Maintaining Avaya Aura® Application Enablement Services

Release 10.2.x
Issue 1
December 2023

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction

Purpose

This document provides general maintenance information for Avaya Aura® Application Enablement Services. The general maintenance activities include, backing up and restoring operations, viewing or downloading log files, starting or stopping services, and restarting AE Services server or web server.

This document is intended for a professional who is involved with the maintenance of AE Services.

Chapter 2: Regulatory information and safety precautions

General safety information

Follow these rules to ensure general safety:

- Observe good housekeeping in the area of the system units during and after maintenance.
  - Place removed covers and other parts in a safe place, away from all personnel, while you service the system unit.
  - Keep your tool case away from walk areas so that people do not trip over the tool case.
- When lifting any heavy object:
  1. Verify that you can stand safely without slipping.
  2. Distribute the weight of the object equally between your feet.
  3. Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
  4. Lift by standing or by pushing up with your leg muscles. This action removes the strain from the muscles in your back. Do not attempt to lift any objects that weigh more than 16 kg (35 lb.) or objects that you think are too heavy for you.
- Do not perform any action that causes hazards to the customer or that makes the equipment unsafe.
- Before you start the system unit, ensure that other technical support staff and customer personnel are not in a hazardous position.
- Do not wear loose clothing that can be trapped in moving parts. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
- Insert the ends of your necktie or scarf inside clothing or fasten the necktie or scarf with a nonconductive clip, approximately 8 cm (3 inches) from the end.
- Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing. Metal objects are good electrical conductors.
- Remove items from your shirt pocket, such as pens and pencils, that could fall into the server as you lean over it.
- Wear safety glasses when you are working in any conditions that might be hazardous to your eyes.
- Avoid dropping any metallic objects, such as paper clips, hairpins, and screws into the server.
- After service, reinstall all safety shields, guards, labels, and ground wires. Replace any safety device that is worn or defective.

- Reinstall all covers correctly before returning the server to service.

Warning:

To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance with international radiated emissions requirements, tighten all captive screws securely so they cannot be loosened without the use of a tool.

Safety Inspection

Use this list to identify potentially unsafe conditions related to the server. When the server was designed and built, the required safety items were installed on each server to protect users and technical support staff from injury. If any unsafe conditions are present, determine how serious the apparent hazard is and whether you can safely continue without first correcting the problem.

Consider these conditions and the safety hazards they present:

- Electrical hazards, especially primary power. Primary voltage on the frame can cause serious or fatal electrical shock.
- Explosive hazards, such as a damaged monitor face or bulging capacitor.
- Mechanical hazards, such as loose or missing hardware.

Perform the following safety checks when servicing this unit:

1. Check exterior covers for damage such as loose, broken, or sharp edges.
2. Shutdown the system and unplug the AC power cords.
3. Check the power cord:
   - Verify that the third-ground connector is in good condition. Use an ohmmeter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and frame ground.
   - Verify that the power cord is the appropriate type.
   - Verify that insulation is not frayed or worn.
4. Check inside the server for any obvious unsafe conditions, such as metal filings, contamination, water or other liquids, or signs of fire or smoke damage.
5. Check for worn, frayed, or pinched cables.
6. Verify that the power-supply cover fasteners, such as screws or rivets, have not been removed or tampered with.
7. If you notice any damage, replace the appropriate system components.

Electrical safety rules

Electrical current from power, telephone, and communication cables can be hazardous. To avoid any shock hazard, you must disconnect all power cords and cables.

Observe the following rules when working on electrical equipment.

- Find the room emergency power-off (EPO) switch, disconnecting switch, or electrical outlet. If an electrical accident occurs, you can then operate the switch or unplug the power cord quickly.
- Do not work alone under hazardous conditions or near equipment that has hazardous voltages.
- Disconnect all power before:
  - Doing a mechanical inspection
  - Working near power supplies
  - Removing or installing servers
- Before you start to work on the server, unplug the power cord. If you cannot unplug it, ask the customer to switch off the wall box that supplies power to the server. Afterwards, lock the wall box in the off position.
- If you must work on a server that has exposed electrical circuits, observe the following precautions:
  - Ensure that another person, familiar with the power-off controls, is near you. Another person must be there to switch off the power if necessary.
  - Stand on suitable rubber mats to insulate you from grounds such as metal floor strips and system unit frames. Obtain the mats locally, if necessary.
  - When using testers, set the controls correctly and use the approved probe leads and accessories for the tester.
  - Use only one hand when working with powered-on electrical equipment. Keep the other hand in your pocket or behind your back. This precaution can prevent current from passing through your body.
- Regularly inspect and maintain your electrical hand tools for safe operational condition. Do not use worn or broken tools and testers.
- Never assume that power was disconnected from a circuit. First, verify that the unit is turned off.
- Always look carefully for possible hazards in your work area. Examples of hazards are moist floors, non-grounded power extension cables, and missing safety grounds.
- Do not touch live electrical circuits with the reflective surface of a plastic dental mirror. The surface is conductive. Touching a live circuit can cause personal injury and damage to the server.
- Use only approved tools and test equipment. Some hand tools have handles covered with a soft material that does not insulate you when working with live electrical currents.
- Many customers place rubber floor mats that contain small conductive fibers to decrease electrostatic discharges near the equipment. Do *not* use this type of mat to protect yourself from electrical shock.

If an electrical accident occurs:

- Use caution. Do not become a victim yourself.

- Turn off power.
- Send another person to get medical aid.

Protecting against ESD damage

Any system component that contains transistors or integrated circuits is sensitive to electrostatic discharge (ESD). ESD damage can occur when there is a difference in charge between objects. Protect against ESD damage by equalizing the charge. The server, the part, the work mat, and the person handling the part must all be at the same charge.

Packaging materials that contain ESD-sensitive components are usually marked with a yellow and black warning symbol.

Caution:

You must observe proper grounding techniques to prevent the discharge of static electricity from your body into ESD-sensitive components.

To avoid damaging ESD-sensitive components:

- Limit your movement. Movement can cause static electricity to build up around you.
- Keep the parts in protective packages until you are ready to install them into the server. If it is necessary to set down a part, put it back into its static-protective package. Do not place the part on the server cover or on a metal surface.
- Place parts on a grounded surface before removing them from their containers.
- Handle the components only after attaching a wrist strap to your bare wrist. Attach the other end of the wrist strap to a ground that terminates at the system ground, such as any unpainted metallic chassis surface.
- Handle a circuit board by the faceplate or side edges only. Avoid touching pins, leads, or circuitry. Hold devices such as a hard disk drive in the same manner. The ESD-sensitive area of these components is located on the bottom surface.

  Caution:

  Make sure that the unprotected part of your hand is not in contact with the non-component side of the board.
- Keep components away from plastics and other synthetic materials such as polyester clothing. Most clothing is insulative and retains a charge even when you wear a wrist strap.
- Do not hand components to another person unless that person is grounded at the same potential level. In general, avoid contact with other people.
- Use the black side of a grounded work mat to provide a static-free work surface. The mat is especially useful when handling ESD-sensitive devices.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.
- Verify that the ESD protective devices you use are ISO 9000 certified as fully effective.

Chapter 3: Remote access

Remote access

Secure Access Link (SAL) uses the existing Internet connectivity of the customer for remote support and alarming. All communication from the customer environment is sent by Secure Hypertext Transfer Protocol (HTTPS).

