AVAYA

Avaya Aura® System Platform R6.4.3
Release Notes
Issue 1.1
October 2018

INTRODUCTION

This document introduces the Avaya Aura® System Platform R6.4.3 and describes new features, known issues and the issues resolved in this release.

WHAT'S NEW IN SYSTEM PLATFORM 6.4.X

Machine Preserving High Availability (MPHA) for Avaya Aura® Application Enablement Services (AE Services) is not supported on System Platform 6.4.x. The MPHA feature is supported on System Platform 6.3.x.

If you are using NIC Bonding, do not upgrade to System Platform 6.4.3.0.01002. A problem has been identified that prevents Virtual Machines from starting if System Platform Service Pack 6.4.3.0.01002 is applied to a System Platform that utilizes NIC bonding; i.e., a bond interface that has been added from the CDOM Webconsole Server Management → Network Configuration screen. If the Bonding Interface section of that screen shows a bond interface administered, do not install the 6.4.3.0.01002 service pack. See PSN027071u for details.

SOFTWARE RELEASE VERSIONS

Release	Date	File Name
Avaya Aura® System Platform R1.0	August 2009	vsp-1.0.0.0.12.iso
Avaya Aura® System Platform R1.1	November 2009	vsp-1.1.0.0.10.iso
Avaya Aura® System Platform Service Pack R1.1.1	February 2010	vsp-1.1.1.0.2.iso
Avaya Aura® System Platform Service Pack R1.1.1.4.2	February 2010	vsp-patch-1.1.1.4.2.noarch.rpm
Avaya Aura® System Platform Service Pack R1.1.1.7.2	April 2010	vsp-patch-1.1.1.7.2.noarch.rpm
Avaya Aura® System Platform Service Pack R1.1.1.9.2	June 2010	vsp-patch-1.1.1.9.2.noarch.rpm
Avaya Aura® System Platform Service Pack R1.1.1.93.2	August 2010	vsp-patch-1.1.1.93.2.noarch.rpm
Avaya Aura® System Platform Service Pack R1.1.1.94.2	November 2010	vsp-patch-1.1.1.94.2.noarch.rpm

Release	Date	File Name
Avaya Aura® System Platform Service Pack R1.1.1.97.2	February 2011	vsp-patch-1.1.1.97.2.noarch.rpm
Avaya Aura® System Platform Service Pack R1.1.1.98.2	December 2011	vsp-patch-1.1.1.98.2.noarch.rpm
Avaya Aura® System Platform R6.0 (700500262)	June 2010	vsp-6.0.0.0.11.iso
Avaya Aura® System Platform Patch R6.0.0.1.11	August 2010	vsp-patch-6.0.0.1.11.noarch.rpm
Avaya Aura® System Platform S8300D Pre-Upgrade Patch R6.0.0.2.11	February 2011	vsp-patch-6.0.0.2.11.noarch.rpm
Avaya Aura® System Platform Pre-Upgrade Patch R6.0.0.3.11	May 2011	vsp-patch-6.0.0.3.11.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.1 (700500858)	August 2010	vsp-6.0.1.0.5.iso
Avaya Aura® System Platform S8300D Pre-Upgrade Patch R6.0.1.2.5	February 2011	vsp-patch-6.0.1.2.5.noarch.rpm
Avaya Aura® System Platform Pre-Upgrade Patch R6.0.1.3.5	May 2011	vsp-patch-6.0.1.3.5.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.2 (700501130)	November 2010	vsp-6.0.2.0.5.iso
Avaya Aura® System Platform Service Pack Patch R6.0.2.1.5	November 2010	vsp-patch-6.0.2.1.5.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.2.3.5	February 2011	vsp-patch-6.0.2.3.5.noarch.rpm
Avaya Aura® System Platform S8300D Pre-Upgrade Patch R6.0.2.5.5	April 2011	vsp-patch-6.0.2.5.5.noarch.rpm
Avaya Aura® System Platform Pre-Upgrade Patch R6.0.2.6.5	May 2011	vsp-patch-6.0.2.6.5.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.3 (700500929)	February 2011	vsp-6.0.3.0.3.iso
Avaya Aura® System Platform Service Pack R6.0.3.1.3	April 2011	vsp-patch-6.0.3.1.3.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.3.3.3	August 2011	vsp-patch-6.0.3.3.3.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.3.4.3	September 2011	vsp-patch-6.0.3.4.3.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.3.6.3	December 2011	vsp-patch-6.0.3.6.3.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.3.7.3	April 2012	vsp-patch-6.0.3.7.3.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.3.9.3	June 2012	vsp-patch-6.0.3.9.3.noarch.rpm
Avaya Aura® System Platform Service Pack R6.0.3.10.3	January 2013	vsp-patch-6.0.3.10.3.noarch.rpm

