Avaya Aura® System Platform R6.0.3 Service Pack Release Notes

Issue 1.9
April 2013

INTRODUCTION

This document introduces the Avaya Aura® System Platform Release 6.0.3 Service Pack and describes known issues and the issues resolved in this release.

WHAT'S CHANGED IN SYSTEM PLATFORM 6.0.3

- **Native SNMPV2 alarming support** has been added to enable System Platform to raise alarms through any SAL gateway without the need to run an embedded SAL gateway. Multiple SNMP trap destinations are supported allowing alarms to be simultaneously sent to one or more SAL gateways, System Manager, and one or more customer Network Management Systems.

  Users have the capability to add, edit, and remove SNMP trap destinations through the 'SNMP Trap Receiver Configuration' page of WebConsole. Users can also disable/re-enable the embedded SAL gateway through the 'SAL Gateway Management' page of the WebConsole.

  In prior releases, System Platform relied on the built-in customer NMS alarming support in the SAL Gateway to deliver alarms to a customer NMS. Now System Platform can send alarms directly to the customer NMS by adding the NMS as a trap destination in the 'SNMP Trap Receiver Configuration' page.

- **Multiple DVD Support**
  Multiple DVD Support has been added to System Platform in order to provide a local template installation method for templates that span multiple DVDs due to size.

  In order to use this new functionality, perform the following actions:
  1. Insert a CD/DVD and select 'View CD/DVD'.
  2. Disk contents will be displayed. The WebConsole will, by default, select all files in the CD/DVD to be copied. The user must deselect those files that do not need to be copied. Note that the GUI will not deselect children when a directory is deselected, and that all files that are selected will be copied, regardless if the parent directory is copied or not. Once the final selection has been made, select 'Copy Files'.

3. The WebConsole will copy the selected contents into the 'cdrom' subdirectory of /vsp-template in the CDOM. ***If files with the same name already exist, they will be overwritten***. A new panel will appear with the list of the labels of the disks from which files have been copied.
4. Repeat Steps 1 through 3 until all CD/DVDs are copied.
5. When all desired files have been copied, the user will need to provide the final location for the files. While CD/DVDs have been loading, the WebConsole has collected the names of all ovf files present on the disks and filled in the dropdown box. At this point, the user can make a new selection, or type a new name. The text in this box will be the final subdirectory under /vsp-template in which the files will be moved. If the field is left blank, the files will be copied directly under /vsp-template.

- **WebLM Address Configuration Support** has been added to the 'System Configuration' page.
  - If the user changes the address elements and the resulting address is not the local WebLM server, the system will stop the local WebLM application. If the local WebLM application has been stopped, a Tomcat reboot will re-start it.
  - If the user reverts back to the original values, the local WebLM application will be re-started.
  - If the user leaves the values blank, the WebConsole will reset the values to the original defaults.

- **Updated WebLM Certificate**
  The current certificate used for https access to WebLM expires on March 31st, 2011. A fix has been included in this service pack with an updated certificate that will expire in September of 2025. When System Platform updates the WebLM certificate, those guest VMs that are accessing WebLM in System Platform's CDOM may need to update their keystores in order to accept this certificate.

SOFTWARE RELEASE VERSIONS

Application	File Name
Avaya Aura® System Platform R1.1	vsp-1.1.0.0.10.iso
Avaya Aura® System Platform R1.1.1	vsp-1.1.1.0.2.iso
Avaya Aura® System Platform R1.1.1.4.2	vsp-patch-1.1.1.4.2.noarch.rpm
Avaya Aura® System Platform R1.1.1.7.2	vsp-patch-1.1.1.7.2.noarch.rpm
Avaya Aura® System Platform R1.1.1.9.2	vsp-patch-1.1.1.9.2.noarch.rpm
Avaya Aura® System Platform R1.1.1.93.2	vsp-patch-1.1.1.93.2.noarch.rpm
Avaya Aura® System Platform R1.1.1.94.2	vsp-patch-1.1.1.94.2.noarch.rpm
Avaya Aura® System Platform R6.0	vsp-6.0.0.0.11.iso
Avaya Aura® System Platform R6.0.0.1.11	vsp-patch-6.0.0.1.11.nonarch.rpm
Avaya Aura® System Platform R6.0.1	vsp-6.0.1.0.5.iso
Avaya Aura® System Platform R6.0.2	vsp-6.0.2.0.5.iso
Avaya Aura® System Platform R6.0.2.1.5	vsp-patch-6.0.2.1.5.noarch.rpm
Avaya Aura® System Platform R6.0.2.3.5	vsp-patch-6.0.2.3.5.noarch.rpm
Avaya Aura® System Platform R6.0.3	vsp-6.0.3.0.3.iso

