Product Support Notice

PSN #	PSN004496u

Original publication date: 20-May -15. This is Issue #01, published date: 20-May-15.	Severity/risk level	Medium	Urgency	When convenient

Name of problem	System Manager support for Leap Second June 2015.

Products affected

Avaya Aura® System Manager: All releases up to 6.3.12 (System Platform based template and VMWare OVA)

Problem description

On June 30th 2015, a leap second will be added to keep UTC clocks in sync with global rotation. This second will be added at 06-30-2015 23:59:60. System Manager Implementation guidelines recommend using network NTP servers for keeping System Manager Clock in sync(Note: in System Platform based deployments System Manager gets its time synced from System Platform). If for some reason NTP is not being used for clock synchronization, or if the enterprise NTP server that System Manager (or System Platform) gets its clock sync from does not support accounting for leap seconds, then the leap second will not be properly accounted for by the System Manager server. Even if NTP is enabled, there is a possibility the log message generated by the leap second adjustment to the messages log could cause a server panic resulting in an outage.

Resolution

Upgrading the System Manager software to release 6.3.13 (GA'ed on April 13, 2015) will remediate any issues related to the leap second insertion. In cases where System Manager 6.3.12 or earlier software is in use, upgrading the System Manager server to release 6.3.13 or later will ensure leap second handling, and also ensure that the OS log message will not cause a server outage as well.

Workaround or alternative remediation

System Manage release 6.3.12 and earlier server that are using NTP:

Turn off NTP for the weekend prior to the occurrence of the leap second. After the leap second has passed, re-enable NTP for the System Manager. NTP will slowly bring the server back into time instead of jumping 1 second at once.

Note:

For System Platform based deployments this needs to be done via System Platform web console since System Manager syncs its time with System Platform. When you disable NTP via the System Platform web console the server will be rebooted so this is service affecting.

For VE based System Manager Deployments please follow instructions in the System Manager VE deployment guide on how to enable / disable NTP. After enabling NTP on System Manager it is recommended that you reboot the box.

System Manage release 6.3.12 and earlier server that are NOT using NTP:

The system date/time will need to be manually modified.

Note:

For System Platform based System Manager Deployments you need to make the time change via the System Platform web console. This will be service affecting.

For VE based System Manager Deployments ESXi host time has to be change, Make sure you reboot the box after changing the time to ensure that the services pick up the time change properly. This change would be affected all applications which are deployed in the ESXi host

Remarks

Make sure that the Session Manager time is in sync with the System Manager time. Please refer to the corresponding Session Manager Leap Second PSN (PSN004439u) as well for instructions on how to handle the Leap Second on Session Manager.

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Make sure you perform a full System Manager backup and save it on a remote server prior to the Leap Second weekend.

Download

Obtain the latest 6.3.13 or later service packs for System Manager and Session Manager from the Avaya Support Site. For optimum performance, the same service pack (i.e. SP13) should be used for both System Manager and Session Manager at all times. The 6.3.13 release is available for download on the Avaya Support Site.

Patch install instructions Service-interrupting?

Consult Session Manager and System Manager software upgrade documentation for upgrade details.

Verification

n/a

Failure

n/a

Patch rollback instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

None

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

BusinessPartner Notes

Additional information for BusinessPartners

n/a

Avaya Notes

Additional information for Tier 3, Tier 4, and development

n/a