Avaya Aura® Application Enablement Services R6.1.1 Server and Client Service Pack Release Notes

Issue 1.2
February 2012

INTRODUCTION

This document introduces the Generally Available release of the Application Enablement (AE) Services Release 6.1.1 and describes important notes and known issues.

ENHANCEMENTS

- AE Services R6.1.1 now Supports Microsoft Lync integration, in addition to previously supported LCS and OCS R1 and R2 versions.

  Please refer to Microsoft Lync's published release notes, which documents all known Lync issues and limitations with respect to RCC-based integrations such as AE Services': http://download.microsoft.com/download/3/9/E/39E717E4-CF01-4666-8A32-EE7AE1FAFAC1/Lync_Server_2010_Clients_RTM_Relnotes.htm

- A new capability has been included to administer the ability to disable the Microsoft OCS / Lync auto hold behavior on an AE Services system-wide basis to allow more than one call to be active at the same time on a device. The Microsoft Office Communicator (OC) client will automatically place an active call on a desktop device on hold, if another incoming call is answered on an associated EC500 device (e.g. mobile device). Since this may not be desirable, a new AE Service's Management Console configuration screen called "Auto Hold Configuration" has been implemented to allow an administrator the ability to control this behavior by enabling or disabling auto hold. Disabling auto hold will prevent the Microsoft OC client from being notified of a new incoming call when Microsoft OC controlled device is on an active call.

  Enabling or disabling the auto hold feature on an AE Services server affects every Microsoft OC client registered on the AE Services server. The following are some side effects when auto hold is disabled:

  1. A Microsoft OC alerting window will only be displayed when the Microsoft OC client controlled device is not involved in an active call**.** In other words, it will receive an alerting window if it does not have an active call or the call(s) are on hold (with the exception of the scenarios described in items 4 and 5 below).

2. If two calls are delivered to a device and neither call has been answered, the Microsoft OC client will display two alerting windows. As soon as the last unanswered call is answered, the Microsoft OC client will automatically place the first answered call on hold. This scenario is equivalent to having auto hold enabled.
3. If the first incoming call is answered on an EC500 device, the associated Microsoft OC conversation window will not be able to control the EC500 device. The second call will not generate an alerting window on the Microsoft OC client. Also, when the call is answered on the device, it will neither generate a Microsoft OC conversation window nor put the first call on hold.
4. Bridging: If the first call is picked up by the “Bridge of Extension”, then the second call to that extension will receive the alert window on its Microsoft OC Client. If the first call is picked up by the “Principal Extension” instead of the Bridge, then the second call to the “Principal Extension” will not receive the alert window on its Microsoft OC Client. If the first call is not picked up by the Principal or Bridge but rather by EC500, then the second call to the “Principal Extension” will not get the alerting window on its Microsoft OC Client.
5. When a device is on an active call and Microsoft OC logs out and logs back in without disconnecting the call, the first new incoming call will receive the alerting window.

