import process

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 the CSV format.

   The system displays the import status at the top of the page.

   When the import is successful, the system 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, the system 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.`
Reset	Resets the added entry and clears the text box.

Administering the default configuration

About this task

Using the Default page, you can maintain internal Dynamic 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 displays the SIPHA1 and SIPPASSWORD settings. The Avaya UC clients use these SIP credentials for Unified login. • If you clear the check box, the Dynamic Configuration does not display the SIPHA1 and SIPPASSWORD 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.
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.

Name	Description
	• If you clear the check box, the system hides the obscured settings (OBSCURE_PREFERENCES) in the Dynamic Configuration response.
Scopia synchronization interval	Specifies the days for synchronizing the settings of the Scopia server configurations. The system performs periodic synchronization to retrieve a list of users and their virtual rooms from the Scopia server. The Dynamic Configuration service prints the virtual room number for the user. For example: SET CONFERENCE_VIRTUAL_ROOM 453 The days can be from 1 through 10.
Scopia server	Specifies the Scopia server URL. This field is specific to the Scopia server. The default Scopia Management XML API ports are: • For TCP: 3336. For example: http://myscopia.mgmt.avaya.com:3336 • For TLS: 3346. For example: https://myscopia.mgmt.avaya.com:3346 For establishing a TLS connection, Avaya Aura® Device Services and Scopia must be configured with same trusted System Manager certificates. For more information, see *Administrator Guide for Avaya Scopia® Management for Aura Collaboration Suite* and *Avaya Scopia® Management XML API Reference Guide* on the Avaya Support website.

Button	Description
Save	Saves the default configuration settings.
Get Status	Gets the connection status of the Scopia server.
Cancel	Resets any changes made on the page.

Split Horizon DNS Mapping overview

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.

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 IP addresses of the Presence server 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.

Related links

Mapping IP address to FQDN on page 92

Enabling Split Horizon DNS mapping on page 93

Split Horizon DNS Mapping field descriptions on page 93

Mapping IP address to FQDN

About this task

Use this procedure to map the IP address to 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**.

   The system displays the Split Horizon DNS Mapping page.
3. Click **Add**.

   The system 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**.

Related links

Split Horizon DNS Mapping overview on page 91

Enabling Split Horizon DNS mapping

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **DNS Mapping**.

   The system displays the Split Horizon DNS Mapping page.
3. Select the **Enable Split Horizon DNS Mappings** check box.

Related links

Split Horizon DNS Mapping overview on page 91

Split Horizon DNS Mapping field descriptions

Name	Description
Search	Searches the values from the list of entries for the typed search string.
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.

Related links

Split Horizon DNS Mapping overview on page 91

Web deployment administration

Web Deployment service overview

Using the Web Deployment service, you can provide appcast for the clients. Currently, you can create appcast only for the Avaya Equinox® desktop clients. On the Web Deployment page, you can add, edit, or delete an appcast item from the appcast table that is at the bottom of the page.

The Web Deployment service supports the upload and download of the client installer that has software update files. The system creates the upload folder automatically at the time of deployment or upgrade. The administrator can also store any files that are necessary for customer to download. The customer can download the necessary files from `https://<aads_server_address>:8445/acs/resources/webdeployment/downloads/<file_name_with_extension>`. The upload service operates from the directory `/opt/Avaya/DeviceServices/ClientInstallers/`.

Example of the Upload URL: `<https://IP address>:8445/admin/upload`

Example of the Download URL: `<https://IP address>:8445/acs/resources/downloads/>`.

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, the Avaya Equinox® client for Windows or Mac will get the APPCAST_URL setting from the Dynamic Configuration service response for the Web Deployment service.

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

Uploading and hosting CA certificate files on Avaya Aura® Device Services server

About this task

Use this procedure to upload CA certificate files to host on Avaya Aura® Device Services server.

Procedure

1. Go to, `/opt/Avaya/DeviceServices/ClientInstallers` on both Avaya Aura® Device Services servers and transfer the CA certificate files in this directory.

2. Run the following command to change the ownership of the certificate file:

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

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

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

   Note:

   You can combine all the CA certificate files into a single file or set the autoconfiguration setting SET TRUSTCERTS to the following:

   ```
   SET TRUSTCERTS https://<aads-server-fqdn>:8443/acs/resources/
   webdeployment/downloads/cert1.crt,https://<aads-server-fqdn>:
   8443/acs/resources/webdeployment/downloads/cert2.crt, https://
   <aads-server-fqdn>:8443/acs/resources/webdeployment/downloads/
   cert23.crt.
   ```

Configuring software update deployment

About this task

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

Procedure

1. Log on to the Avaya Aura® Device Services web administrator portal.
2. In the left navigation pane, click **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.

3. 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, the system automatically adds `Avaya Communicator` before the given title.

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

   The system displays: `Avaya Equinox for Windows Version 2.0: Critical update`

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

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

5. In the **Version** field, type the version detail of the Avaya Equinox® client release.
6. In the **OS** field, select one of the platforms of the Avaya Equinox® client release:
   - Windows
   - Macintosh

7. In the **File** field, click **Choose File** to upload a plug-in file (Avaya Equinox® client installer) from the local system.

   The file must be of the `.exe`, `.msi`, or `.dmg` format. Maximum size for uploading the client installer is 100 MB.

   The upload service accepts alphanumeric characters, white spaces, dots, minus, and square brackets.

   After you upload the file, the system auto populates the **Size (in bytes)** and the **MD5 Hash** field.

8. 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.

   The system displays a pop up to specify the user credentials to upload the client installer and a confirmation dialog box to indicate the upload status.

9. 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 credential for client authentication.

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

    the system populates the data in the table at the bottom of the page with the details of **Product Title**, **Description**, **Version**, **Publish Date**, **OS**, **Language**, **Type**, and **Download URL**. To edit or delete a specified setting, you can double-click to select an entry.

Editing an appcast item

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.

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

   The system displays the Edit appcast item page.

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

   The system populates the updated data in the table at the bottom of the page.

Deleting an appcast item

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.
3. On the bottom of the Software Update Deployment page, click an entry in the table.

   The system displays the Edit appcast item page.
4. Click **Delete**.

   The system displays the Delete item page.
5. Click **Yes**.

Managing picture settings

About this task

Use this procedure to configure various settings of user pictures.

Procedure

1. Log on to Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Pictures** > **Configuration**.

   The system displays the Pictures Configuration page.
3. Select the **Allow users to upload their own photos** check box.
4. Click **Save**.

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**.

   The system 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.

Related links

Cluster Nodes field descriptions on page 98

Cluster Nodes field descriptions

Name	Description
Virtual IP	Displays the virtual IP address if a virtual IP address is configured. This is used as a load balancer node.
Virtual IP Master	Displays the virtual IP master node if a virtual IP address is configured.
Virtual IP Backup	Displays the virtual IP backup node if a virtual IP address is configured.
Seed Node IP	Displays the IP address of the seed node of the cluster.

Related links

Monitoring cluster nodes on page 97

Logs and alarms

Log management

The system stores the common log at `/opt/Avaya/DeviceServices/7.1.0.0.<build-number>/logs/AADS.log`.

You can view additional messages at `/opt/Avaya/DeviceServices/7.1.0.0.<build-number>/tomcat/8.0.24/logs/catalina`. These messages can be the logs generated during the start of Avaya Aura® Device Services.

