AVAYA

Avaya Aura® Application Enablement Services R6.3.3 Server and Client Release Notes

Issue 1.13
August 2018

INTRODUCTION

This document introduces the Generally Available release of the Application Enablement (AE) Services Release 6.3.3 and describes important notes and known issues.

WHAT'S NEW IN AE SERVICES 6.3.3?

- AE Services vApplication support for VMWare (version 5.0, 5.1 and 5.5)
- CTI events to support 21 digits
- CTI events for undelivered calls
- Security enhancements to support FIPS and JITC
- CallVisor Local Area Network (CVLAN) and Telephony Services Application Programming Interface (TSAPI) are now supported on MS Windows 2012
- Virtual IP for Geo Redundant High Availability

For additional information, please reference the Avaya Aura® Application Enablement Services Overview at https://downloads.avaya.com/css/P8/documents/100171739

SOFTWARE RELEASE VERSIONS

Application Enablement Services Application	File Name
Avaya Aura® Application Enablement Services 6.3.3 Software Only 32-bit and 64-bit in 32-bit compatibility mode - 700508344	swonly-6.3.3.0.10-20140513.iso
Avaya Aura® Application Enablement Services 6.3.3 Hardware Bundled Upgrade for S8510 - 700508342	bundled-6.3.3.0.10-20140513.iso
Avaya Aura® Application Enablement Services 6.3.3 on System Platform – 700508346	aes-6.3.3.0.10.iso
System Platform R6.3.4 - 700508413	vsp-patch-6.3.4.08011.0.noarch.rpm
System Platform R6.3.5 - 700509883	vsp-patch-6.3.5.01003.0.noarch.rpm
System Platform R6.3.6 - 700509882	vsp-patch-6.3.6.01005.0.noarch.rpm
System Platform R6.3.7 - 700509921	vsp-6.3.7.0.05001.iso
System Platform R6.3.8 - 700511786	vsp-patch-6.3.8.01002.0.noarch.rpm
System Platform R6.3.8 - 700513382	vsp-patch-6.3.8.02001.0.noarch.rpm
System Platform R6.3.8	vsp-patch-6.3.8.03001.0.noarch.rpm
System Platform R6.4 - 700512428	vsp-patch-6.4.0.0.17006.iso
System Platform R6.4.1 - 700513383	vsp-patch-6.4.1.0.01008.noarch.rpm
System Platform R6.4.2 – 700514043	vsp-patch-6.4.2.0.01003.noarch.rpm
System Platform R6.4.3	vsp-patch-6.4.3.0.01002.noarch.rpm
Avaya Aura® AE Services 6.3.3 Virtualization Enablement (VE) vAppliance	AES-6.3.3.0.10.20140513-e50-00.ova
Avaya Aura® Application Enablement Services 6.3.3 RPM-Only Installer	aesvcs-6.3.3.0.10-featurepack.zip
Avaya Aura® Application Enablement Services 6.3.3 CallVisor Local Area Network (CVLAN) Client Linux 32-bit and 64-bit in 32-bit compatibility mode	cvlan-client-linux-6.3.3-103.bin
Avaya Aura® Application Enablement Services 6.3.3 CVLAN Client MS Windows 32-bit and 64-bit in 32-bit compatibility mode	cvlan-client-win32-6.3.3-103.zip
Avaya Aura® Application Enablement Services 6.3.3 Telephony Services Application Programming Interface (TSAPI) Client Linux 32-bit and 64-bit in 32-bit compatibility mode	tsapi-client-linux-6.3.3-103.bin
Avaya Aura® Application Enablement Services 6.3.3 TSAPI Client MS Windows 32-bit and 64-bit in 32-bit compatibility mode	tsapi-client-win32-6.3.3-103.zip
Avaya Aura® Application Enablement Services 6.3.3 TSAPI SDK Linux 32-bit and 64-bit in 32-bit compatibility mode	tsapi-sdk-linux-6.3.3-103.bin
Avaya Aura® Application Enablement Services 6.3.3 TSAPI SDK MS Windows 32-bit and 64-bit in 32-bit compatibility mode	tsapi-sdk-win32-6.3.3-103.zip

Application Enablement Services Application	File Name
Avaya Aura® Application Enablement Services 6.3.3 Java Telephony Application Programming Interface (JTAPI) SDK Linux	jtapi-sdk-6.3.3.26.bin
Avaya Aura® Application Enablement Services 6.3.3 Java Telephony Application Programming Interface (JTAPI) SDK MS Windows	jtapi-sdk-6.3.3.26.exe
Avaya Aura® Application Enablement Services 6.3.1 Web Service - System Management SDK Linux	smssvc-sdk-6.3.3.0.107.bin
Avaya Aura® Application Enablement Services 6.3.1 Web Service - System Management SDK MS Windows	smssvc-sdk-6.3.3.0.107.exe
Avaya Aura® Application Enablement Services 6.3.3 Device Media Call Control (DMCC) .Net SDK 32-bit and 64-bit in 32-bit compatibility mode	dmcc-dotnet-sdk-6.3.3.0.14.exe
Avaya Aura® Application Enablement Services 6.3.3 Web Services - Telephony SDK Linux 32-bit and 64-bit in 32-bit compatibility mode	telsvc-sdk-6.3.3.0.107.bin
Avaya Aura® Application Enablement Services 6.3.3 Web Services - Telephony SDK MS Windows 32-bit and 64-bit in 32-bit compatibility mode	telsvc-sdk-6.3.3.0.107.exe
Avaya Aura® Application Enablement Services 6.3.3 DMCC XML SDK Linux 32-bit and 64-bit in 32-bit compatibility mode	cmapixml-sdk-6.3.3.0.107.bin
Avaya Aura® Application Enablement Services 6.3.3 DMCC XML SDK MS Windows 32-bit and 64-bit in 32-bit compatibility mode	cmapixml-sdk-6.3.3.0.107.exe
Avaya Aura® Application Enablement Services 6.3.3 DMCC Java SDK Linux 32-bit and 64-bit in 32-bit compatibility mode	cmapijava-sdk-6.3.3.0.107.bin
Avaya Aura® Application Enablement Services 6.3.3 DMCC Java SDK MS Windows 32-bit and 64-bit in 32-bit compatibility mode	cmapijava-sdk-6.3.3.0.107.exe
Avaya Aura® Application Enablement Services Product Management Information Bases (MIBs)	aesvcs-product-mibs-6.3.3.0.107.zip
Standard MIBs	standard-mibs-6.3.3.0.107.zip

