Product Support Notice

PSN #	PSN004418u				
Original publication date: 15-Jun-15. This is Issue #01, published date: 15-Jun-15.		Severity/risk level	Medium	Urgency	When convenient
Name of problem	Avaya Aura® Application Enablement (AE) Services 6.3.3 Super Patch 4 Release Notes				
Products affected					
Avaya Aura® Application Enablement (AE) Services Release 6.3.3 (all offer types)					
Problem description					

What is fixed in this Patch?

Note:
For all users that do not already have the AE Services 6.3.3 Linux Security Update Patch 2 installed, this Super Patch should be installed after the Linux Security Update Patch 2, or its security updates, specified under PSN004416 is installed.

This patch contains the following updates to the DMCC Service:

Issue AES-14134:
Following a DMCC restart or HA fail-over of the AE Services server, the DMCC stations would sometimes be unregistered within a few minutes. The issue was tracked down to a disagreement between Communication Manager and AE Services of the expected Q931 sequence number. This patch provides a fix to reset the Q931 sequence number when the Q931 channel is re-established in TTS mode.

Issue AES-13842:
Under a heavy call load, a Communication Manager (CM) server interchange was performed. After the interchange, it was found that some of the DMCC stations were in the busy state, when CM considered them to be idle. This patch attempts to ensure that AE Services and CM agree on the final state of the DMCC stations, after the interchange.

Issue AES-14171:
In the event of a DMCC restart or HA fail-over of the AE Services server, any privileged session (i.e. a session established by a trusted application) would fail to reconnect to DMCC. This patch fixes the issue, allowing the privileged session to be re-established after the fail-over.

Issue AES-14343:
A "reset system 4" command on Communication Manager (CM) causes it to unregister all of its phones. However, the phone extensions registered to the CM via AE Services do not unregister correctly, and the AE Service clients are not informed of the unregistration. This patch enables the TCP heartbeat between CM and the AE Services server to allow the AE Services to unregister its extensions correctly, and to inform its client applications.

Issue AES-13985:
This fixes a problem where a Failed event was not sent to the DMCC client in some call scenarios. An example is when a DMCC application has a call control monitor on extension A. When extension A calls extension B, which is on a remote Communication Manager, and the call fails because B is busy, a Failed event was not sent to the DMCC application. A Failed event is now sent to the DMCC application.

Issue AES-14329:
The UCID is not properly formatted if the UCID sequence number is greater than 32768 in the GetCallInformationResponse of the DMCC CallInformation service. This patch fixes this issue.

This patch contains the following updates to the TSAPI Service:

Issue AES-13996:
An application that is registered as a routing server would not receive a RouteEnd event when the call ended before the application responded to the RouteRequest. This patch fixes this issue.

Issue AES-13993:

The CallCleared event did not contain the reason the call failed in some cases. An example is when a DMCC or TSAPI application sends a MakePredictiveCall request and the call fails because an answering machine was detected. The CallCleared event did not contain the reason the call failed. This has been fixed by this patch and the reason the call failed (e.g. answering machine detected) is in the private data of the CallCleared event.

This patch contains the following updates to the CVLAN Service:

Issue AES-13941:

Based on rare timing, it was possible for the CVLAN server to incorrectly decide that a CVLAN client connection was bad, and it would terminate that client connection. An error would be placed in the AE Services error logs indicating that "Recv() failed with errno -13". This patch fixes this issue.

This patch contains the following updates to the AE Services Management Console:

Issue AES-14289:

After installation of the AE Services 6.3.3 Super Patch 1, clicking on the "Apply Changes" button of the AE Services Management Console "Security | Standard Reserved Ports" web page disables ICMP PING functionality causing the AE Services server not to respond to standard server "ping". This patch corrects this issue, and allows the AE Services server to correctly respond to "pings".

Issue AES-14328:

When the timezone on the AE Services server is set to Western Europe (i.e. CEST or any other timezone with more than three letters in the abbreviated timezone), some of the time related information was not shown on the TSAPI clients page of the AE Services Management Console. This patch fixes this issue.