Monitoring the 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/7.1.0.0.<build-number>/logs/AADS.log
   ```

   The system displays the logs generated during run time.

Setting up the log level

About this task

Use this procedure to select the level of detail that you want to capture in log files.

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Log Management** > **Log Level**.

   The system displays the Adjust Service Logging Level page.
3. In the **Logger** field, select one of the following:
   - Avaya Aura Device services Logs: Collects the logs generated by the Avaya Aura® Device Services server.
   - Client Application Service Logs: Collects the logs generated by the client application.
   - System Logs: Collects all the system logs.
   - All Logs: Collects all the logs generated by the Avaya Aura® Device Services server and the system.
4. In the **Current logging level** field, select one of the following:
   - 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: option provides detailed logs. The dynamic configuration and web deployment services use this information for debugging purposes, such as, method started and method finished.

> ⚠ **Warning:**
>
> Setting logs at FINE logging level can affect system performance.

- FINEST: provides very detailed logs on frequent events. These logs can impact server performance.

> ⚠ **Warning:**
>
> Setting logs at FINEST logging level can affect system performance.

5. Click **Save**.

Managing logs

About this task

Use this procedure to adjust log levels and collect log files. Support personnel can use the collected log files to assist with troubleshooting.

Procedure

1. In the Navigation pane, click **Logs Management** > **Log Level**.
2. In the Adjust Service Logging Level area, do the following:
    a. From the **Logger** drop-down menu, select the log type.

    b. From the **Current logging level** drop-down menu, select the level of detail that you want captured in log files.

    c. Click **Save** to apply your changes.
3. In the Collect Logs area, do the following:
    a. **(Optional)** To limit the size of the download, type a number between 1 and 20 in **Number of rotated log files to collect (1–20)**.

    This setting specifies the number of files from the log file history to include in the log collection. Leaving this setting empty collects all available logs.

    b. To collect logs for a node, click **Collect** in the corresponding row.

    c. To download the collected logs for a node, click **Download**.

    d. For a cluster, if logs from all the nodes are required, repeat steps 3.b on page 100 and 3.c on page 100.

Alarms

The alarms that Avaya Aura® Device Services triggers are visible in System Manager.

To begin alarm reporting on System Manager, you must set up SNMP user and target profiles. For more information, see *Administering Avaya Aura® System Manager*.

Table 1: Avaya Aura® Device Services alarms

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
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

Alarm description	Severity	Event code	SNMP OID
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
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

Alarm description	Severity	Event code	SNMP OID
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
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

Alarm description	Severity	Event code	SNMP OID
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
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

Alarm description	Severity	Event code	SNMP OID
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
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

Related links

Setting up the log level on page 99

Setting up Serviceability Agents for alarms on System Manager

Before you begin

Associate the Avaya Aura® Device Services server with the configured Session Manager.

On System Manager, set up an SNMPv3 user profile from **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMPv3 User Profiles**.

Set up an SNMP target profile from **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMP Target Profiles**.

About this task

To receive Avaya Aura® Device Services alarms in System Manager, you must set up Serviceability Agents.

Procedure

1. Log on to System Manager.
2. Click **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.

3. Select the Avaya Aura® Device Services host name, and click **Manage Profiles**.
4. Click the **SNMP Target Profiles** tab.
5. In the Assignable Profiles section, click the SNMP profile you created, and click **Assign**.
6. Click the **SNMPv3 User Profiles** tab.
7. In the Assignable Profiles section, select the SNMPv3 profile created, and click **Assign**.

   System Manager is now ready to receive alarms from Avaya Aura® Device Services.

Chapter 7: LDAP server configuration

LDAP server configuration

You must configure the enterprise LDAP server to authenticate the users and administrators of Avaya Aura® Device Services. When you log in to the Avaya Aura® Device Services web administration portal, the system displays the enterprise LDAP server that you configure at the time of Avaya Aura® Device Services deployment.

Creating groups in LDAP

About this task

The procedure to create groups might differ depending on the type of enterprise directory used. You must refer the documentation for your enterprise directory to create groups. This section describes the steps for creating LDAP groups in Active Directory.

Procedure

1. Access Active Directory.
2. Click the **roles** organizational unit.
3. Click the Create Group icon.
4. In the **Group name** field, type the group name and click **OK**.

   You must create the following groups in the enterprise directory that you use:

   - AADSAdmin
   - AADSAuditor
   - AADSUsers
   - AADSServiceAdmin
   - AADSServiceMaintenance
5. To add a user to the group, right-click the user and click **Add to a group**.
6. In the **Enter the object names to select** field, type the group name, and click **OK**.

Adding a new enterprise LDAP Server

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. Click the plus (+) icon.

   The system displays New Directory tab.
4. In the **Enterprise-Directory Type** field, click the LDAP Server directory that you want to add.
5. In the **Provenance Priority** field, click **Modify**.

   The system displays the Source Provenance Priority pop-up window.
6. In the **Provenance Priority** column, type the priority of the enterprise LDAP Server directory.
7. In the Confirm Action pop-up window, click **OK**.
8. In the Server Address and Credentials section, specify the parameters of the enterprise LDAP Server directory.
9. Click **Save**.

Related links

Enterprise LDAP Server Configuration field descriptions on page 108

Enterprise LDAP Server Configuration field descriptions

New Directory

Name	Description
Enterprise-Directory Type	Specifies the name of the enterprise directory. The options are: • ActiveDirectory_2008 • ActiveDirectory_2012 • Novell 8.8 • Domino 8.5.3 • LDS_2012 • LDS_2008 • OpenLDAP 2.4.31

Name	Description
	• OracleDirectoryServer 5.2
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
Secure LDAP	Indicates whether the LDAP Server connection is secure or not.
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.
Address	Specifies the IP address of LDAP Server. This field is mandatory.
Port	Specifies the port of LDAP Server. This field is mandatory.
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.

Name	Description
	For example: for Active Directory, you can use "domain\user", "user@domain", as well as the actual DN of the user object. 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 admin user.
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
Use additional Base Context DN	Enables Avaya Aura® Device Services contact search and quick search. You can add maximum 10 Base Context DNs of the same value. The primary Base Context DN is used for authentication and additional Base Context DNs are used for Avaya Aura® Device Services contact search and quick search. If you select this check box, you can see the **View/ Edit** button. Auto-configuration will use only 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. An example of attribute is, `mail` This field is mandatory.
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 This field is mandatory.
Roles Context DN	Specifies the complete Distinguished Name (DN) to search for a user role, that is, for Role Filter.

Name	Description
	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: • 0: For searching only for the object • 1: For including one level in the LDAP hierarchy in the search • 2: For including subtree in the LDAP hierarchy in the search The default value is 2.
Role Recursion	Specifies whether role recursion is enabled. The options are: • true • false
Administrator Role	Specifies the admin role in which the admin users are assigned.
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) • German (de) • English (en)

Name	Description
	- 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.
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 LDAP Server.

Configuring additional base context DNs

About this task

Use this procedure to add additional base context DNs. Additional base context DNs are used for Avaya Aura® Device Services contact search and quick search. You can add maximum 10 base context DNs for one LDAP source.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. In the Server Address and Credentials section, select the **Use additional Base Context DN** check box and click **View/Edit**.
4. In the Additional Base Context DN Configuration window, click **+**.
5. Select the base context DN and in the **Base Context DN** field, provide the value of base context DN.
6. Click **Save**.

Importing an LDAP trusted certificate

About this task

To use a secure LDAP Server, you must import a trusted certificate.

Before you begin

Ensure that you have security administrator role to perform this operation.

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. In the **Server Address and Credentials** section, do the following:
   a. Select the **Secure LDAP** check box.
   b. Click **Import Certificate**.
   c. In the Import Certificate window, click **Choose File** and select the certificate from your local system.
   d. Click **Apply**.

      The system uploads the certificate to a secure LDAP Server. If a certificate is already uploaded, the system overwrites the existing certificate.

Administering the LDAP Server configuration

Procedure

1. Log on to the Avaya Aura® Device Services interface.

2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. Modify the details of the enterprise directory.
4. Click **Save**.

Related links

Enterprise LDAP Server Configuration field descriptions on page 108

Modifying enterprise directory attribute mappings

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. In the Server Address and Credentials section, click **Modify Attribute Mappings**.

   The system displays the Enterprise Directory Mappings page.
4. In the Modify LDAP Attribute Mappings section, modify the value of the attributes.
5. Click **Save**.

Configuring Windows Authentication for Active Directory

Before you begin

Important:

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

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. 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.

4. 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> /pass +rndPass /crypto all /
kvno 0
```