SOFTWARE RELEASE VERSIONS

Application Enablement Services Application	File Name
Avaya Aura® Application Enablement Services 6.1.1 CVLAN Client Linux 32-bit and 64-bit in 32-bit compatibility mode	cvlan-client-linux-6.1-469.i386.rpm
Avaya Aura® Application Enablement Services 6.1.1 CVLAN Client MS Windows 32-bit and 64-bit in 32-bit compatibility mode	cvlan-client-win32-6.1-469.zip
Avaya Aura® Application Enablement Services 6.1.1 TSAPI Client Linux 32-bit and 64-bit in 32-bit compatibility mode	tsapi-client-linux-6.1-469.i386.rpm
Avaya Aura® Application Enablement Services 6.1.1 TSAPI Client MS Windows 32-bit and 64-bit in 32-bit compatibility mode	tsapi-client-win32-6.1-469.zip
Avaya Aura® Application Enablement Services 6.1.1 TSAPI SDK Linux 32-bit and 64-bit in 32-bit compatibility mode	tsapi-sdk-linux-6.1-469.i386.rpm
Avaya Aura® Application Enablement Services 6.1.1 TSAPI SDK MS Windows 32-bit and 64-bit in 32-bit compatibility mode	tsapi-sdk-win32-6.1-469.zip
Avaya Aura® Application Enablement Services 6.1.1 JTAPI SDK	jtapi-sdk-6.1.0.94.zip
Avaya Aura® Application Enablement Services 6.1.1 Web Service - System Management SDK	smssvc-sdk-6.1.1.90.zip
Avaya Aura® Application Enablement Services 6.1.1 DMCC .Net SDK 32-bit and 64-bit in 32-bit compatibility mode	dmcc-dotnet-sdk-6.1.1.45.zip
Avaya Aura® Application Enablement Services 6.1.1 Web Services - Telephony SDK 32-bit and 64-bit in 32-bit compatibility mode	telsvc-sdk-6.1.1.90.zip
Avaya Aura® Application Enablement Services 6.1.1 DMCC XML SDK 32-bit and 64-bit in 32-bit compatibility mode	cmapixml-sdk-6.1.1.90.zip
Avaya Aura® Application Enablement Services 6.1.1 DMCC Java SDK 32-bit and 64-bit in 32-bit compatibility mode	cmapijava-sdk-6.1.1.90.zip
Avaya Aura® Application Enablement Services 6.1.1 Software Only 32-bit and 64-bit in 32-bit compatibility mode - 700501915	swonly-r6-1-1-30-20110520.iso
Avaya Aura® Application Enablement Services 6.1.1 Hardware Bundled Upgrade for S8510 32-bit and 64-bit in 32-bit compatibility mode - 700501914	700501914.iso
Avaya Aura® Application Enablement Services 6.1.1 on System Platform 32-bit and 64-bit in 32-bit compatibility mode - 700501916	aes-r6-1-1-30.iso
System Platform Pre-Upgrade Patch R6.0.2.6.5	vsp-patch-6.0.2.6.5.nonarch.rpm
System Platform Service Pack R6.0.3 - 700500929	vsp-6.0.3.0.3.iso
System Platform Patch R6.0.3.1.3	vsp-patch-6.0.3.1.3.noarch.rpm
Avaya Aura® Application Enablement Services Product MIBs	aesvcs-product-mibs-6.1.1.90.zip
Standard MIBs	standard-mibs-6.1.1.90.zip

IMPORTANT NOTES

- AE Services 6.1.1 supports Red Hat Enterprise Linux 5.0 Update 5 for 32-bit x86

- AE Services 6.1.1 is compatible with the following Bundled Server: Dell 1950 (S8510)

- AE Services 6.1.1 on System Platform is compatible with the following Servers:
  - IBM x3550 M2 (S8800)
  - Dell R610

- AE Services 6.1.1 on System Platform is compatible with the following versions of System Platform:
  - System Platform R6.0.3

- AE Services 6.1.1 is compatible with the following Communication Manager Releases and Platforms:
  - Communication Manager 4.x (S8300, S8400, S8500, S87xx) - with the following limitation: Once Communication Manager 4.x reaches its End of Manufacturers Support, AE Services 6.1 support of Communication Manager 4.x is limited to any issues that can solely be addressed in the AE Services software.
  - Communication Manager 5.0 (S8300, S8400, S8500, S87xx)
  - Communication Manager 5.1 (S8300, S8400, S85xx, S87xx)
  - Communication Manager 5.2 (S8300, S8400, S85xx, S87xx)
  - Communication Manager 5.2.1 (S8300, S8400, S85xx, S87xx, S8800)
  - Communication Manager 6.0 (S8300D, S8510, S8800)
  - Communication Manager 6.0.1 (S8300D, S8510, S8800)

- Communication Manager 6.0.1 is compatible with the following AE Services Releases:
  - AE Services 5.2.x
  - AE Services 6.1

Avaya SIP Endpoints Supported by AE Services TSAPI							
Endpoint	Administered as	Endpoint Firmware	AE Services Release	CM/ASM Pair		General Telephony	Agent Features
				CM- ES Version	ASM Version		
9620	9620SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9640	9640SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9640G	9640SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9630G	9600SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9650	9600SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9608	9640SIP	6.0 SP1	6.1.x	6.0.1	6.1 SP2	yes	no
9611	9640SIP	6.0 SP1	6.1.x	6.0.1	6.1 SP2	yes	no
9621	9640SIP	6.0 SP1	6.1.x	6.0.1	6.1 SP2	yes	no
9641	9640SIP	6.0 SP1	6.1.x	6.0.1	6.1 SP2	yes	no