Application	File Name
Avaya Aura® System Platform R6.0.3.1.3	vsp-patch-6.0.3.1.3.noarch.rpm
Avaya Aura® System Platform R6.0.3.3.3	vsp-patch-6.0.3.3.3.noarch.rpm
Avaya Aura® System Platform R6.0.3.4.3	vsp-patch-6.0.3.4.3.noarch.rpm
Avaya Aura® System Platform R6.0.3.6.3	vsp-patch-6.0.3.6.3.noarch.rpm
Avaya Aura® System Platform R6.0.3.7.3	vsp-patch-6.0.3.7.3.noarch.rpm
Avaya Aura® System Platform R6.0.3.9.3	vsp-patch-6.0.3.9.3.noarch.rpm
Avaya Aura® System Platform R6.0.3.10.3	vsp-patch-6.0.3.10.3.noarch.rpm

Release History:

Date	Build	Change(s)
August 2009	1.0.0.1.12	Controlled Introduction R1.0
November 2009	1.1.0.0.10	General Availability R1.1
February 2010	1.1.1.0.2	Service Pack R1.1.1
February 2010	1.1.1.4.2	Service Pack Patch R1.1.1.4.2
April 2010	1.1.1.7.2	Service Pack R1.1.1.7.2
June 2010	1.1.1.9.2	Service Pack Patch R1.1.1.9.2
June 2010	6.0.0.0.11	General Availability R6.0
August 2010	6.0.0.1.11	Patch R6.0.0.1.11
August 2010	6.0.1.0.5	Service Pack R6.0.1.0.5
August 2010	1.1.1.93.2	Service Pack Patch R1.1.1.93.2
November 2010	1.1.1.94.2	Service Pack Patch R1.1.1.94.2
November 2010	6.0.2.0.5	Service Pack R6.0.2.0.5
November 2010	6.0.2.1.5	Service Pack Patch R6.0.2.1.5
February 2011	6.0.2.3.5	Service Pack Patch R6.0.2.3.5
February 2011	6.0.3.0.3	Service Pack R6.0.3.0.3
April 2011	6.0.3.1.3	Service Pack Patch R6.0.3.1.3
August 2011	6.0.3.3.3	Service Pack Patch R6.0.3.3.3
October 2011	6.0.3.4.3	Service Pack Patch R6.0.3.4.3
February 2012	6.0.3.6.3	Service Pack Patch R6.0.3.6.3
March 2012	6.0.3.7.3	Service Pack Patch R6.0.3.7.3
June 2012	6.0.3.9.3	Service Pack Patch R6.0.3.9.3
January 2013	6.0.3.10.3	Service Pack Patch R6.0.3.10.3

Upgrades

Upgrades to R6.0.3 are supported from the following releases:

RELEASE	MINIMUM REQUIRED VERSION
R1.1.1	R1.1.1.0.2 + Patch 1.1.1.xx.2
R6.0	R6.0.0.0.11 + Patch 6.0.0.x.11
R6.0.1	R6.0.1.0.5 + Patch 6.0.1.x.5
R6.0.2	R6.0.2.0.5 + Patch 6.0.2.x.5

Check for the latest System Platform patch (certified by the application/template) prior to upgrading to R6.0.3.

Resolved Issues and Enhancements

1. High Availability setup failed if special characters were in the admin password.

2. Added checks for valid IP addressing and netmasks during installation to ensure the av-public bridge is created.

3. In previous releases, NICs added after installation were not detected.

4. The ‘raid_status’ command supports the H200 RAID controller on the Dell R610.

5. In R6.0.2, avrollback upgrade may not have automatically redirected users back to the login page. This issue has been resolved in R 6.0.3.

6. In R6.0.X, bonding fail-back takes five minutes or more when the port was connected to a separate layer-2 switch. The bonding in R6.0.3 has been improved.

7. During an upgrade, High Availability configurations are checked and reconfigured (if necessary) in R6.0.3.

8. Added backup sets for ssh host keys to support restore operations on a replaced server.

9. In previous releases, CDOM collected broadcast logs from other devices not intended for CDOM resulting in false alarms. This issue has been resolved.

10. In previous releases, installation of a template patch was delayed when the DNS was unreachable.

11. Improved patch installation timeout handling and user interface error messaging.

12. Reduced ‘getlogs’ output file size by implementing the higher data compression algorithm, bzip2.

13. Improved the password change procedure on the help page for ‘password rules’ from the WebConsole.

14. The CPU usage CVS file was missing the maximum and average values in the ‘Server Management’ | ‘Performance Statistic’ section of the WebConsole.

15. Changing Domain-0 hostnames via the ‘Network Configuration’ page resulted in duplicate entries in the ‘/etc/hosts’.

16. Kernel security and bug fix updates:
    - RHSA-2011:00004-01: See https://rhn.redhat.com/errata/RHSA-2011-0004.html for details.