For uploading from a customer to Avaya or an Avaya Business Partner, SAL requires a bandwidth of at least 90 Kbs with round trip latency no greater than 150 ms.

Business Partners without the SAL Concentrator must provide their own IP-based connectivity, for example, B2B VPN connection, to deliver remote services.

To access the Session Manager server, customer must establish a vSphere connection or use the services port.

Chapter 4: AE Services general maintenance

Backing up the server data

About this task

Use this procedure to back up the AE Services server data, which includes configuration data files, AE Services user database, certificates, and the license file.

Backup taken in the non secure mode can only be restored in the non secure mode. Backup taken in the secure mode can only be restored in the secure mode.

A web browser is required for accessing the AE Services web interface.

The average size of AE Services full backup is 10 MB, but it can increase up to 1 GB depending on the size of Historical Metric Data Collector (HDMC). For information about HMDC and supported browsers, see *Administering Avaya Aura® Application Enablement Services*.

Procedure

1. On the AE Services Management Console main menu, click **Maintenance** > **Server Data** > **Backup**.
2. To encrypt the backup file, do one of the following :
   a. Select the **Encrypt Backup File** check box, and click **Continue**.
   b. In the **Password** field, enter the password you want to use for the encrypted backup file.

      This password must contain 15 to 256 characters. This password should not contain: apostrophe (`'`), backslash (`\`), single quote (`'`), double quote (`"`), and percent (`%`).
   c. In the **Confirm Password** field, re-enter the password.
   d. Click **Continue**.
3. On the Database Backup Continue page, click the **here** link to download the log file.

Restoring the server data

About this task

Restoring the AE Services server data involves restoring a copy of the AE Services database and restarting AE Services. The AE Services database includes configuration data files, the user database, certificates, and the license file.

Backup taken in the non-secure mode can be restored in the non-secure mode. Backup taken in the secure mode can be restored in the secure mode.

If the size of a backup file is greater than 10 MB, use the Command Line Interface (CLI) to restore the server data.

Note:

Remove the Geo Redundant High Availability (GRHA) configuration before restoring the database backup. If you restore the backup when GRHA is enabled, GRHA might not work properly. If this happens, remove GRHA and then reconfigure.

Procedure

1. On the main menu AE Services Management Console, click **Maintenance** > **Server Data** > **Restore**.
2. On the Restore Database Configuration page, click **Browse** and locate the AE Services database backup file to use.

   For example: `<hostname>_<AES version>_aesvcsdb05052013.tar.gz.enc` if the file is encrypted, or `<hostname>_<AES version>_aesvcsdb05052013.tar.gz` if the file is not encrypted.
3. Click **Restore**.
4. On the Restore Database Configuration page, click **Restart Services**.

   Caution:

   If you make any changes on the AE Services Management Console in the interval between clicking **Restore** and **Restart Services**, the restore does not occur.

Restoring the server data using the command line interface

About this task

Use the Command Line Interface (CLI) to restore the server data when the size of a backup file is greater than 10 MB.

Note:

Remove the Geo Redundant High Availability (GRHA) configuration before restoring the database backup. If you restore the backup when GRHA is enabled, GRHA might not work properly. If this happens, remove GRHA and then reconfigure.

Procedure

1. Log in to the AE Services as a root user.
2. To copy the backup file to the `/tmp` directory, use the following command:

   ```
   cp <backup file> to /tmp
   ```

3. To restore the server data, do the following:
   - Run the following command to restore with the GRHA configuration:

     ```
     /opt/mvap/bin/Restore.sh -L </path/to/LargeAESBackupFIle.tar.gz>
     ```

   - Run the following command to restore without the GRHA configuration:

     ```
     /opt/mvap/bin/Restore.sh -L -n </path/to/LargeAESBackupFIle.tar.gz>
     ```

4. Run the following commands to restart the services:

   ```
   systemctl restart DBService
   systemctl restart aesvcs
   systemctl restart sohd
   systemctl restart nftables
   systemctl restart httpd
   systemctl restart tomcat
   systemctl restart snmpd
   systemctl restart subagent1
   systemctl restart subagent2
   ```

   Note:

   Restart if both GRHA and sohd are running.

Logs

Use the Logs subtab to access the following types of AE Services log files:

Subtab name	Description
Audit Logs	To view administrative changes made through the AE Services web interface.
Error Logs	To view CRITICAL, WARNING, and FYI messages generated by Call Control services you are licensed to use.
Install Logs	To verify the success of an installation or upgrade, or to troubleshoot problems.

Table continues…

Subtab name	Description
Security Logs	To access the following log files: • Client access log files: To view information about client activity. • Command log files: To view information about system activity and errors. • System reset log files: To view a record of when the AE Services server was stopped and started.
Syslog	To view system activity. Only the security administrator and system administrator can access system log files.
AIDE Logs	To view the AIDE service activities and errors. AIDE log files are not available for the Software-only server.
User Management Service	To view the User Management service activities and errors.

Related links

Viewing log files on page 14
Downloading log files on page 15
The getlogs utility using CLI on page 15
Command outputs, configuration files, and logs on page 16

Viewing log files

Procedure

1. From the AE Services Management Console main menu, select **Status > Logs > <*log file*>** where <*log file*> can be:
   - Audit Logs
   - Error Logs
   - Install Logs
   - Security Logs > Client Access Logs
   - Security Logs > Command Logs
   - Security Logs > System Reset Logs
   - Syslog
   - AIDE Logs
   - User Management Service Logs

   Note:

   AIDE Logs are not available for the Software-Only server.
2. Click **View**.

Related links

Logs on page 13

Downloading log files

Procedure

1. From the AE Services Management Console main menu, select **Status > Logs > *<log file>*** where *<log file>* can be:
   - Audit Logs
   - Error Logs
   - Install Logs
   - Security Logs > Client Access Logs
   - Security Logs > Command Logs
   - Security Logs > System Reset Logs
   - Syslog
   - AIDE Logs
   - User Management Service Logs

   Note:

   AIDE Logs are not available for the Software-Only server.
2. Select the check box(es) for the log file(s) you want to download.
3. Click **Download**.
4. On the **Download** page, click the **here** link to download the log file.

Related links

Logs on page 13

The getlogs utility using CLI

The getlogs utility is used to collect the necessary logs and configuration for troubleshooting an AE Services server. This utility has been enhanced in Release 8.1.3.4 to get the logs for a custom period.

Run the following command for the **`getlogs.sh`** utility configuration:

```
getlogs.sh [options]
```

Table 1: Provides details of the options to run the getlogs utility command

Command	Example	Description
`getlogs.sh`	**`getlogs.sh`**	Collects all the logs available on the AE Services server.

Table continues…

Command	Example	Description
getlogs.sh *<days>*	**getlogs.sh 6**	Specify the number of days for which the logs are to be captured. As per the example, the command collects the logs of last 6 days.
getlogs.sh *<From date> <To date>*	**getlogs.sh 2021-08-03 2021-08-05**	Specify the date range in the format of YYYY-MM-DD. As per the example, the command collects the logs from August 3, 2021 to August 5, 2021.
getlogs.sh *<week>*	**getlogs.sh week**	As per the example, the command collects the logs of last one week or 7 days.
getlogs.sh *<month>*	**getlogs.sh month**	As per the example, the command collects the logs of last one month or 30 days.

Note:

getlogs.sh [options] also collects all the important command outputs and configuration files.

Run the utility as root user.