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

```
ktpass /out c:\tomcat.keytab /mapuser aads_principal@EXAMPLE.COM /princ HTTP/
aads.example.com@EXAMPLE.COM /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.

5. 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.

Modifying the provenance priority

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. Click the **Enterprise Directory** tab that you want to use to modify the provenance priority.
4. In the **Provenance Priority** field, click **Modify**.

   The system displays the Source Priority Configuration pop-up window.
5. In the **Provenance Priority** column, type the priority level.

   You can assign a value between 2 to 10. You cannot assign Provenance priority 1as 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.
6. Click **Save**.

Setting up user synchronization with LDAP Server

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. In the User Synchronization Update Instructions section, do the following:
   a. Specify a date and time to schedule the synchronization of Avaya Aura® Device Services users with the Enterprise LDAP Server users.
   b. Select the **Repeat** check box and click the day to set up a recurring event for synchronization.
   c. Click **Save**.
4. **(Optional)** To immediately synchronize the user data:
   a. Click **Force LDAP Sync**.
   b. Click **Save**.

Adding a trusted host

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **Trusted Hosts**.

   The system displays the Trusted Hosts page.
3. Click **Add**.

   The system displays a new row to add the host.
4. In the new row, type the IP address or FQDN of the trusted host.

   ✱ **Note:**

   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.
5. Click **Save**.

   The system displays the message: `Trusted Hosts data is successfully edited`.

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 interface or the Avaya Aura® Device Services configuration script: **`sudo /opt/Avaya/DeviceServices/<aads_version>/CAS/<aads_version>/bin/configureAADS.sh`**.

You can enable CORS for the service and admin interfaces.

Service Interface

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

Admin Interface

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

Enabling Cross-Origin Resource Sharing for Service Interface

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **CORS Configuration** > **Service Interface**.

   The system displays the Cross-Origin Resource Sharing for Service interface page.
3. Select the **Enable Cross-Origin Resource Sharing** check box.

   The system displays the **Allow access from any origin** and **Specific Domain(s)** fields.
4. 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.
5. Click **Save**.

   The system 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`. The system then reloads the Avaya Aura® Device Services Nginx configuration to apply CORS changes.

   For service interface, the system applies the CORS configuration for the root `/`.

Enabling Cross-Origin Resource Sharing for Admin Interface

Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **CORS Configuration** > **Admin Interface**.

   The system displays the Cross-Origin Resource Sharing for Admin interface page.
3. Select the **Enable Cross-Origin Resource Sharing** check box.

   The system displays the **Allow access from any origin** and **Specific Domain(s)** fields.
4. 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.
5. Click **Save**.

   The system 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`. The system then reloads the Avaya Aura® Device Services Nginx configuration to apply CORS changes.

The system applies the specified CORS configuration for admin interface to `/admin/webdeployment/upload URL`, for example, `https://<aads_server>:8445/admin/webdeployment/upload`.

Chapter 8: 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.

Related links

Increasing the size of an AWS disk volume on page 120
Updating an existing stack with a new CloudFormation template on page 122

Increasing the size of an AWS disk volume

About this task

Use this procedure to add additional storage to the system by increasing the size of an attached disk and then allocating the free space to volumes on the disk. You cannot decrease the size of a disk.

Procedure

1. On the Amazon Web Services 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.

   The system 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
   - disk4

   For more information about disk options, see Block device descriptions on page 122.

6. In the **EBS ID** field, click the ID.

   The system 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. Log in to the system using the SSH console or PuTTY.
13. If you added storage to disk1, restart the system for the changes to take effect.

    A restart is not required when increasing the size of the other disks.
14. To use the newly allocated space, update the file system by running the following commands:

    a. `sys volmgt --summary`: To view the current disk space allocation for each volume.

       The order of block devices shown on the EC2 management console might not match the order of the devices shown in the summary tool output. Reference the devices by name and not by their display order.

    b. `sys volmgt --scan`: To scan the disks for newly allocated space.

       Important:

       If prompted, restart your system before continuing.

    c. `sys volmgt --extend [ <n>m | <n>g | <n>t | --remaining ]`: To assign unallocated disk space to the volumes on a disk, specifying the amount of space you want to add to each volume. Repeat this step for each volume that you want to extend.

       For example, to extend the size of the `/var/log/Avaya volume` on disk1 by 10 GiB, run the `\sys volmgt --extend /var/log/Avaya 10g` command.

       For more information, run the `sys volmgt --hhelp` command.

    d. `sys volmgt --summary`: To review the disk space allocation for each volume after the changes are made.

Related links

AWS-specific management options on page 120
Block device descriptions on page 122

Block device descriptions

Block device on AWS	Disk number	Description
/dev/sda1	disk1	Stores operating system and application software.
/dev/xvdb	disk2	Stores application logs.
/dev/xvdb	disk3	Stores application data.
/dev/xvdd	disk4	Stores database commit logs.

Related links

Increasing the size of an AWS disk volume on page 120

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 *Deploying Avaya Aura® Device Services*.

Procedure

1. Sign in to the Amazon Web Services Management 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.

Related links

AWS-specific management options on page 120

Chapter 9: Back up and restore operations

Backup and restore checklist

Perform the following tasks to backup and restore Avaya Aura® Device Services. In the cluster environment, you must backup and restore each node in the cluster separately.

Note:

After restoring Avaya Aura® Device Services on a new OVA, you must re-configure SSH RSA Public key and SSH RSA Private key on the seed node in a cluster environment. The re-configuration also updates the new RSA key of the other nodes.

No.	Task	Description	✔
1	Back up Session Manager to preserve data such as LDAP settings and tables.	See Backing up user data storage on page 124.	
2	Back up Avaya Aura® Device Services.	See Backing up Avaya Aura Device Services on page 125.	
3	If data changed on Session Manager, restore the database on Session Manager.	See Restoring user data storage on page 126.	
4	Run the binary installer for Avaya Aura® Device Services.		
5	Restore Avaya Aura® Device Services.	See Restoring Avaya Aura Device Services on page 127.	

Backing up user data storage

About this task

Use this procedure to run a backup immediately. Running the backup on demand does not alter the nightly backup schedule.

Procedure

1. On the Home page of the System Manager web console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.

2. Click **Backup and Restore**.
3. Select the Session Manager or multiple Session Manager instances on which you want to run the backup.
4. Click **Backup**.
5. Click **Confirm**.

Backing up Avaya Aura® Device Services

About this task

You must back up each node in a cluster separately. Avaya Aura® Device Services backs up the following data:

- Trust/Keystores
- Installation settings
- Session Manager connectivity details
- System Manager connectivity details
- Nginx configuration settings
- Configuration files

If you specify a backup directory, the backup is created in that directory. If you do not specify a backup directory, the backup is created in the current working directory.

Before you begin

Back up Session Manager to preserve data, such as LDAP settings.

In the cluster environment, set the seed node in the cluster section of the installer and set any additional nodes as non seed node.

Procedure

1. Log in to Avaya Aura® Device Services using the administrator credentials that were defined during the OVA deployment.
2. To create a backup, run the following command:

   ```
   app backup -t -d /home/<admin> <backup_file_name>
   ```

   For example:

   ```
   app backup -t -d /home/<admin> backup2016
   ```

   In this example, the backup was created in the `/home/<admin>` directory. The backup file name specified is backup2016.
3. In a cluster environment, repeat the above steps for every node in the cluster.

BackupAADS.sh options

The backupAADS.sh script is located in the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin` directory.

You can use the following options with the `backupAADS.sh` script:

-h Prints usage options for the `backupAADS.sh` script.

-d Specifies the directory for the backup.

-t Creates the backup as a `.tar` file.

-v Displays information for debugging.

Restoring user data storage

The restore operation:

- Only restores call history information that exists in the backup file.
- Deletes call history information that exists only in the database.

Procedure

1. On the Home page of the System Manager web console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select the Session Manager on which to run the restore operation.
4. Click **Restore**.
5. In the **Restore File** column, select the appropriate file you want to restore from the drop-down menu.
6. 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.
7. Click **Confirm** to send a request to each Session Manager to begin the restore operation using the selected file, or click **Cancel** to cancel the restore request.

Restoring Avaya Aura® Device Services

About this task

You can restore a backup of an Avaya Aura® Device Services node with the `restoreAADS.sh` utility. You must restore each node in a cluster separately.

Before you begin

- Back up Avaya Aura® Device Services using the `backupAADS.sh` script.
- In a standalone environment, run the binary installer by providing the node IP address, Session Manager IP address, and System Manager data and then exit the installer at the Results of installation Script screen.

  After running the binary installer, if Session Manager data has changed, restore the database on Session Manager.
- In the cluster environment, run the binary installer on every node in a cluster starting with the seed node.