Release	Date	File Name
Avaya Aura® System Platform R6.2 (700501399)	March 2012	vsp-6.2.0.0.27.iso
Avaya Aura® System Platform Service Pack R6.2.0.2.27	April 2012	vsp-patch-6.2.0.2.27.noarch.rpm
Avaya Aura® System Platform Service Pack R6.2.1.0.9 (700504042)	July 2012	vsp-6.2.1.0.9.iso
Avaya Aura® System Platform Service Pack R6.2.1.3.9	November 2012	vsp-patch-6.2.1.3.9.noarch.rpm
Avaya Aura® System Platform R6.2.2 (700504627)	December 2012	vsp-patch-6.2.2.06002.0.noarch.rpm
Avaya Aura® System Platform R6.2.2.08001.0	February 2013	vsp-patch-6.2.2.08001.0.noarch.rpm
Avaya Aura® System Platform R6.2.2.09001.0	March 2013	vsp-patch-6.2.2.09001.0.noarch.rpm
Avaya Aura® System Platform R6.3 (700505971)	May 2013	vsp-6.3.0.0.18002.iso
Avaya Aura® System Platform R6.3.1	October 2013	vsp-patch-6.3.1.08002.0.noarch.rpm
Avaya Aura® System Platform R6.3.1 (for the Avaya Aura® Solution for Midsize Enterprise)	October 2013	vsp-patch-6.3.1.08003.0.noarch.rpm
Avaya Aura® System Platform R6.3.4 (700508413)	September 2014	vsp-patch-6.3.4.080011.0.noarch.rpm
Avaya Aura® System Platform R6.3.5 (700509883)	October 2014	vsp-patch-6.3.5.01003.0.noarch.rpm
Avaya Aura® System Platform R6.3.6 (700509882)	March 2015	vsp-patch-6.3.6.01005.0.noarch.rpm
Avaya Aura® System Platform R6.3.7 (700509921)	June 2015	vsp-6.3.7.0.05001.iso
Avaya Aura® System Platform R6.3.8 (700511786)	March 2016	vsp-patch-6.3.8.01001.0.noarch.rpm *(replaced by 6.3.8.01002.0)*
Avaya Aura® System Platform R6.3.8 (700511786)	March 2016	vsp-patch-6.3.8.01002.0.noarch.rpm
Avaya Aura® System Platform R6.4 (700512428)	September 2016	vsp-patch-6.4.0.0.17004.iso *(replaced by 6.4.0.0.17006)*
Avaya Aura® System Platform R6.4 (700512428)	October 2016	vsp-patch-6.4.0.0.17006.iso
Avaya Aura® System Platform R6.4.1 (700513383)	July 2017	vsp-patch-6.4.1.0.01008.noarch.rpm
Avaya Aura® System Platform R6.3.8.02001	September 2017	vsp-patch-6.3.8.02001.0.noarch.rpm
Avaya Aura® System Platform R6.4.2	April 2018	vsp-patch-6.4.2.0.01003.noarch.rpm

Release	Date	File Name
Avaya Aura® System Platform R6.3.8.03001	August 2018	vsp-patch-6.3.8.03001.0.noarch.rpm
Avaya Aura® System Platform R6.4.3*	**August 2018**	**vsp-patch-6.4.3.0.01002.noarch.rpm**

* If you are using NIC Bonding, do not upgrade to System Platform 6.4.3.0.01002. A problem has been identified that prevents Virtual Machines from starting if System Platform Service Pack 6.4.3.0.01002 is applied to a System Platform that utilizes NIC bonding; i.e., a bond interface that has been added from the CDOM Webconsole Server Management → Network Configuration screen. If the Bonding Interface section of that screen shows a bond interface administered, do not install the 6.4.3.0.01002 service pack. See PSN027071u for details.

