Avaya Aura® System Platform R6.0.2 Service Pack Release Notes

Issue 1.3
March 2012

INTRODUCTION

This document introduces the Avaya Aura® System Platform Release 6.0.2 Service Pack and describes known issues and the issues resolved in this release.

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 R6.0.1	vsp-6.0.1.0.5.iso
Avaya Aura® System Platform R6.0.2	vsp-6.0.2.0.5.iso

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	6.0.1.0.5	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	6.0.1.0.5	Service Pack R6.0.2.0.4

Upgrades

Upgrades to service pack 6.0.2.0.5 from patch 1.1.1.93.2 or higher, release 6.0.0.0.11 or service pack 6.0.1.0.5 are supported.

Resolved Issues

1. In service pack 6.0.1.0.5, if a new authentication file was installed on the System Platform system, logging into the WebConsole using the Avaya Services login did not work. This has been resolved in service pack 6.0.2.0.5. There is a manual workaround for the issue in service pack 6.0.1.0.5 which can be applied by the Avaya Services Team, but upgrading to service pack 6.0.2.0.5 is highly recommended.

2. In previous releases, if System Platform was installed via an upgrade, then IP forwarding was automatically disabled. With IP forwarding disabled, it was not possible for a services engineer to directly connect to the System Platform WebConsole through the services port. In R6.0.2, IP forwarding is enabled after an upgrade.

3. In previous releases, administering the same IP address for the Gateway and DNS under the 'General Network Settings' section generated a validation error. The Gateway and DNS can have the same IP Address in R6.0.2.

4. Previously, Gateway IP address changes were not being reflected on the WebConsole or in the network files. This issue has been resolved.

5. The backup and restore from the WebConsole did not backup or restore the Enterprise LDAP configuration of the TLS certificate. These issues have been resolved.

6. Some system restores were failing due to timeout errors. This issue has been resolved.

7. The scheduled backup was not starting for some time zones.

8. Some upgrades were failing do to insufficient disk space. A system check has been implemented to prevent upgrades on systems with insufficient space.

9. The core dump setting may have been lost after an upgrade. This issue has been resolved.

10. If the grub password was configured, future upgrades may have failed. The grub password can now be configured without future upgrades failing.

11. Users were not able to change their password within 24 hours of account creation. Users can now change their password right after account creation.

12. Password entered or left as default could not be changed for 24 hours after installation. This issue has been resolved.

13. Deleting a template which contained a dedicated NIC caused the port to become inoperable. This issue has been resolved.

14. Upload of a patch from a local file system was failing. This issue has been resolved.

15. The WebConsole 'Security Configuration' page deleted the login banner after a user pressed enter/return. This issue has been resolved.

16. If the system crashed or Tomcat rebooted during a template installation with the pre-install webapp launched, the WebConsole would not be accessible after Tomcat restarted. This issue has been resolved.

17. Log configuration file issues in Domain-0 and CDOM which may have caused disk space issues resulting in a critical outage (the system may be unreachable) have been resolved.

18. Harmless IPMI Watchdog error cc on cmd 24 on the Dell 1950 servers has been resolved.

19. On the HP ProCurve server, if NTP was configured, the system time was incorrect. This issue has been resolved.

20. On the HP ProCurve server, shutdown events were not being logged. This issue has been resolved.

21. Previous releases allowed the start up of High Availability with an uncommitted upgrade on either node which resulted in the upgrade rolling back to a previous state with an incorrect configuration. In R6.0.2, High Availability will not be allowed to start if there is an uncommitted upgrade on either node.

22. Unnecessary alarms were being generated by a DRBD data integrity verification between primary and secondary nodes.

23. The WebConsole was not accessible from the Services port on the standby server after a failover. This issue has been resolved.

24. Kernel security and bug fix updates (RHSA-2010:0504-1):
    - Multiple flaws were found in the mmap and mremap implementations. A local user could use these flaws to cause a local denial of service or escalate their privileges. (CVE-2010-0291, Important)
    - A NULL pointer dereference flaw was found in the Fast Userspace Mutexes (futexes) implementation. The unlock code path did not check if the futex value associated with pi_state->owner had been modified. A local user could use this

flaw to modify the futex value, possibly leading to a denial of service or privilege escalation when the pi_state->owner pointer is dereferenced. (CVE-2010-0622, Important)

- A NULL pointer dereference flaw was found in the Linux kernel Network File System (NFS) implementation. A local user on a system that has an NFS-mounted file system could use this flaw to cause a denial of service or escalate their privileges on that system. (CVE-2010-1087, Important)
- A flaw was found in the sctp_process_unk_param() function in the Linux kernel Stream Control Transmission Protocol (SCTP) implementation. A remote attacker could send a specially-crafted SCTP packet to an SCTP listening