- In the cluster environment, first install the seed node and then install backup and any addition nodes. While installing the backup node and any additional node, in the **Cluster Configuration** section, set the initial cluster node to `N` and provide the seed node IP address to add node to the cluster.
- To restore the single node in the cluster, if the node is a seed node, in the **Cluster Configuration** section, set the initial cluster node to `Y`. If the node is backup node or any additional node, in the **Cluster Configuration** section, set the initial cluster node to `N` and provide the seed node IP address.

Procedure

1. Log in to Avaya Aura® Device Services using the administrator credentials that were defined during the OVA deployment.
2. Run the following command to change the ownership of the backup file:

   ```
   sudo chown -R <admin_user:admin_grp> <full_path_to_backup_tar_file>
   ```
3. Run the following command to restore the backup file:

   ```
   app restore /home/<admin>/<backup_tar_file>
   ```

   For example:

   ```
   app restore /home/<admin>/backup2016_uc-aads1-traffic
   ```

   In this example, the backup file is `backup2016_uc-aads1-traffic.tar`.
4. In a cluster environment, repeat the above steps for every node in the cluster.
5. From another node in a cluster, set up RSA public and private keys. For more information, see *Deploying Avaya Aura® Device Services*.
6. After the restoration is complete, restart services by running the following command:

   ```
   sudo service AADSService restart
   ```

RestoreAADS.sh options

The `restoreAADS.sh` script is located in the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin` directory.

You can use the following options with the `restoreAADS.sh` script:

-h Displays usage options for the `restoreAADS.sh` script.

-c Restores only configuration files.

-s Skips sha256 checksum validation.

-S Displays sha256 checksums.

Chapter 10: Upgrades and migrations

You can upgrade from one version to another within an Avaya Aura® Device Services release. You must perform a migration to move from Release 7.1 to 7.1.2, and the operating system is changed as part of the process.

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSN), and Product Correction Notices (PCN) for the product or solution on the Avaya Support Web site at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

Upgrading Avaya Aura® Device Services

About this task

Use this procedure to upgrade Avaya Aura® Device Services.

If you add a third load, the upgrade will fail and the system will prompt you to remove the old load.

Important:

In a cluster environment, perform these steps for all nodes, starting with the seed node.

Before you begin

- Download the latest binary file.
- Ensure the system has only two loads installed at a time.

Procedure

1. Upgrade the system layer.

`ucapp-system-7.1.x.x.x.tgz` is an example of a system layer upgrade artifact.

2. Make the required adjustments to the partitioning 2.0 volumes.
    a. Confirm that the system is on partitioning version 2.0 using the **`sys versions`** command.
    b. Set the `/media/data` volume to 20.0 GiB.
3. Upgrade the application layer.
    a. Log on to the Avaya Aura® Device Services server as an administrator.
    b. Type `app removeinactive` to remove the inactive Avaya Aura® Device Services version.
4. Transfer the binary file to the administrator home folder on the Avaya Aura® Device Services server by using a file transfer tool of your choice.
5. Type `chmod 755 aads-7.1.2.x.xxx.bin` to make the file executable.
6. Type `sudo ./aads-7.1.2.x.xxx.bin` to start the upgrade.

    After the upgrade is complete, restart services, and then check DRS replication on System Manager.

Rolling back Avaya Aura® Device Services

About this task

You can roll back to a previously installed Avaya Aura® Device Services version if the previous Avaya Aura® Device Services version is still present on the server. The rollback operation cannot be performed on the first Avaya Aura® Device Services version installed. The service will not be available during the rollback.

In the cluster environment, perform the roll back operation on the non-seed nodes first. You must begin with the last node on which you performed the upgrade operation. After you perform roll back operation on all secondary non-seed nodes, perform rollback operation on the seed node.

In a cluster, you must roll back every node before the nodes are started.

Procedure

1. Clear the dynamic settings from the database. To clear the database do the following:
    a. Go to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/`
    b. Run the following command as a non-root user:

    ```
    sudo ./clitool-acs.sh cleanAutoConfigTestConfigurations
    ```
2. Log on to the Avaya Aura® Device Services server as an administrator.
3. Run the following command:

    ```
    sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/uninstaller/rollbackAADS.sh
    ```

In this command, <version> is the latest Avaya Aura® Device Services release that you have installed.

4. In an Avaya Aura® Device Services cluster, run the same command on every node to roll back to the previous version.
5. After rolling back every node in the cluster, run the following command to start Avaya Aura® Device Services:

   ```
   sudo /etc/init.d/AADSService start
   ```

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. Go to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/`.
3. Run the following command as a non-root user:

   ```
   sudo ./clitool-acs.sh upgradeAutoConfigTestConfigurations
   ```

   This command automatically upgrades the existing test configurations.

Running patch to allow Avaya Equinox® for Windows to reach Web Deployment service

About this task

For software updates through Avaya Equinox® for Windows client, you must apply a patch by following the instructions in this section. The patch opens port 8442 for 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 Equinox® for Windows clients and ESG servers in your environment.

If you have only Avaya Aura® Device Services and Avaya Equinox® 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 Equinox® for Windows to reach Web Deployment service

- disable: to revert the workaround to allow Avaya Equinox® for Windows to reach 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/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/IP Address>:8442/acs/resources/webdeployment

Running the patch to allow Avaya Aura® Web Gateway to reach Avaya Aura® Device Services auto-configuration service

About this task

You can perform this task only if you have Avaya Aura® Web Gateway server setup in the Avaya Aura® Device Services environment and if the REST certificate policy is set to NONE. on the Avaya Aura® Device Servicesadministration user interface.

You must run the **`dynamicconfigurations-patch.sh`** script to allow the connection between Avaya Aura® Web Gateway and Avaya Aura® Device Services auto-configuration service using certificate policy. This patch opens the port 8440 for auto-configuration service and the Avaya Aura® Device Services provides the auto-configuration service on the port 8440.

You must run this patch after every upgrade or rollback or migration of Avaya Aura® Device Services to allow Avaya Aura® Web Gateway to reach Avaya Aura® Device Services auto-configuration service.

You can use the patch with the following arguments:

- **enable:** To open port 8440 to allow Avaya Aura® Device Servicescommunicate with Avaya Aura® Web Gateway.
- **disable:** to close port 8440 from nginx and iptables.

Procedure

1. Go to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/`.
2. Run the following command:

   ```
   sudo ./dynamicconfigurations-patch.sh enable
   ```

Avaya Aura® Device Services migration

The following are the phases for migrating Avaya Aura® Device Services Release 7.1 to Release 7.1.2:

1. Preparing for migration
   - Creating a full system backup before the scheduled migration.
   - Recording configuration values from the existing Avaya Aura® Device Services Release 7.1 servers.
   - Moving logs and home directory content to safe locations.
2. Deploying new servers
   - Deploying new Avaya Aura® Device Services Release 7.1.2 OVAs to create new virtual machines for each node in the cluster.
3. Completing migration
   - Installing and configuring Avaya Aura® Device Services Release 7.1.2.
   - Running the upgrade script.
   - Starting Avaya Aura® Device Services.

Important:

The steps in this procedure are based on the VMware vSphere Client for Windows application. If you are using the VMware vSphere web client, you must know how to perform these tasks using the web client interface.

You must use the original host name and IP address from the Release 7.1 servers when deploying the new OVA.

Note:

The following migration procedures provide steps for a cluster environment. If you are working with a standalone Avaya Aura® Device Services server, disregard the references to other cluster nodes.

Preparing for migration

About this task

Use this procedure to collect data from existing the Avaya Aura® Device Services servers to migrate to the new Avaya Aura® Device Services server.

To improve efficiency when working with clusters, you can perform some steps simultaneously on all nodes in the cluster.

You can start this data collection procedure before the maintenance window because nothing is altered on 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 7.1.2.

Procedure

1. Do the following to determine the seed node in a cluster:

   In a standalone environment, the node in the solution is the seed node.

   a. In your web browser, type the following URL:

      ```
      https://<AADS-FQDN>:8445/admin
      ```

   b. Log on to Avaya Aura® Device Services web administration portal using the administrator credentials configured in the LDAP server.

   c. Navigate to **Cluster Configuration** > **Cluster Nodes**.

2. Back up the user data storage on Session Manager to preserve data, such as LDAP settings and tables.

   For more information, see Backing up user data storage on page 124.

3. Open a Linux shell on the seed node of the current Avaya Aura® Device Services solution, using the Linux administrator account credentials.

4. On each node in the cluster, run the following command to create a full backup:

   ```
   app backup -t -d <home-directory-of-admin-user>
   ```

   The system creates a file named `<date>_<hostname>.tar` in the home directory of the administrative user.
5. On each node in the cluster, run the following command to collect the current system logs:

   ```
   app collectlogs collect
   ```

   Transfer the log file that the system creates in `/var/log/Avaya/collected-logs` to an off-board storage location, using a file transfer program such as SFTP or SCP for the file transfer.

   Note:

   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. On each node in the cluster, 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. On each node in the cluster, copy backup files and other content that you want to keep in the home directories to an off-board storage location, using a file transfer program such as SFTP or SCP for the file transfer.

To add read permissions to files that you want to keep, use the administrative user information recorded earlier.

To add permission to the backup file, run the following command:

```
sudo chown admin:admingrp <date>_<hostname>.tar
```

8. For each virtual machine in the cluster, use the original installation notes to record the OVA profile used while deploying the original OVA.

Next steps

Deploy the new servers.

Deploying the new servers

About this task

Use this procedure to deploy and prepare Release 7.1.2 virtual machines for the migration. To improve efficiency, you can perform many steps simultaneously across all the nodes in the cluster.

Before you begin

- Ensure that you have created system backups and saved the required server information by completing the migration preparation procedure. For more information, see Preparing for migration on page 134.
- Obtain the latest Avaya Aura® Device Services installer and OVA. For more information, see Latest software updates and patch information on page 129.

Procedure

1. Run the following command on each node in the cluster to stop Avaya Aura® Device Services 7.1 and verify that the services are stopped:

```
svc aads stop
svc aads status
```

2. On each node in the cluster, run the following command to shut down the Avaya Aura® Device Services Release 7.1 servers and turn off the power:

```
sudo shutdown -hP now
```

3. Deploy the Avaya Aura® Device Services Release 7.1.2 OVA.

   a. Deploy the Avaya Aura® Device Services OVA for the seed node.

   b. Configure the new server with the server configuration information you saved from the Avaya Aura® Device Services Release 7.1 seed node.

   c. Attach the new virtual machine to the same network as in Release 7.1.

   d. Repeat these steps for each additional node in the cluster.

   Tip:

   For easy correlation of the nodes, you can assign to a new virtual machine a name that is similar to the previous virtual machine name, but indicates that it is for Avaya Aura®

Device Services Release 7.1.2. This is the display name of the virtual machine that vSphere Client displays and not the Linux host name. The Linux host name must remain the same as the recorded host name from the previous release.

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 home directory of the administrative user 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

Use this procedure to complete the migration of data from Avaya Aura® Device Services Release 7.1 to Release Avaya Aura® Device Services 7.1.2.

To improve efficiency, you can perform many steps simultaneously across all nodes in the cluster.

Before you begin

Ensure that you have completed the following tasks:

- Preparing for migration on page 134.
- Deploying the new servers on page 136.

Ensure that all of the required Session Manager servers are running and reachable.

Procedure

1. Transfer the backup file that you created from the corresponding Release 7.1 server to the home directory of the administrator, using a file transfer program, such as SFTP or SCP.

    Ensure that you transfer the backup file for the corresponding host name.

2. Run the Avaya Aura® Device Services Release 7.1.2 binary installer to completion on the seed node first, then run it to completion on the backup node, and then on other nodes in the cluster. Run the following command:

    ```
    sudo /opt/Avaya/csa-<new-version>.bin -- --migrate <home-directory-of-admin-user>/
    <date>_<hostname>.tar
    ```

Important:

- This command is a single Linux command and must be entered as a single line even if it appears as two lines in this document.
- Ensure that a double dash (`--`) separates the installer file name from the remainder of the command.
- Ensure that a double dash (`--`) prefixes the migrate argument.

3. Run the following command to completion on the seed node first, then run it to completion on the backup node, and then on the other nodes, running to completion on each node before moving to the next node:

```
cdto misc
sudo ./finishUpgrade.sh
```

4. Do the following to re-enroll with System Manager on the seed node first, then on the backup node, and then on all other nodes in the cluster:

   a. Run the application configuration tool:

   ```
   app configure
   ```

   b. Select **Front-end host, System Manager and Certificate Configuration**.

   c. Select **System Manager Enrollment Password** and enter the System Manager enrollment password that you recorded from the corresponding Release 7.1 node.

   d. Select **Use System Manager for certificates** and select **No** to retain the certificates from the previous system.

   The system displays new menu items for configuring a custom certificate for each interface. Leave these values unchanged unless you are importing new third party certificates.

   Important:

   The system automatically deletes the certificate migrated from the previous system if you a select a menu item to configure a custom certificate. Do not use the custom certificate menu items if you want to retain the certificates from the previous system.

   e. Select **Keystore password** and enter the keystore password that you recorded from the corresponding Release 7.1 node.

   f. Select **Apply** and respond to additional prompts so that the system applies the changes.

   g. From the **Main Menu**, select **Continue** and then **Yes** to restart the services.

   If IWA was enabled on Avaya Aura® Device Services 7.1 build, the keytab file needs to be imported again after migration to Avaya Aura® Device Services 7.1.2.

5. For a cluster environment, on the seed node, configure the SSH/RSA public and private keys to enable internode SSH communications for the cluster.

   For more information, see *Deploying Avaya Aura® Device Services*.

6. For each node in the cluster, run the following command to verify that the services are running:

   ```
   svc aads status
   ```

Next steps

Perform the required post-installation procedures as described in *Deploying Avaya Aura® Device Services*.

Rolling back migration

About this task

Use this procedure to roll back to the previous release.

Rolling back to the previous release requires deleting the new release virtual machines and turning the power back on for the virtual machines from the previous release.

Procedure

1. Sign in to the VMware VSphere Client.
2. Turn off the power for all of the new release virtual machines in the cluster.

   You must restore the Session Manager data back to a version that is compatible with the previous release. Use the Session Manager backup created during the migration preparation procedure when restoring the data. For more information, see Restoring user data storage on page 126.
3. Delete all the virtual machines for the new release, but do not delete the virtual machines from the previous release.
4. Turn on the power for each previous release virtual machine in the cluster, starting with the seed node, then the backup node, and finally the remaining nodes in any order.

Chapter 11: Troubleshooting

DRS remains in Ready to Repair state

Cause

Tomcat must restart to register the DRS URL.

Solution

Restart Tomcat by using the AADSTomcat restart service.

Restarting tomcat changes the DRS state to repairing, synchronizing, and then synchronized.

DRS remains in repairing state for a long time

Cause

Avaya Aura® Device Services logs are set in FINESTlevels, because of which huge nginx logs are created during drs process, thereby causing connection timeouts.

Solution

1. Change the log level of Avaya Aura® Device Services log to WARN level.
2. From System Manager, mark the node for repair again.

   After the node is synchronized, you can change the log level back to FINEST.

Related links

Setting up the log level on page 99
List of attributes to index

DRS remains in not polling state

Cause

System Manager and Avaya Aura® Device Services are not in the same DNS or the `/etc/hosts` file of System Manager.

If the FQDN is resolved, you need not use host files and the DRS not polling error does not occur.

Solution

1. If the System Manager host file does not have the Avaya Aura® Device Services IPs, add the IPs to the `/etc/hosts` file, and vice versa.
2. Log in to Avaya Aura® Device Services.
3. Go to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin` and run the `configureAADS.sh` script.
4. Reconfigure System Manager details again and wait till the DRS configure process is complete.

DRS fails with constraint error

Cause

DRS fails with constraint error.

Solution

1. If replication fails with constraint error, try manual repair from the System Manager admin GUI.
2. If the above step 1 fails, re-register DRS using the following steps:
   a. Go to the directory `/opt/Avaya/DeviceServices/<build>/CAS/<build>/drs`.

   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 showing the below exception:

```
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:
170)
 at com.avaya.acs.cli.AadsCryptoToolCliApp.main(AadsCryptoToolCliApp.java:104)
```

Solution

1. Go 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 the 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 while using an earlier version.

If you are using an older version of PuTTY, you might receive an `Access Denied` error when pasting the response code.

Solution

Update PuTTY to the latest version.

ESG cannot connect to Avaya Aura® Device Services when REST Certificate Policy is set to none

Occurs in a deployment with Avaya Aura® Device Services and Avaya Aura® Web Gateway, if both Avaya Aura® Device Services Web deployment feature for desktops, and WebRTC calls feature with Avaya Aura® Web Gateway is being used.

Solution

Set the certificate validation policy in Avaya Aura® Device Services Admin GUI to Optional. Do not set the certificate validation policy to none.

Web Deployment binaries for Avaya Equinox® client for Windows and Mac must be moved to another web server or follow the instructions below to add the binaries to Avaya Aura® Device Services web server on a unchallenged web port. The client cannot send certificates to Avaya Aura® Device Services WebDeployment service in this release.

Note:

Web Deployment feature is only accessible within the Enterprise network or through VPN.

Failed to generate new private key

Condition

Avaya Aura® Device Services configuration utility closes abruptly while configuring the SSH/RSA Public/Private keys.

Cause

The `/home` directory is full. Therefore, the system is not able to create `/authorized_keys` file and the system displays a disk space check warning in the log file.

Solution

Clean up the `/home` directory.

Check for updates feature is not working

Condition

The Check for Updates feature on Avaya Equinox® client on Windows gives an Update Error.

Solution

1. Add the virtual FQDN of System Manager in the hosts file of Windows system where the Avaya Equinox® client is installed.

   The hosts file is located at `C:\Windows\System32\drivers\etc\`. Add the entry in the following format.

   ```
    <IP Address> <virtual FQDN of System Manager>
   ```

2. Exit the Avaya Equinox® client and ensure that the client is not running in the Windows Task Manager.

3. On the command prompt, run the following command as an administrator:

   ```
   ipconfig /flushdns
   ```

4. Restart the Avaya Equinox® client.
5. If the Check for Updates feature is still not working, go to, **Client Settings** > **Support**.
6. Click **Reset Application**.
7. Re-configure the Avaya Equinox® client and log in to the client.

   You can re-configure the Avaya Equinox® client using Auto-configuration web URL or by manually entering all the required settings.

Slow Avaya Aura Device Services performance

Cause

The network latency between all Avaya Aura® Device Services and their respective Session Managers is more than 5 ms.

Solution

The network latency between all Avaya Aura® Device Services and their respective Session Managers must be less than 5 ms.

Unable to access administration UI when the primary node SM is nonoperational

In a cluster, if the SM associated with the primary AADS node is nonoperational, the AADS administration UI is unavailable.

Solution

Administrator must use the FQDN for the other nodes in order to access AADS admin UI, when the primary node is nonoperational.

PPM certificate error

Condition

If you upgrade Session Manager earlier than release 6.2 FP4 to 7.0.1 or later, before installing Avaya Aura® Device Services, the system displays a PPM certificate error while adding contacts. The system displays an error because Session Manager expects a SIP CA certificate. To resolve this error, install a SIP CA certificate from the CLI.

Solution

1. Log in to Avaya Aura® Device Services with administrator credentials.

2. Go to `/opt/Avaya/DeviceServices/7.1.x.0.xxx/CAS/7.1.x.0.xxx/bin`
3. Type `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 users which cannot be repaired automatically by the audit requires manual procedure to fix the data. Such users are known as faulty users. You can repair faulty users manually by de-registering or re-registering users in Avaya Aura® Device Services.

Procedure

1. Log in to the Avaya Aura® Device Services as an administrator.
2. Go to, `/opt/Avaya/DeviceServices/<version>/CAS<version>/misc`.
3. Run the following command to get the list of faulty users:

   ```
   sudo ./clitool-acs.sh dataIntegrityAuditDiagnostics fetchFaultyUsers
   ```

   The Contact Integrity Audit identifies and generates a list faulty users.
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 a user is de-registered, log out and log in again to the Avaya Aura® Device Servicesenabled client for the user.

   If the faulty users does not get repaired with the above steps, perform further investigation on the user’s contact data.

Exception in the AADS.log file

Condition

When running any CLI tool command in Avaya Aura® Device Services, the `AADS.log` file shows the following exception:

```
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.

The AADS.log file contains contact integrity logs

Condition

The `AADS.log` file contains the following logs:

```
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...
```

Presence of these logs indicates that the check to decide whether the Contact Integrity Audit is needed to run or not. This check does not mean that the Audit was executed and hence does not put extra burden on system resources.

Unable to publish Dynamic Configuration for a Group in Domino LDAP and OpenLDAP

Condition

Unable to publish Dynamic Configuration for a Group in Domino LDAP and OpenLDAP.

Solution

1. For Domino LDAP, ensure the following:
    - The `dominoGroup` object class and the `dn` attribute has different group name.
    - Each user in that group has the `dominoAccessGroups` attribute that contains distinguished name of the group.
2. If the group does not have attributes by default, add the attributes to the existing group or user.

Note:

To add any new attribute to the existing group or user, the corresponding group or user must have the `extensibleObject` object class in the entry.

3. For OpenLDAP, ensure the following:
    - Each group entry has a `distinguishedName` attribute with distinguished name of that group.
    - Each user in that group has the `memberOf` attribute with distinguished name of that group.
4. To add the `memberOf` module in OpenLDAP, do the following:
    a. Go to, `/install/config/`, for example, `/etc/openldap/slapd.d`.

    b. Create the `memberof.ldif` file with the following properties:

    ```
    dn: cn=module,cn=config
     cn: module
     objectClass: olcModuleList
     objectClass: top
     olcModulePath: /var/lib/ldap
     olcModuleLoad: memberof

    dn: olcOverlay=memberof,olcDatabase=
    {2}
    bdb,cn=config
     objectClass: olcConfig
     objectClass: olcMemberOf
     objectClass: olcOverlayConfig
     olcOverlay:
    {1}
    memberof
     olcMemberOfDangling: ignore
     olcMemberOfRefInt: TRUE
     olcMemberOfGroupOC: groupOfNames
     olcMemberOfMemberAD: member
    ```

    c. Run the following command:

    ```
    ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/memberof.ldif
    ```

    d. Run one of the following commands to restart the LDAP service:

    ```
    systemctl restart slapd
    ```

    ```
    service slapd restart
    ```

    Note:

    To add any new attribute to the existing group or user, the corresponding group or user must have the `extensibleObject` object class in the entry.

Chapter 12: System layer (OS) 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.

This section only applies to systems deployed in VMware or AWS virtual environments using Avaya-provided OVAs. As the customer, you are responsible for updating the operating system when Avaya Aura® Device Services is installed as a sofware-only application onto , using update artifacts from Red Hat.

The process to install a system layer update involves the following steps:

- Determine if the system layer update is applicable to the given virtual machine. If the update is not applicable, then there is no action required.
- Download, extract, and stage the update.
- Install the update during a maintenance window.

Related links

Determining if a system update is applicable on page 148
Downloading, extracting, and staging a system layer update on page 149
Installing a staged system layer update on page 151

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. It is possible that the machine was 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:

   The patch level reported by the above command is not used at this time, and is to be ignored.

Next steps

If the above system version is already on the recommended system update, then no further action is required.

If the above system version is lower than the recommended system update version, then continue with the process to download and stage the update.

Related links

System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs on page 148

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 site, 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 installation of the update.

Procedure

1. Download the update from the Avaya Support web site.
2. Transfer the update to the admin account of the server to be updated, using standard file transfer methods, such as SFTP or SCP.
3. Log in to the admin account of the server using SSH
4. To extract the update, use the following command:

   ```
   tar -zxf ucapp-system-3.2.0.0.9.tgz
   ```

5. To stage the update, change to the required directory and perform the following staging command:

   ```
   cd ucapp-system-3.2.0.0.9
   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-3.2.0.0.9.tgz
   rm -rf ucapp-system-3.2.0.0.9
   ```

   Tip:

   It is recommended to clean 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.

7. To verify that the update has been staged, query the status:

   ```
   sysUpdate --status
   ```

   Note:

   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.

   Tip:

   If a system update is staged in error, the staged update can be deleted as follows. It is not possible to delete a staged update once the installation of the update has started.

   ```
   sysUpdate --delete
   ```

   For additional help with the **`sysUpdate`** command, use one of the following commands. The **`--help`** option provides command line syntax. The **`--hhelp`** option provides verbose help.

   ```
   sysUpdate --help
   sysUpdate --hhelp
   ```

Next steps

Install the staged update during a maintenance window.

Related links

System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs on page 148

Installing a staged system layer update

About this task

After a system update is staged, it can then be installed. 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.

Procedure

1. Log in to the administrative account using SSH.
2. Type `sysUpdate --install` to start the installation

   Tip:

   The progress of the update can be monitored using one of the following commands. The first command uses the Linux tail browser, whereas the second uses the Linux less browser.

   ```
   sysUpdate --monitor
   sysUpdate --monitor less
   ```

   The status of the update can be queried using the command:

   ```
   sysUpdate --status
   ```

   You can obtain logs of the current, and previous, system layer update installations, by using the following command. This command places a zip file of the logs in the current working directory.

   ```
   sysUpdate --logs
   ```

Related links

System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs on page 148

Chapter 13: Resources

Documentation

See the following related documents at http://support.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.	Sales Engineers, Solution Architects, Support Personnel
Administering Avaya Aura® Session Manager	Administer the Session Manager interface.	Sales Engineers, Solution Architects, Support Personnel

Related links

Finding documents on the Avaya Support website on page 152

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.

4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Related links

Documentation on page 152

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

  Note:

  Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Appendix A: Virtualization

Thin vs. thick deployments

When creating a virtual disk file, VMware ESXi uses a thick type of virtual disk by default. The thick disk pre-allocates the space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are pre-allocated for that virtual disk.

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.
- By implementing thin provisioned disks, you are able to over-allocate storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the format may cause the thin provisioned disk to grow to full size. For example, if you present a thin provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the Microsoft Windows format tool writes information to all sectors on the disk, which in turn inflates the thin provisioned disk to full size.