Meltdown and Spectre Vulnerabilities

In order to mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers will need to provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.

Once these patches are received by Avaya, Avaya will test these patches with the applicable Avaya products to determine what, if any, impact these patches will have on the performance of the Avaya product.

Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.

Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.

The customer is responsible for implementing, and the results obtained from, such patches.

The customer should be aware that implementing these patches may result in performance degradation.

Upgrades

System Platform 6.4.x has an upgraded Tomcat that rejects SSLv3 connections to protect against POODLE attacks. This POODLE remediation, previously released as a hot fix via PSN027021u, is inherent in 6.4.x and 6.3.8 and cannot be disabled. Before installing 6.4.x, please verify any installed templates have been patched with POODLE remediations to use TLSv1 instead of SSLv3. Upgrading System Platform to 6.4.x without first remediating the templates will cause sanity heartbeat failures.

Before upgrading or updating System Platform, please make sure that /home directories do not contain any large files. If large files are present in the /home directories, they can prevent backup and restore from working correctly and the system configuration and licenses may not be fully restored after the upgrade.

Upgrades to 6.4.3 are only supported from 6.4.x.

Upgrades to 6.4.0 are supported from 6.3.x, 6.2.2.x, 6.2.1.0.9 and 6.2.0.2.27. Please refer to the application template documentation for additional upgrade information.

Upgrades from 6.0.3.x directly to 6.4.0 may fail. Please first upgrade 6.0.3.x to 6.3.0.0.18002, then to 6.4.0.

Occasionally, installing System Platform 6.4.3 on Dell R630 server running System Platform 6.4.0 with 12 cores may fail and corrupt the dom0 boot image. Before installing System Platform 6.4.3 on a Dell R630 with 12 cores, install the following pre-upgrade patch. You can check the number of cores on your server from the Server Management, System Information page.

- Upload the vsp-patch-dom0-mem-v01.bsx patch to dom0 /tmp directory
- Log in to dom0 as root
- Install the patch by running the following command:
  sh /tmp/vsp-patch-dom0-mem-v01.bsx
- Install System Platform 6.4.3

Please reference the Upgrading Avaya Aura® System Platform document for additional information.

The System Platform compatibility matrix (PSN003312u) is maintained at: https://support.avaya.com/css/P8/documents/100135000. Please check the compatibility matrix to ensure the template is certified with Services Virtual Machine 3.0 prior to upgrading.

System Platform Upgrade Paths

From 6.4.x:

6.4.x → 6.4.3

Installing the SP 6.4.3 patch on an S8300D server running SP 6.4.2 can take up to 3 hours. Installing the pre-update patch, patch-patcher-1.0.bsx (PLDS ID: SP00000115), will help reduce this update time to about 1-1/2 hours.

- Log in to System Platform CDOM (udom) as root
- Copy the patch-patcher-1.0.bsx file to the /tmp directory
- Change directory to /tmp and install the patch by running the following command:
  sh patch-patcher-1.0.bsx
- Install the SP 6.4.3 patch

From 6.3.x:

6.3.x → 6.4.0 → 6.4.3

From 6.2.x:

6.2.x → 6.4.0 → 6.4.3

From 6.0.3:
6.0.3.4.3 (or later 6.0.3.x.3) → 6.3.0.0.18002 → 6.4.0 → 6.4.3
Pre 6.0.3.4.3 must first upgrade to 6.0.3.4.3 or later 6.0.3.x.3 (6.0.3.10.3 recommended).

Upgrading Services-VM

System Platform 6.4 is packaged with Services-VM 2.0.0.9, which is a transient Services-VM with a non-functioning SAL Gateway. Customers who wish to utilize the SAL Gateway in the Services-VM MUST upgrade to Services-VM 3.0 or later. Please see the Services-VM 2.0.0.9 release notes and implementation guide.

> The Services-VM 2.0.0.9 Release Notes can be accessed at:
> https://downloads.avaya.com/css/P8/documents/101029162
>
> The Services-VM 2.0.0.9 Implementation Guide can be accessed at:
> https://downloads.avaya.com/css/P8/documents/101029164

Upon installing System Platform 6.4 or upgrading to System Platform 6.4, Services-VM (if used by the customer) should be upgraded to Services-VM 4.0 if the application template is certified for Services-VM 4.0 as shown on the System Platform compatibility matrix.