IMPORTANT NOTES

- Reference PSN020346u for AE Services Spectre and Meltdown vulnerabilities.

- AE Services 6.3.3 supports Red Hat Enterprise Linux 5.0 Update 10 for 32-bit x86

- AE Services 6.3.3 is compatible with the following Bundled Server: Dell 1950 (S8510)

- AE Services 6.3.3 on System Platform is compatible with the following servers:
  - IBM x3550 M2 (S8800)
  - Dell R610 (4GB RAM, H200 RAID Controller, 2x146 GB HDDs)
  - Dell R610 (6GB RAM, H700 RAID Controller, 2x300 GB HDDs)
  - HP DL360G7 (12GB RAM, P410i RAID Controller, 2x300GB HDDs)
  - HP DL360G8 (16GB RAM, P420i RAID Controller, 2X300 GB HDDS)
  - The Dell Power Edge R620 server is expected to include the following components:
    - one 2.30GHz 6-core Intel E5-2630 processor
    - 16GB (4x4GB) system memory
    - two 2.5" 300GB 10K RPM SAS hard drives (with RAID-1 controller, 256MB cache)
    - four 10/100/1000Base-T Ethernet interfaces
    - one DVD±R/W SATA optical drive
    - one 495W standard power supply
    - 10,000Base-T Ethernet interface (option for VSST support)

- AE Services 6.3.3 on System Platform is compatible with the following versions of System Platform:
  - System Platform R6.3.4.08011.0
  - System Platform R6.3.5.01003.0
  - System Platform R6.3.6.01005.0
  - System Platform R6.3.7.0.05001
  - System Platform R6.3.8.01002.0
  - System Platform R6.3.8.02001.0
  - System Platform R6.3.8.03001.0
  - System Platform R6.4.0.0.17006 (Machine Preserving High Availability not supported)
  - System Platform R6.4.1.0.01008 (Machine Preserving High Availability not supported)
  - System Platform R6.4.2.0.01003 (Machine Preserving High Availability not supported)
  - System Platform R6.4.3.0.01002 (Machine Preserving High Availability not supported)

- AE Services 6.3.3 is compatible with the following release(s) of WebLM:
  - WebLM 6.3.4

- AE Services 6.3.3 is compatible with the following Communication Manager Releases:
  - Communication Manager 5.2.1
  - Communication Manager 6.0.x
  - Communication Manager 6.2
  - Communication Manager 6.3
  - Communication Manager 6.3.2
  - Communication Manager 6.3.6 and newer (i.e. CM 6.3.X service packs)

Avaya SIP Endpoints Supported by AE Services							
Endpoint	Administered as	Endpoint Firmware	AE Services Release	CM/ASM Pair		General Telephony	Agent Features
				CM- ES Version	ASM Version		
9620	9620SIP	2.6 SP12	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	No
9640	9640SIP	2.6 SP12	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	No
9640G	9640SIP	2.6 SP12	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	No
9630G	9630SIP	2.6 SP12	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	No
9650	9600SIP	2.6 SP12	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	No
9608	9608SIPCC	6.4	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	Yes
9611	9611SIPCC	6.4	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	Yes
9621	9621SIPCC	6.4	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	Yes
9641	9641SIPCC	6.4	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	Yes
Avaya Flare	9641SIP	Flare for Windows Ver 2.0.0.15	6.3.3	6.3.6 (6.3 FP4)	6.3.8 (6.2 FP4)	yes	No

Note 1 - Agent Buttons Supported:

Agent Login/Logout

After Call Work (ACW)

Auxiliary (AUX) Work

Auto-In/Manual-in

Release

Agent Event Package (16CC)

Release History:

