

Avaya Session Manager

- Administration, upgrades and maintenances
 - App sequence checklist
 - Syslog
 - SMnetSetup
 - Registering Session manager with System Manager ver 10.1
- Troubleshooting
 - Session Manager - Certificate renewal
 - Logs
 - shell commands

Administration, upgrades
and maintenances

App sequence checklist

SM:

Home / Services / Inventory / Manage Elements

-Add CM element and synchronize

Home / Elements / Routing

-Add CM SIP Entity

-Add CM Entity Link

-Add CM Routing Policy

(Dial Patterns are not needed for SIP phones, but may be added towards CM for VM and SIP trunks)

Home / Elements / Session Manager / Application Configuration

-Add Application for CM. CM SIP Entity & CM Element added previously.

-Add Application Sequence with CM App as the only sequence.

Home / Users / User Management / Manage Users

-When adding a SIP user, Origination/Termination Sequence is set to CM App Sequence

CM:

If the SIP user was added correctly, a SIP station should also be added to CM.

Ch station xxxx (sip phone previously created in SM)

-pg6 SIP Trunk: AAR

ch trunk x (x= trunk group created for SM)

-Numbering Format=private

ch route x (x= route pattern added for SM)

-Group No = SIP trunk to SM that matches the SIP entity created in SM; FRL=0; Numbering Format=Lev0-pvt

ch aar analysis 0

-dial string created for sip extension range with route pattern created previously for SM and Call Type=lev0

ch private-numbering 0

-create Ext Code that matches the sip extension range

Items that are usually missed when setting up an Aura SIP phone environment are the last two.

Syslog

Configuring System Manager logs for Syslog server

Updated: 10/29/2019

You can direct System Manager security logs to remote Syslog server. Also, you can configure general and security logs for the Syslog server.

About this task

Perform the following procedure to configure security audit logs for the Syslog server.

Procedure

1. Log on to System Manager web console.
 2. Click **Services** > **Events**.
 3. Click **Logs** > **Log Settings**.
 4. On the Log Settings page, in the **Logger** column, select `com.avaya.security.iam.audit`.
 5. Click **Edit**.
 6. On the Edit Logger page, click **Attach**.
 7. On the Attach Appender page, in the **Select Appender** field, select **SYSLOG**.
 8. Click **Commit**.
- Add SYSLOG as an appender for the audit log.

Note:

To modify the Syslog configuration, select the SYSLOG appender and click **Edit**.

Administration, upgrades and maintenances

SMnetSetup

run SMnetSetup

get enrollment pwd first from System Manager

Enter the IP Address of System Manager

[10.10.220.113]:

Changes:

Virtual fqdn from active.smgr.com to choosahostname.lab.mylab.com

Primary SMGR fqdn from avaya-smgr.localdomain to chooseahostname-LABSYSMGR.mylab.COM

Enter the Enrollment Password that matches the value in System

Manager administration (Security -> Certificates --> Enrollment Password).

Enrollment Password:

.....

Waiting for Management components to startup...

Thu Jun 24 11:37:46 CDT 2021: DRS Replication registration succeeded

Please go to the System Manager Replication Page to check the synchronization state

check symmetric logs

/var/log/Avaya/mgmt/drs/

Registering Session manager with System Manager ver 10.1

On system Manager Navigate to the Elements > Routing > SIP Entities page and add the Session Manager and Branch Session Manager as a SIP entity. (here you specify the IP for the Security Module)

Replication

Inventory

Routing ×

SIP Entity Details

Commit

Cancel

General

* Name: sessionmanager

* IP Address: 192.168.10.208

SIP FQDN: avaya-asm.htf.com.mx

Type: Session Manager

Notes:

Location: local

Outbound Proxy:

Time Zone: America/Monterrey

Minimum TLS Version: Use Global Setting

Credential name:

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

Entity Links

Add new Element for session manager, select previous sip entity and specify the session manager management IP address.

General

SIP Entity Name

Description

*Management Access Point Host Name/IP

*Direct Routing to Endpoints

Avaya Aura Device Services Server Pairing

Maintenance Mode ☐

Security Module

SIP Entity IP Address

*Network Mask

*Default Gateway

*Call Control PHB

*SIP Firewall Configuration

Monitoring

Enable SIP Monitoring ☒

*Proactive cycle time (secs)

*Reactive cycle time (secs)

*Number of Tries

*Number of Successes

Enable CRLF Keep Alive Monitoring ☐

*CRLF Ping Interval (secs)

Navigate to the Services> Security> Certificates> Enrollment Passwordpage and type an Enrollment Password.

Aura® System Manager 10.1

Home Licenses Solution Deployment Manager Routing Security x

Security ^

Certificates ^

Authority

Enrollment Passw...