This patch contains the following updates to the AE Services Server:

Issue AES-14230:

When the AE Services was operating in License ERROR mode (without a license), any application request, which required the use of a license could be delayed by 15 - 20 seconds. This patch eliminates the delay.

Issue AES-13846 and AES-14309:

This patch removes unused and weak ciphers.

Issue AES-14170:

Currently the AE Services server backup script backs up the local LDAP configuration as raw files. In AE Services 7.0, the LDAP backend database has changed and therefore we cannot restore the raw LDAP configuration files. This change uses the slapcat utility to export the LDAP configuration to LDIF formatted text, which can then be restored on the AE Services 7.0 server.

Issue AES-14250:

When restoring the AE Services backup data, AE Services removes the WebLM server location from the database. This patch fixes this issue.

Issue AES-13939:

If GRHA is enabled, upgrading the active server to a newer Super Patch or Feature Pack, does not upgrade the standby server. This patch fixes this issue.

Issue AES-13983:

AE Services keeps certain run-time data in memory mapped files. To remove possible interactions with disk I/O, these mapped files are now implemented in shared memory instead of backed by disk.

Issue AES-14224:

On some VMware offer installs, the environment ISO remained attached to the DVD device of the deployed AE Services VM. In some situations, high CPU or disk I/O usage has been experienced. Since the eject command was not included in the VM, a user was unable to eject the environment ISO from the CLI. This patch adds support for the eject command.

Resolution

Install Super Patch 4 for AE Services 6.3.3

Workaround or alternative remediation

n/a

Remarks

1. What AE Services rpm/s is updated by AE Services 6.3.3 Super Patch 4?

aesvcs-install-scripts-hooks-6.3.3.0.107-4.noarch.rpm
aesvcs-linux-config-6.3.3.0.107-4.noarch.rpm
aesvcs-tomcat-config-6.3.3.0.107-4.noarch.rpm
aesvcs-platform-6.3.3.0.107-4.noarch.rpm
aesvcs-sms-6.3.3.0.107-1.noarch.rpm
aesvcs-callcontrol-6.3.3-115.i386.rpm
aesvcs-snmp-6.3.3.0.107-4.noarch.rpm
aesvcs-watchdog-config-6.3.3.0.107-4.noarch.rpm
sohd-0.0.3-24.aes.i386.rpm
eject-2.1.5-4.2.el5.i386.rpm

2. Are there new features or enhancements included in AE Services 6.3.3 Super Patch 4?

Yes.

3. What must application suppliers do to be compatible with AE Services 6.3.3 Super Patch 4? (recompile, re-link, etc.)

This Super Patch is fully compatible with AE Services 6.3.3 Clients and SDKs.

4. Is applying AE Services 6.3.3 Super Patch 4 service affecting?

The AE Services server will be out of service for 20 to 30 minutes while the patch is being applied.

5. With which Application Enablement Services release(s) is AE Services 6.3.3 Super Patch 4 compatible?

This patch is compatible with all AE Services 6.3.3 offer types.

6. Is the AE Services 6.3.3 Super Patch 4 cumulative?

Yes, this patch includes the fixes provided by the previous AE Services 6.3.3 patches.

7. Is the AE Services 6.3.3 Super Patch 4 compatible with Application Enablement Services 6.3.1 and earlier servers?

No. The AE Services 6.3.3 Super Patch is only supported with AE Services 6.3.3.

8. Is the AE Services 6.3.3 Super Patch 4 available for all Offer Types?

Yes. Please use the appropriate procedure for the upgrade, i.e. via the Patch Management menu in the web console of the System Platform for Virtual Appliance offer and directly on the AE Services server for Bundled, VMware or Software Only.

9. What are the CM requirements for the Application Enablement Services 6.3.3 Super Patch 4?

AE Services 6.3.3 supports CM 6.x and later.

Note:

Certain functionality on AE Services 6.3.3 requires CM versions later than CM 6.x

Patch Notes

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

Backup before applying the patch

Please take a backup of the AE Services server data before applying the AE Services 6.3.3 Super Patch 4.