Related links

Logs on page 13

Command outputs, configuration files, and logs

The **getlogs.sh** command collects the following command outputs, configuration files, and logs:

Command outputs

/sbin/ethtool eth0

/bin/date +"%Z GMT%:z"

/sbin/hwclock --show

/bin/uname -a

/usr/bin/uptime

/opt/mvap/bin/swversion

/bin/rpm -qa |sort

/bin/ps axfg

/bin/ps -eFlfww

/usr/bin/top -bn1

/usr/bin/slabtop -o

/usr/sbin/ip addr show

/bin/df -lh

/usr/bin/du / --max-depth=1 -h

/sbin/ebtables -L

/bin/netstat -i

/bin/netstat -lnp

/sbin/ip route show

/sbin/ip link show up

/sbin/arp -env

/bin/date +"%Z GMT%:z"

Configuration files

/etc/redhat-release

/etc/hosts

/etc/resolv.conf

/etc/ntp.conf

/etc/sysconfig/network-scripts/ifcfg-eth0

/etc/sysconfig/network-scripts/ifcfg-eth1

/etc/sysconfig/network-scripts/ifcfg-eth2

/etc/sysconfig/network-scripts/ifcfg-lo

/etc/rc.d/rc.local

/etc/sysctl.conf

/opt/mvap/conf/aesvcs_aide.conf

/opt/mvap/conf/Avaya_Global_EULA_Software_License_Terms.pdf

/opt/mvap/conf/avayaLicense

/opt/mvap/conf/avayaLicenseConfirm

/opt/mvap/conf/dbStore.str

/opt/mvap/conf/dmcc-core.mlet

/opt/mvap/conf/dmcc-logging.properties

/opt/mvap/conf/dmcc-user.mlet

/opt/mvap/conf/dmcc-user.mlet.active

/opt/mvap/conf/dmcc-user.mlet.standby

/opt/mvap/conf/dmcc-wrapper.conf

/opt/mvap/conf/ha.conf

/opt/mvap/conf/jaaspam.conf

/opt/mvap/conf/javaManager.properties

/opt/mvap/conf/javaManager.properties.bak

/opt/mvap/conf/javaManager.propertiesbak

/opt/mvap/conf/javaSubagent.properties
/opt/mvap/conf/JTAPILog4j.properties
/opt/mvap/conf/lcm-core.mlet
/opt/mvap/conf/lcm-logging.properties
/opt/mvap/conf/lcm-user.mlet
/opt/mvap/conf/lcm-user.mlet.active
/opt/mvap/conf/lcm-user.mlet.mega.active
/opt/mvap/conf/lcm-user.mlet.standby
/opt/mvap/conf/lcm-wrapper.conf
/opt/mvap/conf/mapLic
/opt/mvap/conf/mcs-agent-logging.properties
/opt/mvap/conf/mcs-agent-wrapper.conf
/opt/mvap/conf/mvapinfo.security
/opt/mvap/conf/oamjpam.conf
/opt/mvap/conf/passwordAudit
/opt/mvap/conf/snmp_agent_wrapper.conf
/opt/mvap/conf/tracedefines
/opt/mvap/conf/tracemask
/opt/mvap/conf/tracemask.readme
/opt/mvap/conf/trustedcert.properties
/opt/mvap/conf/user-configuration.properties
/opt/mvap/conf/v31To30mapping.xml
/opt/mvap/conf/v40To31mapping.xml
/opt/mvap/conf/v41To40mapping.xml
/opt/mvap/conf/v42To41mapping.xml
/opt/mvap/conf/v52To42mapping.xml
/opt/mvap/conf/v61To52mapping.xml
/opt/mvap/conf/v62To61mapping.xml
/opt/mvap/conf/v631To63mapping.xml
/opt/mvap/conf/v633To631mapping.xml
/opt/mvap/conf/v63To62mapping.xml
/opt/mvap/conf/v70To633mapping.xml
/opt/mvap/conf/v711To70mapping.xml

/opt/mvap/conf/v801To711mapping.xml

/opt/mvap/conf/v813To81mapping.xml

/opt/mvap/conf/v81To801mapping.xml

/proc/meminfo

/proc/cpuinfo

/proc/partitions

/proc/interrupts

/proc/mounts

Logs

/var/log/

/var/log/avaya/

/var/log/avaya/aes/*

/var/log/sa/*

/var/log/messages*

Related links

Logs on page 13

Service Controller (start, stop, and restart services)

Use the Service Controller (**Maintenance > Service Controller**) to start, stop, and restart any of the following services:

- ASAI Link Manager
- DMCC Service (Device, Media, and Call Control)
- CVLAN Service
- DLG Service
- Transport Layer Service
- TSAPI Service
- WTI Service: By default, this service is in a stopped state.

Additionally, the Service Controller provides the following capabilities:

- Restart AE Server - stops and starts (restarts) all services listed on the Service Controller page. Restarting the AE Server does not start and stop the Web Server.
- Restart Linux - stops and starts (restarts) the Linux operating system, as well as the AE Server (all services listed on the Service Controller page) and the Web Server.

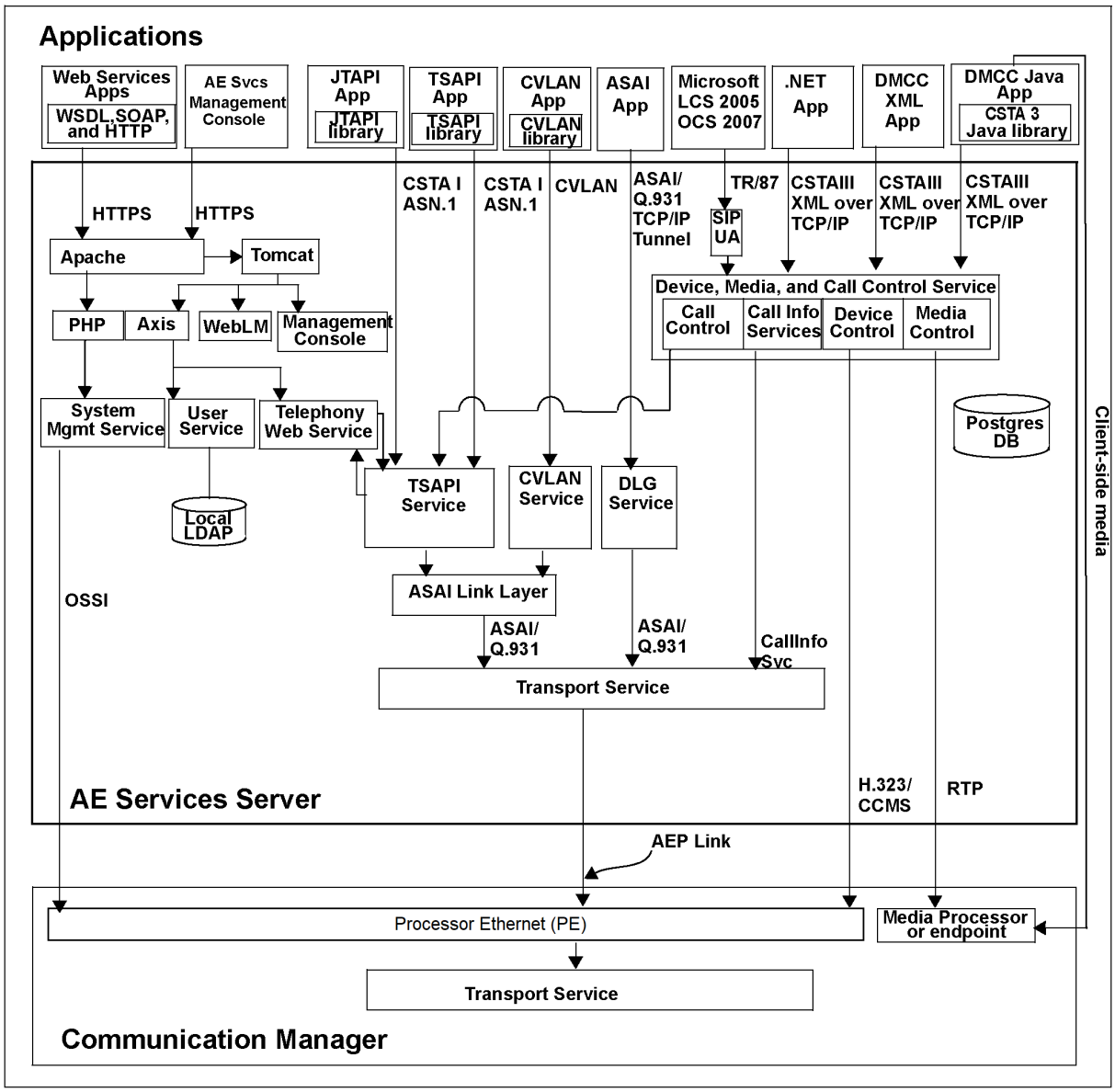
- Restart Web Server - Stops and starts (restarts) Apache, Web Telephony Interface (WTI), and Tomcat Web Server.