    - RHSA-2010:0839-01:
        - A NULL pointer dereference flaw was found in the io_submit_one() function in the Linux kernel asynchronous I/O implementation. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2010-3066, Moderate).

        - A flaw was found in the xfs_ioc_fsgetxattr() function in the Linux kernel XFS file system implementation. A data structure in xfs_ioc_fsgetxattr() was not initialized properly before being copied to user-space. A local, unprivileged user could use this flaw to cause an information leak. (CVE-2010-3078, Moderate).

        - The exception fixup code for the __futex_atomic_op1, __futex_atomic_op2, and futex_atomic_cmpxchg_inatomic() macros replaced the LOCK prefix with a NOP instruction. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2010-3086, Moderate).

        - A flaw was found in the tcf_act_police_dump() function in the Linux kernel network traffic policing implementation. A data structure in tcf_act_police_dump() was not initialized properly before being copied to user-space. A local, unprivileged user could use this flaw to cause an information leak. (CVE-2010-3477, Moderate).

        - A missing upper bound integer check was found in the sys_io_submit() function in the Linux kernel asynchronous I/O implementation. A local, unprivileged user could use this flaw to cause an information leak. (CVE-2010-3067, Low).

    - RHSA-2010:0839-01:
        - A NULL pointer dereference flaw was found in the io_submit_one() function in the Linux kernel synchronous I/O implementation. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2010-3066, Moderate).

        - A flaw was found in the xfs_ioc_fsgetxattr() function in the Linux kernel XFS file system implementation. A data structure in xfs_ioc_fsgetxattr() was not initialized properly before being copied to user-space. A local, unprivileged user could use this flaw to cause an information leak. (CVE-2010-3078, Moderate).

- The exception fixup code for the __futex_atomic_op1, __futex_atomic_op2, and futex_atomic_cmpxchg_inatomic() macros replaced the LOCK prefix with a NOP instruction. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2010-3086, Moderate).

- A flaw was found in the tcf_act_police_dump() function in the Linux kernel network traffic policing implementation. A data structure in tcf_act_police_dump() was not initialized properly before being copied to user-space. A local, unprivileged user could use this flaw to cause an information leak. (CVE-2010-3477, Moderate).

- A missing upper bound integer check was found in the sys_io_submit() function in the Linux kernel asynchronous I/O implementation. A local, unprivileged user could use this flaw to cause an information leak. (CVE-2010-3067, Low)

17. Pluggable Authentication Modules Security Update – RHSA-2010:0819-01.
Pluggable Authentication Modules (PAM) provide a system whereby administrators can set up authentication policies without having to recompile programs that handle authentication.

- It was discovered that the pam_namespace module executed the external script namespace.init with an unchanged environment inherited from an application calling PAM. In cases where such an environment was untrusted (for example, when pam_namespace was configured for setuid applications such as su or sudo), a local, unprivileged user could possibly use this flaw to escalate their privileges. (CVE-2010-3853).

- It was discovered that the pam_mail module used root privileges while accessing users' files. In certain configurations, a local, unprivileged user could use this flaw to obtain limited information about files or directories that they do not have access to. (CVE-2010-3435).

- It was discovered that the pam_xauth module did not verify the return values of the setuid() and setgid() system calls. A local, unprivileged user could use this flaw to execute the xauth command with root privileges and make it read an arbitrary input file. (CVE-2010-3316).

18. The following instructions only apply to new installations of Avaya Aura® Conferencing, Avaya Aura® Messaging, Avaya Session Border Controller Solution, 1x Client Enabled Services 6.1, and Avaya Aura® Solution for Midsize Enterprise templates on System Platform R6.0.3. Secure Access Link (SAL) models must be added by implementing the following instructions:

    1. SSH into CDOM as an admin user and switch to root user.
    2. cd /opt/avaya/SAL/gateway/upgradeScripts
    3. /bin/sh upgradeSALModels.sh
    4. Output of the script will be echoed to CDOM's console and can be used to check status of model upgrade process. The upgrade process will take approximately 5 minutes.

    Performing the above steps is strongly recommended before configuring SAL on new System Platform installations where the SAL model may not be present in the solution template.

Known Issues and Workarounds

1. **Applying System Platform patches on High Availability (HA) failover systems.**
   Unless the release notes for a patch specify otherwise, apply the patch on both machines if the patch includes a Domain-0 patch. Always check the patch release notes for the detailed information on how to apply the patch on HA systems. ***On a HA failover system, stop HA and remove the HA configuration before applying the patch and apply it on the System Platform Management Consoles of both the primary and secondary nodes*.**

   For any operation that requires HA to be stopped (platform upgrade, template upgrade and patch application), the stop HA should be followed by the removal of the HA configuration. The user may then configure and start HA after the operation is completed.

