Product Support Notice

PSN #	PSN020296u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 07-Apr-17. This is Issue #06, published date: 26-Sep-17.

Severity/risk level	Medium	Urgency	When convenient

Name of problem

Avaya Aura® Application Enablement (AE) Services 7.0.1 Super Patch is available.

Products affected

Avaya Aura® Application Enablement (AE) Services 7.0.1 (all offer types)

Problem description

Avaya Aura® Application Enablement (AE) Services 7.0.1 Super Patch 5 is available.

NOTE: Application Enablement Services Super Patches are cumulative meaning Super Patch 5 includes all of the content/fixes of previous 7.0.1 Super Patches as well as the new content/fixes specified in the Resolution section of this PSN.

NOTE: This Super Patch is compatible with AE Services release 7.0.1 only. This Super Patch is compatible with all AE Services 7.0.1 offer types. AE Services 7.0.1 is compatible with CM 6.x and higher releases, but higher CM releases might be required for some AE Services 7.x functionality to operate. This Super Patch is fully compatible with AE Services 7.0 clients and SDKs.

NOTE: Patch installation instructions for this Super Patch are different from those of previous Super Patches. Review the Patch install insructions in this PSN for additional detail.

NOTE: Any configuration changes made after applying the Super Patch will not be retained if the Super Patch is removed/uninstalled.

Review the Remarks section of this PSN for details on the content/fixes included in Super Patch 4.
Review PSN004831u for details on the content/fixes included in Super Patch 3.
Review PSN004730u for details on the content/fixes included in Super Patch 2.

Resolution

NOTE: Patch installation instructions for this Super Patch are different from those of previous Super Patches. Review the Patch install insructions in this PSN for additional detail.

AE Services Super Patch 5 includes the following additional (in addition to fixes in previous Super Patches) content/fixes:

AES-15083 - Needed to restart tomcat5 after a database restore to get a license.
AES-15305 – An error occurred when trying to access SMS XML schema links on the SMS test page.
AES-15437 - SMS logging was not working.
AES-15664 – An SNMP port was disabled if SNMP Version 3 was enabled and used “Following IP Addresses”.
AES-15909 - DMCC registrations would sometimes fail.
AES-15931 - Double quote characters are included in Challenge passwords.
AES-15984 – The current snapshot data report could not be saved as a csv file.
AES-16028 - List public unknown-numbering always failed when the number of records was large.
AES-16248 – When Network firewall rules were executed from Network status present under Diagnostics, an error “sudo: no tty present and no askpass program specified” was encountered.
AES-16254 - SMS (OSSICM process on AES) closed the socket connection to CM after reading 0 bytes of data.
AES-16279 - HMDC did not always clean up old data.
AES-16349 – A security fix for the issue identified in PSN020297u is included.
AES-16389 – A missing DMCC station keepalive (KA-RRQ) caused CM to unregister a station.
AES-16401 – The option to create a self-signed certificate was removed.
AES-16414 – The priority of getlogs.sh compression processes was lowered.
AES-16422 - Sessions were not listed in alphabetical order.
AES-16435 - Changes to AE Service IP (Local IP) connectivity settings were undone after a Linux restart.
AES-16530; AES-16250; AES-15729; AES-15730; AES-16258 – Help pages were updated.
AES-16531 – The DBService did not recover automatically after if it went down.
AES-16553 – The /var/log/wtmp file size impacted login response times so file rotation occurred more frequently.
AES-16556 – A utility is now available to update the AES IP address in XSD & WSDL files if the IP address is changes post installation.

Workaround or alternative remediation

n/a

Remarks

AE Services Super Patch 4 includes the following content/fixes (included for historical purposes):

AES-15096 – AE Services failed to start successfully during recovery from split brain in GRHA configurations.
AES-15341 – The DMCC client application redirect media (RedirectMedia) request was failing to properly redirect media.
AES-15348 - Per design AE Services should allocate 50% of system memory to the DMCC JVM process. However, AE Services was allocating only 512 MB (1/2 of what should have been allocated) to the DMCC JVM process when the server had 2 GB of memory.
AES-15506 - An incorrect connection state was returned for the PSTN called party in a Snapshot Call response when a Snapshot Call request was sent by the application between the Originated event report and Alerting event report.
AES-15626 – A memory leak occurred if DMCC client applications made RouteSelect or RouteEnd requests. With this fix no memory leak occurs when RouteSelect and RouteEnd requests are made.
AES-15660 - In a certain call scenario AE Services was not providing the deviceID in the Established event report over the device monitor association to the application.
AES-15804 – The Telephony Web Service stopped working with an "OutOfMemory" error in the catalina.log file after a certain amount of time because Tomcat could not create new thread.
AES-15819 – When an internal AE Services process threw a Java exception that was logged via syslog, the internal process responsible for processing the exception log message died/terminated.
AES-16011 – During the AE Services server restore phase an emergency backup is created to recover from a failed restore. The emergency backup/restore omitted some data that prevented the emergency restore from operating as expected.
AES-16012 – When recovering from split brain in GRHA configurations if forced synchronization/refresh took more than one minute to successfully complete, the system could enter a state of perpetual synchronization attempts (a synchronization/refresh loop).
AES-16020 – The Tomcat service failed to start successfully during recovery from split brain in GRHA configurations.
AES-16025 – If multiple encryption modes were specified (e.g., "aes" and "none") during registration, redirect media requests (RedirectMedia) failed to redirect media.
AES-16130 – Make the AE Services integration with CA-PAM more secure.
AES-16135 – Make the log utility more secure.