Endpoint	Administered as	Endpoint Firmware	AE Services Release	CM/SES Pair		General Telephony	Agent Features
				CM Version	SES Version		
9620	9620SIP	2.5(GA)	5.2.x	5.2.1	5.2.1	yes	no
9640	9640SIP	2.6	5.2.x	5.2.1	5.2.1	yes	no
9640G	9640SIP	2.6	5.2.x	5.2.1	5.2.1	yes	no
9630G	9600SIP	2.6	5.2.x	5.2.1	5.2.1	yes	no
9650	9600SIP	2.6	5.2.x	5.2.1	5.2.1	yes	no
16CC	4620SIPCC	SIP16CC_1_0_12_010_b001.bin	5.2.x	5.2.1	5.2.1	yes	yes (note 1)

Note 1 - Agent Buttons Supported:

Agent login/logout

After call work

Auxiliary work

Auto/manual in

Release

Agent Event Package (16CC)

Release History:

Date	Server Build	Change(s)
03/2007	47-3	General Availability R4.0
06/2007	50-1	General Availability R4.0.1
12/2007	31-2	General Availability R4.1
04/2008	4.1.16	General Availability R4.1.1 JTAPI Client/SDK
05/2008	19-4	General Availability R4.2
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	General Availability R5.2
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	General Availability R6.1
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

KNOWN ISSUES AND WORKAROUNDS

- **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 JTAPI, TSAPI, CVLAN, and 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 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 spontaneous 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. Spontaneous 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.

- **Avaya Aura® Contact Center High Availability Configuration Settings**

  Avaya Aura® Contact Center High Availability Deployment settings need to be changed as follows:

  1. Start a console session on the AE Services server (locally, via service port, or remotely, using e.g. PuTTY).

  2. Login as sroot or root.

  3. Uncomment and set the properties in /opt/mvap/conf/user-configuration.properties as listed below:

     ```
     ##################################################################
     #
     # cmapi.nist_ssl_socket_retry: The server will attempt to re-establish an
     # outbound TLS socket connection multiple times after a failure occurs if
     # set to true.
     ```

```
#
# cmapi.nist_ssl_socket_timeout: The interval of time in milliseconds
# that the server waits for a TLS socket connection to be established.
#
#########################################################################
cmapi.nist_ssl_socket_retry=false
cmapi.nist_ssl_socket_timeout=1000
```

4. Log into the AE Services Management Console using a browser. Set the parameter "Network | TCP Settings | TCP Retransmission Count" to 2

AE Services depends on an open source third party SIP stack which uses Java old IO sockets and synchronizes on a lock when it sends User Agent Server (UAS) data over a TLS connected SIP User Agent Client (UAC). The UAS cannot immediately detect when the UAC is disconnected from the network for the reason that the default TCP retransmission timeout is more than 10 minutes. Furthermore, when the send socket queue for a disconnected UAC is filled up on a busy UAS, other UAC messages to be sent are blocked due to the synchronization. For Avaya Aura® Contact Center High Availability setups, the active and standby members receive the same call control events. On a busy system, when the active member is disconnected from the network, the standby member stops receiving the events after a short while, since the active member's send queue fills up with the retransmitted call control events. This condition clears after the TCP retransmission times out for the active member and the TLS connection socket is closed.

The above workaround recommends that an administrator lower the default Linux system wide TCP retransmission count to 2 or a suitable value on the AE Services Management Console. This enables the UAS to detect a disconnected UAC and close the associated TLS connection within a few seconds. However, under poor network conditions, a TCP retransmission count of 2 is known to cause performance degradation for other AE Services that depend on an application level heartbeat mechanism to detect a disconnected peer. This workaround should only be deployed on a solid and stable network.