> The System Platform compatibility matrix (PSN003312u) is maintained at:
> https://support.avaya.com/css/P8/documents/100135000.
>
> The *Services-VM 3.0 Implementation Guide* can be accessed at:
> http://support.avaya.com/css/P8/documents/100175348
>
> The *Services-VM 3.0 Release Notes* can be accessed at:
> http://support.avaya.com/css/P8/documents/100175352

There are two profiles of Services_VM supported in Services-VM 4.0. On “CSR2 and CSR3” hardware type “Services_VM Medium” Profile is supported and on “CSR1 and Other” hardware type “Services_VM Small” profile is supported.

Example Upgrade Paths

For the System Platform upgrade paths pertaining to this release notes (System Platform 6.4) the following potential upgrade/install scenarios exist:

6.0.3 → 6.3.0 → 6.4.0 → 6.4.3; After the System Platform upgrade, if no further action is taken, the Services-VM, if enabled, will be version 2.0 (2.0.0.0.15) as a result of the System Platform upgrade from 6.0.3 → 6.3.0 → 6.4.0 → 6.4.3. For this upgrade path, the Services-VM, if required, must be upgraded to release 4.0 using the web page at System Platform management console → Virtual Machine Management → Templates.

6.2.x → 6.4.0 → 6.4.3 and for 6.3.x → 6.4.0 → 6.4.3; For these System Platform upgrade paths, the Services_VM is not automatically upgraded. After the System Platform upgrade, if no further action is taken, the Services-VM version will be unchanged from its original

version. For these upgrade paths, the Services-VM, if required, must be upgraded to release 4.0 using the web page at System Platform management console → Virtual Machine Management → Templates.

For new installs of System Platform 6.4:
Install System Platform 6.4 (6.4.0.0.17004.iso); After the System Platform 6.4 is installed, the Services-VM, if required, must be upgraded to release 4.0 using the web page at System Platform management console → Virtual Machine Management → Templates.

Please reference the *Upgrading Avaya Aura® System Platform* document at http://support.avaya.com for additional information.

Resolved Issues and Updates

1. **System Platform had certain vulnerabilities described in the following Avaya Security Advisories. To see these documents, go to http://support.avaya.com and search for the ASA numbers. Xen Security Advisories can be viewed here: https://xenbits.xen.org/xsa/**

    - ASA-2017-027 qemu-kvm security and bug fix update (RHSA-2017-0309)
    - ASA-2017-034 qemu-kvm security update (RHSA-2017-0352)
    - ASA-2017-054 openssl security update (RHSA-2017-0286)
    - ASA-2017-063 tigervnc security and bug fix update (RHSA-2017-0630)
    - ASA-2017-066 qemu-kvm security and bug fix update (RHSA-2017-0621)
    - ASA-2017-067 samba security and bug fix update (RHSA-2017-0662)
    - ASA-2017-068 samba4 security and bug fix update (RHSA-2017-0744)
    - ASA-2017-074 wireshark security and bug fix update (RHSA-2017-0631)
    - ASA-2017-086 qemu-kvm security update (RHSA-2017-1206)
    - ASA-2017-092 samba4 security update (RHSA-2017-1271)
    - ASA-2017-093 curl security update (RHSA-2017-0847)
    - ASA-2017-094 bash security and bug fix update (RHSA-2017-0725)
    - ASA-2017-095 glibc security and bug fix update (RHSA-2017-0680)
    - ASA-2017-101 jasper security update (RHSA-2017-1208)
    - ASA-2017-102 openssh security and bug fix update (RHSA-2017-0641)
    - ASA-2017-106 gnutls security, bug fix, and enhancement update (RHSA-2017-0574)
    - ASA-2017-109 rpcbind security update (RHSA-2017-1267)
    - ASA-2017-112 sudo security update (RHSA-2017-1382)
    - ASA-2017-116 coreutils security and bug fix update (RHSA-2017-0654)
    - ASA-2017-117 nss and nss-util security update (RHSA-2017-1100)
    - ASA-2017-120 libtirpc security update (RHSA-2017-1268)
    - ASA-2017-150 glibc security update (RHSA-2017-1479)
    - ASA-2017-154 glibc security update (RHSA-2017-1480)
    - ASA-2017-190 sudo security update (RHSA-2017-1574)
    - ASA-2017-266 samba4 security update (RHSA-2017-2791)
    - ASA-2017-281 openssh security update (RHSA-2017-2563)
    - ASA-2017-286 nss security update (RHSA-2017-2832)
    - ASA-2017-299 samba security update (RHSA-2017-2789)
    - ASA-2017-337 samba4 security update (RHSA-2017-3278)
    - ASA-2018-071 qemu-kvm security update (RHSA-2018-0516)
    - ASA-2018-089 libvorbis security update (RHSA-2018-0649)
    - ASA-2018-105 python-paramiko security update (RHSA-2018-1124)
    - ASA-2018-130 java-1.8.0-openjdk security update (RHSA-2018-1188)
    - The following CVE fixes from ASA-2018-140 kernel security and bug fix update (RHSA-2018-1319)
        - CVE-2017-8824 kernel: Use-after-free vulnerability in DCCP socket
        - CVE-2017-13166 kernel: v4l2: disabled memory access protection mechanism allowing privilege escalation
    - ASA-2018-158 dhcp security update (RHSA-2018-1454)
    - ASA-2018-165 java-1.8.0-openjdk security update (RHSA-2018-1650)

