Avaya Solution & Interoperability Test Lab

Application Notes for NetIQ AppManager with Avaya Aura® Session Manager and Avaya Aura® System Manager – Issue 1.0

Abstract

This document describes a solution comprised of Avaya Aura® Session Manager Release 7.0, Avaya Aura® System Manager Release 7.0 and NetIQ AppManager 9.1. AppManager is used to deliver systems management solution for Session Manager and System Manager using SNMP. A NetIQ AppManager module (SNMP Traps) that monitors SNMP alarms for Avaya Aura Session Manager and its associated System Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

This document describes a solution comprised of Avaya Aura® Session Manager Release 7.0, Avaya Aura® System Manager Release 7.0 and NetIQ AppManager 9.1.

To perform the monitoring functions, AppManager uses the following interfaces into the Avaya IP Telephony environment.

- Simple Network Management Protocol (SNMP) v3 – AppManager uses SNMP v3 to collect configuration and status information from Avaya Aura® Session Manager and Avaya Aura® System Manager.
- Simple Network Management Protocol (SNMP) v2 – AppManager uses SNMP v2 to collect new traps and create traps source automatically; in this case it is Avaya Aura® Session Manager.

AppManager includes Knowledge Scripts that create jobs that gather data for call quality and call activity metrics and stores the data in the SQL database. Each Knowledge Script can be customized to collect data for reporting and send proactive alerts for data in the supplemental database. The following Knowledge Scripts were run during the compliance testing:

- *SNMPTraps TrapMonitor* script can discover SNMP v2 traps event from Session Manager by monitoring for new coming traps and SNMP v2 trap sources can be created and discovered automatically.

- *Discovery_SNMPtraps* script to discover SNMP v3 source devices; in this case they are Session Manager and System Manager which require an additional handshake on engine ID.

- *SNMPTraps_TrapMonitor* script monitor traps for SNMP v3 trap sources discovered from *Discovery_SNMPtraps* script.

- *Discover_NetworkDevice* script discovers the Session Manager and System Manager using SNMP to query the device characteristics such as SNMP, Interfaces, LAN Links, Host Resource and IP Subsystem.

- *Recommended* knowledge script group for monitoring each device discovered by *Discover_NetworkDevice* script, scripts included: NetworkDevice_Device_Uptime, _Device_Ping, _Interface_Health, _IPSubsystem_Util, _LANLink_Util.

- Graph Data: After a monitoring interval has been completed, data streams will be visible in the Graph Data pane for viewing in the chart.

2. General Test Approach and Test Results

The focus of this interoperability compliance testing was primarily to verify the basic functionalities of AppManager such as System Discovery via SNMP v2 and SNMP v3, Reporting Events, Monitoring System Health and Device Inventory. AppManager can work with Session Manager and System Manager System with no adverse impact on system or any other management interfaces.

The serviceability testing cases were performed by disconnecting and reconnecting the LAN cable to AppManager Server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The general test approach was to use AppManager as system management solution for Session Manager and System manager using SNMP. The following features were executed during compliance test:

- Discovery of Session Manager using SNMP v2.
- Discovery of Session Manager and System Manager using SNMP v3.
- Retrieving inventories information from Session Manager and System Manager Device such as Interfaces, LAN Links, Host Resource and IP Subsystem.
- Monitor health of Session Manager and System Manager such as Uptime, Ping and Health.
- Viewing collected data using Graph Chart.

2.2. Test Results

The objectives outlined in S**ection 2.1** were verified and met. All tests were executed and passed.

2.3. Support

For technical support on AppManager, please contact NetIQ technical support team:

- **Telephone:** 1-713-418-5555
- **Email:** Support@netiq.com
- **Web Site:** https://www.netiq.com/support/default.asp

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing between Session Manager, System Manager and AppManager.