- **AE Services Manual Database restore from 3.x release requires OAM re-login**

  When manually restoring a 3.x database from the AE Services Management Console, be sure to log-out after the restore and then log back in before performing any administration. This is required to synchronize user passwords and if not performed, certain administrative functions such as User Management may not be available from OAM until the re-login.

- **ASAI – The collect digits option in the route select message is no longer supported**
  There is a feature that is documented in the ASAI Technical reference (no longer published) that allows an application to collect digits through a Route Select message.

  Implications for TSAPI include: When sending private data with a cstaRouteSelectInv() service request, the collectCode parameter passed to attV7RouteSelect(), attV6RouteSelect(), or attRouteSelect() should be initialized with a Collect Code Type of UC_NONE.

  Implications for JTAPI include: The methods LucentRouteSession.selectRouteAndCollect() and LucentRouteSession.selectRouteWithDigits() are not supported. If invoked, each of these methods will throw a TsapiMethodNotSupportedException.

- **Cannot get license version from WebLM Server**
  If the error message “Cannot get license version from WebLM Server” is displayed on the “Maintenance | Server Data | Restore Database Configuration” screen after a restore, and a license file exists in the backup image, go to the “AE Services” screen to view the license information for each AE Service. If the license in the backup image is invalid, install the 6.X license file to resolve the issue. Be sure to uninstall any previous license files (i.e. 5.X license, or 4.X) prior to installing the 6.X license file.

- **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.

- **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 the customer is not using and stops that listening port from being reported as a risk on a security audit.

- **CVLAN and DLG Services may not show the correct license mode after recovering from restricted mode with the AE Services on System Platform Offer with High Availability**
  If the CVLAN service enters license restricted mode and the licensing error is fixed, the license mode may still appear to be restricted even though the CVLAN service is functioning normally. This will occur if any of the administered CVLANs do not have the "proprietary" check box selected.

  If the DLG service enters license restricted mode and the licensing error is fixed, the license mode will still appear to be restricted even though the DLG service is functioning normally.

- **DMCC/TR87 can not properly track call made to Vector Directory Numbers (VDNs) or hunt-groups**
  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. When a call reaches a VDN and is answered on the far end by an agent or the call reaches a hunt group, Office Communicator will create a phantom screen pop and any further transfers will result in new screen pops. Suppressing bridged call appearances for the station 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 the customer is not using and stops that listening port from being reported as a risk on a security audit.

- **Firewall changes requiring restart are service affecting**

- **IPv6 issue with the DMCC Java SDK**
  When attempting to connect to the AE Server's IPv6 address using the DMCC Java SDK from Microsoft Windows, the user will see the following error message: "java.net.SocketException: Address Family not supported by protocol family"

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

- **Local WebLM Server Port Number**

  If you have upgraded to AE Services 6.1.X from an earlier release of AE Services, the local WebLM server may be configured to use port 443. Most AE Services customers will see improved WebLM performance if the port number is changed from 443 to 8443. Use this procedure to change the port number for the local WebLM server to 8443:

  1. Use a web browser to log into the Application Enablement Services Management Console.
  2. Select "Licensing | WebLM Server Address".
  3. If the value of the WebLM IP Address is 127.0.0.1 and the value of the WebLM Port is 443, change the value of the WebLM Port to 8443 and click on "Apply Changes".
  4. When the confirmation screen is displayed, click on "Apply".
  5. For the Bundled or AE Services on System Platform Server offers, select “Security | Standard Reserved Ports”.
  6. If the “TOMCAT HTTPS – 8443” row is not checked, then click it and click “Apply”.

  After changing the WebLM Port, restart several of the AE Services:

  1. Select "Maintenance | Service Controller".
  2. Set the check boxes for "ASAI Link Manager", "CVLAN Service", "DLG Service", "Transport Layer Service", and "TSAPI Service", and click on "Restart Service".
  3. When the confirmation screen is displayed, click on "Restart".