- ASA-2018-184 qemu-kvm security update (RHSA-2018-1660)
- ASA-2018-199 sssd and ding-libs security and bug fix update (RHSA-2018-1877)
- ASA-2018-200 glibc security and bug fix update (RHSA-2018-1879)
- ASA-2018-212 qemu-kvm security update (RHSA-2018-2162)
- Xen Security Advisory 258: Information leak via crafted user-supplied CDROM
- Xen Security Advisory 259: x86: fix slow int80 path after XPTI addition
- Xen Security Advisory 260: [PATCH 10/49] x86/traps: Fix %dr6 handing in #DB handler
- Xen Security Advisory 261: x86/vpt: add support for IO-APIC routed interrupts
- Xen Security Advisory 262: x86/HVM: guard against emulator driving ioreq state in weird ways
- Update java-1.8.0-openjdk for Red Hat Enterprise Linux 6

2. **[SYSPLAT-1488] Corrected a vulnerability in JSF configurations.**

3. **[SYSPLAT-1562] Time zone updates implemented in tzdata-2018c.**

4. **[SYSPLAT-1566] Occasionally, Dom0 on System Platform 6.4.2 may run out of memory and kill off less critical processes.**

Known Issues and Workarounds

1. **In a System Platform High Availability (HA) system, do not make user administration changes including password modifications on the standby/secondary server before starting HA on the primary server.**
   Upon starting HA:
   - Changes made on the standby server cause the primary server to unexpectedly synchronize to the latest (new/modified) settings.
   - LDAP replication, by default, captures the most recent administrative entries made on either the primary server or the standby/secondary server.

   These conditions can result in an unexpected updates to the primary server.

2. **Applying System Platform patches on 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.

3. **In a HA configuration, any hardware maintenance (e.g. replacing hard disks or power modules) must be conducted on the standby server after it is powered**

down.
If the current active server needs hardware maintenance, perform an interchange to make it a standby server and then perform the maintenance operation after the server is powered down.

If this guideline is not followed, it is possible that the HA system may not work as desired once the hardware is replaced.

4. **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.

5. **After HA has finished synchronizing the drives, do not immediately perform a manual interchange.**
   Some processes are still running and this may cause an issue if a manual interchange is performed too quickly. Wait 90 seconds before starting a manual interchange after the synchronization is complete. This issue is only present immediately after the drives synchronize. A manual interchange can be conducted normally at any other time.

6. **Virtual Machine state shows as "stopped" when running Machine Preserving High Availability (MPHA).**
   During a MPHA operation or after an interchange, a machine's state may briefly show as "stopped" on the Management Console Manage page. This is only a display issue and machine operation is completely unaffected.