  Warning:

  It is generally understood that stopping and starting (or restarting) a service is potentially disruptive to applications. Doing so can result in dropped connections and lost associations.

  For an illustration of service dependencies, see Schematic view of an configuration on page 21.

Schematic view of an AE Services configuration



About stopping services

The following table shows service dependencies and explains the effects of stopping the services listed on the **Service Controller** page.

Note:

A stopped AE Service will remain in a stopped state after a server reboot.

Service	Impact of stopping the service
DMCC Service (Device, Media, and Call Control)	If you stop the DMCC service, you lose functionality of the following: • All DMCC services • All WTI services • AE Services implementation of Microsoft Office Live Communications Server 2005, Microsoft Office Communications Server 2007. All other AE Services continue to operate.
Web Telephony Interface (WTI) Service	If you stop the WTI service, you lose WTI functionality, but all other AE Services continue to operate.
DLG Service	If you stop the DLG service, you lose DLG functionality, but all other AE Services continue to operate.
CVLAN Service	If you stop the CVLAN service, you lose CVLAN functionality, but all other AE Services continue to operate.
TSAPI Service	If you stop the TSAPI service, you lose TSAPI functionality and the following clients will not operate: • TSAPI • JTAPI • Telephony Web Service • DMCC with Call Control • WTI service • Microsoft Office Live Communications Server 2005, Microsoft Office Communications Server 2007. All other AE Services continue to operate.
ASAI Link Manager	• If you stop the ASAI Link Manager, you lose ASAI link level functionality. DMCC with Call Information Services continues to communicate with Communication Manager. The TSAPI service and the CVLAN service continue to run, but they can not communicate with the Transport Layer and Communication Manager. - DLG applications and Device, Media, and Call Control applications that only use device and media control can continue to communicate with Communication Manager. - DMCC with Call Control cannot communicate with Communication Manager. • If you restart the ASAI Link Manager you do not have to restart the TSAPI service, the CVLAN service, Telephony Web service, or the Device, Media, and Call Control service. These services will recover. All their clients, however, would need to reconnect.

Table continues…

Service	Impact of stopping the service
Transport Layer Service	• If you stop Transport Layer Services, the following services continue to run: the ASAI Link Manager, the TSAPI service, JTAPI, the CVLAN service, the DLG service, Device, Media, and Call Control with Call Information services, and Device, Media, and Call Control with Call Control services and Snapshot services, but they cannot communicate with Communication Manager. • Device, Media, and Call Control applications that only use device and media control continue to operate and can communicate with Communication Manager. • If you restart the Transport Layer Service, you do not have to restart the ASAI Link Manager, the TSAPI service, the CVLAN service and the Device, Media, and Call Control service. These services will recover. You will, however, need to restart the DLG service. Also if you restart the Transport Layer service, clients of the following services would need to reconnect: TSAPI, Telephony Web service, Device, Media, and Call Control with Call Information services, Device, Media, and Call Control with Call Control services and Snapshot services, CVLAN, DLG.

Restarting the AE Services server and the web server

About this task

Use this procedure to restart the AE Services server and the web server after you install your own certificates.

Apache and Tomcat do not use the default server certificate. Instead, they use self-signed certificates. If you install your own certificates, AE Services, Apache, and Tomcat must be restarted so that they all use the same certificate.

Before you begin

Get system administration privileges to perform this task.

Procedure

1. On the AE Services Management Console main menu, click **Maintenance** > **Service Controller**.
2. On the Service Controller page, click **Restart AE Server**.

   The system restarts the ASAI Link Manager, the DMCC service, the CVLAN service, Transport Layer service, and the TSAPI service.
3. On the confirmation page, click **Restart** to restart the AE Services server.
4. On the AE Services Management Console main menu, click **Maintenance** > **Service Controller**.
5. On the Service Controller page, click **Restart Web Server**.

   The system restarts Apache and Tomcat.
6. On the Restart Web Server page, click **Restart** to restart the web server.

7. On the AE Services log in screen, log in to AE Services.

Remote syslog server overview

AE Services records log files using the remote syslog (rsyslog) server. The rsyslog is a utility for processing and managing log files. The DMCC, LCM, HMDC, SNMP subagent, AE Services management console deployed on the web server use the log4j adaptor.

TSAPI, Transport Layer, CVLAN, ASAI Link Manager, and HTTPD services record log files using glibc syslog.

With remote system logging, log messages conform to Avaya CEC requirements.

You can view the rsyslog configuration for the services in the `/etc/rsyslog.d/` file directory. The file names are as follows:

- `mavp.conf`: TSAPI, Transport Layer, CVLAN, ASAI Link Manager rsyslog configuration files.
- `aesvcs.conf`: DMCC, LCM rsyslog configuration files.
- `catalinaRsyslog.conf`: AE Services management console and web server rsyslog configuration files.
- `httpdRsyslog.conf`: HTTPD rsyslog configuration files.

Watchdog and ossicm log files are not logged using the rsyslog server.

System Logging

On the System Logging subtab, you can enable remote logging, specify the remote log server destination and port to send the AE Services server log files. You can also configure trace and log levels using the Log Manager.

Note:

TSAPI log files are not sent to the remote server.

Configuring the trace or logging levels

About this task

Use this procedure to configure the trace or logging levels by using the Log Manager for the following services:

- ASAI Link Manager
- CVLAN Service

- DLG Service
- Management Console
- Transport Layer Service
- TSAPI Service
- Web Telephony Interface (WTI) Service
- DMCC Service

The trace level setting might not correspond to any predefined choice on the Log Manager page. If so, the Log Manager page displays the exact string assigned to the service in the `tracemask` file. This entry is read only.

Important:

Do not change the trace logging levels without consulting an Avaya engineer. Keeping the trace logging levels always enabled or increasing logging levels might degrade the system performance as there is a chance that `/var/log` partition may run out of space. In this scenario AE Services server will not generate any alarm.