Manage Certificat...

Manage Entity Cla...

Configuration v

Enrollment Password

Enrollment password has been set by admin on April 18, 2023 8:46:49 PM -06:00.

Time Remaining: 671 hour 59 mins

New Password

* Password expires in:

* Password:

* Confirm Password:

Enrollment is usually done at the initial deployment of Session Manager, you can also perform a manual enrollment process by running initTM, this not always work and its recommended to redeploy session manager and run wizard from CLI after fresh installation.

```

Converting container_keystore.bcfks to JKS format.
Setting up Syslog certificates and Restarting Syslog.
Successfully wrote certificate chain to file /opt/Avaya/asset/packages/active-version/etc/cert/servers/http-unique.pem
Trust Management initialization completed successfully.
Tue Apr 18 22:47:02 CDT 2023: DRS Replication initialization started.
.
Unconfiguring DRS client
Executing # Dropping DRS schema from swap database
SUCCESS # Dropping DRS schema from swap database
Unregistering from DRS master
Unable to unregister from configured master
Executing # Drop DRS schema and user
SUCCESS # Drop DRS schema and user
Successfully unconfigured DRS client
Executing # Creating DRS schema and user
SUCCESS # Creating DRS schema and user
Executing # Setting up client secure-store for DB parameters
SUCCESS # Setting up client secure-store for DB parameters
Configuring node as DRS replica
Checking whether DRS configuration exists
DRS not configured! Configuring ...
Executing # Configuring SymmetricDS pre-requisites
SUCCESS # Configuring SymmetricDS pre-requisites
Executing # Creating symmetric.properties
SUCCESS # Creating symmetric.properties
Executing # Creating replica DRS tables
SUCCESS # Creating replica DRS tables
Updating host-address and port required for JMX communication
Executing # Checking whether value entered for jmx-port is a numeric value or not
SUCCESS # Checking whether value entered for jmx-port is a numeric value or not
Successfully updated host-address and port required for JMX communication
Executing # Updating JMX properties
SUCCESS # Updating JMX properties
Successfully configured node as DRS replica
Register replica node with System Manager DRS master started. [1/1]
Sending configurations to master node
Successfully sent aggregated configuration to master node
Executing # Sending registration information to DRS master
SUCCESS # Sending registration information to DRS master
Register replica node with System Manager DRS master succeeded.
Starting Management
.
Waiting for Management components to startup...
Tue Apr 18 22:47:44 CDT 2023: DRS Replication registration succeeded
Please go to the System Manager Replication Page to check the synchronization state

Restarting processes to pick up certificate changes

```

Validate replication on services, replication, session manager.

Logon to session manager via ssh and run initTM (/opt/Avaya/bin/initTM).

```

cust@avaya-asm bin]$ initTM
Downloading System Manager root CA
Unable to download System Manager root CA, rc = 28

Enter the Enrollment Password that matches the value in System
Manager administration (Security -> Certificates --> Enrollment Password).
Enrollment Password:
Enrollment Password again:
Trust Management Initialization started.
Trust Management Initialization with System Manager started.

```

Fail to replicate

validate hostname /etc/hosts to make sure both system manager and session manager have fqdn on their host files