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

  This is a known problem in OCS 2007 R2 that does not exist in LCS 2005. The following workaround is recommended:

  1. The first attempt to make a call from an active OC 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 after an AE Services restart. To re-establish phone integration, sign-out of OC 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 Extended Key Usage (EKU) or specify an EKU for Server and Client Auth. 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 or Software-Only 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/100068114

- **Sametime Upgrade from 8.0 to 8.02 Loses the Telephony Service Provider Policy Setting**
  When Sametime is upgraded from 8.0.0 to 8.0.2, the telephony service provider is not enabled as a default. Re-enable the Telephony Service Provider field in the Sametime Policy. The IBM software problem report is SLEE7NKJRJ.

- **Sametime Connect 8.0.2 – Calls Cannot Be Made to the Client when "Display Incoming Invitation" Is Unchecked**
  When a Sametime client unchecks "Preferences | Notifications |Telephony notifications | Display incoming invitation" in Sametime Connect 8.0.2, Sametime calls cannot be made to that particular client. IBM has provided Hotfix # DAMD-7NJKJA.

- **SIP Issues**
  - When using 3rd party call control to make a call on a SIP endpoint to a VDN that has a vector step to collect digits after an announcement, the announcement will not be played and the digits entered will not be forwarded.

  - When using 3rd party call control to make a call using a Communication Manger 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 AAR and 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 transport type is set to TLS, the 3rd party call control application may fail during transfer and conference.

  - The Single Step Transfer service does not work reliably for SIP stations.

  - Going off-hook on a SIP station followed by on-hook does not generate an INITIATED event.

  - Using Third party Call control when a call is made from a SIP station, the INITIATED event is slightly delayed as compared to other station types. Subsequent events are not delayed.

  - ACD calls that are delivered to SIP endpoints are generating Alerting Event reports that do NOT contain the split/skill extension from the associated call.

  - Avaya has observed intermittent problems with SIP endpoints in the 2.6SP4 and prior releases particularly with scenarios that result in 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 anticipate that future endpoint releases will address them fully.

- **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 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.

- **TSAPI Service Initialization Fails When IPv6 is Disabled**
  When IPv6 is disabled on the AE Services server, the TSAPI Service will fail to initialize.

  Symptoms of this issue include:
  - TSAPI clients are unable to connect to the TSAPI Service because there are no advertised services.
  - The AE Services Management Console "Status | Status and Control | TSAPI Service Summary | Tlink Status" page reports "Tlink not found".
  - The AE Services $MVAP_LOGS/log. file contains errors similar to:
    "DriverService::peerAcceptorOpen(): Couldn't bind socket to address [::]1066; error: Address family not supported by protocol"

  The workaround is to ensure that IPv6 is enabled for the Linux operating system.

  Typically, this issue only arises on Software-Only offers, as IPv6 is enabled by default on the Hardware Bundled and AE Services on System Platform offers.

- ## WebLM Enterprise Model – Using HTTPS

  Run this workaround if <u>all three</u> 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 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.

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 R6.0.3 release notes at https://support.avaya.com/css/Products/P0585/Release%20Notes%20&%20Software%20Update%20Notes

SYSTEM PLATFORM PRE-UPGRADE PATCH 6.0.2.6.5

Apply vsp-patch-6.0.2.6.5.noarch.rpm to System Platform R6.0.2 prior to upgrading to R6.0.3. This pre-upgrade patch resolves upgrade issues from R6.0.2 to R6.0.3 if the latest SAL VSPU model has been pushed to System Platform.

SYSTEM PLATFORM SERVICE PACK PATCH 6.0.3.1.3

This patch addresses the following issues:

1. OpenLDAP startup script not running bdb recovery
2. Alarm threshold configuration changes not matching R1.1
3. WebLM Truststore used for enterprise licensing not updated with new SIP CA signed certificates
4. Physically removed USB device still shown as attached to CDOM after failed upgrade
5. High Availability may not start after System Platform and Midsize Business Template upgrades
6. Upgrading a template with multiple virtual machines (VMs) caused unchanged VMs to be re-installed
7. CDOM webpage inaccessible after System Platform upgrade to R6.0.3.0.3 running the Midsize Enterprise template due to the large size of the template's backups
8. Template upgrade workflow stalled on VM Data Restore task
9. Password rules help information did not match user documentation
10. Enterprise LDAP filter restricts search base to the authenticated userDn
11. Backup failed to run on CDOM when Midsize Business Template or Communication Manager templates installed
12. SAL model update for Presentation Services
13. Upon stopping a VM, continuous XEN errors appear in the log file, which generate numerous alarms