Procedure

1. On the AE Services Management Console main menu, click **Status** > **Log Manager** .
2. On the Log Manager page, make your changes to the appropriate settings.
3. Click **Apply Changes**.
4. On the Log Manager Confirmation page, click **Apply**.

Log and trace file retention

Set the period for retaining log and trace files from 0 to 180 days. AE Services deletes the retained log and trace files after the retention period. The default retention period is 30 days. AE Services appends the timestamp to the file name in the following format: `yyyy-mm-dd-timestamp`.

You can retain the following log files:

- All log files in the `/var/log/sssd` folder
- `/var/log/httpd/error.log`
- `/var/log/avaya/aes/mvap.log`
- `/var/log/messages`
- `/var/log/secure`
- `/var/log/tomcat/catalina.log`
- `/var/log/httpd/error.log`
- `/var/log/avaya/aes/oam-admin/audit.log`
- `/var/log/avaya/aes/oam-admin/login-auth.log`

- `/var/log/avaya/aes/sec.log`
- `/var/log/avaya/aes/dmcc-error.log`
- `/var/log/avaya/aes/ws-telsvc-error.log`
- `/var/log/avaya/aes/dmcc-jtapi-error.log`
- `/opt/mvap/lib/mgmt/logs/default.debug.log`
- `/var/log/avaya/aes/mgmt/logs/default.debug.log`
- `/var/log/tomcat/mgmt/logs/default.debug.log`
- `/var/log/avaya/aes/telrestsvc.log`

You can retain the following trace files:

- `/var/log/avaya/aes/dmcc-nist.log`
- `/var/log/avaya/aes/dmcc-trace.log`
- `/var/log/avaya/aes/DLG/trace.out`
- `/var/log/avaya/aes/TSAPI/csta-trace`
- `/var/log/avaya/aes/common/trace.out`
- `/var/log/avaya/aes/TSAPI/g3trace.out`
- `/var/log/avaya/aes/ws-telsvc-trace.log`
- `/var/log/avaya/aes/trans-serv/trace.out`
- `/var/log/avaya/aes/asailink/trace.out`
- `/var/log/avaya/aes/CVLAN/trace.out`
- `/var/log/avaya/aes/ossicm.log`

You cannot retain the `alarm.log` and `importsdb.log` log files. AE Services deletes the file contents within one day.

If the disk space is filled to more than 90%, AE Services deletes at least 25% log and trace files. AE Services deletes older files first.

Related links

Retaining log and trace files on page 27
Deleting log files on page 28
Deleting trace files on page 29
Retaining logs by using the command line interface on page 29
Retaining traces by using the command line interface on page 30
Deleting log files using the command line interface on page 30
Deleting trace files using the command line interface on page 30

Retaining log and trace files

About this task

Configure log and trace file retention period using the Log Manager. You can compress and store log files for a specific period and later retrieve the retained data, for example, for an audit procedure. AE Services deletes the retained log and trace files when the retention period is over.

Procedure

1. On the AE Services management console, go to **Status** > **Log Manager** > **Log and Trace Retention**.
2. In **Log Retention**, type the log retention period.

   You can type 0 to 180 days. The default value is 30 days.
3. In **Trace Retention**, type the trace retention period.

   You can type 0 to 180 days. The default value is 30 days.
4. Click **Set Retention**.
5. Click **Apply**.

   AE Services stores the log and trace files for the specified retention period.

Related links

Log and trace file retention on page 25
Log and Trace Retention field descriptions on page 27

Log and Trace Retention field descriptions

Name	Description
Log Retention	Log retention period between 0 and 180 days. The default value is 30 days.
Trace Retention	Trace retention period between 0 and 180 days. The default value is 30 days.

Button	Description
Set Retention	To apply the retention period you specified. AE Services displays the Log and Trace Retention Confirmation page.
Restore Defaults	To restore the default values. AE Services displays the Restore Log and Trace Retention page.
Cancel Changes	To cancel the changes.

Related links

Retaining log and trace files on page 27

Deleting log files

About this task

If you do not need specific log files for your application, delete these log files with the Log Manager. Make sure that log files do not contain important information. For example, you do not need these log files for troubleshooting.

The following log files are affected by performing the mentioned procedure:

- All log files in the `/var/log/sssd` folder
- `/var/log/httpd/error.log`
- `/var/log/avaya/aes/mvap.log`
- `var/log/messages`
- `/var/log/secure`
- `/var/log/tomcat/catalina.log`
- `/var/log/httpd/error.log`
- `/var/log/avaya/aes/oam-admin/audit.log`
- `/var/log/avaya/aes/oam-admin/login-auth.log`
- `/var/log/avaya/aes/sec.log`
- `/var/log/avaya/aes/dmcc-error.log`
- `/var/log/avaya/aes/ws-telsvc-error.log`
- `/var/log/avaya/aes/dmcc-jtapi-error.log`
- `/opt/mvap/lib/mgmt/logs/default.debug.log`
- `/var/log/avaya/aes/mgmt/logs/default.debug.log`
- `/var/log/tomcat/mgmt/logs/default.debug.log`
- `/var/log/avaya/aes/telrestsvc.log`

When you use High Availability, AE Services deletes log files only from the active server.

Procedure

1. On the AE Services management console, go to **Status** > **Log Manager** > **Clear Logs**.
2. In **Clear Logs Period**, type the retention period.

   You can type 0 to 180 days.
3. To delete log files older than the specified period, click **Clear Logs (days)**.
4. **(Optional)** To delete all log files, click **Clear All Logs**.
5. Click **Apply**.

Related links

Log and trace file retention on page 25

Deleting trace files

About this task

Delete trace files with the Log Manager. For example, when you resolve an issue, you can delete related trace files that are no longer needed.

The following traces are affected by performing the mentioned procedure:

- `/var/log/avaya/aes/dmcc-nist.log`
- `/var/log/avaya/aes/dmcc-trace.log`
- `/var/log/avaya/aes/DLG/trace.out`
- `/var/log/avaya/aes/TSAPI/csta-trace`
- `/var/log/avaya/aes/common/trace.out`
- `/var/log/avaya/aes/TSAPI/g3trace.out`
- `/var/log/avaya/aes/ws-telsvc-trace.log`
- `/var/log/avaya/aes/trans-serv/trace.out`
- `/var/log/avaya/aes/asailink/trace.out`
- `/var/log/avaya/aes/CVLAN/trace.out`
- `/var/log/avaya/aes/ossicm.log`

When you use High Availability, AE Services deletes trace files only from the active server.

Procedure

1. On the AE Services management console, go to **Status** > **Log Manager** > **Clear Traces**.
2. In **Clear Traces Period**, type the retention period.

   You can type 0 to 180 days.
3. To delete trace files older than the specified period, click **Clear Traces (days)**.
4. **(Optional)** To delete all trace files, click **Clear All Traces**.
5. Click **Apply**.

Related links

Log and trace file retention on page 25

Retaining logs by using the command line interface

Procedure

1. Log in to the AE Services as a Data Controller user.
2. Use the following command for log retention: **`retention –l <0–180>`**.

   Here, 0–180 is the number of days for which you can retain the logs.
3. Use the following command to display the current log retention period: **`retention –l`**.

4. Log out of AE Services.

Related links

Log and trace file retention on page 25

Retaining traces by using the command line interface

Procedure

1. Log in to the AE Services as a Data Controller user.
2. Use the following command for trace retention: **`retention –t <0–180>`**.

   Here, 0–180 is the number of days for which you can retain the traces.
3. Use the following command to display the current trace retention period: **`retention –t`**.
4. Log out of AE Services.