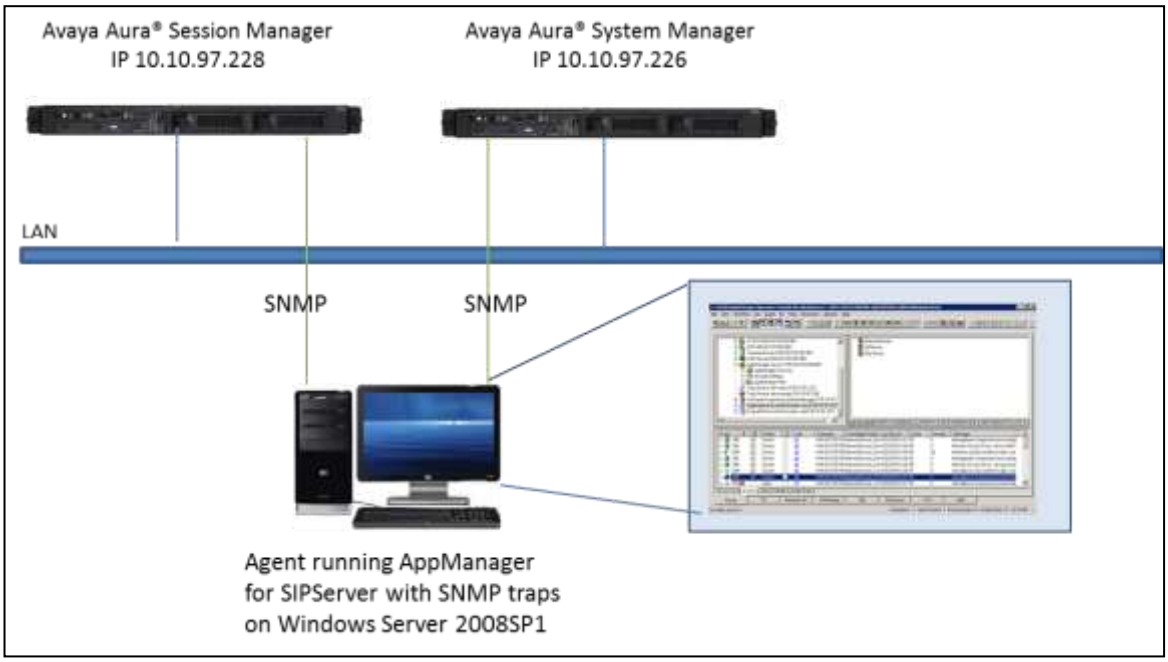


Figure 1: Test Solution Configuration

4. Equipment and Software Validated

Equipment/Software	Release/Version
Avaya Aura® Session Manager in Virtual Environment	7.0 SP2
Avaya Aura® System Manager in Virtual Environment	7.0.0.2
NetIQ AppManager Server: Server hosting AppManager AppManager AppManager for NetworkDevice AppManager for SNMPTraps	 Windows Server 2008 SP1 SW Version 9.1 (Build 9.1.1.419) 7.5.64 8.1.14