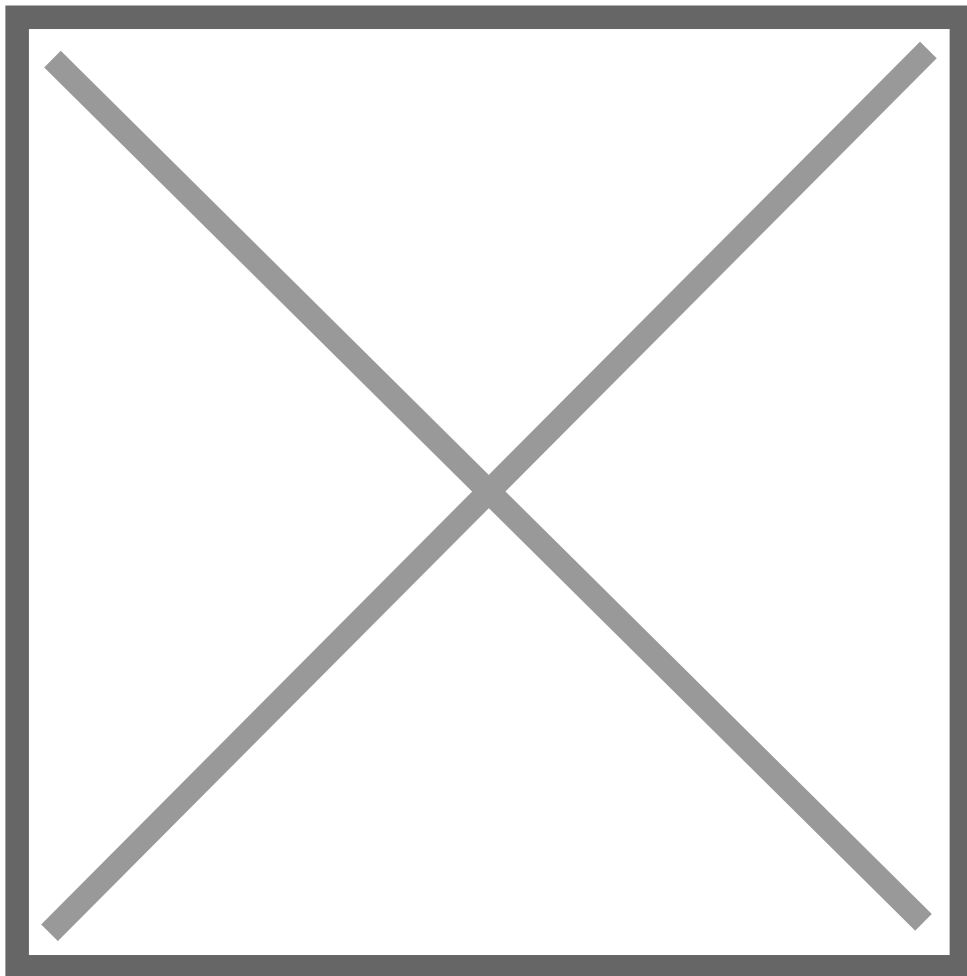
```
[cust@avaya-asm ~]$ cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1      localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.10.209 avaya-asm.htf.com.mx avaya-asm Asm
192.11.13.17 smgrvirtual.htf.com.mx smgrvirtual AsmSysMgr
192.168.10.210 smgr.htf.com.mx smgr AsmSysMgr1
```

```
root >cat /etc/hosts
127.0.0.1      localhost.localdomain localhost
192.168.10.210 smgr.htf.com.mx smgr
::1           localhost6.localdomain6 localhost6
192.168.10.210 smgrvirtual.htf.com.mx smgrvirtual
192.168.10.209 avaya-asm.htf.com.mx avaya-asm
```