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Backup AE Services server data before applying the Super Patch:

1. Log into the AE Services Management Console using a browser.
2. From the main menu, select **Maintenance > Server Data > Backup**.
   AE Services backs up the database, and displays the **Database Backup** screen, which displays the following message
   `The backup file can be downloaded from` **`Here`**
3. Click the **Here** link.
   A file download dialog box is displayed that allows the backup file to be either opened or saved (named as: *serverName_SoftwareVersion*_aesvcsdb*ddmmyyyy*.tar.gz. Where ddmmyyyy is the date stamp).
4. Click **Save**, and download the backup file to a safe location that the upgrade will not overwrite For example, save the file to your local computer or another computer used for storing data backups.

Download

Instructions to download the AE Services Super Patch binary file:

Download from Avaya Support:

1. Go to Avaya Support (http://support.avaya.com).
2. Hover over **Support by Product >** and select **Downloads**
3. In **Enter Product Name** enter "*Avaya Aura Application Enablement Services"* and select *"7.0.x"* from the **Choose Release** drop-down menu.
4. Select **Avaya Aura AE Services 7.0.1 Super Patches, 7.0.x**.
5. Select **7-0-1-0-SuperPatch_5.bin, 7.0.x**.
6. Select **Download**.

Download from PLDS:

7. Go to PLDS (https://plds.avaya.com).
8. Select **View Downloads**.
9. In the **Search by Download** tab enter **AES00000602** in the **Download pub ID** search box.
10. Select **Download**.

The MD5 checksum is included with the PLDS download description.

Patch install instructions — Service-interrupting?

Notes: Yes

1. Installation of this Super Patch will cause AE Services to be out of service for 20 to 30 minutes.
2. This Super Patch is only compatible with AE Services release 7.0.1.
3. To patch GRHA configurations patch the active server and the installer will automatically patch the standby server.

These patch install instructions apply to the VMware or Software Only offers:

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely using SSH for example)
2. Secure copy **7-0-1-0-SuperPatch_5.bin** to the **/tmp** directory on the AE Services server.
3. As the root user, execute the following from the command line:
   cd /tmp
   chmod 750 7-0-1-0-SuperPatch_5.bin
   ./7-0-1-0-SuperPatch_5.bin
4. Follow any on-screen instructions that are presented until the patch install completes.

Verification

Perform the following steps to verify the Super Patch installation:

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely using SSH for example).
2. Log in
3. Run the following command to verify the installation of the Super Patch:
   swversion

   The swversion command displays a message similar to the following:

   ********** Patch Numbers Installed in this system are **********
   ====
   7.0.1.0.5
   ====

4. Log into the AE Services Management Console using a web browser.
5. From the main menu, click **Status**.
6. On the Status page, verify that all previously licensed services are running.
7. Validate the server configuration data, as follows:
   - On the main menu click **Networking**
   - Under **AE Service IP (Local IP)**, verify that the settings are correct.
   - Under **Network Configure**, verify that the displayed settings are correct.
   - Under **Ports**, verify that the settings are correct.
8. Check all of the remaining Management Console pages listed under **AE Services** and **Communication Manager Interface**. Verify that the information is complete and correct.

Note: Follow these procedures to restore AE Services server data **only if the AE Services server configuration data has changed**.

1. From the main menu of the AE Services Management Console, select **Maintenance > Server Data > Restore**.
   The Management Console displays the Restore Database Configuration screen. The initial state of the Restore Database page provides you with two basic functions:

- Text box with the **Browse** button, which provides the means to select a backup file to use for the Restore process. Alternatively, you can type a fully qualified name (FQDN) of the backup file in the text box.
- **Restore** button that starts the Restore process.

2. Click **Browse** and locate the AE Services database backup file that you intend to use (For example: serverName_7-0-1-15-0_aesvcsdb01012016.tar.gz).
3. Click **Restore**.
   The Management Console redisplays the **Restore Database Configuration** page with the following message.
   "A database restore is pending. You must restart the Database Service and the AE Server for the restore to take effect. To restart these services now, click the Restart Services button below."
4. Click **Restart Services**.
   AE Services restarts the Database Service and the AE Services thereby completing the Restore process.

Failure

Contact Technical Support.

Patch uninstall instructions

NOTE: Any configuration changes made after applying the Super Patch will not be retained if the Super Patch is removed/uninstalled.

Perform the following steps to uninstall the Super Patch:

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely using SSH for example).
2. As the root user, execute the following from the command line:
   update –e 7.0.1.0.5
3. Follow the on-screen instructions.

Follow these procedures to restore AE Services server data **only if the AE Services server configuration data has changed**.

1. From the main menu of the AE Services Management Console, select **Maintenance > Server Data > Restore**.
   The Management Console displays the Restore Database Configuration screen. The initial state of the Restore Database page provides you with two basic functions:
   - Text box with the **Browse** button, which provides the means to select a backup file to use for the Restore process. Alternatively, you can type a fully qualified name (FQDN) of the backup file in the text box.
   - **Restore** button that starts the Restore process.
2. Click **Browse** and locate the AE Services database backup file that you intend to use (For example: serverName_7-0-1-15-0_aesvcsdb01012016.tar.gz).
3. Click **Restore**.
   The Management Console redisplays the **Restore Database Configuration** page with the following message.
   "A database restore is pending. You must restart the Database Service and the AE Server for the restore to take effect. To restart these services now, click the Restart Services button below."
4. Reboot the AE Services server by executing the **shutdown –r now** command.

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.