   Failure to remove HA before performing a platform upgrade could lead to an incorrect configuration of the system and the inability to start HA. This condition could lead to the necessity of re-installing System Platform on the affected systems.

2. **When configuring HA after applying System Platform patch 6.0.3.3.3, the configuration will fail with the following error displayed on the WebConsole:**

   "Failover configuration failed for IP: 192.168.xx.xx. Message:"

   The workaround is to apply System Platform patch 6.0.3.4.3 or later before configuring HA. Note that removal of patch 6.0.3.3.3 will not resolve the problem. Patch 6.0.3.4.3 or later must be installed. If patch 6.0.3.3.3 has not been installed, then HA can be configured (prior to installing 6.0.3.3.3)."

3. **HA failover systems, 'hosts allow' and 'hosts deny' settings on the 'Security Configuration' page on each node must permit ssh access from the other node's CDOM and Domain-0.**

4. **An upgrade from R1.1.1 to 6.0 in a HA configuration, CDOM takes approximately 15 minutes.**
   During an upgrade from R1.1.1 to R6.0, even though the platform upgrade status page shows an estimated time of 1 minute and 50 seconds, in real time it takes approximately 15 minutes for the reboot to finish.

5. **When HA is running, changes made in the “User Administration” section of the WebConsole may not be replicated.**
   When HA is started, changes made in the "User Administration" section of the WebConsole will be saved on the active server (e. g “server A”) but will not be replicated to the standby server (e. g “server B”). As a result, after failover to “server B”, all changes will appear to be lost. They are not lost, just unavailable since the changes are only stored on “server A”. So, failover back to “server A” appears to restore those changes. To avoid this issue, immediately after starting HA, do a single failover. This will start replication of the user administration information between the active and standby servers. Replication will continue through all subsequent failovers.

6. **HA configuration may fail if server upgrade histories are not identical.**
   HA configuration may fail if the server upgrade histories are not identical. The upgrade history of the servers can affect the disk free space on a server. As a result, if the server that is to become the standby has a longer upgrade history than the server that is to become the active, then it is possible for the disk free space on two otherwise identical machines to appear different. In this case, the user will see an error message during HA configuration similar to the following:

   Failover configuration failed due to different component versions / parameters found on cluster nodes: Field DISK_FREE_GB Local (preferred) value: XXX Remote (standby) value: YYY The value YYY will be less than XXX

   The best fix for this issue is to reinstall System Platform on the standby server so it has an identical upgrade history as the active. If this resolution is not possible or not practical, then simply reinstalling the standby server with the current System Platform version will fix the issue.

7. **Static routes are not replicated when HA is running.**
   If a static route is added to the network configuration, that route is only saved to the currently active server. If HA is running and a new static route is needed do either of the following two sequences of operations:
   1. Stop HA, add the route, and start HA; or
   2. Add the route, switch over, and add the route again.

8. **From the WebConsole, Static Routes can be added to Public Bridge (av-public) only.**

9. **Network configuration is not restored when restore is run from the System Platform WebConsole**.
   Do not use the restore functionality to make networking changes. This should be performed from the System Platform WebConsole ‘Network Configuration’ page. Ensure the network settings are correct before performing a restore.

10. **To avoid an IP address conflict during installation, do not configure Domain-0's eth0 subnet to 172.20.10.0/32 or any superset.**
Due to a bug in a post-installation module, avprivate will not pick up the subnet the installer selected. Instead, avprivate will use the subnet 172.20.10.0/24. If eth0 is configured to use subnet 172.20.10.0/32 or any superset of the subnet, there will be a IP address conflict. Reinstallation of System Platform is required to resolve the issue.

11. **Configure the System Platform internal network 'avprivate' before template installation.**
Before installing a template, check the 'Network Configuration' page on the System Platform Management Console (select 'Server Management' | 'Network Configuration') to view the addresses allocated on the bridge named 'avprivate'.

    System Platform creates an internal, private bridge that allows virtual machines to communicate with each other. This private bridge does not have any connection to the user's LAN. During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the 'System Domain Network Configuration' screen. However, it is still possible that the addresses selected conflict with other addresses in the network. Since this private bridge is not connected to the user's LAN, this address conflict could result in the failure of System Platform or an installed template to route packets correctly. The internal routing tables might not differentiate between the private bridge and the user's LAN, causing an application to direct packets to some host on the user's LAN rather than to another application within the System Platform server that has that same IP address on the private bridge.