Date	Server Build	Change(s)
03/2007	47-3	Release 4.0
06/2007	50-1	Release 4.0.1
12/2007	31-2	Release 4.1
04/2008	4.1.16	Release 4.1.1 JTAPI Client/SDK
05/2008	19-4	Release 4.2
08/2008	20-5	Service Pack R4.2.1
06/2009	31	Service Pack R4.2.2
09/2009	33	Service Pack R4.2.3
11/2009	98	Release 5.2
02/2010	103	Service Pack R5.2.1
06/2010	105	Service Pack R5.2.2
08/2010	35	Service Pack R4.2.4
02/2011	20	Release 6.1
03/2011	110	Service Pack R5.2.3
06/2011	30	Service Pack R6.1.1
10/2011	111	Avaya Aura® Application Enablement Services 5.2.3 Hardware Bundled Upgrade for S8510
10/2011	31	Avaya Aura® Application Enablement Services 6.1.1 Hardware Bundled Upgrade for S8510
03/2012	32	Service Pack R6.1.2
07/2012	18	Release 6.2
10/2012	114	Avaya Aura® Application Enablement Services 5.2.4 Hardware Bundled Upgrade for S8510
11/2012	18	Avaya Aura® AE Services 6.2 Virtualization Enablement (VE) vAppliance
05/2013	212	Release 6.3
10/2013	19	Release 6.3.1
6/2014	9	Release 6.3.3

AE SERVICES 6.3.3 INSTALLATION NOTES

AE Services 6.3.3 installation order:

1. AE Services 6.3.3 GA offer
2. AE Services 5.2.4 and 6.X Bash Shellshock Remediation (PSN004303u)
3. AE Services 6.3.3 Linux Security Update Patch 3 (PSN004620)
4. AE Services 6.3.3 Super Patch 5 (PSN004621u)

If installing from AE Services 6.3.0 or 6.3.1 to 6.3.3 via the Feature Pack install, then install with the following order:

1. AE Services 6.3.3 Linux Security Update for the Feature Pack ZIP Installation
   This is the RHEL5U8 to RHEL5U10 updated needed for AE Services 6.3.3
2. Avaya Aura Application Enablement Services 6.3.3 RPM Based Installation
3. AE Services 5.2.4 and 6.X Bash Shellshock Remediation (PSN004303u)
4. AE Services 6.3.3 Linux Security Update Patch 3 (PSN004620)
5. AE Services 6.3.3 Super Patch 5 (PSN004621u)

KNOWN ISSUES AND WORKAROUNDS

- **AE Services on System Platform template upgrade where the AE Services Server uses a dual network interface card (NIC) configuration**

  If the AE Services template is configured for a dual NIC, please execute the following steps in order to upgrade the AE Services on System Platform Offer template:

  1. Record the AE Services template existing eth0 IP address, eth1 IP addresses, hostname, and netmask. This information can be obtained using the System Platform Management Console screen, “Server Management | Network Configuration”, in the section titled “Templates – AES”.
  2. Backup the AE Services server data using the AE Services Management Console screen, “Maintenance | Server Data | Backup”.
  3. Delete the current AE Services on System Platform Offer template using the System Platform Management Console screen, “Virtual Machine Management | Templates”.
  4. Install the new AE Services on System Platform Offer template using the System Platform Management Console screen, “Virtual Machine Management | Templates”. During the install process, configure the network data using the information obtained in step 1.
  5. Once the install successfully completes, restore the AE Services server data obtained in step 2 using the AE Services Management Console screen, “Maintenance | Server Data | Restore”.

- **AE Services Session interaction with interchanges on duplicated Communication Manager media servers using the software duplication option**

  Depending on the conditions under which a duplicated Communication Manager server pair utilizing software duplication interchange, AE Services sessions to that Communication Manager may be reset. All Java Telephony Application Programming Interface (JTAPI), Telephony Services Application Programming Interface (TSAPI), CallVisor Local Area Network (CVLAN), and DEFINITY LAN Gateway (DLG) associations with that Communication Manager will be lost and will have to be recovered. The probability of a session being reset is directly proportional to the message rate between an AE Services server and Communication Manager when the interchange occurs, and is equally as likely with a spontaneous interchange (caused by a hard failure) as with a requested interchange (caused by, for instance, a craft request). This issue affects **all** AE Services releases.

  Typically, the Link Resiliency feature introduced in AE Services 3.1 would allow AE Services sessions to survive such interchanges, and, with hardware duplication on Communication Manager, they still do. Starting with Communication Manager release 6.2, AE Services sessions will again survive controlled interchanges with software duplicated Communication Manager media servers (requires no change to

AE Services release), but still will not survive uncontrolled interchanges. Controlled interchanges are those in which the duplicated Communication Manager media servers are communicating with each other throughout the interchange, and covers the majority of interchanges that take place. Uncontrolled interchanges occur when the physical linkage between the Communication Manager media servers is severed during the interchange process (typically caused by physical hardware failure on one of the media servers), and, as such, are not as prevalent as controlled interchanges.

- **CVLAN Linux Client**
  - Before installing the CVLAN Linux client on a Red Hat Linux ES v5.0 system, a separate installation of the following RPM may be required:

    openssl097a-0.9.7a-9.el5_4.2.i386.rpm.

    This RPM may be available with the Red Hat Linux installation media and is also available for download at http://rpm.pbone.net.

  - The CVLAN Linux client may not be able to establish a secure connection to the CVLAN Service when using certificates with SHA2 (e.g., SHA256) signatures. Use certificates with SHA1 signatures instead.

- **CVLAN Services Does Not Display Online**

  If there are no CVLAN links administered, the CVLAN Service will appear as "OFFLINE" on both the AE Services summary page and the Status summary page of the AE Services Management Console. The status will change to "ONLINE" after you administer at least one CVLAN link.

  This is desirable behavior because it stops CVLAN from listening on a port that is not in use and stops that listening port from being reported as a risk on a security audit.