5. Configure Avaya Aura® Session Manager and Avaya Aura® System Manager

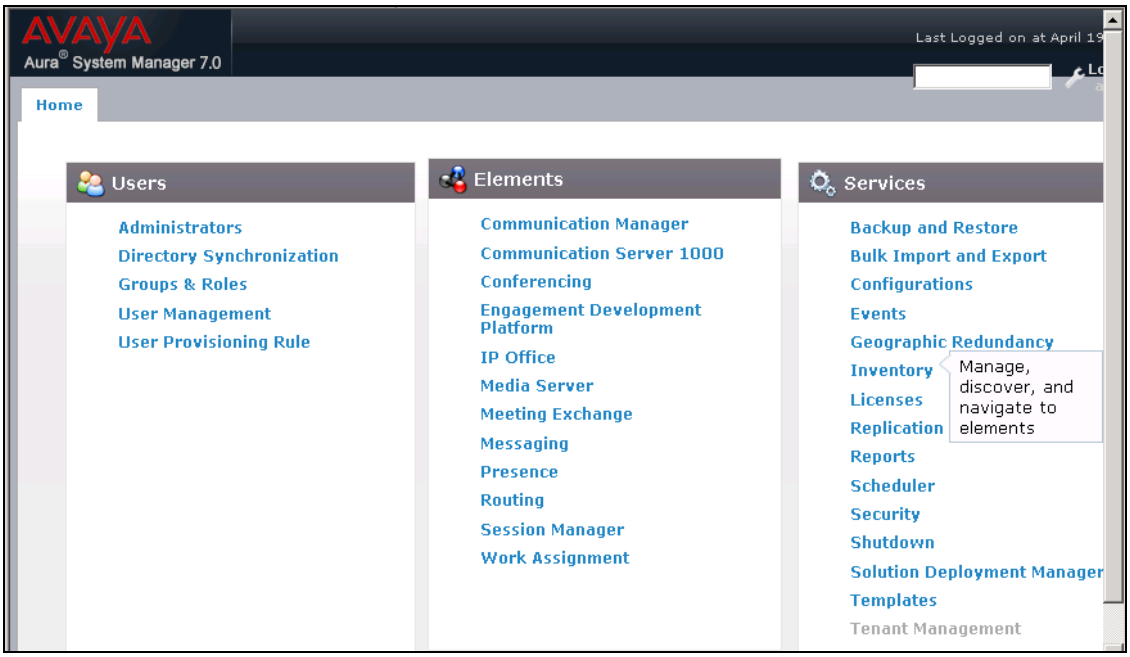
This section describes the steps to configure Session Manager and System Manager to work with AppManager.

Here is a summary of configuration on System Manager:

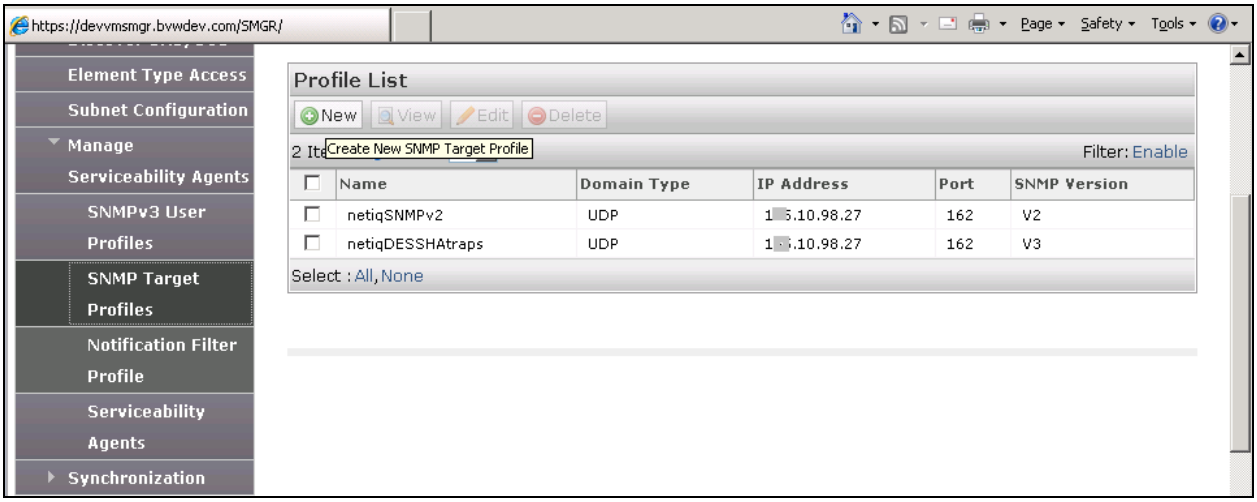
- Create SMNP v2Target Profiles.
- Associate SNMPv2 Profile with Avaya Aura® Session Manager.
- Create SNMPv3 User Profiles.
- Administer SNMPv3 Target Profiles.
- Assign SNMPv3 Target Profile to Avaya Aura® Session Manager and Avaya Aura® System Manager.