Follow these steps to back up the AE Services server data:

1. Login to 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, that 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 you to either open or save the backup file (named as: *serverName*_r*SoftwareVersion*_mvapdb*ddmmyyyy*.tar.gz, where ddmmyyyy is a date stamp).
4. Click **Save**, and download the backup file to a safe location that the upgrade will not affect.
   For example, save the file to your local computer or another computer used for storing backups.

Download

To download the AE Services patch, go to:

A. Avaya Support (http://support.avaya.com/downloads). On the "Downloads" screen, in the textbox labeled "Enter Product Name", enter "Avaya Aura Application Enablement Services" and the release option "6.3.x". If the option "Select a content type" is displayed select the "Download" radio button and click the button labeled "Enter". If the Documents table is displayed, select the link, "View downloads", on the right-hand side of the screen above the Documents table. In the Downloads table locate and select the entry, **Avaya Aura® Application Enablement Services 6.3.3 Super Patch 4** (new entries are inserted at the top of the list).

B. PLDS (https://plds.avaya.com). Select View Downloads. Use the search engine to locate the available downloads for Application Enablement Services using version 6.3 to narrow the search. Locate the entry, **Avaya Aura® Application Enablement Services 6.3.3 Super Patch 4** (new entries are inserted at the end of the list). Alternatively, you can search for the Download ID, which is **AES00000497**.

Note:
All AE Services Software Downloads are now in PLDS, while the Release Notes documents are provided on the Support Site. There will be cross references between the corresponding download entries for patches.

File Name	633_SuperPatch_4.zip
File Size	134.53 MB (141,066,682 Bytes)
MD5 Sum	64f848324d46434f9b9ca21ecac4fa60

Before you start with the installation of the Patch, check the md5 checksum of the file.
Run the following from the command line:
md5sum 633_SuperPatch_4.zip

Note:
If the MD5 checksum does not match what is stated above, do not proceed with the installation of the patch. Download the patch again and check the MD5 checksum again.

Patch install instructions — Service-interrupting?

How to check the detailed AE Services version — Yes

A. For the AE Services on System Platform offer, use the System Platform Management Console (and hence see whether the patch has been applied already):

1. Login to the System Platform Management Console using a browser.
2. Go to **Virtual Machine Management | Manage** (that is the page which should come up after connecting to the web console)

3. Verify that your AE Services VM has AE Services 6.3.3 running (the GA version shows 6.3.3.0.10)
4. Click on that version information to get the detailed version information in a popup window.
5. If the patch is not listed, continue to the next section, "**How to install the Super Patch to the AE Services server**".

   Note:
   When multiple patches for the AE Services server is installed, the System Platform Management Console may show each of the installed patches as "Active" instead of only showing the latest installed patch as "Active" and the previous installed patches as "Installed". While other VM's may use a patch status consisting of "Active", "Installed" and "Uninstalled", AE Services currently only use the patch status "Active" and "Uninstalled".

B. For the Bundled, VMware and Software Only offer, use the AE Services Linux console (and hence see whether the patch has been applied already):

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely using e.g. putty or SSH)
2. As the root user, execute the following command: **swversion**
3. If the patch is not listed, continue to the next section, "**How to install the Super Patch to the AE Services server**".

How to install the Super Patch to the AE Services server.

A. Patch Installation Instructions for the AE Services on System Platform offer

1. On the System Platform (SP) Management Console, click on **Server Management | Patch Management | Download/Upload**
2. Choose the source of the patch (PLDS, HTTP, SP, devices on SP, or local to your PC).
3. After it has been uploaded to SP, click on **Manage** (from the **Patch Management** menu). Now you will see the available patch waiting for installation below the caption **AES**.
4. Once you're ready, click on the **PatchID** link, finally on the **Install** button.
5. Follow the on-screen instructions.

B. Patch Installation Instructions for the Bundled, VMware or Software Only offer:

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely using e.g. putty or SSH)
2. Secure copy **633_SuperPatch_4.zip** to the **/tmp** directory on the AE Services server.
3. As the root user, execute the following from the command line:
   cd /tmp
   update -u --force 633_SuperPatch_4.zip
4. Follow the on-screen instructions.