    If the IP address for Domain-0's interface on 'avprivate' is changed (which appears in the bridge section of the "Network Configuration" page) or for CDOM's interface on 'avprivate' (which appears under CDOM in the Group by Domain section), the addresses must be consecutive with Domain-0's address 1 less than CDOM's (i.e., if CDOM's IP address for its interface on 'avprivate' is 172.20.30.5, then Domain-0's must be 172.20.30.4). Also, the netmask for Domain-0's interface on avprivate must be the same as the netmask for CDOM's interface on 'avprivate' (i.e., if one is changed, the other must change).

    In the event that there is a conflict in the network with the private IP address range, some functions may fail to work properly in System Platform and the installed template. For example, the System Platform WebConsole may be inaccessible from a system that has an IP address in conflict with the private address range.

    Another example includes an IP phone that registers with Communication Manager with the same IP address as Domain-0's or CDOM's address on 'avprivate'. Packets targeted for the phone might actually instead go to Domain-0 or CDOM.

12. **Do not click on the wrench icon to manage an individual virtual machine when logged in via SAL.**
    When logged into the CDOM WebConsole (Virtual Machine Management) to manage any of the virtual machines, do not click on the wrench icon to manage the individual virtual machine (if logged in through SAL) due to security host containment requirements.

13. **Changing the password for the first time while logged into WebLM causes Tomcat catalina.out to error and lists exceptions.**
    This issue resides in WebLM standalone releases (all releases up to 4.5.5). The issue does not impact WebLM functionality.

14. **Upper case hostnames on CDOM are temporarily switched to lower case during an upgrade.**
    If CDOM is given a hostname containing upper case letters, after an upgrade, the CDOM hostname will appear in all lower case letters until CDOM is rebooted. This does not affect any functionality of the system, only the display of the hostname.

15. **The CDOM fully qualified hostname in /etc/hosts is not correct after being renamed from the WebConsole.**
    If a user renames the CDOM hostname using an extension of the old hostname, the CDOM hostname in /etc/hosts hosts file will be misconfigured as shown in the following example:

    Old hostname: hostname.example.com
    New hostname: hostname-2.example.com

    Resulting misconfigured new fully qualified hostname in the /etc/hosts file:
    hostname-2-2.example.com

    When changing the CDOM hostname, do not use an extension of the existing hostname.

16. **System Platform only supports MII Monitoring for NIC Bonding.**
    Another monitoring mechanism, the ARP Monitoring method, doesn't work as expected. Additional information and discussions can be found at https://bugzilla.redhat.com/show_bug.cgi?id=584872

17. **The S8800 server operating system will hang when the remote connection BIOS setting is disabled.**
The S8800 servers will cause grub to hang during boot up if the 'remote connection' BIOS setting is disabled. The setting is enabled in the server BIOS version shipped from Avaya. However, it is disabled in the version shipped directly from IBM.

If the issue is encountered, perform the following steps:
1. Reboot the server and select 'F1 Setup' from the boot menu.
2. Select 'System Settings', then 'Devices' and 'I/O Ports'. Scroll down to the bottom to select 'Console Redirection Settings'.
3. Check the setting for 'Remote Console'. Set the setting to 'enable'.

18. **How to Add ALL:ALL in the Security Configuration Hosts Deny Lists Failover deployment case.**
When adding ALL:ALL in CDOM and Domain-0 hosts deny lists, following these steps:
1. Stop failover if it's running.
2. From the WebConsole, make sure ALL:ALL is NOT in any hosts deny lists on both primary and standby nodes.
3. Configure failover from the WebConsole if it has not been done.
4. ssh login as admin to the primary Domain-0, run "sudo /opt/avaya/ha/scripts/vspha status" to collect all three IP addresses used by primary node. These include the host address, crossover address and udom address. Similarly, login to the standby Domain-0 as admin to collect those three IP addresses used by standby node. Then on the WebConsole 'Security Configuration' page of both primary and standby nodes, add all six IP addresses collected into CDOM and Domian-0 'host allow lists' to allow ALL protocol access.
5. Make sure ALL:localhost is in CDOM hosts allow list on both primary and standby nodes from the WebConsole.
6. Put ALL:ALL into CDOM and Domain-hosts deny list from the WebConsole on both primary and standby nodes.
7. Start failover.

19. **Whitespaces are not allowed in the Solution Element ID (SEID) when configuring a managed device in the SAL user interface.**
When users configure the SEID for a managed device in the SAL Gateway UI, whitespaces are not allowed. The format specified in "Secure Access Link 1.8 Gateway Implementation Guide" (http://support.avaya.com/css/appmanager/public/support?_nfpb=true&_windowLabel=Product_1&Product_1_actionOverride=%2Fportlets%2Fproduct%2FleftNavigationAction) must be strictly followed to avoid errors.

