Product Support Notice

PSN #	PSN003617u

Original publication date: 01-Mar-12. This is issue #14, Published date: 10-Dec-13. | Severity/risk level | High | Urgency | Urgent

Name of problem Avaya Aura Session Manager TLS certificates expiration dates

Products affected

Avaya Aura Session Manager: Releases 1.1.x, 5.2.x, 6.0.x, 6.1.x and 6.2.0

Problem description

Session Manager uses several internal ID certificates to authenticate TLS connections within its internal components and with external entities (i.e. SIP TLS, Jboss mgmt, etc.). Some of these certificates expire within two years from the original installation date. This PSN describes the procedure to renew these certificates in the affected releases outlined above. **PLEASE NOTE THAT FAILURE TO FOLLOW THE BELOW PROCESS COULD RESULT IN A COMPLETE SYSTEM OUTAGE SHOULD THE CERTIFICATES EXPIRE.**

Avaya strongly recommends upgrading all Session Manager and System Manager servers to release 6.3 to take advantage of several new features including enhanced alarming capabilities and automatic renewal of all Avaya certificates without the need for customer intervention.

Resolution

Please note that this PSN should be implemented only after you have completed the System Manager Certificate renewal procedure outlined in PSN003661u available on Avaya's support site.

1- Customers with third party custom certificates will need to have those reinstalled after successfully completing the Avaya certificate verification and /or renewal procedures detailed below.

2- Customers on releases 1.1.x, 5.2.x, 6.0.x and 6.1.x have "root" level access to Session Manager. Please follow the steps below to validate your certificates:

   a) From the Session Manager command line run the command "**su – sroot"** and provide the root user password

   b) Change directory to the following path:
   # **cd /opt/Avaya/SIPAS/current/ServiceDirector/tm/external/keystores**

   c) Type **ls -ltr** and hit enter, this will show two entries:
   -rw---- 1 root root 1984 Feb 16 13:53 system_manager_external_keystore.jks
   -rw---- 1 root root 1984 Feb 16 13:53 sd1_external_keystore.jks

   d) Run the following command and hit enter :
   # **echo | keytool -list -v -keystore sd1_external_keystore.jks 2>&1 | grep -m 1 Valid**

   e) Check the validity of the certificate to make sure it has not expired. Take note of all the expiration dates for reference:
   (Valid from: Thu Feb 16 13:43:17 MST 2012 until: Sat Feb 15 13:43:17 MST 2014)

   f) Run the following command to check the second keystore and hit enter:
   # **echo | keytool -list -v -keystore system_manager_external_keystore.jks 2>&1 | grep -m 1 Valid**

   g) Now run the following command to check the Jboss certificate and hit enter:
   # **echo |keytool -list -keystore /opt/jboss/server/*/conf/tm/keystore/container_keystore.jks -v 2>&1|grep -m 1 Valid**

3- Customers on release 6.2.0 only, use the following process to validate the expiration date of your certificates:

   a) Login to the System Manager and navigate to Home / Elements / Inventory / Manage Elements

   b) Select the Session Manager instance that needs to be validated. Click "More Actions" and select "Configure Identity Certificates".

   c) Select certificate with Common Name "smmgmt" and note the "Valid To" column. This expiration date applies for all three certificate stores in Session Manager release 6.2.0.

4- If the certificates expiration dates are in the future, no immediate action is required. However, if the expiration dates are within weeks or a few months and the customer has no near future plans to upgrade to a newer release, renewing the certificates in this case would be strongly recommended.

5- If any of the certificates have already expired, perform the following steps to reinstall the Session Manager software for releases 1.1.x, 5.2.x, 6.0.x and 6.1.x.The only exception would be release 6.2.0. See details in 5/f.

- The following procedure is service affecting and needs to be schedule and executed within the change control guidelines specific to every customer. Approximate outage time required is between 20-40 minutes.

a) From the System Manager Webpage under **Home/Elements/Session Manager** (release 6.x) or **Session Manager /System Status/System State Administration (**release 5.2.x), select the Session Manager and change the service state to "Deny New Service" ;wait until the active call count is close to zero. Please note if the Jboss certificate has already expired, the System Manager will not be able to manage the Session Manager. The Session Manager will be unreachable from the System Manager web interface and the Database Replication will not work with expired Jboss certificate. If the Jboss certificate has already expired, this step cannot be executed. In this case and for releases 5.2, 6.0.and 6.1 only, you have the option to use the following commands from Session Manager command line to deny service on this server. If you are on release 6.2.0, go to step 5/f.