RESOLVED ISSUES IN AE SERVICES RELEASE 6.1.1

- **Avaya Aura® Application Enablement Services 6.1.1 Hardware Bundled Upgrade for S8510 Expired Certificate**

  The AE Services 6.x Bundled server installation media, ISO and DVD, contained a certificate which expired on Sep. 21, 2011. If an upgrade of the Bundled server is attempted after this date, the upgrade process will fail with the following certificate validation error:

  ERROR: /tmp/common.pem NOT verified to Trusted Root Cert(s) in /etc/opt/avaya/certs/CA (error 200)
  file:/mnt/cdrom/software/common.rpm failed signature verification
  Is /etc/opt/avaya/certs/CA populated with a valid certificate?
  Can't find AES release. Check the CD/DVD and try again
  Ejecting CD/DVD from CD/DVD Drive

  Resolution: For upgrades to AE Services 6.x use the AE Services 700501914.iso Bundled ISO. Reference PSN003417u for additional information.

- **AE Services Server**
  - The efficiency of the restore process was improved by separating the non-critical server data (i.e. alarming records and HMDC tables) which will be restored by a secondary scheduled script. The remaining required tables will continue to be created as part of the normal restore process.

  - After installing or upgrading to AE Services 6.1, email notifications were not issued. This has been resolved in AE Services 6.1.1.

- **CVLAN Clients and SDKs**
  - When installing the CVLAN Windows Client and SDK on a 64-bit version of Windows, the Setup program no longer allows the software to be installed in a subfolder of the 64-bit Program Files folder (typically “C:\Program Files\”). If a subfolder of the 64-bit Program Files folder is selected, then the Setup program will suggest installing the software in the corresponding subfolder of the 32-bit Program Files folder (typically “C:\Program Files (x86)\”).

  - The Certificate Authority certificate file that is installed with the CVLAN Client has been updated to include an additional Avaya CA certificate for establishing secure connections to the AE Services server.

- **DMCC**
  - Removed the check for the “RegisterDevice” request that contained both “telecommuter” and “RTP” parameters. The "telecommuter" and "RTP" parameters are logically mutually exclusive, and a check for such was added in R5.2. However, this check caused a problem for at least one existing application. Thus, the check has been removed for this release. Any application specifying both the "telecommuter" and "RTP" parameters in the "RegisterDevice" request will be registered in Telecommuter mode, and not Client-Media mode.

  - The Certificate Authority certificate file in DMCC .NET, Java, and XML SDKs has been updated to include an additional Avaya CA certificate for establishing secure connections to the AE Services server.

- **JTAPI**
  - In previous releases, JTAPI did not move the calling party's connection state to “CallControlConnection.ESTABLISHED”. In a specific scenario when Station “A” calls an off-switch Station “B”, for specific trunk settings (i.e. ISDN PRI/BRI) in specific countries (i.e. Germany or France), the calling party's connection remained in the “CallControlConnection.INITIATED” state even if the call was answered by the called party and remained in the initiated state for the rest of the call duration.

    If the calling party is being monitored through JTAPI, then JTAPI requires “CSTAOriginatedEvent” to move the calling party’s connection to the “CallControlConnection.ESTABLISHED” state. If JTAPI does not receive “CSTAOriginatedEvent”, then it will simulate the “CSTAOriginatedEvent” and move the calling party’s connection to the “CallControlConnection.ESTABLISHED” state while handling the “CSTADeliveredEvent” for that call. Hence, an extra event, namely, “CallCtlConnEstablishedEv” will be delivered to the JTAPI client applications if it was not already pushed for the calling party.

    .
  - A new API method, namely “getCSTACause(CSTACauseVariant cstaCauseVariant)”, has been introduced in the “ITsapiCallEvent” interface to retrieve the CSTA3 cause value from a JTAPI call event derived from a CSTA Held, CSTA Service Initiated, or CSTA Originated event.