7. **HA configuration is not supported with the use of class B IP addresses (255.255.0.0 mask).**

8. **Occasionally, the System Platform patch installation page continues to display "is being installed" even when the patch is complete.**
   Workaround: Manually refresh the browser via the browser refresh button. System Platform will display "has been successfully installed" if the patch has completed at that time. If "is being installed" remains to be displayed, please continue to wait.
   Note: System Manager updates may take up to 45 minutes to install.

9. **Host names consisting of only numeric digits are not supported.**
   They will not allow System Platform to boot up.

10. **At the end of a template installation on R6.2.2 or later, the modal panel message that indicates installation is complete incorrectly states template upgrade is complete when the message should state template installation is complete.**
    This is only a display issue and the installation is complete when the message

appears.

11. **When installing System Platform R6.3 on a Dell R610 with H200 controllers or IBM 3550 (S8800) with a BR 10i controller, please press 'Continue' if presented with the following warning: "Error: Could not collect RAID controller information".**
    This screen is harmless and can be ignored.

12. **Do not use the media check on an HP DL360 G7, the installation will stall.**
    If this occurs, reboot the server and proceed with the installation without performing the media check.

13. **System Platform upgrades using a USB device are not supported on an HP DL360 G7.**
    When used for System Platform upgrades, USB drives cause boot problems on the HP DL360 G7. USB devices may be used for template upgrades, although the USB drive must not be attached when the System Platform upgrade is performed.

14. **When running System Platform on a S8300D from the gateway, the "session icc" command will not work unless the gateway is running firmware version 30.13.0 or higher.**

15. **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.

16. **The console domain (CDOM) fully qualified hostname in /etc/hosts is not correct after being renamed from the Management Console.**
    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.

    To change the hostname to a new hostname that is an extension of the existing hostname, change the hostname to something else and then make the change to the new hostname. For example, change the original hostname 'hostname.example.com' to 'temp.different.com' and then change it to the

new hostname ‘hostname-2.example.com’.

17. **If the user space on the file system (e.g. /home/admin) contains a file with a space, ‘$’, or bracket in its name, the System Platform backup will fail.**
    Do not use /home/admin for file storage. /home/admin is used for system backup and the presence of additional files may cause issues.

    System Platform 6.3.4 upgrades the WebLM running on Console Domain to the latest release. In order to support the product license file transition during the WebLM upgrade, System Platform creates a backup archive that contains the product license file (if there is a license installed before applying System Platform 6.3.4). The license file will be restored after the new WebLM is deployed.

    If the System Platform backup failed for any reason (for example, the backup fails due to a file with space, $ or brackets in its filename), the license file transition will not complete successfully. The workaround is to manually install the license file after System Platform 6.3.4 is applied via the Management Console.

18. **Users can browse to a previous Console Domain IP address after a new IP address is configured successfully.**
    When changing the IP address of Console Domain, the previous IP address may be cached such that it is still possible to navigate to the old IP address for a short while after a network change. The IP address has changed successfully and the address resolution protocol (ARP) cache within the network will update within 30 minutes. This is only a caching issue and does not affect system operation. No action needs to be taken.

19. **IPv6 address display.**
    When IPv6 is enabled and configured, System Platform only displays Console Domain's and Domain-0's IP v6 addresses on the Manage Machines page. The templates IPv6 addresses (including Services-VM) can be found on the Network Configuration page.

20. **From the Management Console, static routes can only be added to the public bridge (avpublic).**

21. **The Management Console will not be accessible if the Domain-0 disk becomes full.**
    Domain-0 should not be used for file storage. System Platform will rotate log files and remove old tmp files to ensure files and directories are prevented from growing larger than their allowed sizes. However, directly loading large files unrelated to System Platform onto Domain-0 could fill the hard drive and result in system issues.

22. **Internet Explorer (IE) 9 users may experience issues with some of the buttons and responses from the user interface.**

Avaya does not recommend using IE9 with System Platform R6.3.4.

23. **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 High Availability 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).

24. **If the reboot button is selected, but the VM never shuts down or restarts, the Management Console will display the “rebooting” status indefinitely.**
Workaround: In the case where the VM is a Windows HVM, log into Windows from vnc and shutdown the instance gracefully (consult documentation for applications running on Windows operating systems for more information).

