



Avaya Aura™ System Platform R6.0 Release Notes

Issue 2.0

June 2010

INTRODUCTION

This document introduces the Avaya Aura™ System Platform Release 6.0 and describes known issues and the issues resolved in this release.

Please Note: These Release Notes apply for all Avaya software applications and solutions using System Platform R6.0, including Avaya Aura™ Application Enablement Services, Avaya Aura™ Session Manager/System Manager, Avaya Aura™ Conferencing, Avaya Aura™ Session Border Controller and Avaya Aura™ Communication Manager.

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 R6.0	vsp-6.0.0.0.11.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

OVERVIEW

This section lists the known issues for System Platform. Details on workarounds can be found further in the document.

1. Changing System Platform's network configuration causes Domian-0 to become unreachable externally.
2. When performing a System Platform upgrade, the upgrade should be committed before performing other actions.
3. During a template install, the gateway field for a new bridge is not editable.
4. During System Platform installation, only one default gateway should be configured.
5. Network configuration is not restored when restore is run from the System Platform WebConsole.
6. Configure the System Platform internal network 'avprivate' before template installation.
7. Do not click on the wrench icon to manage an individual virtual machine when logged in via SAL.
8. During a System Platform upgrade, the 'Wait for User Input Link' does not work all of the time.
9. Changing the password the first time you login to WebLM causes Tomcat catalina.out to error and list exceptions.
10. The SAL gateway user interface cannot be accessed using Firefox 3 sometimes due to the lack of a valid certificate.
11. IP Forwarding status is set to disabled after an upgrade to R6.0.0.0.11.
12. Avaya SAL Gateway user interface periodically pops up 'Network Connection Interrupted' in Internet Explorer 7.
13. Adding an extra NIC card to an IBM X3550 (S8800) will change the Ethernet port numbers.
14. Upper case hostnames on CDOM are temporarily switched to lower case during upgrade.

- 15.** During a System Platform upgrade from R1.1.1.7.2 to R6.0 in a High Availability configuration, CDOM takes approx 15 minutes to come up completely.
- 16.** The CDOM fully qualified hostname in /etc/hosts is not correct after being renamed from the WebConsole.
- 17.** System Platform R6.0 only supports MII Monitoring for NIC Bonding.
- 18.** Support for the Single Step Installer has been discontinued in System Platform R6.0 and will not be supported going forward.
- 19.** From the WebConsole, Static Routes can be added to the Public Bridge (avpublic) only.
- 20.** Moving hard drives from one server to a replacement server requires System Platform and the Template to be re-installed.
- 21.** System Platform alarms may be delayed slightly after upgrades or reboots.
- 22.** LDAP manager password change is not propagated to the High Availability standby system.
- 23.** Default network gateway router outage results in restart of VM's.
- 24.** DRBD resources not released upon VM shutdown or destroy.

New Features

1. IPv6 support.
2. Bonded NIC Support – the ability to bridge a single virtual NIC to a pair of physical NICs. The NIC bonding mode is for NIC redundancy (active-back-up) and specifically supports the MII mode.
3. Multiple Virtual Disks per Virtual Machine and Upgrade Control – including the ability for a template to specify disks that should not be touched during an upgrade.
4. Upgrading with Unchanged Virtual Machines – System Platform will check when a template is being upgraded if any of the Virtual Machines in the template will remain unchanged (untouched and running during the upgrade) by the upgrade. In addition, any download of the image of the Virtual Machine will be skipped.

Resolved Issues

1. In previous releases, the Services Port CDOM URL redirect service may not have started. This issue has been resolved. The feature allows a services engineer to connect to the WebConsole via the Services port without knowing the CDOM IP address. The issue was only observed by a services engineer accessing System Platform.
2. Previously, the system event log cron job did not empty cache when it was nearly full. This issue has been resolved. Whenever a system event log is generated, it is stored in the system event log cache for other applications to process. When the cache is full, a new log could not be added into the cache and applications which are interested in processing the system event log no longer receive them. A housekeeping application has been enabled to empty the cache when it reaches 80% capacity.
3. Template upgrade failed in previous releases when the OVF descriptor file specifies 'PromptForEpwOnUpgrade=false' in the PromptForEpw element Template. This issue has been resolved.
4. Previously, the backup history reported success even after a failed file transfer. This issue has been resolved.