After applying the Super Patch, reboot the AE Services server.

A. For the AE Services on System Platform offer

1. On the System Platform Management Console, click on **Virtual Machine Management | Manage**.
2. On the Manage Virtual Machines page, click on **Application Enablement Services**
3. On the Application Enablement Services page, click on **Reboot**

B. For the Bundled, VMware or Software Only offer

As the root user execute the following command from the command line:

shutdown –r now

Post Patch Installation Verification:

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely, using e.g. putty)
2. Login as **sroot** or **root**
3. Run the following command to verify the installation of Super Patch 4:
   swversion

   The swversion command should return something similar to the following if Super Patch 4 is installed:
   ********** Patch Numbers Installed in this system are **********
   ====
   4
   ====

   In case you used **swversion -a,** the RPMs will be listed as well below the patch number – this is the 6.3.3 output:
   ********** Patch Numbers Installed in this system are **********
   ====
   4
   aesvcs-install-scripts-hooks-6.3.3.0.107-4.noarch.rpm
   aesvcs-linux-config-6.3.3.0.107-4.noarch.rpm
   aesvcs-tomcat-config-6.3.3.0.107-4.noarch.rpm
   aesvcs-platform-6.3.3.0.107-4.noarch.rpm
   aesvcs-sms-6.3.3.0.107-1.noarch.rpm
   aesvcs-callcontrol-6.3.3-115.i386.rpm
   aesvcs-snmp-6.3.3.0.107-4.noarch.rpm
   aesvcs-watchdog-config-6.3.3.0.107-4.noarch.rpm
   sohd-0.0.3-24.aes.i386.rpm
   eject-2.1.5-4.2.el5.i386.rpm
   ====

   Note:
   Instead of the steps 1 - 3 as listed above, you can use the same procedure as described at the beginning of this section for AE Services on System Platform (which does not require a console login).

4. Login to the AE Services Management Console using a 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:
   - From the main menu, click **Networking**.
   - Under **AE Service IP (Local IP)**, verify that the settings are correct.
   - Under **Network Configure**, verify that the 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.

This completes the installation of the Super Patch.

Follow this procedure only if the AE Services server configuration data has changed.

Follow this procedure to restore the AE Services server data:

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 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_r6-3-3-0-10-0_mvapdb01012015.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.

Verification

See the **Post Patch Installation Verification** section above.

Failure

n/a

Patch uninstall instructions

Follow the **Patch Uninstall Instructions**:

A. Patch Uninstall Instructions for the AE Services on System Platform offer:

1. On the System Platform Management Console, click on **Server Management | Patch Management | Manage**. Now you will see the installed patch as active.

   Note:
   When multiple patches for the AE Services server is installed, the System Platform Management Console may show each of the installed patches as "Active" instead of only showing the latest installed patch as "Active" and the previous installed patches as "Installed". While other VM's may use a patch status consisting of "Active", "Installed" and "Uninstalled", AE Services currently only use the patch status "Active" and "Uninstalled".

2. Click on the **PatchID** link, finally on the **Remove** button.
3. To also remove the patch file itself, click on the **Remove Patch File** button (optional).

B. Patch Uninstall Instructions for the Bundled, VMware or Software Only offer:

1. Start a Linux console session on the AE Services server (locally, via service port, or remotely using e.g. putty or SSH).
2. As the root user, execute the following from the command line:
   update -e 4
3. Follow the on-screen instructions.

Follow this procedure to restore the AE Services server data using the backup data saved during the patch install process:

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 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_r6-3-3-0-10-0_mvapdb01012015.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."

After removing Super Patch 4 and scheduling the restore, reboot the AE Services server.

A. For AE Services on System Platform

1. On the System Platform Management Console, click on **Virtual Machine Management | Manage**.
2. On the Manage Virtual Machines page, click on **Application Enablement Services**
3. On the Application Enablement Services page, click on **Reboot**

B. For the Bundled, VMware or Software Only offer

As the root user, execute the following command from the command line:

shutdown –r now

Do I have to perform any additional steps if I am uninstalling the Super Patch?

No.

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.