R3.1.3 Application Enablement Services Software Only and Bundled Server Release Notes

April 2007

INTRODUCTION

This document introduces the latest release of Application Enablement (AE) Services (Release 3.1.3), and describes important notes and known issues.

Version

Server Release
ISO 48-3

IMPORTANT NOTES

This release of the AE Services is compatible with Communication Manager 3.x, and 4.0.

Release History:

Date	Build	Change(s)
02/06	33-1	General Availability R3.1
05/06	43-2	General Availability R3.1.1
10/06	46-5	General Availability R3.1.2
04/30	48-3	General Availability R3.1.3

KNOWN ISSUES AND WORKAROUNDS

- **AE SERVICES R3.0/R3.0.1 TO R3.1.3 – BUNDLED SERVER ONLY**

  When upgrading the Bundled Server from the 3.0 release to the 3.1.3 release, an additional step must be taken to create the default server web pages for AES.

  Once the upgrade is complete and made permanent, issue the following command:

  rpm -ivh --force /var/disk/rpms/mvap-tomcatconfig-3.1.746-6.noarch.rpm

- **BROWSER ISSUE WITH AUTO-COMPLETE**

  For security reasons, the html input auto-complete feature is now disabled by default. Once R3.1.3 is installed, the customer must change their browser settings to disable the browser's Password Management feature. Follow the steps that apply to the browser you are using.

  For IE: Select **Tools -> Internet Options -> Content -> Auto Complete.** The Option "**User names and passwords on forms**" should be unchecked, and if this option was previously selected, then select the button "**Clear Passwords**" as well. **Select OK** on each screen.

  For Firefox: Select **Edit -> Preferences -> Privacy -> Saved Passwords.** The Option "**Saved Passwords**" should be unchecked, and if this option was previously selected, then select the button "**Clear**" as well. Select **OK** on each screen.

- **INSTALLATION NULL POINTER EXCEPTIONS**

  When the MVAP Service is started for the first time, a "java.lang.NullPointerException" is printed twice. This happens when the Alarm and Log Web Services are deployed. Both services are deployed correctly and work normally even though the exceptions are triggered. Please ignore the "java.lang" null pointer exceptions.

- **HTTP ISSUE**

  When attempting to access the OAM pages, you are automatically switched to use https instead of the regular insecure http protocol. This may cause a problem in which the user is denied access to the tomcat server. The user will see the following error message:

Access Denied (connect_method_denied)

Your request attempted a CONNECT to a port "8443" that is not permitted by default.
This is typically caused by an HTTPS URL that uses a port other than the default of 443.
For assistance, contact your network support team.

Solution:
In order to resolve this issue, the user must turn off the browser's proxy settings or include the IP address or the DNS name of the AE Services server in the "**Proxy Exception's box**".

For IE 6 users, click on "**Tools -> Internet Option -> Connections -> LAN Settings -> Advanced**". In the "**Exception box**", enter the full IP address or the DNS root (whichever you use) of the AE Services server.

For Firefox users, click on "**Tools -> Options -> General -> Connection Settings"** (for Linux version, click on **"Edit -> Preferences -> General -> Connection Settings**"). In the "**No proxy For**" box, enter the full IP address or the DNS root (whichever you use) of the AE Services server.

For Mozilla users, your exception box is in the following location: "**Edit -> Preferences -> Advanced -> Proxies**". In the "**No proxy For**" box, enter the full IP address or the DNS root (whichever you use) of the AE Services server.

- **PROCESS TO CHANGE THE SERVER IP ADDRESS**

  If the IP address of an AE Services server is changed without stopping the server, or if the IP address is changed and then an attempt is made to set the new address through the web pages without stopping the server service (which is using the connection), an error message will be displayed. The error message will appear on the Local IP web page and indicate that the database entry for the IP address does not match the IP address configured on the server. The proper procedure to change the IP address is as follows:

  1. Stop the AE Services server

  2. Update /etc/hosts file with the new IP address

  3. Update CTI OAM > Administration > Local IP with the new IP address. The page should be submitted even if it shows "ANY".

  4. Start the AE Services server

ISSUES RESOLVED FROM THE PREVIOUS RELEASE

- **SECURITY UPDATES/VULNERABILITIES ADDRESSED:**

The following are Security Updates and Vulnerabilities addressed in this release:

- Security Update as per RHSA-2005:527 & RHSA-2005-550: Security Vulnerability, openssh rpm update.
- Security Update: Security Vulnerability, apache http server TRACE debug method enabled.
- Security Update as per RHSA-2007:0064-01: Postgresql security update.
- Security Vulnerability: SQL Injection may be possible
- Security Vulnerability: Directory Listing
- Security Vulnerability: Java Runtime Error Message
- RHEL Update: update DST rpm – Western Australia DST change Updated time zone date file to the latest one (tzdata-2006m-3.el3.noarch.rpm) in RHLE3..