- **DMCC/TR87 cannot properly track call made to Vector Directory Numbers (VDNs) or hunt-groups**

  When a call reaches a VDN and is answered on the far end by an agent or the call reaches a hunt group, Microsoft Office Communicator will create a phantom screen pop and any further transfers will result in new screen pops. This is similar behavior to when a call is alerting on one station and is answered immediately on a different station; DMCC assumes it is a bridged station as there is no differentiation in behavior. Suppressing bridged call appearances for the station (or VDN) alleviates the issue unless the stations involved are SIP stations.

- **DLG Links**

  DLG links may be OFFLINE after recovery from an abnormal shutdown.

- **DLG Service Does Not Display Online**
  If there are no DLG links administered, the DLG Service will appear as "OFFLINE" on both the AE Services summary page and the Status summary page of the AE Services Management Console. The status will change to "ONLINE" after you administer at least one DLG link.

  This is desirable behavior because it stops DLG from listening on a port that is not in use and stops that listening port from being reported as a risk on a security audit.

- **File corruption can occur when the system experiences an ungraceful shutdown**
  The following steps should be taken to prevent an ungraceful shutdown: Do not disrupt the system power. An Uninterruptible Power Supply (UPS) or other type of uninterruptable power backup is a requirement with AE Services running on System Platform. See Chapter 2 of the Installing and Configuring Avaya Aura® System Platform product documentation on support.avaya.com.
  - Sudden loss of power causes an ungraceful system shutdown which can lead to file system corruption. This includes pressing the power button or unplugging the server. See product support notice (PSN) 2987u for additional details.
  - AE Services running on an S8800 Server can experience a non-maskable interrupt (NMI). This can cause an ungraceful shutdown. See PSN 2965u for additional details. Refer to product correction notice (PCN) 1716B Supplement 1 for details on how to remediate this problem.

- **IPv6 issue with the DMCC Java SDK**
  When attempting to connect to the AE Services server's IPv6 address using the DMCC Java SDK from Microsoft Windows, the user will see the following error message: "java.net.SocketException: Permission denied: connect"

  Oracle is tracking this issue with IPv6 addresses for Java NIO channels on Windows. Currently there is no workaround. This issue will be addressed in a future release of Microsoft Windows.

- **JTAPI issue with H.323 stations receiving group calls**
  JTAPI does not deliver the expected events for H.323 stations which receive a group page call. This will be fixed in a future release.

- **Lync 2013 Client Issues**
  The following are known issues with Lync 2013 client. The cumulative update (CU) 2880474 package for Lync 2013: April 2014 has resolved the Conference and Transfer issues described below. More details can be found by searching the internet for “KB 2941643”. The ‘redirecting a call’ remains an issue after this CU is applied.

- **Conferencing a Call**
  When a Lync 2013 client is a participant in a conference call, an orphan conversation window (the call before the conference was established) will remain open after the call ends. The conversation window must be manually closed.

  Note that when an orphan conversation window remains displayed after a call ends, new calls that are answered by the Lync 2013 client will automatically be placed on hold until the orphan window is closed.

- **Transferring a Call**
  When a Lync 2013 client is transferred to another party, the Lync 2013 client that was transferred (transferred party) will have two conversation windows displayed after the transfer is completed. The Transferred party will not be able to end the call using the Lync 2013 user interface. The call must be ended from the device. There are also issues when a Lync 2013 client is transferred to 'an existing conversation' and the (Lync 2013) transferred party is unable to end the call from the user interface.

  Note that when an orphan conversation window remains displayed after a call ends, new calls that are answered by the Lync 2013 client will automatically be placed on hold until the orphan window is closed.

- **Redirecting a Call**
  The Lync clients allow the user to administer mobile, home and 'other' phone numbers. When a Lync client receives a call, the user may redirect the call to one of the administered numbers (in the 'Options' drop down in the alerting window). When a call is redirected to a destination that is a Lync client, the Lync client the call was redirected to will not be able to answer the call from the user interface; the call must be answered by using the device.

- **The Microsoft Office Communicator (OC) client does not re-establish phone integration automatically when the AE Services server is restarted**

  This is a known problem in Office Communications Server (OCS) 2007 R2 that does not exist in Live Communications Server (LCS) 2005. The following workaround is recommended:

  1. The first attempt to make a call from an active OC client after an AE Services restart will fail. Click the "retry" button to re-establish phone integration and also make the call.

  2. Call events will not be reported to an active OC client after an AE Services restart. To re-establish phone integration, sign-out of the OC client and then sign-in again.

- **OCS Integration and Microsoft Certificate Authorities (CA)**
  When using Microsoft as the CA, Microsoft recommends using an Enterprise CA. The Enterprise CA template used to create the AE Services certificate must have the Enhanced Key Usage (EKU) field specified appropriately (Server and Client Auth or neither).

  The LCS/OCS AE Services integration uses Mutual TLS (MTLS) to authenticate server-to-server SIP communication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA to prove the identity of each server to the other.
  The server certificate used for MTLS on both servers must either not specify an EKU or specify an EKU for Server and Client Authorization. When the EKU is not specified the certificate is not restricted to a particular usage. However when the Key Usage field is specified and the EKU is specified as Server and Client Auth, the certificate can only be used by the server for mutual server and client based authentication purposes. If an EKU with only Server Auth is specified, in this scenario, the connecting server certificate will fail authentication and the MTLS connection will not be established.