    For other VMs that hang in the shutdown process, manually issue an “xm destroy” command (ensure the VM is actually stuck, some VMs are slow to shutdown and may take up to 30 minutes). Using the “xm destroy” command on a VM that is in the process of shutting down rather than one that has stalled may result in issues. Advanced users may be able to use “xm console <machine name>” to check the state of the machine from its console. This workaround will require root access.

25. **Depending on the BIOS version, it is possible to receive “Invalid checksum” errors during ACPI processing at boot time.**
These errors occur when the ACPI tables in the BIOS contain incorrect checksums. BIOS vendors often only test their BIOS on Windows. Windows is more lenient with ACPI checksums. As a result, invalid checksums in ACPI tables escape this type of testing. Linux is less forgiving of checksum errors and they are occasionally received during start up.

    These errors are dependent purely on the version of BIOS installed. Sometimes, upgrading the BIOS will resolve the errors. Linux ignores the offending ACPI table and System Platform makes no use of ACPI power management, so these errors are completely benign.

26. **Patch search results may not display.**
When using HTTP to download a patch, System Platform may not locate the patch file when the user enters the full patch URL (one that includes the patch filename). For example, http://www.myfileserver/patchdir/SystemPlatform.rpm may mean System Platform does not locate the patch correctly.

    One workaround is to use just the directory URL and not include the filename.

For example, enter http://www.myfileserver/patchdir and then select the correct patch from the resulting list. However, this will not work if the web server does not allow browsing on that directory.

In that instance, point the web browser at the patch and download it to a PC and then upload it to the server using the Local File System option on the patch upload page.

Using a DVD or USB stick to deliver the patch file to the system would also be valid options.

27. **Some Russian time zone names are missing.**
    Workaround: Select the appropriate time zone using the UTC offset.

28. **After upgrading to System Platform 6.3.7, the System Information page from the Management Console (Webconsole) does not display any information and redirects to the Manage web page. New installs of System Platform 6.3.7 do not exhibit this problem.**
    Workaround:
    - Perform platform upgrade to SP 6.3.7.0.05001
    - Log in to Management Console and commit the upgrade
    - Log in to Domain-0 as root
    - Copy /upg/etc/sysconfig/i18n to /etc/sysconfig using:
      ```
      cp /upg/etc/sysconfig/i18n /etc/sysconfig
      ```

29. **Console Domain should not be used for file storage or staging of large files. Service Packs and Upgrades should be performed using the Console Domain Management Console (Webconsole) where files will be put into the appropriate directories. Directly staging files into /home or other directories can result in performance issues or breakage.**

30. **Upgrading from 6.0.3.10.3 directly to 6.4 may fail.**
    Workaround: Follow the following upgrade path:
    6.0.3.10.3 → 6.3.0.0.18002 → 6.4

31. **Large flat subnets with thousands of devices on them is not a supported configuration. There is an arp cache limit of 1024. When the arp cache is full, it will be unable to communicate with any new hosts until the arp cache times out on other hosts (~60 seconds). Network segregation into smaller subnets like /24 and/or the creation of VLANs is recommended.**

32. **[SYSPLAT-256] On rare occasion, installation of Avaya Aura® Communication Manager (CM) 6.3 Kernel Service Pack on Avaya Aura® Messaging 6.3.0 fails and rolls back.**
    Workaround: Activation of CM KSPs on S8300D servers should not be performed

via the System Platform Webconsole. See PSN020192u.

33. **[SYSPLAT-970] Occasionally, when using Microsoft Internet Explorer 11 or Firefox v35 browsers, the install options on the Patch Management page don't show the correct patch that was downloaded from the Download/Upload page but shows the older patch.**
    Workaround: Navigate away from the Patch Management page and then navigate back to the Patch Management page.

34. **[SYSPLAT-984] Memory leak alarms are generated for rsyslogd.**
    Workaround: This is a false positive as the threshold is set too low for this process. Escalate to services for a workaround per SOLN281790 until the solution is delivered in a future service pack.

35. **[SYSPLAT-1055] Network Parameter Change fails and hangs the system when IP address is changed to an address that is already used on the network.**
    Workaround: Make sure the new IP address is not already in use by pinging the IP address before changing the System Platform IP address.