5.1. Create SNMPv2 Target Profiles

This section describes step to create SNMP target Profile for SNMP v2 on System Manager. Log in **System Manager** with appropriated login credentials; navigate to **Services → Inventory** as show below:

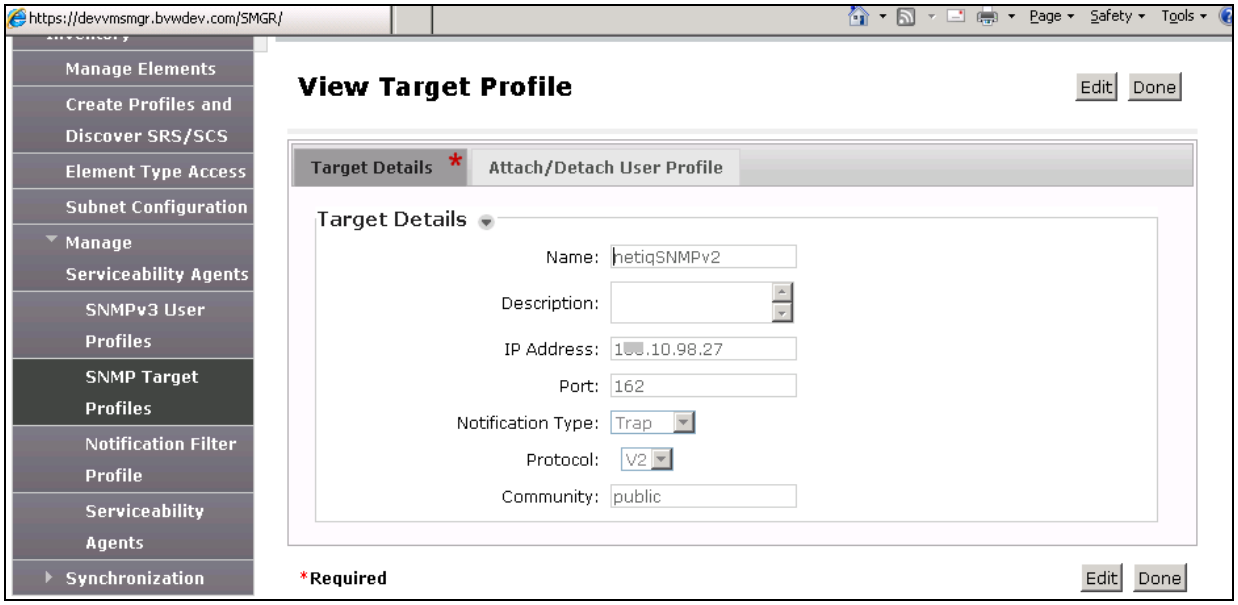


In **Inventory** page, click on New button to add new SNMP Target Profile:



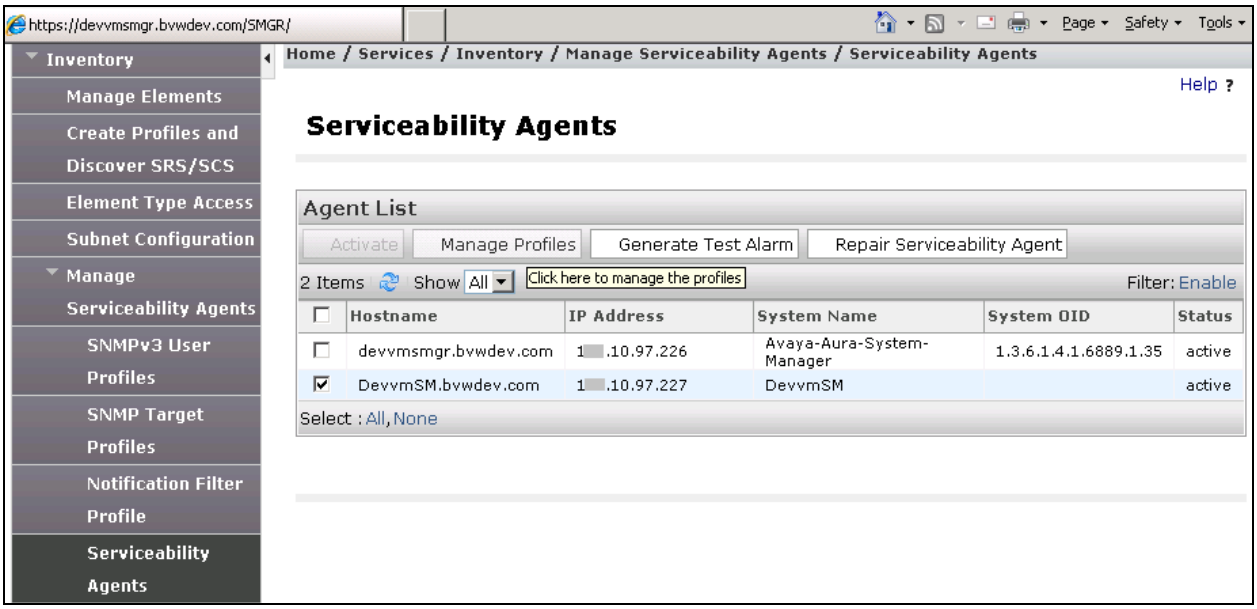
In the **New Target Profile** page, enter the following profile as example in the screenshot below used during compliance test:

- **Name**: Enter any descriptive name such as netiqSNMPv2.
- **IP address**: Enter IP address of AppManager Server, ex: 10.10.98.27.
- **Port**: Use default port 162.
- **Notification Type**: Select Trap.
- **Protocol**: Select v2.
- **Community**: Enter public.



5.2. Associate SNMPv2 Profile with Avaya Aura® Session Manager

Navigate to **Serviceability Agent**, select **Session Manager** from the **Agent List** and click on **Manage Profiles** button.



In **Manage Profile** page, select Profile created in Section **5.1** and click on **Assign** link as shown in below screenshot and click on **Commit** button to save changes.

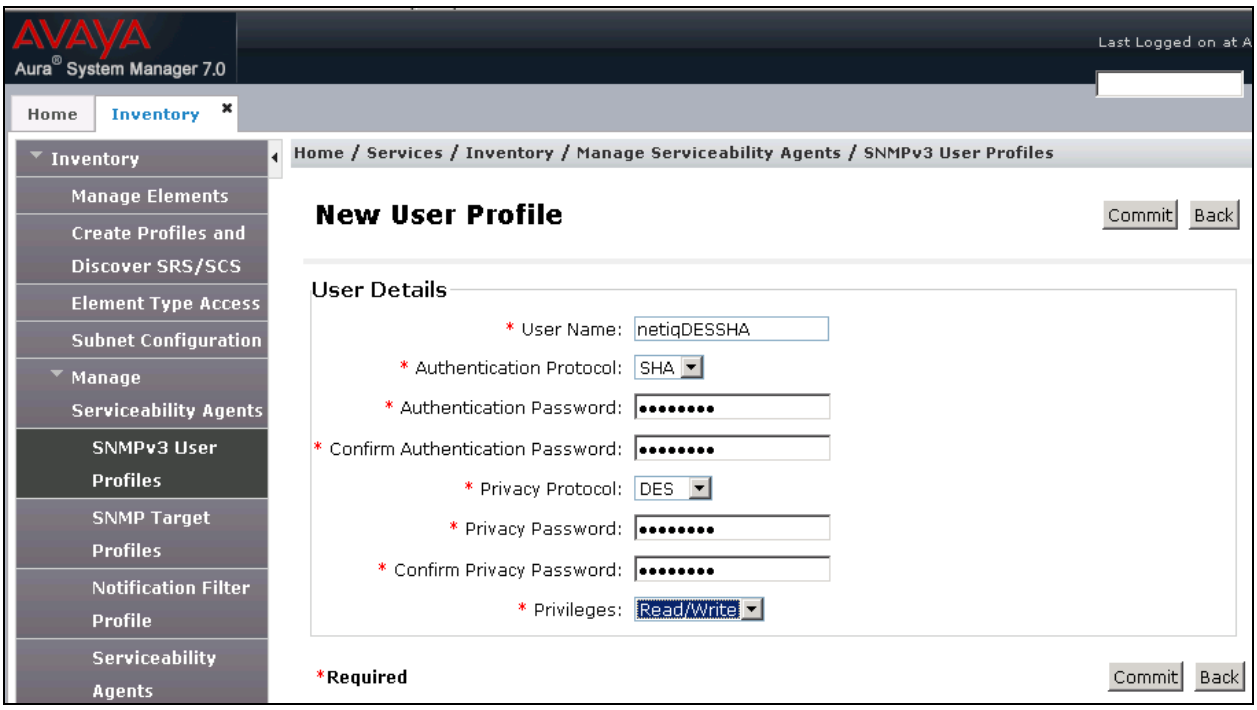
In the **Serviceability Agent,** click on **Generate Test Alarm** to verify that the SNMPV2 trap source is now discovered and appears in the **AppManager** treeview. See detail in Section. This is the end of configuration steps for SNMPv2. Next section will describes step to configure SNMPv3 on **System Manager**.