  The Standalone CA, which may also be used (but is not Microsoft recommended), does not provide configurable templates including some additional features and must adhere to the same certificate generation rules in regards to the EKU field.

  Note that this statement doesn't preclude administrators from using non-Microsoft CAs (e.g. VeriSign).

- **Process to Change the Server Date and Time**
  When the server time is changed by more than five minutes, several of the AE Services must be restarted. While these services will be restarted on their own, the following procedure is recommended for changing the AE Services Bundled, Software-Only, or Virtualization Enablement (VE) vAppliance server time:

  1. Log into the AE Services Management Console.
  2. Select "Maintenance | Service Controller".
  3. Set the check boxes for the ASAI Link Manager, CVLAN Service, DLG Service, Transport Layer Service and TSAPI Service, and then click on "Stop".
  4. When the confirmation screen is displayed, click on "Stop".
  5. Select "Maintenance | Date Time/NTP Service", make the appropriate - changes on the web-page and click "Apply Changes".
  6. When the confirmation screen is displayed, click on "Apply".
  7. Select "Maintenance | Service Controller".
  8. Set the check boxes for the ASAI Link Manager, CVLAN Service, DLG Service, Transport Layer Service and TSAPI Service, and then click on "Start".

  For the AE Services on System Platform server, refer to the Administering Avaya Aura® System Platform document at
  http://support.avaya.com/css/P8/documents/100171730

- **Single Step Transfer Call**
  The Single Step Transfer Call service does not work reliably when transferring a call to a mobile device.

- **SIP Issues**
  - When using 3rd party call control to make a call using a Communication Manager TAC (Trunk Access Code), the call will fail on a SIP phone if the Communication Manager does not have a TN2602AP board. Please note, it is not common practice to use TAC dialing to access trunks. The Automated Alternative Routing (AAR) and Automated Route Selection (ARS) routing features are recommended methods of accessing trunks.

  - If Communication Manager does not have a TN2602AP board, the media encryption on the SIP endpoint should be disabled. The SIP endpoint transport type must be set to TCP or UDP. If the transport type is set to TLS, the 3rd party call control application may fail during transfer and conference. SIP endpoints (by default) will not respond to out of dialog (OOD) REFER messages from Communication Manager (ASAI third party call control and Communication Manager Call Center features) unless the transport mode is TLS. There is a parameter in the endpoint configuration file that can be set to allow ASAI 3PCC on SIP endpoints with TCP.

  - Avaya has observed intermittent problems with SIP endpoints in the 2.6SP4 and prior releases particularly with scenarios that result in Computer Telephony Integration (CTI) requests that occur within a short time span of other CTI requests. It is currently not known when these issues will be completely addressed, but it is anticipated that future endpoint releases will address them fully. As an example, the Single Step Transfer Call service does not work reliably for SIP stations.

- **Transport**
  When a switch connection is deleted, the action is incomplete and any switch connections that are added may not function properly.

  Workaround: Restart AE Services (or at least the Transport Layer Service) after deleting a switch connection.

- **TSAPI Link Administration**
  When a new TSAPI Link is added through the AE Services Management Console ("AE Services | TSAPI | TSAPI Links | Add Link"), the TSAPI Link may be created with a TSDI High Water Mark that is only 32% of the TSDI Size instead of 80%.

  After adding a new TSAPI Link through the AE Services Management Console, select the link on the TSAPI Links page, click "Edit Link", and then click "Advanced Settings". Change the value of the TSDI High Water Mark to 80% (or to the desired

percentage), click "Apply Changes", and then click "Apply". Then use the "Maintenance | Service Controller" page to restart the TSAPI Service.

- **TSAPI Linux Client**
  - Before installing the TSAPI Linux client on a Red Hat Linux ES v5.0 system, a separate installation of the following RPM may be required:

    openssl097a-0.9.7a-9.el5_4.2.i386.rpm.

    This RPM may be available with your Red Hat Linux installation media, and is also available for download at http://rpm.pbone.net.

  - The TSAPI Linux client may not be able to establish a secure connection to the TSAPI Service when using certificates with SHA2 (e.g., SHA256) signatures. Use certificates with SHA1 signatures instead.

- **WebLM Session May Hang**

  Performing one of the following actions on WebLM may hang the session.
  1. Repeatedly uninstalling and installing licenses
  2. Repeatedly refreshing the licensing page

  The current session should be closed and a new session opened.

- **WebLM Enterprise Model – Using HTTPS**

  Run this workaround if all three of the following conditions are true:
  1. The master WebLM Server, which hosts the Enterprise License File (ELF), is not co-located with an AE Services server. The master WebLM server is either a standalone server or it is co-located in System Platform's CDOM.
  2. The local WebLM servers are co-located with AE Services.
  3. HTTPS is in use for communication between the master and local WebLM servers (for example, to push an Allocation License File (ALF) to the local WebLM server on AE Services).

  The Enterprise Web Licensing WebLM patch, "importCertToWebLm.zip", is available on the AE Services CD/DVD ISO media. On the Hardware Bundled DVD, the patch is located in the "Patch" directory. On the Software Only CD, the patch is located in the root directory of the media. On the AE Services on System Platform DVD, the patch is located in the "licenses" directory.
  1. Download importCertToWebLm.zip files to your EWL server.
  2. Unzip the file.
  3. Follow the directions in the README to install.