5. False and missing RAID alarms have been resolved. The following false alarms had been identified that could be triggered when the RAID controller reported the following messages:

1. Storage Service EventID 2124: Redundancy normal
2. Drive Slot sensor Drive X - In Critical Array Deasserted

In addition, alarms have been implemented for the following cases:

1. When the RAID controller reports 'Storage Service EventID: 2348 - Rebuild failed due to errors on the source or target physical disk'
2. When the RAID controller reports 'Drive Slot sensor Drive X - In Failed Array Asserted'

6. Previously, an invalid DNS entry or an unreachable DNS entry did not allow the configuration of High Availability Failover and would fail with the following error:

HANDLER Operation on line: 222 blocked for timeout period, exiting!

7. The WebConsole Tomcat memory leak (approximately 5 MBs per day) has been fixed.

Known Issues and Workarounds

1. **Changing System Platform's network configuration causes Domain-0 to become unreachable externally.**

When changing System Platform's network through the 'Network Configuration' page, the avpublic Gateway on Domain-0 isn't updated to the new Default Gateway value. This causes Domain-0 to be inaccessible externally.

To rectify this issue, navigate to 'Server Management' | 'Network Configuration'. Without making any changes to the displayed network settings select 'Save'. The Gateway value displayed under Domain-0 for avpublic will now match that of the Default Gateway under the General Network Settings. Domain-0 is now accessible externally.

2. **System Platform upgrades should be committed before performing other operations.**

During an upgrade, after the system boots up into the new platform build or release, the user is required to 'Commit' or 'Rollback' the upgrade. While the system is waiting for the user to either 'Commit' or 'Rollback', it is strongly advised that the user **NOT** perform any of the following operations:

1. Delete,
2. Install or
3. Upgrade the Template
4. **Reboot Domain-0** (Rebooting Domain-0 before committing will automatically roll the system back to the old Platform)

Note: System Platform does not prevent the user from performing the operations prior to selecting 'Commit' or 'Rollback'.

If one or more of the above operations is performed, then the operations will actually take effect on the system. Even if the 'Rollback Platform Upgrade' is executed after the actions have been performed, the new changes will be visible in the rolled back System Platform. A 'Commit' of the upgrade would be unaffected by the changes made prior to committing the upgrade.

Also, if changes were made to the system and neither a 'Commit' nor a 'Rollback' was performed for the upgrade for 4 hours, then upon the time expiration of the Deadman's switch (4 hours) the system would be automatically rolled back with the same consequences as that of selecting a rollback.

If one or more operations are executed for template related functionality and the user wanted to recover after committing or rolling back the upgrade, then the user needs to manually (through the WebConsole) rollback the changes. An upgrade rollback would, at that point, not be able to roll the system back. A 'Commit' of the upgrade, on the other hand, would be unaffected by the changes that the user made prior to committing the System Platform upgrade.

3. **During a template install, the gateway field for a new bridge is not editable.**
IP address and netmask for the interface may be provided, but are not required. This is the IP address and netmask of the interface of Domain-0 on the new bridge. To route packets to a specific gateway from this interface, static routes may be added using the 'Static Routes Configuration' page.
4. **During System Platform installation, only one default gateway should be configured.**
Even though a default gateway can be entered for each interface, only one default gateway should be specified (specifying more than one default gateway may result in an unusable internal networking configuration).
5. **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 done from the System Platform WebConsole 'Network Configuration' page. Ensure the network settings are correct before doing a restore
6. **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 on your 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 your 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 this private bridge and your LAN, causing an application to direct packets to some host on your 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 CDM's address on avprivat. Packets targeted for the phone might actually instead go to Domain-0 or CDM.

7. **Do not click on the wrench icon to manage an individual virtual machine when logged in via SAL.**
When logged into the CDM 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.
8. **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.
9. **Changing the password the first time 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.
10. **The SAL gateway user interface cannot be accessed using Firefox 3 sometimes due to the lack of a valid certificate.**
Internet Explorer 7 is supported by the SAL Gateway user interface.
11. **IP forwarding status set to disabled after an upgrade to R6.0.0.0.11.**
If System Platform 6.0.0.0.11 is installed via an upgrade, then IP forwarding will be automatically disabled. With IP forwarding disabled, it is not possible for a services engineer to directly connect to the System Platform WebConsole through the services port. To resolve this issue the user must enable IP Forwarding by executing the following steps:
 1. login to Domain-0 as admin
 2. execute the command: *'ip_forwarding enable'* at the command line

12. **Avaya SAL Gateway user interface periodically pops up 'Network Connection Interrupted' in Internet Explorer 7.**

On Internet Explorer 7, when SAL Gateway user interface and System Platform WebConsole share the same Internet Explorer process, the SAL Gateway user interface will periodically pop up 'Network Connection Interrupted' messages to ask users to reload SAL gateway user interface pages. This problem occurs for 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.