20. **System Platform WebConsole will not be accessible if the disk becomes full.**

21. **Internet Explorer (IE) may not load pages when accessing the Management Console**
When accessing the Management Console page, IE (versions 7, 8 or 9) may display the following error: “Internet Explorer cannot display the webapp”, or it may stay within the current page instead of navigating to the selected page. This happens when a page cannot respond to IE within 30 seconds. The problem has been observed on some template installation/upgrade pages, on the HA configuration page and on the Network Configuration page. If IE is your preferred browser, consider applying the proposed solutions form the Microsoft Knowledge Base 181050 (http://support.microsoft.com/kb/181050).

22. **During a System Platform upgrade, the ‘Wait for User Input Link’ does not work all of the time.**
The workaround is to click on the ‘Home’ button and then click on the ‘Platform Upgrade waiting for user to commit’ button.

23. **System Platform alarms may be delayed slightly after upgrades or reboots.**
If the SAL agent has been shutdown because of a reboot or an upgrade it may create a backlog within the system log files that will need to be processed for alarms.

    To prevent overloading the system, the log file parsing is throttled. If an alarm condition occurs directly after a reboot or upgrade, it may take a several minutes for the alarm to be sent out from System Platform. Depending on the amount of data to be processed, this lag may last for an hour or more as the system catches up.

24. **Rollback of an upgrade may not redirect users to the login page automatically.**
If users want to rollback after they have upgraded their system from R1.1.0.x.x or R1.1.1.x.x system to R6.0.3 system, they may observe that they are never redirected to the Login Page. If this happens, they will have to key in the Login Page’s URL,https://<serverip or hostname>/webconsole, manually.

    If they have installed patch 1.1.1.94.2 onto their system, or their original system is any R6.0 system, they shouldn’t have this problem.

25. **During an upgrade, the VM restore completes, but the commit/rollback is not displayed until the 4-hour timeout is complete.**

26. **A backup set obtained from performing a backup on a particular version of System Platform cannot be used to restore to an older version of System Platform.**

27. **System Platform upgrades using a USB drive are not supported on a HP DL360G7.**
When used for System Platform upgrades, USB drives cause boot problems on the HP DL360G7. They may be used for application template upgrades, although, the USB drive must not be attached when the System Platform upgrade is performed.

28. **To avoid a non-maskable interrupt (NMI) after removing an Avaya Aura® Conferencing 6.0 template, please shutdown the Avaya Aura® Conferencing VMs before removing the template itself.**

System Platform R6.0.3 Service Pack Patches – *please ensure that the appropriate application template has approved the patch prior to installation*

1. **Avaya Aura® System Platform Patch 6.0.3.1.3**

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

   The patch will restart Tomcat, which will require the user to login to the WebConsole.

   MD5 Checksum: cb8a6b7dbe81411dd30610ff6df6cd7e

2. **Avaya Aura® System Platform Patch 6.0.3.3.3**

   This patch resolves the following issues:
   - Domain-0 memory leak due to Xen Libvirt

   The system will automatically restart the System Platform WebConsole.

   Patch 6.0.3.3.3 is a cumulative patch including updates from 6.0.3.1.3.

   MD5 Checksum: 2be76776d633425c4c56fb8b87bc8e3b

3. **Avaya Aura® System Platform Patch 6.0.3.4.3**

This patch includes the following resolutions and updates:

- RHSA-2011:0412-01 important glibc security update
- RHSA-2011:0507-01 moderate apr security update
- Avaya Services ASG logins failed if the LDAP server is down in System Platform
- Multiple watchdog alarms were sent after a BMC reset
- Using 'dom0' as the host name of Domain-0 caused /etc/hosts to lose critical entry dom0.vsp on subsequent hostname changes
- Backup Archive Manager webpage needed to be refreshed with each visit
- Tomcat keystore password resolution
- Tomcat webserver version was shown on the 404 error page
- A fan sensor in critical range on the S8800 server generated an alarm every 5 minutes
- High Availability (HA) could get into a state of continuous failovers. For example, each server in the HA pair has two power supplies inserted, but one power supply on each server has the power cord unplugged. The power supply sensor appeared as critical, so HA initiated a failover to the backup. After running for a few minutes on the newly active server, HA again found the critical power supply sensor and initiated another failover.
- Could not stop HA when the Public NIC of standby node was down
- Configuring or removing failover or initiating a manual failover of HA displayed '???vsp_reboot???' on the System Platform WebConsole HA page
- New static routes did not survive an HA switchover
- The avpublic bridge appeared to lockup when viewing a large file in a virtual machine when going through a tandem ssh connection through Domain-0
- Uploaded patch hangs without an error message if no space is on /vspdata
- Console Domain memory leak and unable to log onto Console Domain using the administrators account – caused by an unclosed ssh connection in the authentication module
- Prevent the Services port NIC events from alarming
- Suppress sending an alarm for "sdc: assuming drive cache: write through" message
- Suppress sending an alarm for "iSCSI daemon with pid=839 started!"
- System Platform still upgraded with an invalid Services VM hostname
- SAL part of restore failed on System Platform 6.0.3.1.3 in some conditions
- SAL SSL Certificate resolution on System Platform
- Banner added to present important platform upgrade notes to users
- Included a validation check of Services VM being in the same subnet as Domain-0 and Console Domain during a platform upgrade
- Restore operation resolved from a fresh install of 6.0.3.1.3 to a backup of patch 1.1.1.98.2
- Enabling IPv6 from the Network Configuration page resolved

The system will automatically restart tomcat following installation of the patch in order for the changes to take effect.