Related links

Increasing the disk size of the Avaya Aura Device Services virtual machine through VMware on page 155
Increasing CPU and Memory of the Avaya Aura Device Services virtual machine on page 157
Increasing the size of a virtual disk on page 157
Increasing the size of a disk volume on a virtual machine on page 158
Increasing the virtual machine disk size in the Appliance Virtualization Platform (AVP) environment on page 160

Increasing the disk size of the Avaya Aura® Device Services virtual machine through VMware

About this task

Use this procedure only in a VMware virtualized environment.

Avaya Aura® Device Services OVA contains three virtual hard disks:

- Hard disk 1

- Hard disk 2
- Hard disk 3

Before you begin

Install the VMware with an Enterprise Plus license.

Procedure

1. Shut down the Avaya Aura® Device Services virtual machine.
2. In the vSphere client inventory, select and right-click the Avaya Aura® Device Services virtual machine and click **Edit Settings**.
3. On the Virtual Machine Properties window, in the **Hardware** tab, select one of the following:
    - **Hard disk 2**
    - **Hard disk 3**
4. Change the hard disk size settings and click **OK**.
5. Restart the Avaya Aura® Device Services virtual machine.
6. Log in to the Avaya Aura® Device Services server.
7. To apply changes to the size of a virtual disk, use the following commands:
    a. To resize an application virtual disk, type the following commands:

    ```
    presize -v /dev/sdb
    lvextend -l +100%FREE /dev/mapper/application_vg-Avaya
    resize2fs /dev/mapper/application_vg-Avaya
    ```

    b. To resize the media data virtual disk, use the following commands:

    ```
    presize -v /dev/sdb
    lvextend -l +100%FREE /dev/mapper/media_vg-Avaya
    resize2fs /dev/mapper/media_vg-Avaya
    ```
8. To extend the memory of the virtual machine, do the following:
    a. On the Virtual Machine Properties window, in the **Hardware** tab, select **Memory**.
    b. Modify the memory value, and click **OK**.
9. To extend the number of CPUs of the virtual machine, do the following:
    a. On the Virtual Machine Properties window, in the **Hardware** tab, select **CPUs**.
    b. Modify the memory value, and click **OK**.
10. To extend the size of disk volumes, use one of the following commands:

    ```
    sys volmgt --extend <volume> <x>m
    sys volmgt --extend <volume> <x>g
    sys volmgt --extend <volume> <x>t
    ```

    Where, *m* indicates megabytes, *g* indicates gigabytes, and *t* indicates terabytes.

Related links

Thin vs. thick deployments on page 155

Increasing CPU and Memory 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, select and right-click the Avaya Aura® Device Services virtual machine and click **Edit Settings**.
3. On the Virtual Machine Properties window, in the **Hardware** tab, click **Memory** or **CPUs**.
4. Do one of the following:
    - Change memory configuration.
    - Change CPU settings.
5. Click **OK** to exit the window.
6. Restart the Avaya Aura® Device Services virtual machine.

Related links

Thin vs. thick deployments on page 155

Increasing the size of a virtual disk

About this task

Each virtual disk holds one or more disk volumes. Before you can increase the size of a disk volume, you must first increase the size of the host disk to provide the required disk space.

This procedure describes how to adjust the size of a virtual disk in the Virtualization Enabled (VE) environment. The VE environment uses the standard VMware infrastructure facilities.

Before you begin

- Ensure that the system layer on the virtual machine has been upgraded to the current Release 3.3. You can verify this using the `sys versions` command.
- Delete all snapshots from the virtual machine. You cannot adjust disk sizes while snapshots exist.
- Determine the disk volume to be increased in size.
- Determine the disk number that hosts the disk volume. You can use the `sys volmgt --summary` command for more information.

Procedure

1. If the virtual machine is installed and running, log in to the system, and shut down the operating system by running the following command:

   ```
   sudo shutdown -h now
   ```

2. Stop your virtual machine if it is still running.
3. Click **Edit Settings**.
4. From the Hardware tab, select the hard disk to be enlarged.
5. In **Disk Provisioning**, enter a higher value for the disk size and select the appropriate unit of measure.
6. Click **OK**.
7. Power on the virtual machine.

Next steps

Increase the size of the disk volume.

Related links

Thin vs. thick deployments on page 155

Increasing the size of a disk volume on a virtual machine

About this task

Use this procedure to increase the size of a disk volume. The upgrade process for an OVA from a previous release requires an increase in the size of one or more disk volumes.

In rare circumstances, Avaya support might recommend specific increments in disk volume sizes to address unexpected disk engineering issues.

Before you begin

Increase the size of the virtual disks that host the volumes to be increased. This process makes new disk space available. For example, if the volume requires an additional 20.0 GiB of space and the host disk is currently 50.0 GiB, then you must change the size of the host disk to 70.0 GiB.

Procedure

1. If the virtual machine is not running, then power it up.
2. Scan the disks on the virtual machine to detect newly available disk space by running the following command:

   ```
   sys volmgt --scan
   ```

   Tip:

   For more information about this command, you can use the following commands:

   - For syntax help: `sys volmgt -h`

- For verbose help: `sys volmgt -hh`

After the scan is complete, an updated file system summary is displayed. The newly available disk space is reported in the Disk > Free column.

3. Allocate all of the unused space on the disk to the target volume by running the following command:

   ```
   sys volgt --extend <volume> --remaining
   ```

   For `<volume>`, specify the name of the volume as it appears in the Volume > Name column.

   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 the following command:

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

   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 a disk has multiple volumes and more than one volume is being increased in size, use one of the following commands to allocate a specific amount of unused space to a volume:

      ```
      sys volgt --extend <volume> <x>m
      sys volgt --extend <volume> <x>g
      sys volgt --extend <volume> <x>t
      ```

      In these commands, `m` means megabytes, `g` means gigabytes, `t` means terabytes, and `<x>` is a decimal number. For example, the following increments the `/var/log` volume by 10.5 GiB:

      ```
      sys volmgt --extend /var/log 10.5g
      ```

4. Verify that the new space has been allocated to the volume by running the following command:

   ```
   sys volmgt --summary
   ```

   Due to disk overhead, the size of the volume reported under the Volume > LVM Size column will never exactly match the size reported under the Volume > File System > Size column.

   a. If you suspect that the file system size is not correct, verify that the operation is complete by running the following command:

      ```
      sys volmgt --status
      ```

   b. If the status is reported as “Complete”, you can correct the situation using `--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 current volume.

Tip:

Similar to using `--extend` to increase volume sizes, you can also monitor the `--extend` operation and gather logs using the following commands:

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

Related links

Thin vs. thick deployments on page 155

Increasing the virtual machine disk size in the Appliance Virtualization Platform (AVP) environment

About this task

Use this procedure to increase the disk size of a virtual machine in the AVPenvironment. You only need to perform this procedure if you have deployed an earlier version of Avaya Aura® Device Services 7.1 to an AVP host and if you need to change the size of the `/media/data` volume. The `/media/data` volume resides on disk 3 and is less than 20 GiB.

Before you begin

Upgrade the system layer on the virtual machine to the current release.

Procedure

1. Upgrade the Avaya Aura® Device Services OVA.

   For more information about upgrading, see Upgrading Avaya Aura Device Services on page 129.

2. Back up the upgraded Avaya Aura® Device Services data.

   For more information about backing up the data, see Backing up Avaya Aura Device Services on page 125.

3. Deploy the Avaya Aura® Device Services OVA.

4. Restore the backed up data.

   For more information about restoring, see Restoring Avaya Aura Device Services on page 127.

Related links

Thin vs. thick deployments on page 155

Index