5.3. Administer SNMPv3 User Profile

In **Inventory** page, select **Manage Serviceability Agents → SNMP3 User Profiles** and click on **New** button to add new user profile as used during compliance test, enter the following example used during compliance test:

- **User Name:** Enter any descriptive name such as netiqDESSHA.
- **Authentication Protocol:** Select SHA.
- **Authentication Password:** Enter any password, in this case default password was used, avaya123.
- **Confirm Authentication Password:** Re-enter password.
- **Privacy Protocol:** Select DES.
- **Privacy Password:** Enter any password, in this case default password was used, avaya123.
- **Confirm Privacy Password:** Re-enter password.
- **Privileges:** Select Read/Write option.

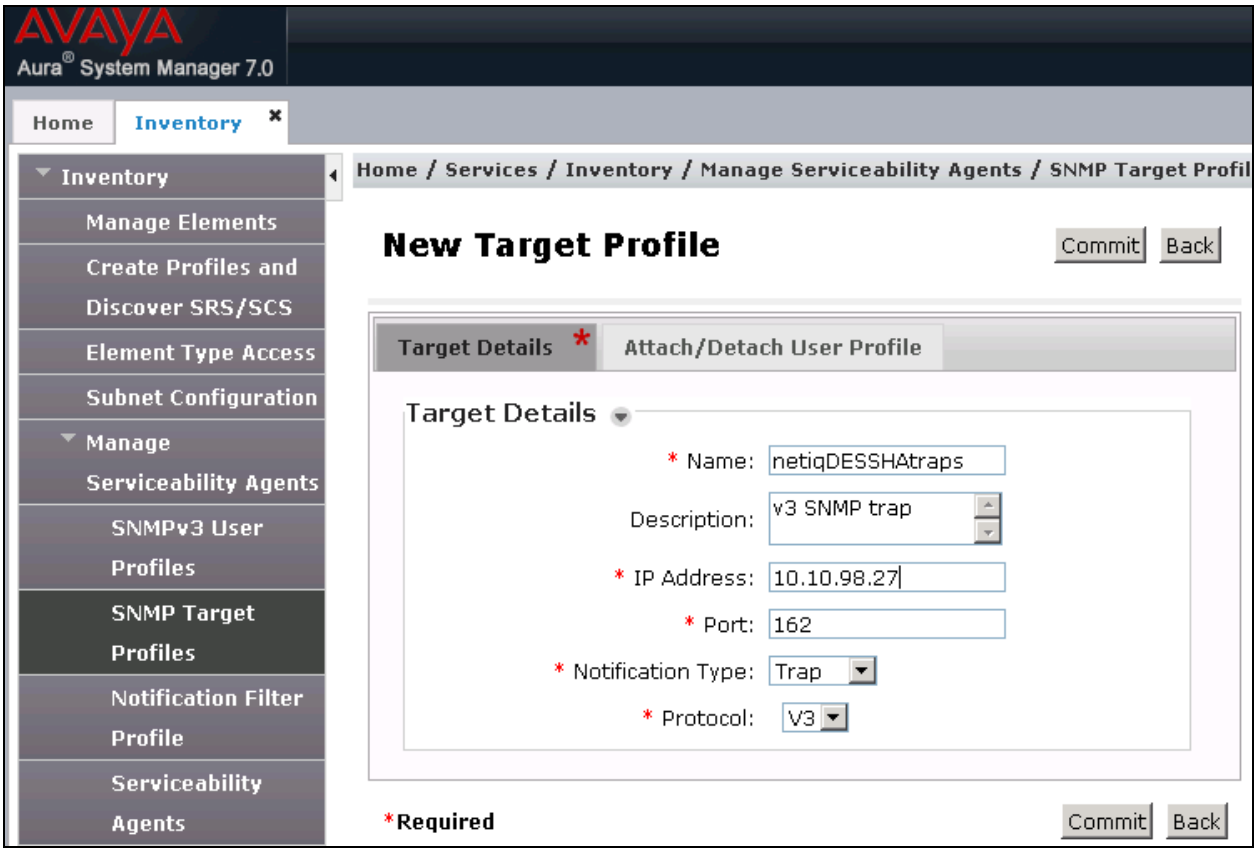
Click **Commit** to save changes.