    In the consultation scenario, this method will return the cause value “LucentEventCause.EC_CONSULTATION” for the connection initiated, established and held events. In the conference scenario (where conference is initiated by pressing the conference button), this method will return cause value “LucentEventCause.EC_CONFERENCE” for the connection initiated, established and held events. In the transfer scenario (where transfer is initiated by pressing the transfer button), this method will return cause value

"LucentEventCause.EC_TRANSFER" for the connection initiated, established and held events. In case there is no CSTA3 cause available for the event, this method will return the CSTA1 cause value associated with that event.

- In previous releases, if logging/tracing is "ON" in JTAPI and the "traceFileCount" variable is set, it is ignored and instead only two files are used.

  JTAPI logging is configurable through "TSAPI.PRO" file. The "traceFileCount" parameter instructs JTAPI about the number of trace files to be maintained before overwriting the existing. If "traceFileCount" parameter was configured in the "TSAPI.PRO" file, JTAPI used to ignore it and maintain only two trace files. JTAPI has been fixed to accept and maintain the exact number of trace files as is configured by the "traceFileCount" parameter in the "TSAPI.PRO" file.
- The Certificate Authority certificate file that is installed with the JTAPI Client has been updated to include an additional Avaya CA certificate for establishing secure connections to the AE Services server.

- **.NET**

  When under a heavy load or if a request took a while to complete, the ServiceProvider.dll was not properly handling a SynchronizationLockException which prevented the invokeID associated with a request from being mapped in the SDK to the issued request. As a result, the response from AE Services was not able to be returned, by the SDK, to the client.

- **Security**

  The following Red Hat Linux security issues have been incorporated into Release 6.1.1:

  1. [RHSA-2011:0004-01] Important: kernel security, bug fix, and enhancement update
  2. [RHSA-2011:0013-01] Moderate: wireshark security update
  3. [RHSA-2011:0025-01] Low: gcc security and bug fix update
  4. [RHSA-2011:0027-01] Low: python security, bug fix, and enhancement update
  5. [RHSA-2011:0170-01] Moderate: libuser security update
  6. [RHSA-2011:0180] pango security update
  7. [RSHA-2011:0197-01] Moderate: postgresql security update
  8. [RSHA-2011:0199-01] Important: krb5 security update
  9. [RHSA-2011:0346-01] Moderate: openldap security and bug fix update
  10. [RHSA-2011:0370-01] Moderate: wireshark security update
  11. [RHSA-2011:0376-01] Moderate: dbus security update
  12. [RHSA-2011:0412-01] Important: glibc security update

- **SIP**
  In previous releases, when using 3rd party call control to make a direct agent call to a busy agent on a SIP endpoint, the call would drop. This issue has been resolved.

- **SNMP**
  The values returned by SNMP GET commands for the amount of memory associated with the DMCC Service (avAesDmccUsedMemory.0, avAesDmccFreeMemory.0, and avAesDmccMaxMemory.0) were incorrectly calculated.

- **TSAPI Client Libraries and SDKs**
  - The Certificate Authority certificate file that is installed with the TSAPI Client has been updated to include an additional Avaya CA certificate for establishing secure connections to the AE Services server.

  - When installing either the TSAPI Windows Client or the TSAPI Windows SDK on a 64-bit version of Windows, the Setup program no longer allows the software to be installed in a subfolder of the 64-bit Program Files folder (typically "C:\Program Files\"). If a subfolder of the 64-bit Program Files folder is selected, then the Setup program will suggest installing the software in the corresponding subfolder of the 32-bit Program Files folder (typically "C:\Program Files (x86)\").

  - When the AE Services 6.1 TSAPI Windows Client is installed on a 64-bit version of Windows, in some scenarios the shortcut "Start | All Programs | Avaya AE Services | TSAPI Client | Edit TSLIB.INI" may point to the wrong location. For AE Services 6.1.1, this issue has been fixed.

  - When the AE Services 6.1 TSAPI Windows Client is installed on a 64-bit version of Windows, the shortcuts for "Apache Software Foundation Notice" and "Apache Software Foundation Notice" may not work correctly. For AE Services 6.1.1, this issue has been fixed.