i. Release 5.2:
   # **ash soapClientUpdateBusyout 1** to Deny new service

ii. Releases 6.0 and release 6.1:
   # **sm set denynewservice true** to Deny new service

iii. # **sm get callcount** to monitor when calls have dropped close to 0

b) Set the enrollment password from System Manager webpage under **Home/Services/Security/Certificates/Enrollment Password** (release 6.x) or **Home/Security/Trust Management/Enrollment Password** (release 5.2.x). If time remaining on the existing password is 0 hours and 0 minutes, select "Password expires in" and chose one or more days. In the password box, you can type your existing password or provide a new one and hit commit.

c) On the Session Manager command line, change directory to **/opt/ASMinstall** and execute **./install.sh (release 6.x)** or **./install.sh -a** (release 5.2.x)**.** Have all IP addresses for System Manger, Session Manager and DNS ready for verification. Confirm the local host name and provide the enrollment password created in step 5/b.

d) Customers with custom certificates can now re-install their third party certificates.

e) Once Session Manager installation completes successfully, place it back in "Accept New Service" from the System Manager Webpage as described in 5/a.

f) Due to new security policies implemented in release 6.2.0 and above. Customers do not have access to user "root" and thus cannot run **install.sh** script or "**sm set and get**" commands. If you are on release 6.2.0 and your certificates have expired, you will need to contact Avaya immediately to remedy this situation. (Possible charges may apply).

6- If Session Manager is version 5.2.x, proceed with reinstalling the server as per step 5. In order to renew the certificates (if any of the certificates are expired or about to expire) on Session Manager 5.2.x, the server needs to be reinstalled.

7- If Session Manager is on release 6.0.x and 6.1.x and any of the certificates are about to expire (but not yet expired) perform the following steps to renew these certificates:

- The following procedure is service affecting and needs to be schedule and executed within the change control guidelines specific to every customer. Approximate outage time required is between 10-30 minutes.

a) From the System Manager Webpage under **Home/Elements/Session Manager**, select the Session Manager and change the service state to "Deny New Service"; wait until the active call count is close to zero.

b) Set the enrollment password from System Manager webpage under **Home/Services/Security/Certificates/Enrollment Password.** If password has expired, renew per the steps in 5/b

c) On Session Manager command line, remove the TMClientInv.xml file:
   # **rm -f /opt/Avaya/jboss-4.2.3.GA/server/s*/conf/tm/TMClientInv.xml**

d) Run # **initTM** from the Session Manager command line.

e) Provide the enrollment password created in step 7/b.

f) The process will then continue without further intervention and once completed, all the certificates will now be valid for a minimum of two years.

g) Customers with custom certificates can now re-install their third party certificates.

h) Place the Session Manger back in "Accept New Service" from the System Manager Webpage under **Home/Elements/Session Manager.**

8- If Session Manger is release 6.2.0 and any of the certificates are about to expire (but not yet expired) per the verification performed in step 3. You can renew these certificates by upgrading Session Manager to any of the following releases; 6.2.1,

6.2.2, 6.2.3 or 6.2.4 using the **upgradeSM.sh** script. Please visit http://support.avaya.com and search for "Upgrading Avaya Aura Session Manager release 6.2" for complete details on how to perform this upgrade.

Workaround or alternative remediation

Avaya strongly recommends upgrading System and Session Manager to release 6.3. In release 6.3, certificates are renewed automatically before they expire and without the need for customer intervention.

Remarks

1) Please note that this PSN should be implemented only after you have completed the System Manager Certificate renewal procedure outlined in PSN003661u available on Avaya's support site.
2) **FAILURE TO FOLLOW THE ABOVE STEPS TO RENEW THE SESSION MANAGER CERTIFICATES MAY EVENTUALLY LEAD TO CERTIFICATE EXPIRATION AND THE TERMINATION OF INTERNAL AND EXTERNAL TLS CONNECTIONS WITHIN THIS SESSION MANAGER INSTANCE RESULTING IN A SERVICE OUTAGE.**
3) **IT IS THE CUSTOMER'S RESPONSIBILITY TO VERIFY THE CERTIFICATES EXPIRATION DATES AND TO TAKE PROACTIVE MEASURES TO RENEW OR RECOVER FOLLOWING THE STEPS OUTLINED IN THIS PSN. AVAYA WILL CHARGE TIME AND MATERIAL FOR ANY CUSTOMER ENGAGEMENTS RELATED TO IMPLEMETING THIS PSN.**
4) In some occasions you might notice a status of "Ready for Repair" in System Manger webpage under **Home/Services/Replication**. If this is the case, follow the procedure below to recover:
   - In System Manger webpage under **Home/Services/Replication**, click on the replica group that needs to be repaired
   - If more than one Session Manger is administered, check the box next to the one that needs repair
   - Click Repair
   - Wait until the repair process completes and the Synchronization Status changes to "Synchronized"
4) Also see related PSN 003909 (Avaya Aura Session Manager Management certificate expiration alarms)

Patch Notes

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

Backup before applying the patch

n/a

Download

n/a

Patch install instructions

n/a

Service-interrupting?

n/a

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

Not Susceptible

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.