Patch 6.0.3.4.3 is a cumulative patch including updates from 6.0.3.1.3 and 6.0.3.3.3.

MD5 Checksum: 3f2d9a5a83c0f8f75c24e5039a352b8f

4. **Avaya Aura® System Platform Patch 6.0.3.6.3**

This patch includes the following resolutions and updates:

- RHSA-2011:1380-01 Critical java-1.6 0-openjdk Security Update
- RHSA-2011:1212-1 Important Red Hat Enterprise Linux 5.7 Kernel Security and Bug Fix Update
- RHSA-2011:1241-1 Moderate ecryptfs-utils Security Update
- SAL watchdog memory leak resolved
- Improved High Availability (HA) handling of changes to grub.conf in HA setup
- Administrator account information replicated between HA pairs
- Improved system monitoring of RAID battery power levels
- Cross Frame Scripting vulnerability fixed in System Platform login page
- Tomcat version upgraded to 6.0.33
- Openldap upgraded to version 2.4.26
- dhclient has been removed from Domain-0 in System Platform
- JRE version updated
- Use of SSLv2 ciphers disabled for the WebConsole and the WebLM server
- Added 32 bit RPMS to support LinuxShield installation
- Added support for the New Russian daylight savings rules
- Media Services dedicated NIC physical Ethernet port assignment corrected
- Resolved an occasional update problem when changing System Platform to a different IP network address range
- Resolved upgrades via CDROM not working
- Resolved upgrades via USB on the HP DL360G7 not working. NOTE: Do not leave the USB drive attached to the server when it is booting.
- Safeguard implemented to prevent patching while HA is sync'ing
- Increased validation checks when upgrading from R6.0.3.X.X to R6.2. The R6.2 Services VM hostname should not match other hostnames on the system.
- Templates can now be patched before they are committed allowing customers to evaluate the patch prior to committing
- Resolved an Avaya Services WebConsole login issue
- Optimized Domain-0 processing of XML to reduce CPU usage
- Optimized the System Platform upgrade process
- Resolved a GUI issue where validation errors would occasionally not be displayed
- Improved NTP sync and configuration
- Resolved a minor issue where deleting a template would require two attempts before succeeding

Application of this patch is service effecting.

The system (Domain-0, Console Domain and all Virtual Machines) will automatically restart following installation of the patch in order for the changes to take effect.

Patch 6.0.3.6.3 is a cumulative patch including updates from 6.0.3.1.3, 6.0.3.3.3 and 6.0.3.4.3.

MD5 Checksum: bb78713398d87ecce6691955b704f2bd

5. **Avaya Aura® System Platform Patch 6.0.3.7.3**

This patch includes the following resolutions and updates:

- After application of System Platform patch 6.0.3.6.3, the SAL Gateway user interface service will not start; therefore, the user is unable to access the SAL Gateway user interface to configure and administer SAL and its managed elements.

Application of this patch is service effecting.

The system (Domain-0, Console Domain and all Virtual Machines) will automatically restart following installation of the patch in order for the changes to take effect.

Patch 6.0.3.7.3 is a cumulative patch including updates from 6.0.3.1.3, 6.0.3.3.3, 6.0.3.4.3 and 6.0.3.6.3.

MD5 Checksum: 3b94e6ab7956c3c6928f4bf3e93e948a

6. Avaya Aura® System Platform Patch 6.0.3.9.3

Issues have been reported while using the network change page to change the system's IP addresses. An IP address change should NOT be attempted without consulting the compatibility matrix for information: https://downloads.avaya.com/css/P8/documents/100135000.

The following message is now displayed on the network change page:

WARNING

IP address changing is NOT supported by all templates. Please check the System Platform Compatibility Matrix.

Attempting to change IP address on a template that does not support it will result in the system having to be re-installed.

When upgrading high availability (HA) systems from 6.0.3 to 6.2 or later, HA should be stopped and its configuration removed prior to a platform upgrade. The software now has a check to prevent a platform upgrade if HA is configured.