Troubleshooting

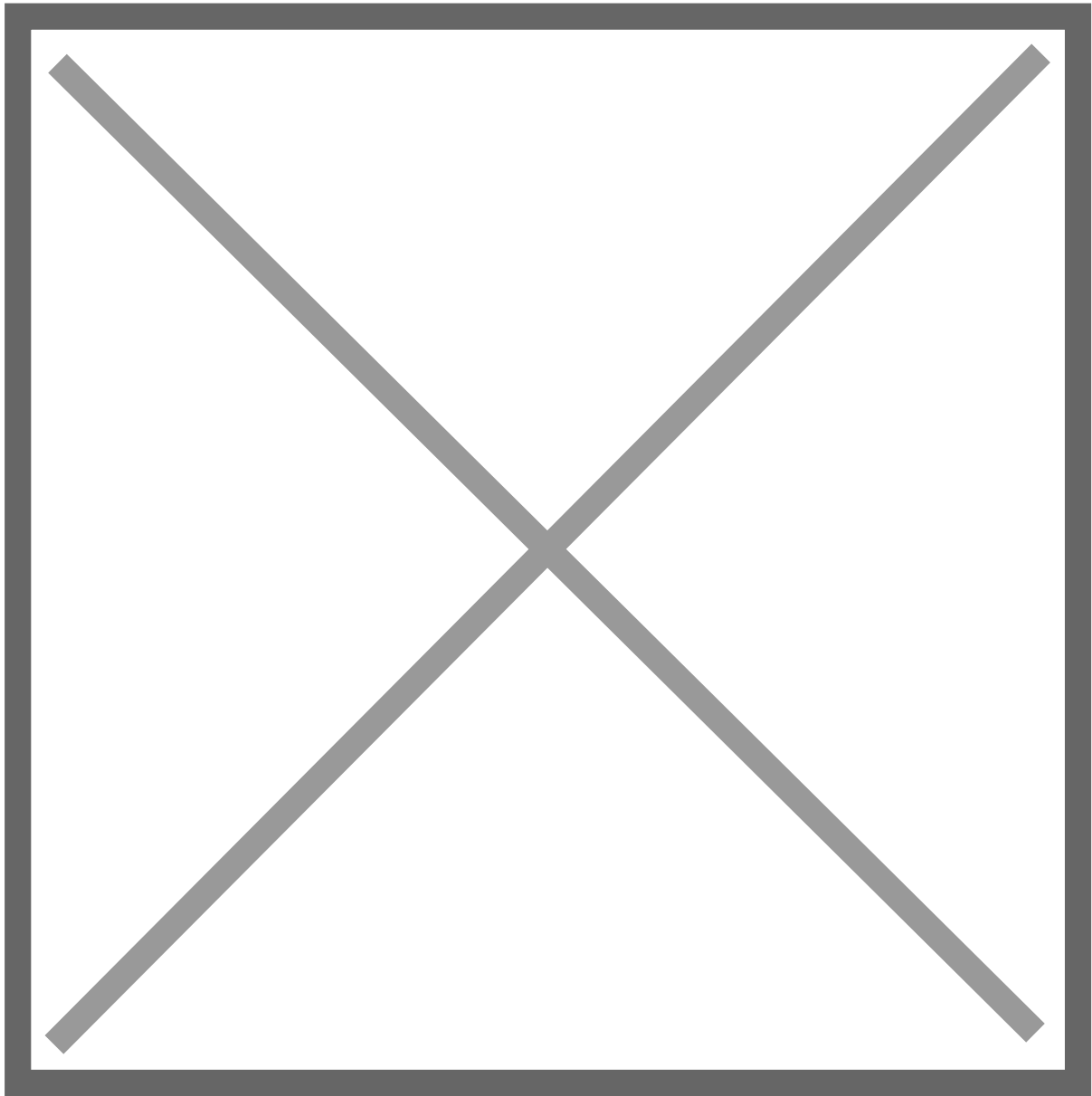
Session Manager - Certificate renewal

In the last few days, we have received multiple emails from Avaya for alarm OP_MMTC20048 in our Session Manager 8.x, this is the information included in the email:

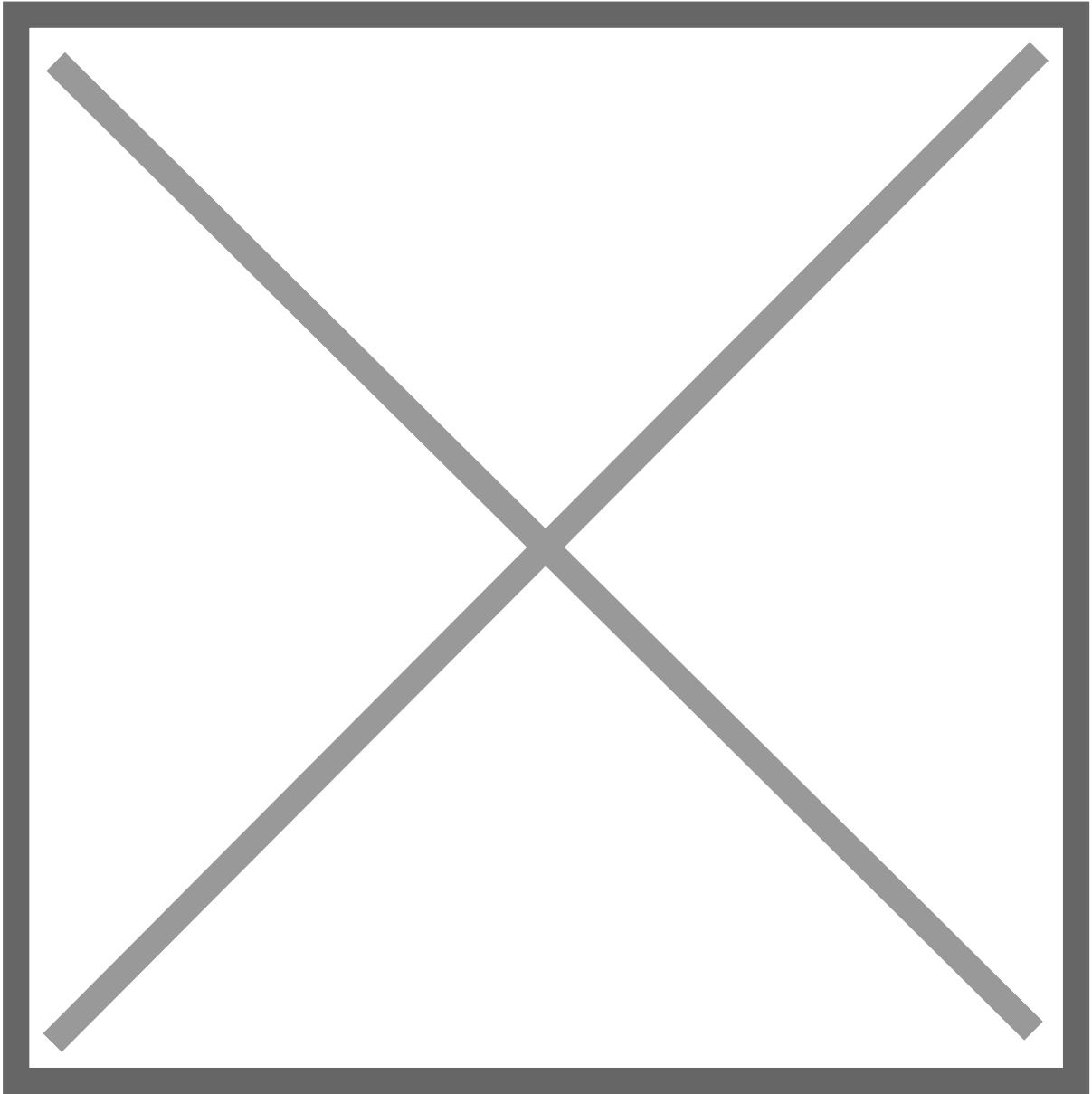


After verifying the System Manager those alarms can be found in (as shown in the image below)

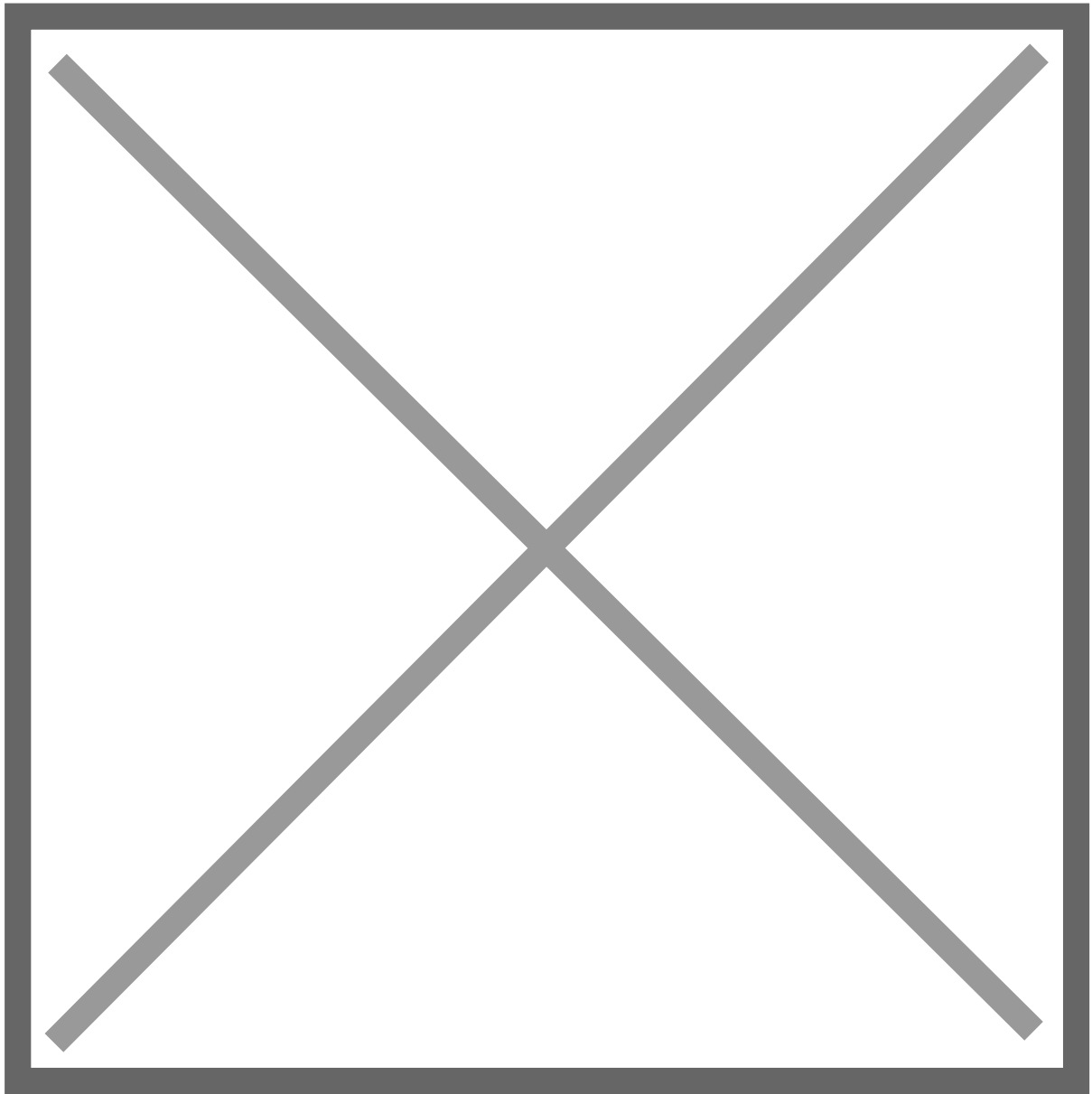
Services -> Events -> Logs -> Log Viewer