Related links

Log and trace file retention on page 25

Deleting log files using the command line interface

About this task

Set the number of days before which to delete log files using the command line interface. The default value is 0. If you keep the default value, AE Services deletes all log files except the currently written files.

Procedure

1. Log in to the AE Services command line interface as a datacontroller or cust user.
2. In the command promt, run the following command: **`logClear -l <0-180>`**.

   You can type 0 to 180 days.

Related links

Log and trace file retention on page 25

Deleting trace files using the command line interface

About this task

Set the number of days before which to delete trace files using the command line interface. The default value is 0. If you keep the default value, AE Services deletes all trace files except the currently written trace files.

Procedure

1. Log in to the AE Services command line interface as a datacontroller or cust user.
2. In the command promt, run the following command: **`logClear -t <0-180>`**.

   You can type 0 to 180 days.

Related links

Log and trace file retention on page 25

Debugging CTI session

Enabling TSAPI service logging

Procedure

1. On the AE Services Management Console main menu, click **Status** > **Log Manager** > **Trace Logging Levels**.
2. In the TSAPI Service field, select **Everything on except mutex**.
3. Click **Apply Changes**.

Result

Logs are stored at:

- `/var/log/avaya/aes/common/trace.out`
- `/var/log/avaya/aes/TSAPI/csta_trace.out`
- `/var/log/avaya/aes/TSAPI/g3trace.out`

Enabling DMCC service logging

Procedure

1. On the AE Services Management Console main menu, click **Status** > **Log Manager** > **Trace Logging Levels**.
2. From the DMCC Service, select **Finest** for all the fields.
3. Click **Apply Changes**.

Result

Logs are stored at:

- `/var/log/avaya/aes/dmcc-trace.log`

Capturing g3peek data containing CTI session information

About this task

Use this procedure to capture g3peek data containing CTI session information information.

Procedure

1. Log in to the Application Enablement Services CLI interface.
2. Run the following command: `G3pdCmdUtility -v dump 12345 CAS <PBX NAME> <CAS ID>`.

Result

The system generates the `/tmp/g3peek12345.out` file.

Displaying TSAPI Service license information

About this task

Use this procedure to display TSAPI Service license information.

Procedure

1. Log in to the Application Enablement Services CLI interface.
2. Run the following command: **`licenseInfo TSAPI tsrv`**.

Chapter 5: Location of AE Services log files

Device, Media, and Call Control Service

All logs are in /var/log/avaya/aes, as follows:

- dmcc-api.log
- dmcc-error.log
- dmcc-trace.log
- dmcc-nist.log
- dmcc-wrapper.log.*x* (where *x* is a number from 1 to 4. The first wrapper log, dmcc-wrapper.log, is not numbered.)
- database.log
- reset.log

WTI

Log file is in /var/log/avaya/aes, as follows:

- telrestsvc.log

DLG Service

AE Services provides the same logs that were provided with the MAPD-based DLG.

All logs except the trace log are in the `/var/log/avaya/aes` directory, as follows:

- Security (client) log: `sec.log`
- Error log: `mvap.log`
- Command log: `cmd.log`
- Reset log: `reset.log`

- Trace log: `/var/log/avaya/aes/common/trace.out`

CVLAN Service

AE Services provides the same logs that were provided with the MAPD-based CVLAN and CVLAN Release 9 and Release 9.1 for Linux.

All logs except the trace log are in `/var/log/avaya/aes`, as follows:

- Security (client) log: `sec.log`
- Error log: `mvap.log`
- Command log: `cmd.log`
- Reset log: `reset.log`
- Trace log: `/var/log/avaya/aes/common/trace.out`

TSAPI Service

All logs, except the trace log and the G3trace log, are in `/var/log/avaya/aes`, as follows:

- Security (client) log: `sec.log`
- Error log: `mvap.log`
- Command log: `cmd.log`
- Reset log: `reset.log`
- Trace log: `/var/log/avaya/aes/common/trace.out`
- G3trace logs are located in the `/var/log/avaya/aes/TSAPI` directory. This directory includes `g3trace.out`and `csta_trace.out`.
- Import SDB log: `importsdb.log`

Telephony Web Service

The Telephony Web Service infrastructure includes Tomcat and the TSAPI Service. Any major failure in either Tomcat or the TSAPI Service will affect the Telephony Web Service.

All logs are in /var/log/avaya/aes/tomcat, as follows:

- ws-telsvc-api.log

- ws-telsvc-error.log
- ws-telsvc-trace.log

System Management System Web Service

The System Management Service uses the Linux syslog and Apache logs.

Chapter 6: Data Encryption

From Release 10.1, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Avaya Solutions Platform 130 and VMware Virtualized Environment. Once you deploy the application with data encryption, you cannot disable data encryption after deployment.

By enabling Data Encryption, your Communication Product's certain Operational data and Log Files will be encrypted. You will be prompted to enter a passphrase that will be used to create or access an encryption key. You must remember the encryption passphrase, if not it can result in locking up the system. Secondly, you will be asked to configure the option for local key storage.

It is important to note that the encryption of the disk may have a performance impact. For further information, refer to the Avaya Product Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

By disabling Data Encryption, your Communication Product's Operational data and Log Files will not be stored in encrypted partitions.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is selected, you need to reenter the encryption passphrase whenever the application reboots.

During reboot, the application prompts you to enter the encryption passphrase on VM console at first boot and upon entering the correct encryption passphrase, the system mounts all the encrypted disks.

Note the following:

- If a common encryption passphrase is used for all the encrypted partitions, but an incorrect encryption passphrase is entered in first attempt, then you have to enter the correct encryption passphrase for every partition at least once.
- Multiple failures on encryption passphrase boots the system into the Maintenance/Emergency mode. To get the prompt again, you need to reboot the system.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is not selected during OVA deployment, the application creates the Local Key Store and the system does not prompt you to type the encryption passphrase whenever the application reboots to mount the encrypted disks. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

Encryption of Application Enablement Services partitions

When you enable data encryption for Application Enablement Services, the system encrypts the following partitions that have personal data.

- `/var/mvap/database`
- `/var/log`
- `/var/log/audit`
- `/var/lib/ldap`

Remote Key Server

When you enable data encryption for an application, you can set up remote key server. You can add multiple remote key servers. When you add a remote key server for the first time, the application disables the local key store. You can enable the local key store again after adding a remote key server. However, it is not recommended to enable local key store when the remote key server configuration exists.

If there is only one empty slot, then you cannot add a new remote key server or a new passphrase. You can use a total of 32 slots. The last empty slot is a “reserved” slot and you can use that only for changing the passphrase.

Application checks for the remote key server accessibility every 15 minutes. If any of the remote key server goes down, the application generates a Warning alarm. If all remote key servers are not accessible, then the application generates a Minor alarm.

Data Encryption password policy

The encryption passphrase must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.

Ensure that you keep the encryption passphrase safe. You need the encryption passphrase later.

Data encryption commands

The following CLI commands are available to make changes to the data encryption settings.

encryptionPassphrase command

Using the **encryptionPassphrase** command you can manage the encryption passphrase after deploying the application.

Syntax

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

add	Displays the prompts to add the encryption passphrase.
change	Displays the prompts to change the encryption passphrase.
remove	Removes the encryption passphrase.
list	Displays the encryption passphrase and slot assignment.

Considerations

You must deploy the application with data encryption.