- **TSAPI FAULTED IN MEMORY**

The TSAPI Service process could encounter a buffer overflow condition that was not handling properly. The fix allows TSAPI process to properly handle a buffer overflow condition.

- **TSAPI SERVICE G3PD DRIVER FAULTED**

A memory fault due to a race condition was addressed. The race condition occurred when a TSAPI client sent a CSATMonitorStop request immediately after the TSAPI service had ended the monitor on its own because Communication Manager (CM) aborted the ASAI association.

- **TSAPI INTERMITTENTLY DID NOT CLEAR CONFERENCE CALLS**

TSAPI service intermittently did not send back CSTAClearCallConf message for CSTAClearCall request.

- **G3PD ISSUES RESOLVED**

  - The system crashed when it received a CSTAClearCall request from a client with a Null Party ID.

  - G3PD faulted when TSAPI trace was turned on in the tracemask file. The G3PD could fault while formatting trace messages whose data values contained certain character sequences, such as “%s”.

  - G3PD incorrectly removed monitors in certain transfer scenarios. G3PD removed internally established monitors during transfers.

  - Intermittently, CSTAClearCall Event returned Call ID “0”.

  - G3PD's Sanity Thread sometimes created a loop performing continuous Value Queries.

  - The CSTA Silent Monitor Event Cause (31) will now have priority over the CSTA Transfer Event Cause. In a scenario where a call has a service observer and the call has been transferred, events will now contain the CSTA Silent Monitor Event Cause instead of the CSTA Transfer Event Cause.

- **DUPLICATE DELIVERED EVENTS**

  When a station with a coverage path to a station was monitored and sim-bridging was enabled on CM, duplicate Delivered events were reported. This will no longer occur. A single set of events will be sent under these conditions.

- **DMCC LISTENING INTERFACE**

  The DMCC Listening Interface issue resolved the Client IP connectivity to either listen on all NIC’s using the ANY option or a specific NIC. It was subsequently discovered that a side effect of the change prevented applications running locally on the server from connecting on the 127.0.0.1 address when a specific Client Connectivity IP address was specified. If the well known public IP address of the server was used, then the local application was able to successfully establish a connection. In order to resolve this issue, the 127.0.0.1 address will be enabled by default whenever the ANY option is not specified for Client Connectivity.

- **DMCC CLIENT CONNECTIVITY**

  It was discovered that the OAM setting from the Local IP screen for DMCC Client Connectivity was not affected by a configuration change. Basically when a user changed the Client Connectivity setting from "ANY" to a specific IP address listed in the drop-down menu on the Local IP Screen, DMCC continued to connect using the "ANY" option. The problem was related to the fact that the property was not passed to DMCC. As a result, the "ANY" value was used by default. The fix for this issue involved a modification to allow the Client IP connectivity property to be read by DMCC to determine which NIC to use to establish a client side listener socket.

- **DMCC RACE ISSUE RESOLVED**

  There was a race condition in the DMCC Service. While one thread was cleaning up a session, another thread was getting a device ID. The device ID request succeeded, and after that the ID could not be released or acquired by a new session.

- **SAMP PPP – BUNDLED ONLY**

  Intermittently, the upgrade wizard did not preserve the existing PPP addresses for the client and server. The upgrade caused the PPP address to revert back to the default settings.

- **ROOT AND CUST ACCOUNTS NOW PRESERVED – BUNDLED ONLY**

  The Bundled Server upgrade wizard was enhanced to preserve the root and cust accounts during upgrades.

- **SYSTEM MANAGEMENT SERVICE**

  System Management Service WSDL was enhanced to remove the login prompt which impeded dynamic lookup of the WSDL.

- **RPM OWNERSHIP CHANGE**

  The mvap-platform RPM changed all ownership on/opt/mvap/* after Patch 1 was applied. This affected the System Management Service. In this release, proper ownership has been identified for each RPM in the /opt/mvap/ directory.

- **SDB SYNCHRONIZATION**

  AES was unable to perform synchronization between the SDB and CUS data store. The root cause stemmed from the ability to properly delete a user from the CUS data store. Once the system is in this state CUS will be unable to add or delete any additional users. The deletion issue has been resolved.

- **TSAPI CRASH**

  Certain flags used by the ASAI library are now properly set to prevent the TSAPI service from crashing during shutdown.

- **G3PD CORE DUMP**

  The system crashed due to a bad format string in an error condition.

- **OAM LINK STATUS CONNECTIONS**

  When displaying link status information through OAM Status and Control, the Switch Connection Summary Screen was not always showing the correct status after making a change to the link. It now shows correct status after a change to the link.

- **AES UPDATE COMMAND**

  AES update command has been enhanced to handle the installation of rpms that have dependencies on other rpms.

- **DAY LIGHT SAVINGS TIME ISSUE**

  JDK Time Zone information was added to the R3.1.3 install script to correct a time discrepancy in the OAM after Day Light Savings occurred.

- **DATECONFIG**

  Dateconfig has been enhanced to automatically stop and restart the NTP service.