Then applying the Event ID = OP_MMTC20048, all alarms are related to identity certificates used by Session Manager for different services:

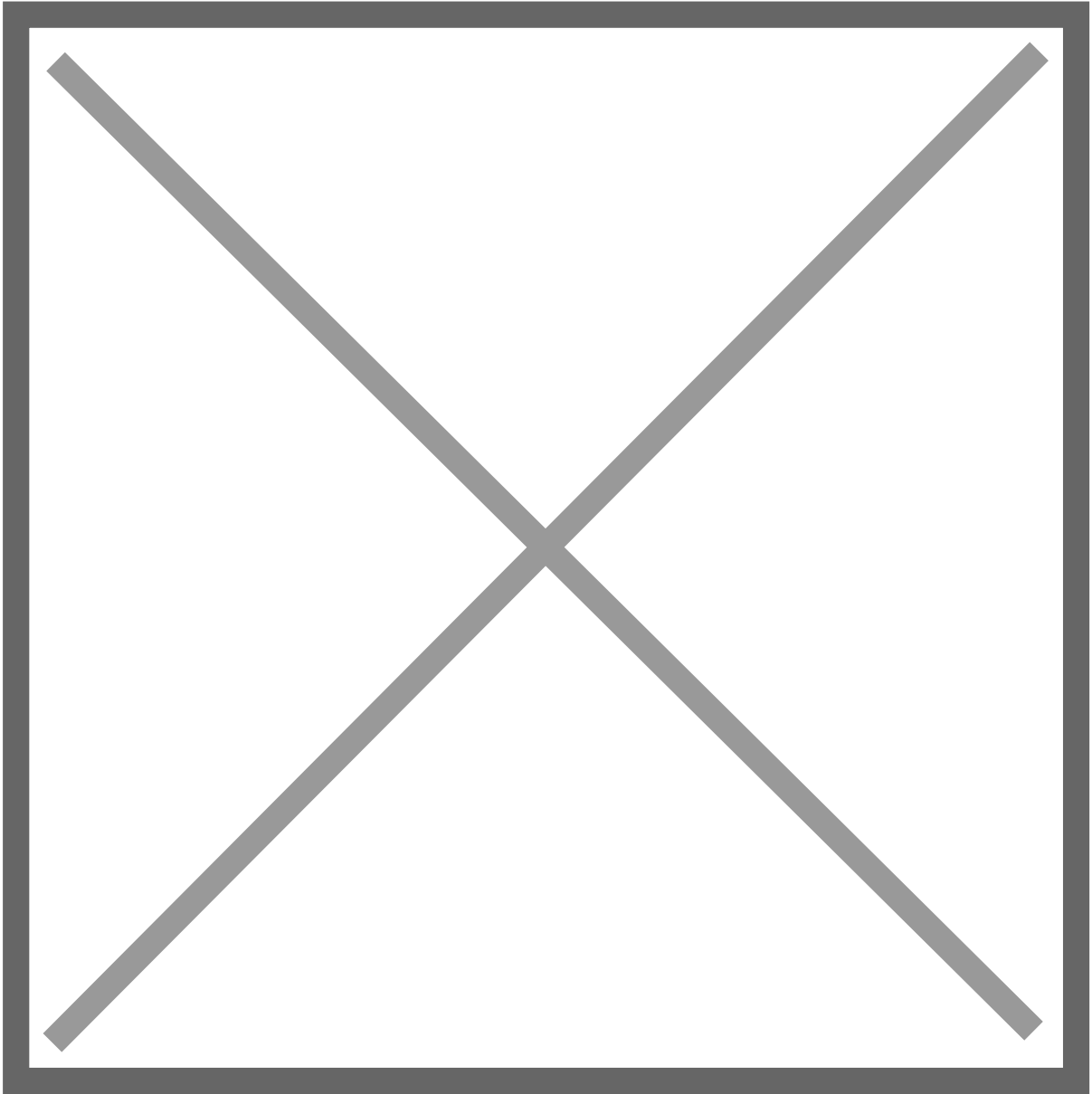


With all the previous information let's the identity certificates in that Session Manager, navigate to
Services -> Inventory -> Manage Elements