25. Kernel security and bug fix updates [RHSA-2010:0723-01]:
    - A buffer overflow flaw was found in the ecryptfs_uid_hash() function in the Linux kernel eCryptfs implementation. On systems that have the eCryptfs netlink transport (Red Hat Enterprise Linux 5 does) or where the "/dev/ecryptfs" file has world writable permissions (which it does not, by default, on Red Hat Enterprise Linux 5), a local, unprivileged user could use this flaw to cause a denial of service or possibly escalate their privileges. (CVE-2010-2492, Important)
    - A miscalculation of the size of the free space of the initial directory entry in a directory leaf block was found in the Linux kernel Global File System 2 (GFS2) implementation. A local, unprivileged user with write access to a GFS2-mounted file system could perform a rename operation on that file system to trigger a NULL pointer dereference, possibly resulting in a denial of service or privilege escalation. (CVE-2010-2798, Important)
    - A flaw was found in the Xen hypervisor implementation when running a system that has an Intel CPU without Extended Page Tables (EPT) support. While attempting to dump information about a crashing fully-virtualized guest, the flaw could cause the hypervisor to crash the host as well. A user with permissions to configure a fully-virtualized guest system could use this flaw to crash the host. (CVE-2010-2938, Moderate)
    - Information leak flaws were found in the Linux kernel's Traffic Control Unit implementation. A local attacker could use these flaws to cause the kernel to leak kernel memory to user-space, possibly leading to the disclosure of sensitive information. (CVE-2010-2942, Moderate)
    - A flaw was found in the Linux kernel's XFS file system implementation. The file handle lookup could return an invalid inode as valid. If an XFS file system was mounted via NFS (Network File System), a local attacker could access stale data or overwrite existing data that reused the inodes. (CVE-2010-2943, Moderate)
    - An integer overflow flaw was found in the extent range checking code in the Linux kernel's ext4 file system implementation. A local, unprivileged user with write access to an ext4-mounted file system could trigger this flaw by writing to a file at a very large file offset, resulting in a local denial of service. (CVE-2010-3015, Moderate)
    - An information leak flaw was found in the Linux kernel's USB implementation. Certain USB errors could result in an uninitialized kernel buffer being sent to

user-space. An attacker with physical access to a target system could use this flaw to cause an information leak. (CVE-2010-1083, Low)

26. Kernel security update (RHSA-2010:0704-01):
"The compat_alloc_user_space() function in the Linux kernel 32/64-bit compatibility layer implementation was missing sanity checks. This function could be abused in other areas of the Linux kernel if its length argument can be controlled from user-space. On 64-bit systems, a local, unprivileged user could use this flaw to escalate their privileges. (CVE-2010-3081, Important)"

    For additional information, please reference https://rhn.redhat.com/errata/RHSA-2010-0704.html.

27. Apache Tomcat security updates:
    - When deploying WAR files, the WAR files were not checked for directory traversal attempts. This allows an attacker to create arbitrary content outside of the web root by including entries such as ../../bin/catalina.sh in the WAR. To mitigate this finding, only administrators who access the system from management workstations deployed on the management vlan, are allowed to login to upload files (including WAR files) to the tomcat server. To further mitigate this finding administrative access to the Tomcat server is protected with TLS, two factor authentication using the CAC card and role-based access control. (CVE-2009-2693 and CVE-2009-2902)
    - Default behavior for the autoDeploy attribute on Windows. This is Windows specific, not applicable to Linux. (CVE-2009-2901)
    - Windows installer defaults to a blank password. This is Windows specific, not applicable to Linux. (CVE-2009-3548)

28. Updated the 'OpenLDAP' from 2.4.11 to 2.4.23 to incorporate the following bug fixes listed at http://www.openldap.org/software/release/changes.html.

29. The following instructions only apply to new installations of Avaya Aura Conferencing, Avaya Aura Messaging and Avaya Session Border Controller Solution Templates on System Platform R6.0.2. Secure Access Link (SAL) models must be added using 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. **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.

2. **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.

3. **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.

4. **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.

5. **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.

6. **Avaya SAL Gateway user interface periodically pops up 'Network Connection Interrupted' in Internet Explorer 7.**
   On Internet Explorer 7, when the SAL Gateway user interface and the System Platform WebConsole share the same Internet Explorer process, the SAL Gateway user interface will periodically pop up 'Network Connection Interrupted' messages requesting users to reload the SAL Gateway user interface pages. This problem occurs when accessing the SAL Gateway via the 'Launch SAL Gateway Management Portal' button in System Platform WebConsole.

   Workaround:
   1. Open two Internet Explorer windows;
   2. Open the SAL Gateway user interface via https://<CdomIPAddress>:7443/salgateway/ in one IE window and open System Platform WebConsole via https://<CdomIPAddress>/webconsole in the other;
   3. Check the task manager on Windows to make sure there are two new iexplore.exe processes in the task manager window.

   Microsoft has provided a fix for this issue which can be downloaded from http://support.microsoft.com/kb/282402.

   This issue does not occur in Internet Explorer 8 or Firefox 3. On these browsers, users can log in to the System Platform WebConsole, go to 'Server Management' | 'SAL Gateway Management' and click the button 'Launch SAL Gateway Management Portal' to access the SAL Gateway.

7. **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.

8. **An upgrade from R1.1.1 to 6.0 in a High Availability 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.

9. **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.

10. **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

11. **From the WebConsole, Static Routes can be added to Public Bridge (avpublic) only.**

12. **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.

13. **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 R6.0.2 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.

14. **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'.

15. **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.

16. **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.

17. **High Availability 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.**

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

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