Product Support Notice

© 2016 Avaya Inc. All Rights Reserved.

PSN #	PSN004439u				
Original publication date: 06-Mar-15. This is Issue #04, published date: 14-Dec-16.		Severity /risk level	High	Urgency	Immediately

Name of problem

Avaya Aura® Session Manager support for Leap Second

Products affected

- Avaya Aura® Session Manager all Releases
- Avaya Aura® Branch Session Manager all Releases

Problem description

At times a leap second must be added to keep the UTC clocks in sync with global rotation. Refer to the NIST site (https://www.nist.gov/pml/time-and-frequency-division/leap-seconds-faqs) for details related to leap seconds and when they occur. *Session Manager Implementation* guidelines, recommends using network NTP servers for keeping the System Manager and Session Manager clocks in-sync. If for some reason NTP is not being used for clock synchronization, or if the enterprise NTP server that Session Manager gets its clock sync from does not support accounting for leap seconds, then the leap second will not be properly accounted for by the Session Manager server.

Also on Session Manager Releases prior to 6.3, 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

Upgrade Session Manager software to release 6.3.13 or later will remediate any issues related to the leap second insertion.

a. If Session Manager is running 6.3 base loads prior to 6.3.13, and using NTP to synchronize the clocks, this will also be handled correctly.

b. In cases where Session Manager 6.2 or earlier software is in use, upgrading the Session 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

Session Manager Release 6.3 and later servers that are using NTP:

No action is required for these servers. NTP will allow the time adjustment to occur automatically.

Session Manager Release 6.3 and later servers that are NOT using NTP:

The system date/time will need to be manually modified using the SMnetSetup tool to adjust for the leap second after the leap second has passed. This could be service affecting and it is recommended that Session Manager be placed into a Deny New Service state prior to changing the time, and then returned to service after the time adjustment is complete. Upgrading to Session Manager 6.3.13 with updated timezone files will allow Session Manager to adjust for the leap second automatically. If 6.3.13 or later upgrade is not possible, the procedures below should be followed to adjust for the leap second after the leap second time has passed.

1) The Session Manager server should be placed into a Deny New Service state.
2) Run SMnetSetup to set the system date and time accordingly.
3) Run maintenance tests on Session Manager after it reboots and ensure all tests pass before continuing.
4) Return Session Manager to service by placing it into an Accept New Service State.

Session Manager Release 6.1.6 through 6.2 servers that are using NTP:

Due to the operating system error that could cause a panic when the leap second log message occurs, it is recommended that NTP be disabled on Session Manager servers prior to the occurrence of the leap second. And after the leap second has passed, re-enable NTP for Session Manager. NTP will slowly bring the server back into time instead of jumping 1 second at once. Follow the procedure below to accomplish this:

1) The Session Manager server should be placed into a Deny New Service state.
2) Run “SMnetSetup” to disable NTP.
3) Run “stop –ac” to stop all Session Manager services.
4) Run “start –a” to restart all Session Manager services.
5) Run maintenance tests on Session Manager after services restart and ensure all tests pass before continuing.
6) Return Session Manager to service by placing it into an Accept New Service State.
7) After the leap second has passed, continue on here.
8) The Session Manager server should be placed into a Deny New Service state.

9) Run SMnetSetup to re-enable NTP.
10) Run "stop –ac" to stop all Session Manager services.
11) Run "start –a" to restart all Session Manager services.
12) Run maintenance tests on Session Manager after services restart and ensure all tests pass before continuing.
13) Return Session Manager to service by placing it into an Accept New Service State.

Session Manager Release 6.2 and earlier servers that are NOT using NTP:

The system date/time will need to be manually modified using the SMnetSetup tool to adjust for the leap second after the leap second has passed. This could be service affecting and it is recommended that Session Manager be placed into a Deny New Service state prior to changing the time. Follow the process below to accomplish this.

5) The Session Manager server should be placed into a Deny New Service state
6) Run SMnetSetup to set the system date and time accordingly.
7) Run "stop –ac" to stop all Session Manager services.
8) Run "start –a" to restart all Session Manager services.
9) Run maintenance tests on Session Manager after services restart and ensure all tests pass before continuing.
10) Return Session Manager to service by placing it into an Accept New Service State.

Session Manager Release 6.1.5 and earlier servers that are using NTP:

Due to the operating system error that could cause a panic when the leap second log message occurs, it is recommended that NTP be disabled on Session Manager servers prior to the occurrence of the leap second. And after the leap second has passed, re-enable NTP for Session Manager. NTP will slowly bring the server back into time instead of jumping 1 second at once.

For Session Manager 6.1.5 and earlier, there was a problem with SMnetSetup not properly preventing the watchdog service from starting ntpd on reboots. As a result the below process can be used to disable ntpd on Session Manager, but if for some reason Session Manager reboots, the ntpd service will restart. If it is desired to have ntpd disable persist on system reboots on 6.1.5 and earlier Session Manager servers, contact Avaya Services and they can assist you with doing this. If you are not concerned with the system rebooting between the time ntpd is disabled and after passing of the leap second, then the below procedure can be followed to disable ntpd on a running 6.1.5 or earlier Session Manager server:

Follow the procedure below to accomplish this:

1) The Session Manager server should be placed into a Deny New Service state.
2) Run **SMnetSetup** to disable NTP.
3) Run **stop –ac** to stop all Session Manager services.
4) Run **start –a** to restart all Session Manager services.
5) Run maintenance tests on Session Manager after services restart and ensure all tests pass before continuing.
6) Return Session Manager to service by placing it into an Accept New Service State.
7) After the leap second has passed, continue.
8) The Session Manager server should be placed into a Deny New Service state.
9) Run **SMnetSetup** to re-enable NTP.
10) Run **stop –ac** to stop all Session Manager services.
11) Run **start –a** to restart all Session Manager services.
12) Run maintenance tests on Session Manager after services restart and ensure all tests pass before continuing.
13) Return Session Manager to service by placing it into an Accept New Service State.

Remarks

n/a

Patch Notes

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

Backup before applying the patch

Refer to Session Manager and System Manager upgrade documentation for details on how to upgrade 6.2 and earlier software loads to 6.3.13 or later to avoid the possibility of the log message kernel panic at the time of the leap second.

Download

Obtain the latest 6.3.13 Release or later service packs for Session Manager and System Manager from PLDS. For optimum performance, the same service pack (i.e. SP13) should be used for both Session Manager and System Manager at all times.

© 2016 Avaya Inc. All Rights Reserved.

Patch install instructions	Service-interrupting?
Refer to *Session Manager and System Manager software upgrade documentation* for upgrade details.	Yes

Verification

n/a

Failure

n/a

Patch uninstall 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.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.

BusinessPartner Notes

Additional information for BusinessPartners

n/a

Avaya Notes

Additional information for Tier 3, Tier 4, and development

n/a