13. **Adding an extra NIC card to an IBM X3550 (S8800) will change the Ethernet port numbers.**

Verify all the Ethernet ports. For example, adding an extra NIC card can result in the following:

New Cards = eth0 and eth1

- eth0 moved to eth2
- eth1 moved to eth3
- eth2 moved to eth4
- eth3 moved to eth5

14. **Upper case hostnames on CDOM are temporarily switched to lower case during 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, but only the display of the hostname.

15. **An upgrade from R1.1.1.7.2 to 6.0 in a High Availability configuration, CDOM takes approximately 15 minutes.**

During an upgrade from R1.1.1.7.2 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 5 minutes for the reboot to finish.

16. **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.

17. **System Platform R6.0 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

18. **Support for the Single Step Installer has been discontinued in System Platform R6.0 and will not be supported going forward.**

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

20. **Moving hard drives from one server to a replacement server requires System Platform and the Template to be re-installed.**

If hard drives are moved to a new server, System Platform needs to be re-installed. In the event of a chassis failure of a server and the existing hard drives being moved to the replacement hardware System Platform needs to be re-installed.

All existing data on the hard drives will be lost. The Disaster Recovery procedure in the event of chassis failure will be to move the hard drives to the new chassis, re-install System Platform and then reload the customer configuration from a remote backup file. It is important to maintain remote system backups. If the server chassis fails without a remote backup file, it will need to be reconfigured manually.

If a single hard drive is moved into an existing raid to replace a failed hard drive, re-installation is not required as the operation works correctly.

21. 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 may create a backlog within the system of 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.

22. LDAP manager password change is not propagated to the High Availability standby system.

The LDAP replication is configured between cluster systems in High Availability configurations. Scripts use a hard-coded default password (root01) for LDAP replication. If a user plans to use or is using High Availability and the password is changed (during installation or anytime later), the replication will not work.

Please contact Avaya Services for resolution to this issue.

23. Default network gateway router outage results in restart of VM's.

All virtual machines (CDOM and template VMs) are restarted when the default network gateway becomes unreachable for longer than 30 seconds. It is caused by the fact that Pacemaker is event-based and it immediately initiates failover upon the received update of the pingd attribute. When the update from the remote node is processed, the failover is aborted and VMs are started again.

To prevent the VM restart, perform the following steps through the WebConsole before the scheduled gateway outage:

1. Log in to WebConsole as an admin user
2. Navigate to 'Server Management' | 'Failover' page
3. Ensure that 'Switch Over' button is displayed. If it is not, do not continue unless the system is fixed (wait for DRBD resync and check the cable connection)
4. Click on the button 'Stop standby CRM' and confirm displayed warning
5. Wait until the 'Switch Over' button disappears and the button 'Start standby CRM' is displayed
6. Perform required maintenance on the gateway
7. Log in to WebConsole as an admin user
8. Navigate to 'Server Management' | 'Failover'
9. Click on the 'Start standby CRM' button
10. Wait until the 'Switch Over' and 'Stop standby CRM' buttons are displayed again

If the WebConsole is not available, perform the following steps:

1. Ensure that both nodes are interconnected with a crossover connection and it works reliably
2. Disconnect the public network cable from the standby node
3. Perform required maintenance on the gateway
4. Connect the public network cable to standby node

24. DRBD resources not released upon VM shutdown or destroy.

During failover operations that require the shutdown of resources (failover, switchover, or Stop HA) there may be cases when DRBD resources are still being accessed by processes after the VMs are shut down or destroyed. As a result, these DRBD resources cannot be released. System Platform High Availability will not continue the release procedure and will try to activate the standby node. This will fail since resources are still active on the active node.

The outcome is a Standby/Standby system (no VM running on any node).

If this situation is encountered, please contact Avaya Support Services.