5.4. Administer SNMPv3 Target Profiles

Configure AppManager as target profile to receive traps. Navigate to **SNMP Target Profiles**, click on **New** button to add new target profile as profile display in below screenshot used during compliance test:

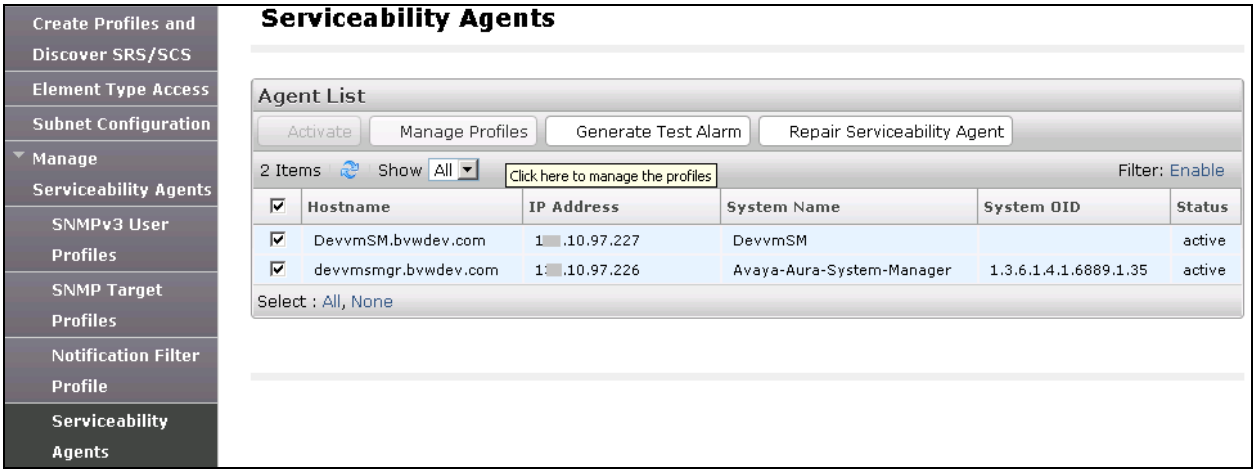
- **Name:** Enter any descriptive name, ex: netiqDESSHAtraps.
- **Description:** Enter any description if needed.
- **IP Address:** Enter IP address of AppManager's PC, ex: 10.10.98.27.
- **Port:** Use default value 162.
- **Notification Type:** Select Trap type.
- **Protocol:** Select V3.