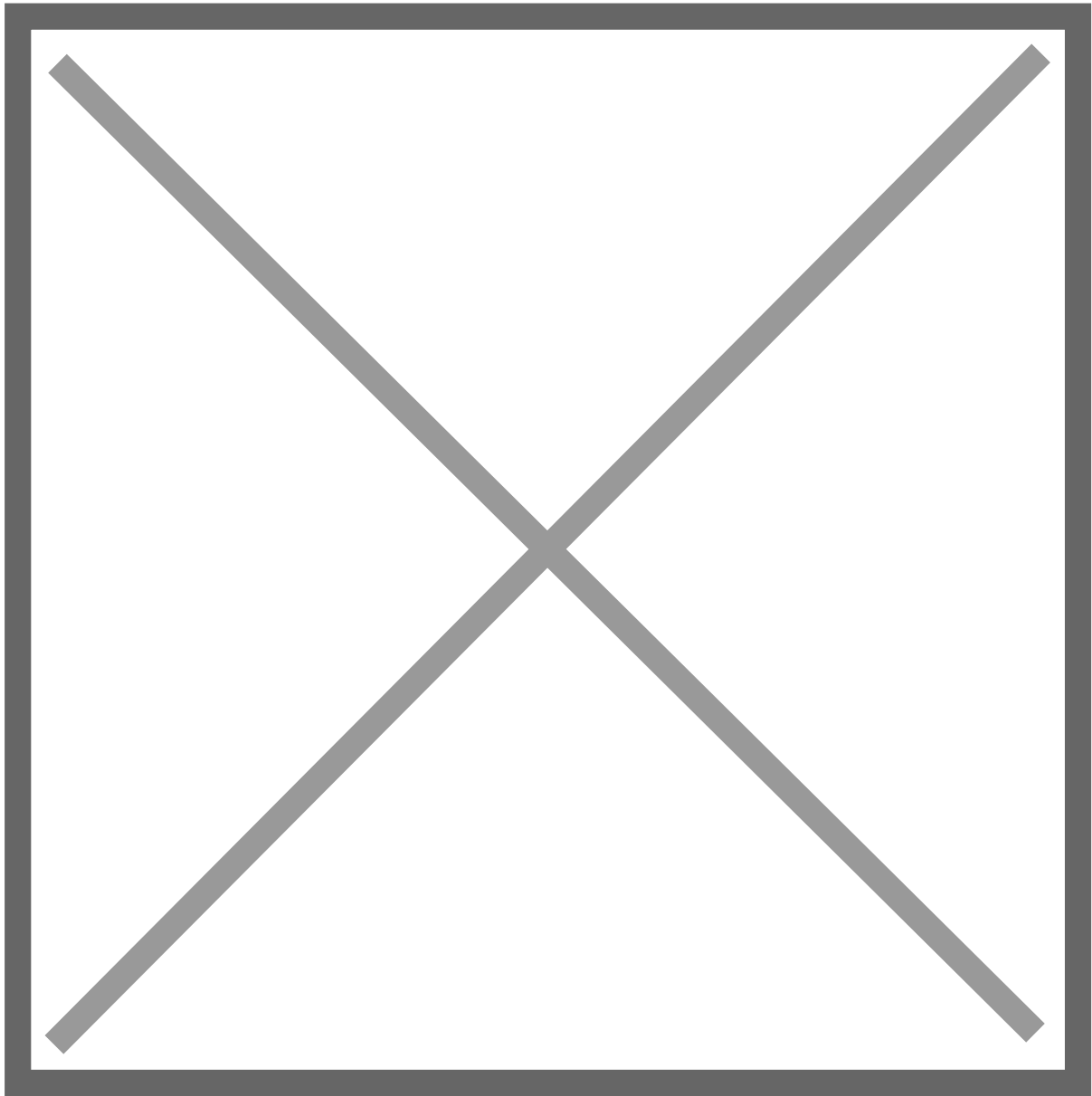


Then with the IP address or name select the Session Manager and click on

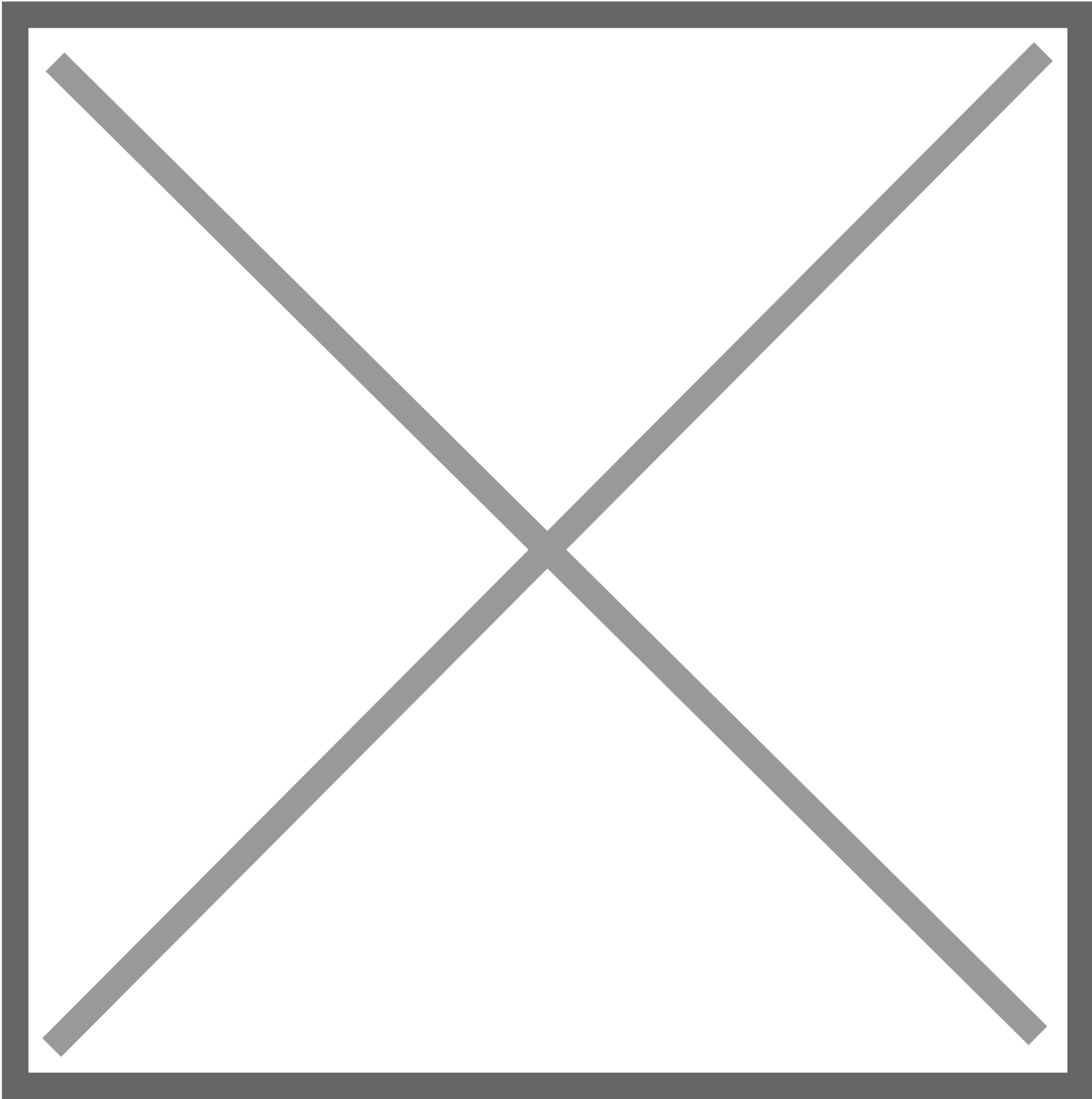
More Actions -> Manage Identity Certificates



In the next page it displays the ***Valid To*** information (when certificate expires)



To renew the certificates, select one by one each entry and select the renew button, this is not a service impacting but changes will be applied until Session Manager is rebooted (apply the renewal under a maintenance window to renew all certificates and reboot).



Logs

Asset Logs

navigate to /var/log/Avaya/asset/

```
/var/log/Avaya/asset/asset.log:Mar  4 00:37:56 denusvm-asesmgr1 AasSipMgr[5168]:  
prv/src/AsITlsData.cpp::verify_callback(312:AsIConnector_5326):verify_callback: Error verify_error =  
10: certificate has expired , Issuer: /CN=System Manager CA/OU=MGMT/O=AVAYA Subject:  
/CN=denusvm-asesmgr1.continuumgbl.com/O=Avaya/C=US RootCA 0  
/var/log/Avaya/asset/asset.log:Mar  4 00:38:12 denusvm-asesmgr1 AasSipMgr[5168]:  
prv/src/AsITlsData.cpp::verify_callback(312:AsIConnector_5326):verify_callback: Error verify_error =  
10: certificate has expired , Issuer: /CN=System Manager CA/OU=MGMT/O=AVAYA Subject:  
/CN=denusvm-asesmgr1.continuumgbl.com/O=Avaya/C=US RootCA 0  
/var/log/Avaya/asset/asset.log:Mar  4 00:38:16 denusvm-asesmgr1 AasSipMgr[5168]:  
prv/src/AsITlsData.cpp::verify_callback(312:AsIConnector_5326):verify_callback: Error verify_error =  
10: certificate has expired , Issuer: /CN=System Manager CA/OU=MGMT/O=AVAYA Subject:  
/CN=denusvm-asesmgr1.continuumgbl.com/O=Avaya/C=US
```

Event Logs

to /var/log/Avaya/sm
operationalEvent.log

PPM Logs

/var/log/Avaya/jboss/SessionManager/ppm.log

Troubleshooting

shell commands