Adding encryption passphrase

About this task

Use the **encryptionPassphrase add** command to add encryption passphrase.

You can add a maximum of seven encryption passphrases, if free slots are available.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.
2. Type **encryptionPassphrase add**.
3. In **Enter existing passphrase**, type the encryption passphrase.
4. In **Enter new Passphrase**, type the new encryption passphrase.
5. In **Retype Passphrase**, retype the encryption passphrase.

Changing encryption passphrase

About this task

Use the **encryptionPassphrase change** command to change the existing encryption passphrase.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.
2. Type **encryptionPassphrase change**.

3. At the prompt, in **Current Passphrase**, type the encryption passphrase.
4. In **Enter new Passphrase**, type the new encryption passphrase.
5. In **Retype Passphrase**, retype the encryption passphrase.

   The application displays the following message.

   ```
   Passphrase successfully changed.
   ```

Removing encryption passphrase

About this task

Use the **encryptionPassphrase remove** command to remove the existing encryption passphrase. You cannot remove all encryption passphrases, the application retains minimum one encryption passphrase.

If you attempt to delete the last encryption passphrase, the system displays the following message:

```
The last passphrase cannot be removed!
```

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.
2. Type **encryptionPassphrase remove**.
3. At the prompt, in **Passphrase to remove**, type the existing encryption passphrase.

   The application displays the following message.

   ```
   Passphrase successfully removed.
   ```

Displaying encryption passphrase and slot assignment

About this task

Use the **encryptionPassphrase list** command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.
2. Type **encryptionPassphrase list**.

   The application displays the details based on the system configuration.

```
Slot        Status      Passphrase/Remote Server
-----------------------------------------------
Key Slot 0: ENABLED     Passphrase
Key Slot 1: ENABLED     Passphrase
Key Slot 2: ENABLED     Passphrase
Key Slot 3: ENABLED     Passphrase
Key Slot 4: ENABLED     Passphrase
```

```
Key Slot 5: Disabled    empty
Key Slot 6: Disabled    empty
Key Slot 7: Disabled    empty
.......
.......
.......
Key Slot 31: Disabled    empty
```

encryptionRemoteKey command

Using the **encryptionRemoteKey** command you can manage the remote key server after deploying the application.

Syntax

```
encryptionRemoteKey [add | remove | list]
```

add	Displays the prompts to add the remote key server.
remove	Removes the remote key server.
list	Displays the remote key server and slot assignment.

Considerations

You must deploy the application with data encryption.

Adding remote key server

Before you begin

Ensure that the remote key server is configured and accessible.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.

2. Type **encryptionRemoteKey add** <Address> <Port>.

   Where:

   Address is the IP address or FQDN of the remote key server.

   Port is the port number of the remote key server. If you do not enter the port number the application uses the value of default port as 80.

3. In **Enter existing passphrase**, type the existing encryption passphrase.

   If the remote key server is not configured, the application displays the following message.

   ```
   Remote key server not found
   ```

   If the remote key server is configured, the application adds the remote key server. When you add a remote key server for the first time, the application disables the local key store.

Removing remote key server

About this task

Use the **encryptionRemoteKey remove** command to remove the existing remote key server.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.

2. Type **encryptionRemoteKey remove** <Address>.

   Where:

   Address is the IP address or FQDN of the remote key server.

   You must use the same IP address or FQDN value that you used to add the remote key server.

3. In **Passphrase**, type the existing encryption passphrase.

   The application removes the remote key server and displays the following message:

   ```
   RemoteKey successfully removed.
   ```

Displaying remote key server and slot assignment

About this task

Use the **encryptionRemoteKey list** command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.

2. Type **encryptionRemoteKey list**.

   The application displays the details based on the system configuration.

```
Slot        Status      Passphrase/Remote Server
-----------------------------------------------
Key Slot 0: ENABLED     Passphrase
Key Slot 1: ENABLED     <IP Address of Remote Key Server>
Key Slot 2: ENABLED     Passphrase
Key Slot 3: DISABLED    empty
Key Slot 4: DISABLED    empty
Key Slot 5: DISABLED    empty
Key Slot 6: DISABLED    empty
Key Slot 7: DISABLED    empty
.......
.......
.......
Key Slot 31: DISABLED    empty
```

encryptionLocalKey command

Using the **encryptionLocalKey** command you can enable or disable the local key store after deploying the application with data encryption.

Syntax

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

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

Considerations

You must deploy the application with data encryption.

Enabling local key store

About this task

Use the **encryptionLocalKey enable** command to enable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.
2. Type **encryptionLocalKey enable**.
3. At the prompt, in **Enter existing passphrase**, type the existing encryption passphrase.

   If the local key store is already enabled, the application displays the following message.

   ```
   Local key store is already enabled.
   ```

Disabling local key store

About this task

Use the **encryptionLocalKey disable** command to disable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.
2. Type **encryptionLocalKey disable**.

   The application displays the following message.

   ```
   Local keystore removed
   Local Key Store is now disabled.
   ```

Viewing data encryption status

About this task

The **encryptionStatus** command displays information about encryption on the system.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.

   For Application Enablement Services, log in with root privileged credentials.

2. Type `encryptionStatus`.
3. When the system prompts, type the password.

   For example, if the local key store is configured, the system displays the following status:

   ```
   Data Encryption: enabled
   Local Key Store: enabled
   Encryption Passphrase Required at Boot-time: no
   ```

   For example, if the remote key server is configured, the system displays the following status:

   ```
   Data Encryption: enabled
   Local Key Store: disabled
   Encryption Passphrase Required at Boot-time: yes
   remoteKeyServers: <remoteServer1: <remoteServerIPAddress> accessible>
   ```

Chapter 7: AE Services Management Console connectivity tests

AE Services Management Console connectivity tests

Use the following diagnostic utilities in AE Services Management Console to check connectivity:

Note:

When AE Services server is configured in the secure mode, AE Services does not support tests under **Utilities** > **Diagnostics** > **AE Services**.

- **ASAI Test** — Use the ASAI Test utility to determine if the AE Server is communicating with Communication Manager. The ASAI Test utility sends a heartbeat message over any of the CVLAN or TSAPI links you have configured between the AE Server and Communication Manager. (**Utilities > Diagnostics > AE Service > ASAI Test**)
- **Ping Host** — Use the Ping Host utility to determine if the hostname or IP address you specify exists and is accepting requests. (**Utilities > Diagnostics > Server > Ping Host**)
- **DMCC Test** — Use the DMCC Test to test the DMCC configurations. (**Utilities > Diagnostics > AE Service > DMCC Test**)
- **TSAPI Test** — TSAPI Test is a simple test application that makes a call between two stations, primarily to verify that the client is set up correctly and the TSAPI Service has been administered correctly. TSAPI Test applies to TSAPI, JTAPI, and Telephony Web Service applications. (**Utilities > Diagnostics > AE Service > TSAPI Test**)
- **TR/87 Test** — Use the TR/87 Test utility to run tests for DMCC applications and the AE Services implementation for Microsoft Office Live Communications Server 2005, Microsoft Office Communications Server 2007. (**Utilities > Diagnostics > AE Service > TR/87 Test)**. Some of the tests may require you to administer the dial plan in AE Services before you can execute some of the TR/87 tests.