36. **[SYSPLAT-1095] Performing a system upgrade when one or more filesystems are full may cause the System Platform Web Console to become inaccessible.**
    Workaround: Make sure to check for available space in all filesystems prior to attempting the upgrade.

37. **[SYSPLAT-1103] The System Platform Web Console is inaccessible with the error "on cdom "service tomcat restart" Redirecting him to first page."**
    Workaround: Enter the following commands from dom0 and cdom:
    - On dom0: "rm /var/network-config-last-save-faliure"
    - On cdom: "service tomcat restart"

38. **[SYSPLAT-1123] Direct upgrade from System Platform 6.0.3.10.3 to 6.3.7 fails on an Avaya S8300D server.**
    Workaround: When upgrading from System Platform 6.0.3.10.3 to 6.3.7 on an Avaya S8300D server, first upgrade to 6.3.0.18002 and then upgrade to 6.3.7.

39. **[CM-11026] Activation of Avaya Aura® Communication Manager (CM) Kernel Service Pack (KSP) on S8300D servers may fail.**
    Workaround: Activation of CM KSPs on S8300D servers should not be performed via the System Platform Webconsole. See PSN020192u.

40. **[SYSPLAT-1158] The following partially incorrect message may appear when installing or removing the System Platform 6.3.8 patch: "This action is service affecting as it reboots dom0. If this patch is removed, any changes made to LDAP users and passwords since this patch was installed will be lost. Do you want to continue?"**
    Workaround: The correct message should be: "This action is service affecting as it

reboots dom0. Do you want to continue?" Changes made to the LDAP users and passwords are persistent across patch installs and removals, as well as reboots of dom0.

41. **[SYSPLAT-1210] Due to the changes required to support rotating the security keys associated with remote maintenance access through the Access Security Gateway (ASG) (see PSN027026u), the specific Application Certificate information no longer displays on the CDOM webconsole under Authentication File.**

42. **Machine Preserving High Availability (MPHA) for Avaya Aura® Application Enablement Services (AE Services) is not supported on System Platform 6.4. The MPHA feature is supported on System Platform 6.3.x.**

43. **Application Enablement Services 6.3.3 on System Platform 6.4.x could hang when running on an S8800 with a BR10i RAID Controller.**
    Workaround: If AES 6.3.3 is running on an S8800 with the BR10i RAID controller, do not upgrade to System Platform 6.4.x. AES 6.3.3 Super Patch 7 has been certified with System Platform 6.3.8, so that should be used instead of System Platform 6.4. See PSN027043u for details.

44. **[SYSPLAT-1433] On rare occasions, stopping High Availability fails and could corrupt the standby system.**
    Workaround: Try stopping High Availability again. Reinstall the standby system if it becomes corrupt.

45. **[SYSPLAT-1441] On rare occasions, System Platform 6.4.x patch install fails while rebooting of the server.**
    Workaround: If the server does not shut down and reboot in 30 minutes, power-cycle the server.

46. **[SYSPLAT-1447] The Server Management High Availability page does not list the Active Server and the Reason for the failover in the HA History section.**

47. **[SYSPLAT-1567] Installing the SP 6.4.3 patch on an S8300D server running SP 6.4.2 can take up to 3 hours. Installing the pre-update patch, patch-patcher-1.0.bsx, will help reduce this update time to about 1-1/2 hours.**
    - Log in to System Platform CDOM (udom) as root
    - Copy the patch-patcher-1.0.bsx file to the /tmp directory
    - Change directory to /tmp and install the patch by running the following command: sh patch-patcher-1.0.bsx
    - Install the SP 6.4.3 patch

48. **[SYSPLAT-1568] When installing System Platform 6.4.3 patch on an S8300D server, user may not see an intermediate page with the following content:**
    `"System Platform is restarting... Please wait at least 5`

`minutes before trying to login again. The browser will automatically redirect to the login page."` **Instead, user will see a login page after the patch has successfully installed.**

49. **[SYSPLAT-1571] Virtual Machines do not start if System Platform Service Pack 6.4.3.0.01002 is applied to a System Platform that utilizes NIC bonding; i.e., a bond interface that has been added from the CDOM Webconsole Server Management → Network Configuration screen. If the Bonding Interface section of that screen shows a bond interface administered, do not install the 6.4.3.0.01002 service pack. See PSN027071u for details.**