- **WebLM access may be denied**
  The WebLM server emdedded in the AE Services server may not be accessible using port 443 when AE Service secure mode is enabled or if the AE Services Apache web server is configured to require a connecting client (browser or application) to provide a client identity certificate. As a workaround, either use port 8443 or a WebLM server external to the AE Services server.

KNOWN ISSUES AND WORKAROUNDS FOR AE SERVICES ON SYSTEM PLATFORM

System Platform issues affecting the AE Services on System Platform server are listed in the System Platform R6.3.4/6.3.5/6.3.6/6.3.7/6.3.8 release notes at https://support.avaya.com/

- Customers using the WebLM server co-resident in System Platform to provide licensing services to the AE Services VM could potentially have their licenses removed during the System Platform upgrade process from an earlier 6.x release to the 6.3.4/6.3.5/6.3.6/6.3.7/6.3.8/6.4.x release. In previous System Platform 6.x releases, the WebLM server was able to support multiple Host ID's. In the System Platform 6.3.4/6.3.5/6.3.6/6.3.7/6.3.8/6.4.x release, the WebLM server has been updated to only support the Primary Host ID.

  Based on your current AE Services release, please execute the following procedure to determine if your WebLM license will be affected.

  AE Services 6.1.x and 6.2.x System Platform users:
  1. SSH into the Domain-0 VM and promote your account to the root user
  2. Execute the following command to obtain Domain-0's Host ID (aka HWaddr):
     ifconfig | grep eth0
  3. The output should be similar to the following where the Host ID is in bold font:
     eth0 Link encap:Ethernet HWaddr **00:12:3A:BC:DE:FG**
  4. SSH into the Console Domain VM and promote your account to the root user
  5. Execute the following command:
     cd /opt/avaya/vsp/tomcat/webapps/WebLM/licenses/
  6. Execute the following command:
     grep APPL_ENAB *
  7. The output should be similar to the following where the item in bold is the file name
     wlm12345678license.xml:<LAR platformType="APPL_ENAB" sid="1234456" version="1.0">

     Note: If no output is displayed, an AE Services license is not installed in the System Platform WebLM. Otherwise continue.
  8. Using the obtained Domain-0 Host ID without any colons and the AE Services license file name, execute the following command:
     grep <Dom0-Host-ID> <AESvcs-License-File-Name>

For instance, using the example Host ID from step 3 and the example AE Services license file name from step 7:
"grep 00123ABCDEFG wlm12345678license.xml"

9. Verify the Primary Host ID is specified in the license file.
    - If the Primary Host ID is **not** displayed after executing the grep command, please contact Avaya Services to obtain a new license based on the Primary Host ID.
    - If the Primary Host ID is displayed after executing the grep command, please proceed with the upgrade process.

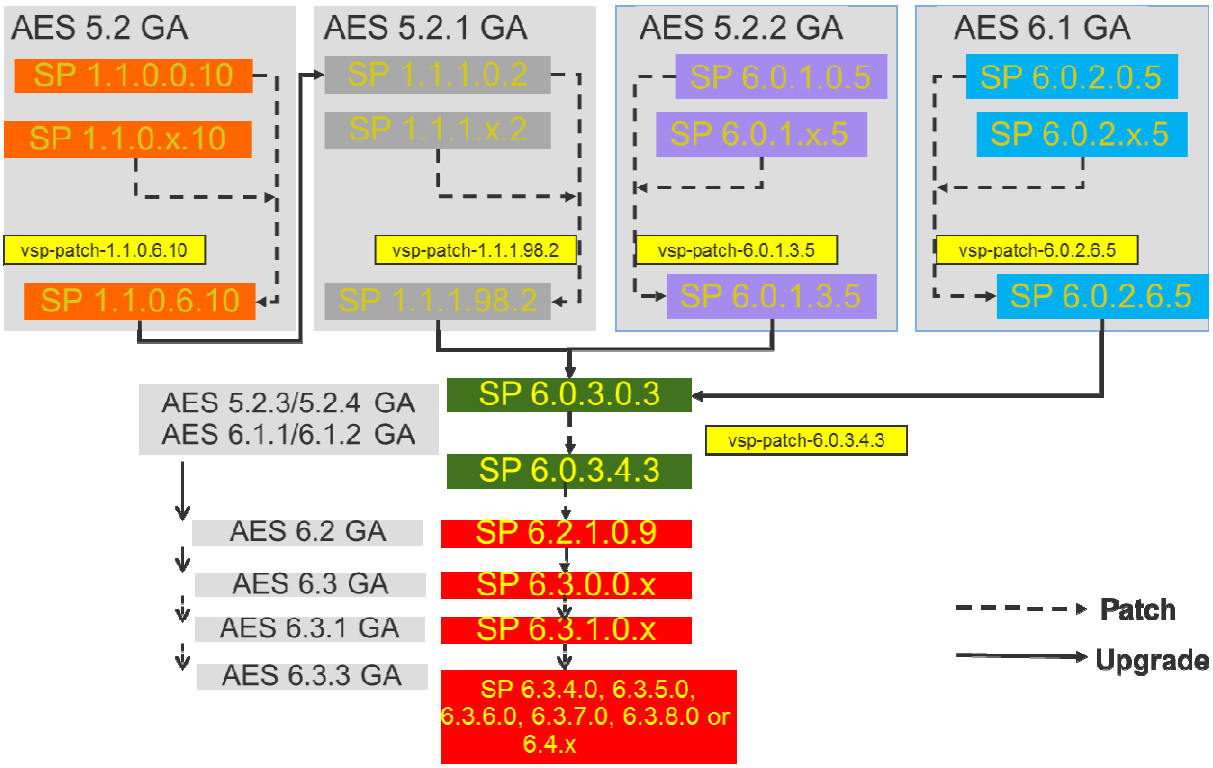
AE Services 6.3.0 System Platform users:

1. Login to the System Platform Management Console
2. Navigate to **"Server Management | License Management"**
3. Click the button labeled **"Launch WebLM License Manager"**
4. Login to the WebLM Management Console
5. Using the WebLM menu, select **"Server Properties"**
6. Note the Host ID specified as **"Primary Host ID"**
7. Using the WebLM menu, select **"Licensed products | APPL_ENAB | Application_Enablement"**
8. In the displayed AE Services license, locate the label **"License File Host IDs"**
9. Verify the Primary Host ID from step 6 is specified in the license file.
    - If the Primary Host ID is **not** specified in the license file, please contact Avaya Services to obtain a new license based on the Primary Host ID.
    - If the Primary Host ID is specified in the license file, please proceed with the upgrade process.

- AES 6.3.3 with System Platform 6.4.x does not support Machine Preserving High Availability (MPHA). AES 6.3.3 with System Platform 6.3.x does support MPHA.

- For information about Meltdown And Spectre Vulnerabilities in relation to AES 6.3.x, please see PSN0203046u on the Avaya Technical Support web site

- **SYSTEM PLATFORM UPGRADE PATHS**



RESOLVED ISSUES IN AE SERVICES RELEASE 6.3.3

- **Agent Events**
  AES-17496: Avaya Aura® Workforce Optimization were not provided with AgentEvents privileges.

- **ASAI Link Layer**
  When tracing was enabled and the trace file reached its maximum size, the ASAI Link Layer could erroneously reset a CTI link.

- **CVLAN SERVICE**
  - The CVLAN Service could crash when being taken offline if another process was listening on either of the CVLAN TCP ports.

  - When starting the CVLAN Service, sometimes the error message “Unexpected termination for primitive 55” was logged.

- **High Availability**
  Secondary WebLM Address no longer disappears when Geo Redundancy High Availability (HA) is enabled

- **JTAPI**
  - The Call.connect() API would sometimes fail with an error message "Could not meet post-conditions of connect()", even though the call proceeds properly.

  - When creating secure connections on Windows, the JTAPI application would sometimes hang for up to 30 seconds, then fail with an exception.

- **Management Console**
  - Attempting to manage a large number of devices using the Security Database screens may cause the web interface to become slow or none responsive. A modification has been made to allow the management of a large number of devices using the Security Database screens in a more efficient manner.

  - AE Service server management console alarm viewer no longer displays the following alarm messages in the “Alarm Message” column whenever a Geo Redundancy HA related alarm is cleared or created.

- **.Net**
  - For all the events that use or support "lastRedirectionDevice", the .NET SDK does not parse the XML message correctly. The .NET SDK event handlers, Delivered, Established, Failed, Network-Reached and Queued, has been modified to properly parse for "lastRedirectionDevice".

- The .NET SDK read and write socket thread has been modified to work independent of one another. In prior releases, a lock was used to throttle the read thread while a write operation was being performed. Occasionally, this would cause locks associated with the processing of other requests to timeout.

- In prior releases, when a read exception is thrown, the entire application would be terminated. With this release, the SDK will terminate the affected Application Session instead of the entire application (one application can have multiple DMCC Application Sessions) and fire a SocketClosed event handler to inform the customer application of the socket termination.

Security

- AES-17523: The error "Certificate Chain too Long" would be seen if more than one certficate was present in the certificate chain 2.

- Fixes for the following Apache Tomcat security issues have been incorporated into AE Services 6.3.3:
  1. CVE-2013-4590: Application provided XML files such as web.xml, context.xml, *.tld, *.tagx and *.jspx allowed XXE which could be used to expose Tomcat internals to an attacker.
  2. CVE-2013-4322: Incomplete fix for CVE-2012-3544 (Denial of Service).
  3. CVE-2014-0033: Session fixation still possible with disableURLRewriting enabled
  4. CVE-2013-4286: Incomplete fix for CVE-2005-2090 (Information disclosure)

- The following Red Hat Linux security advisories have been incorporated into AE Services 6.3.3:
  1. [RHSA-2013:1292-01] Moderate: kernel security and bug fix update
  2. [RHSA-2013:1348-01] Moderate: Red Hat Enterprise Linux 5 kernel update
  3. [RHSA-2014:0108-01] Moderate: kernel security and bug fix update
  4. [RHSA-2014:0285-01] Important: kernel security, bug fix, and enhancement update
  5. [RHSA-2013:1449-01] Moderate: kernel security and bug fix update
  6. [RHSA-2013:1475-01] Moderate: postgresql and postgresql84 security update
  7. [RHSA-2014:0249-01] Important: postgresql security update
  8. [RHSA-2013:1135-01] Moderate: nss and nspr security, bug fix, and enhancement update
  9. [RHSA-2013:1156-01] Moderate: httpd security update
  10. [RHSA-2013:1302-01] Low: xinetd security and bug fix update
  11. [RHSA-2013:1409-01] Moderate: xinetd security update
  12. [RHSA-2013:1411-01] Moderate: glibc security and bug fix update
  13. [RHSA-2013:1458-01] Moderate: gnupg security update
  14. [RHSA-2014:0016-01] Moderate: gnupg security update
  15. [RHSA-2013:1457-01] Moderate: libgcrypt security update
  16. [RHSA-2014:0247-01] Important: gnutls security update

17. [RHSA-2013:1813-01] Critical: php53 and php security update (fixed by PHP update to 5.4.23-2)
18. [RHSA-2013:1814-01] Critical: php security update (fixed by PHP update to 5.4.23-2)

- The version of PHP installed on AE Services has been updated to 5.4.23-2. The full list of issues fixed in this release is available at http://www.php.net/ChangeLog-5.php#5.4.23.