  Note:

  The Host AA settings for AE Services (**Security > Host AA**) have an effect on the TR/87 Test utility. If you enable host authorization, the authorized hosts list must include the Peer Certificate CN (which is the Server Certificate Subject Name). Because the TR/87 Test utility depends on the Host AA settings and uses the same certificate that is used by Tomcat, you must restart the Web Server after adding a server certificate.
- **Email Notification** - You can enable email notifications from the AE Services server. If a license error occurs or the server switches to restricted mode, AE Services sends you an

email notification using Simple Mail Transfer Protocol (SMTP). You can configure up to three email addresses that you want to use to receive notifications. (**Utilities > Email Notification)**

- **Trace Route** - Use the Trace Route page to run the traceroute command. The traceroute trace command allows you to trace packet routing from the AE Services server to the destination host. You can trace packet routes for network troubleshooting. A traceroute command output can indicate where the longest delays occur along the path. (**Utilities > Diagnostics > Server> Trace Route)**
- **Network Status** - Use the Network Status page to run the netstat command. The netstat command provides the information about network status and server connections running over TCP/IP.

Note:

Advanced Options are available only to Avaya Services technicians and System Administrators. When you select **Advanced Options**, the Network Status page shows a list of netstat command options.

Related links

Testing a TSAPI link on page 45
Testing a CVLAN link on page 45
Testing DMCC configuration on page 46
Testing the TR/87 service on page 46
Enabling email notifications on page 47
Running a Trace Route test on page 48

Testing a TSAPI link

Procedure

1. From the AE Services Management Console main menu, select **Utilities > Diagnostics > AE Service > ASAI Test**.
2. On the **ASAI Test** page, select a link number.
3. Click **Test**.

   The **ASAI Test Result** page indicates whether the test succeeded or failed

Related links

AE Services Management Console connectivity tests on page 44

Testing a CVLAN link

Procedure

1. From the AE Services Management Console main menu, select **Utilities > Diagnostics > AE Service > ASAI Test**.
2. On the **ASAI Test** page, select a link number.
3. Click **Test**.

The **ASAI Test Result** page indicates whether the test succeeded or failed

Related links

AE Services Management Console connectivity tests on page 44

Testing DMCC configuration

About this task

Make first-party and third-party calls to test DMCC configuration for a sample application.

Procedure

1. On the AE Services management console, go to **Utilities > Diagnostics > AE Service > DMCC Test**.
2. On the DMCC Test page, in **User**, type the user ID.
3. In **User Password**, type the user password.
4. Clear the **TLS** check box.
5. In **Switch Name**, select the required switch.
6. **(Optional)** In **Switch IP**, select the IP address of the switch.
7. In **Caller Extension**, type the caller extension.
8. In **Caller Extension Password**, type the password for the caller extension.
9. In **Callee Extension**, type the extension that receives the call.
10. In **Callee Extension Password**, type the password for the extension that receives the call.
11. Do one of the following:
    - To make a first-party call, click **Make First Party Call**.

      AE Services displays the test results on the First Party Call Test Result page.
    - To make a third-party call, click **Make Third Party Call**.

      AE Services displays the test results on the Third Party Call Test Result page.

Related links

AE Services Management Console connectivity tests on page 44

Testing the TR/87 service

About this task

Use the TR/87 service test to verify that you have administered the caller in Active Directory and dial plan for the caller's number. You can also verify if you can monitor the user's phone.

Procedure

1. On the AE Services management console, go to **Utilities** > **AE Service** > **TR/87 Test**.

2. In the TR/87 Service section, in the **From SIPURI** field, type the calling party's phone number in the SIP URI format.

   For example, `sip:username@example.com`

   You must use the SIP URI for a TR/87-controlled phone.
3. In the **From TelURI** field, type the calling party's phone number in the Tel URI format.

   For example, `tel:+13031234488`
4. Click **TR87 service**.

   Your browser displays the TR/87 service test results.

Related links

AE Services Management Console connectivity tests on page 44

Enabling email notifications

About this task

You can enable email notifications from the AE Services server. If a license error occurs or the server switches to restricted mode, AE Services uses Simple Mail Transfer Protocol (SMTP) to send you an email notification.

You can configure up to three email addresses to use to receive notifications.

Before you begin

Obtain the SMTP hostname or IP address from your provider.

Procedure

1. On the AE Services management console, go to **Utilities** > **Email Notification**.
2. On the Email Notification page, select **Enable Email Notification**.
3. In **SMTP Server Name**, type the SMTP server hostname or IP address.
4. In **SMTP Port**, type the SMTP port number.

   The default port is 25.
5. In **From Email Address**, type the hostname of the AE Services server to receive notifications.
6. In the Enable Email Address section, select the check box and type the email address you want to use to receive notifications.

   You can add up to three email addresses.
7. **(Optional)** To send a test notification, click **Test**.

   AE Services sends a test notification to the email address that you specify.
8. To apply the changes, click **Apply**.

Related links

AE Services Management Console connectivity tests on page 44

Running a Trace Route test

About this task

Use this procedure to test packet routing from the AE Services server to the destination host.

Procedure

1. On the AE Services management console, go to **Utilities** > **Diagnostics** > **Server** > **Trace Route**.
2. In the **Destination Host Name/IP Address** field, enter the hostname or IP address of the destination.

   You must use an explicit IPv4 or IPv6 address. Do not use an address in the combined IPv4 and IPv6 format.
3. **(Optional)** To display numerical IP addresses instead of host names, select **Print Addresses Numerically**.
4. **(Optional)** To bypass normal routing tables and send packets directly to a host, select **Bypass routing tables and send directly to host**.
5. **(Optional)** To enter an IP address of the AE Services server to use as a source, select **Use IP address as the source address**.
6. Click **Execute**.

   Your browser displays the Trace Route test results.

Related links

AE Services Management Console connectivity tests on page 44

Chapter 8: Resources

Application Enablement Services documentation

The following table lists the documents related to Application Enablement Services. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Application Enablement Services Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide	Installing TSAPI and CVLAN Client and SDK	Customers and sales, services, and support personnel
Using		
Upgrading Avaya Aura® Application Enablement Services	Upgrading Application Enablement Services applications.	System administrators and IT personnel
Administering Avaya Aura® Application Enablement Services	Administering Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel
Avaya Aura® Application Enablement Services Data Privacy Guidelines	Describes how to administer Application Enablement Services to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation		
Deploying Avaya Aura® Application Enablement Services in Virtualized Environment	Deploy Application Enablement Services applications in Virtualized Environment	Implementation personnel
Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments	Deploy Application Enablement Services applications in Software-Only and Infrastructure as a Service Environments	Implementation personnel
Maintenance and Troubleshooting		

Table continues…

Title	Description	Audience
Maintaining Avaya Aura® Application Enablement Services	Maintaining Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel

Related links

Finding documents on the Avaya Support website on page 50
Accessing the port matrix document on page 50
Avaya Documentation Center navigation on page 51

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Select Release**, select the appropriate release number.

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

Related links

Application Enablement Services documentation on page 49

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list

8. In **Choose Release**, select the required release number.
9. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
10. Press **Enter**.

Related links

Application Enablement Services documentation on page 49

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon ( ).

Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Related links

Application Enablement Services documentation on page 49

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
20980W	What's New with Avaya Aura®

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 53

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.

   The system displays the Avaya Support page.

5. Click **Support by Product** > **Product-specific Support**.
6. In **Enter Product Name**, enter the product, and press `Enter`.
7. Select the product from the list, and select a release.
8. Click the **Technical Solutions** tab to see articles.
9. Select **Related Information**.

Related links

Support on page 53

Index

M

P

R

S

T

V

W