This patch includes the following:

- The System Manager back up process has been optimized; the System Manager back up files will now be smaller in size (System Manager template only)
- Unneeded NTP message that resulted in an alarm has been removed
- Resolved the issue where moving the clock forward does not update the LDAP certificate and expiration dates
- Upgraded system rpm packages to latest recommended releases
- The System kernel has been updated with https://rhn.redhat.com/errata/RHSA-2011-1479.html
- Contains updated time zone packages – 2012b tzdata and tzdata-java
- Contains an upgraded OpenJDK
- Resolved the issue where a DNS replying to nonexistent hostnames with an IP would interfere with System Platform installation
- Resolved the issue where logins would be slow if the DNS server is not reachable
- Underscores are now allowed to be entered in the enrolment password field (System Manager and Session Manager templates only)

- When running Communication Manager in a duplex setup with servers that have dual power supplies, the active server losing 1 power supply will now not cause an interchange. The system will alarm the failure, but not interchange for a single power supply failure. (Communication Manager duplex template only)
- Resolved an issue where a minor IPMI fault could cause multiple alarms and trigger a fail over in HA
- Resolved an issue where the system could crash during high I/O with a Dell H200 disk controller
- Resolved an issue where UDP packets may not get forwarded to an HVM guest VM
- Resolved an issue with rollback to 6.0.3 after upgrading to 6.2 where the Services VM was not cleaned up

Application of this patch is service effecting.
The system (Domain-0, Console Domain and all Virtual Machines) will automatically restart following installation of the patch in order for the changes to take effect.

Patch 6.0.3.9.3 is a cumulative patch including updates from 6.0.3.1.3, 6.0.3.3.3, 6.0.3.4.3, 6.0.3.6.3 and 6.0.3.7.3.

MD5 Checksum: 860fcb54db2f08dcf1cc65f03ff6b178

7. Avaya Aura® System Platform Patch 6.0.3.10.3

This patch includes the following:
- Password requirements have been added to the appropriate Management Console pages.
- Upgrades will now log an error if the ovf file checksum does not match.
- Hardware monitoring and alarming related to chassis status is fixed.
- False alarm around free space on disk exceeding threshold when no template is installed, is fixed.
- An issue where NTPD (Network Time Protocol Daemon) would not start if the “NTP FQDN (Fully Qualified Domain Name)” contained a hyphen, is fixed.
- Change to: An issue causing a DomU (Virtual Machine) panic/reboot under specific circumstances related to CD/DVD drive inserts, is fixed.
- Resolved the issue of LDAP backups failing occasionally.
- Added monitoring of the HP Integrated Management Log for the HP ProLiant DL360 G7 server for critical alarmable conditions.
- RHSA-2012-0007: kernel security, bug fix, and enhancement update.
- A home directory for a user is now created on Domain-0 when a user is created via the Management Console.
- Removed the unnecessary alarm “Caught signal 15”.
- Reference PSN 3314. On the "SAL Enterprise" page of the SAL Gateway UI, if the "Secondary Enterprise" was previously set to "secavaya.com", then the value and port are changed to that for "Primary Enterprise". On the "Remote Server" page, if the "Secondary Server Host Name / IP Address" was previously set to "secaxeda.com", then the value and port are changed to that of "Primary Server Host Name / IP Address"

- Failure to send alarms/traps following a change to the hostname of Console Domain is fixed.
- False alarms regarding low/weak battery while the battery is in a ‘Learn Cycle’ is not raised anymore.

Application of this patch is service effecting.
The system (Domain-0, Console Domain and all Virtual Machines) will automatically restart following installation of the patch in order for the changes to take effect.

Patch 6.0.3.10.3 is a cumulative patch including updates from 6.0.3.1.3, 6.0.3.3.3, 6.0.3.4.3, 6.0.3.6.3, 6.0.3.7.3 and 6.0.3.9.3.

MD5 Checksum: 7d93d87a740ff35281572449da3faccb

Documentation Updates and Corrections *(reprinted from the R6.0.1 Release Notes for ease of use)*

Administering Avaya Aura® System Platform

Chapter 5: User Administration
Section: Changing your System Platform password

The following should be added to the end of the section:

The following table summarizes the password rules for LDAP accounts (admin, cust and new users created from WebConsole). The rules apply whenever LDAP accounts password is changed from WebConsole or shell.

Rules	Default	Strong Password
Password Min Length	8	15
Complexity	Upper-case letter used as the first character, digit used as the last character, username are not counted in password length. More than 5 repeating characters are counted as 5 in password length.	At least 1 uppercase, 1 lowercase, 1 digit, 1 special character. Upper-case letter used as the first character, digit used as the last character, username are not counted in password length. More than 5 repeating characters are counted as 5 in password length.
Change Interval	min 1 day, no max	min 1 day, max 90 days
Password History	10	10
Similarity	Permit	Deny