- **SIP**
  - Going off-hook on a SIP station followed by on-hook no longer generates an INITIATED event.
  - Using 3rd party call control when a call is made from a SIP station, the INITIATED event is no longer slightly delayed as compared to other station types. Subsequent events are not delayed.

- **SNMP**
  The SNMP subagent on AE Services would return incorrect values for the status of active CVLAN clients which have been configured with a hostname instead of an IP address. This was also visible in OAM as incorrect values for the "Number of CVLAN Clients" and "Client Status" on the CVLAN Service Summary page.

- **System Management Services**
  - AES-17134: The "IP Srevices" Model on AE Services System Management Services (SMS) did not return any response when field specific requests were sent.
  - AES-15539: SMS services stopped working after sometime. OSSICM process became non-responsive.

- **Transport Service**
  When establishing a secure connection with Communication Manager, the Transport Service did not verify the certificate provided by Communication Manager.

- **TSAPI Windows Client**
  When installing the TSAPI Windows Client on a 64-bit version of Windows, the setup program would sometimes display an “Existing File Found” dialog box. The dialog box erroneously reported that an existing copy of a TSAPI Window Client DLL was installed in C:\Windows\system32, though it was not.

- **TSAPI Service**
  - Software changes delivered to AE Services 6.3.0 could cause the TSAPI Service to crash during some call scenarios involving bridged call appearances.

- When a call was transferred to a hunt group with no available agents and an agent subsequently became available, the callingDevice field in the corresponding CSTA Delivered event contained the device ID of the transferring station instead of the device ID of the other party on the call.

- When the CSTA Route Select service was used to route a call from one monitored VDN to another, the newDestination field in the corresponding CSTA Diverted event contained the device ID of the original VDN instead of the new VDN.

- If a call to a VDN with an adjunct route step was placed on hold and then retrieved using the CSTA Retrieve Call service before the call was routed, the lastRedirectionDevice field in the subsequent CSTA Delivered event contained the device ID of the calling station instead of the device ID of the VDN.

- If an application invoked the CSTA Answer Call service to answer a call at a station extension for which the TSAPI Service could not acquire a second ASAI domain control, the corresponding CSTA Established event did not provide any private data.

- When a call was answered by a coverage answer group member, the TSAPI Service did not always provide CSTA Diverted events for all of the other members of the coverage answer group.

- If a call was queued to several hunt groups, the CSTA Snapshot Call service did not include all of the hunt groups in the confirmation event.

- In some conference and transfer scenarios, the TSAPI Service would attempt to acquire a second ASAI Call Control association for a call when processing a CSTA Clear Call service request for that call.

- When one conference participant transferred the call to another one of the conference participants, the TSAPI Service would send a CSTA Connection Cleared event indicating that the conference participant to whom the call was transferred had dropped off of the call.

- When a station user presses the Drop button to drop off of a call, a new call is initiated. If an agent used the Drop button to drop off of a predictive call (created with the CSTA Make Predictive Call service), any CSTA events reported during the first 10 seconds of the new call contained the call ID of the predictive call instead of the call ID of the new call.

- When a predictive call was conferenced or transferred, the secondaryOldCall parameter in the corresponding CSTA Conferenced or CSTA Transferred event could contain the wrong call ID.

- When a monitored predictive call was conferenced or transferred with another monitored call, monitors for the predictive call could receive an extra CSTA Call Cleared event.

- After a predictive call was conferenced or transferred, monitors for the call could receive events containing the wrong call ID.

- Ten seconds after a predictive call was conferenced or transferred, monitors for the call could stop receiving events.

- If an unsupervised conference was performed on a predictive call, when the added party answered the call, monitors for the call could receive a CSTA Retrieved event instead of a CSTA Established event.

- If the TSAPI Service received a service request for a monitored station while it was performing recovery actions for a previous, failed CSTA Alternate Call, CSTA Consultation Call, CSTA Reconnect Call, or ATT Single Step Transfer Call service request for the same station, the TSAPI Service might stop reporting events for that station extension. Further, in some cases the TSAPI Service did send station monitors a CSTA Monitor Ended event to indicate that they would no longer receive events.

- If a client application connected to one of the TSAPI Encrypted Tlink ports and did not complete the OpenSSL handshake, the TSAPI Service would stop processing connection requests for other clients.

- When starting the TSAPI Service, sometimes the error message “Unexpected termination for primitive 55” was logged.

- Handling of WebLM “Feature Not Found” errors has been improved.

- The Persistent AAO Audit has been improved to clean up ASAI Association Objects more efficiently when they reach the administered Persistent AAO Maximum Age.