  - The Setup program for the TSAPI Windows Client provides a dialog box for updating the list of AE Services Servers in the TSLIB.INI file. Prior to AE Services 6.1.1, the "Delete" button on this dialog box did not remove the selected entry from the TSLIB.INI file.

  - Prior to AE Services 6.1.1, if two different threads of a TSAPI application invoked acsOpenStream() at the same time, the TSAPI Windows Client library could cause the application to crash.

  - Prior to AE Services 6.1.1, the TSAPI Spy program did not always update the Streams List when a stream was closed.

- Prior to AE Services 6.1.1, the TSAPI Spy program could crash if the trace file name was changed while the “Log to File” option was enabled.

- Prior to AE Services 6.1.1, the TSAPI Exerciser program that is included with the TSAPI Windows SDK did not display the User to User Information (UUI) that was included in the private data accompanying a cstaClearConnection() service request.

- For AE Services 6.1.1, logic has been added to the TSAPI Linux Client library to release additional resources before exiting.

- **TSAPI Service:**
  - Beginning with AE Services 6.1.1, the TSAPI Service has been enhanced to reduce the number of ASAI requests sent to CM for call scenarios involving external parties.

  - Prior to AE Services 6.1.1, the TSAPI Service did not provide consistent field values in CSTA Unsolicited events for Automatic Callback Call scenarios where the called party was a local station extension.

  - Prior to AE Services 6.1.1, the TSAPI Service did not provide the correct sequence of CSTA Unsolicited events for calls that were treated by a converse vector step.

  - In AE Services 6.1, there was a TSDI memory leak in the TSAPI Service when processing ASAI Call Redirected events. As a result, the TSAPI Service would eventually activate flow control and would stop accepting service requests. This issue has been resolved in AE Services 6.1 Super Patch 2 and in AE Services 6.1.1.

  - Prior to AE Services 6.1.1, the TSAPI Service did not always report the correct value for Total TSDI Memory in Use. (This value can be viewed through the AE Services Management Console by selecting “Status | Status and Control | TSAPI Service Summary” and then clicking the “TSAPI Service Status” button.)

  - Prior to AE Services 6.1.1, the TSAPI Service did not always provide the correct sequence of CSTA Unsolicited events for Direct-Agent Call scenarios where the calling device in the Direct-Agent Call service request is a logical agent ID and the resulting call is queued.

  - Prior to AE Services 6.1.1, the Single Step Transfer Call service did not provide trunk information in the private data accompanying the CSTA Delivered events for the transferred called.

- Prior to AE Services 6.1.1, the Single Step Transfer Call service did not release all of its resources in some failure scenarios. As a result, subsequent attempts to invoke the Single Step Transfer Call service could fail with error Resource Busy.

- Prior to AE Services 6.1.1, the TSAPI Service could stop processing requests for a station if an application issued a Consultation Call service request for the station immediately after issuing a Hold Call service request for the station.

- Prior to AE Services 6.1.1, in some cases the TSAPI Service would provide the wrong Connection ID Device ID Type (STATIC_ID instead of DYNAMIC_ID) for the dropped connection in a CSTA Connection Cleared event.
- Prior to AE Services 6.1.1, in some cases the TSAPI Service would provide the wrong Device ID Type (IMPLICIT PUBLIC instead of EXPLICIT PRIVATE LOCAL NUMBER) for the agentDevice in a CSTA Logged On or CSTA Logged Off event. This could occur if the agent extension number was seven digits or more and the agent extension number was not being monitored.

- For AE Services 6.1.1, logic has been added to the TSAPI Service to release additional resources before exiting.

- Prior to AE Services 6.1.1, the TSAPI Service message tracing facility did not provide the device ID type for dynamic device IDs.

- **WEB OAM**

  The field “Minimum acceptable password length (PASS_MIN_LEN)” on page “Security | PAM | Global Password Aging” was never used as a parameter to validate the minimum password length. The field “Minimum acceptable password length (PASS_MIN_LEN)” on page “Security | PAM | Global Password Aging” has been removed from OAM. To enforce minimum password length functionality, use the “Minimum length of a new password (minlen)” field from the “Security | PAM | PAM Module” page.