To assign SNMPv3 user to SNMPv3 Target Profile, click on **Attach/Detach User Profile** tab, select user profile create in Section **5.3** and click on Assign link to assign user to this new target profile. Click **Commit** to save changes.

5.5. Assign SNMPv3 Target Profile to Avaya Aura® Session Manager and Avaya Aura® System Manager

Navigate **to Serviceability Agents**, select Session Manager and System Manager in the **Agent List** as display in below screenshot.

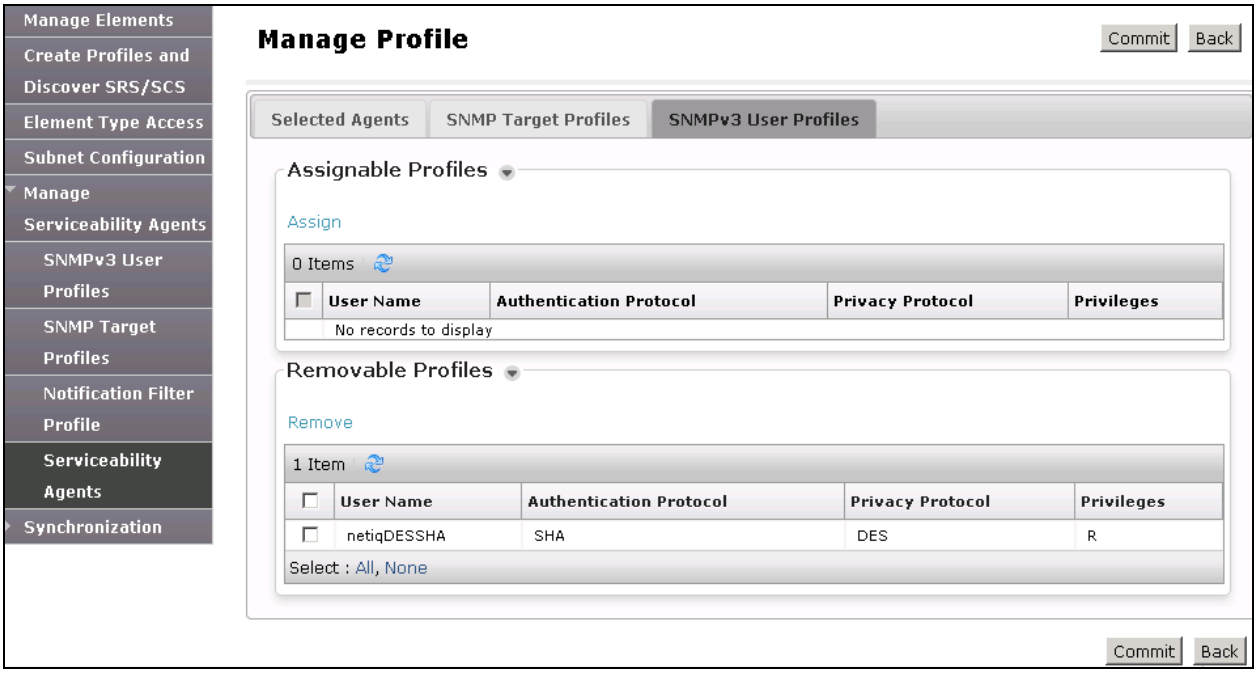


Click on **Manage Profiles** button and verify selected Agents are listed in **Selected Agents** tab.

Click on **SNMP Target Profile** tab, select target profile create in **Section 5.4**, in this case, netiqDESSHAtraps and click on assign link as display below:

Click on SNMPv3 User profiles tab, select user created in **Section 5.3**, in this case netiqDESSHA as shown below.

Click **Commit** button to save assigned user and target profiles as display below screenshot.



6. AppManager Configuration

This section describes the steps to configure AppManager. This section assumes that AppManager has been installed. For more information about installing AppManager or about AppManager system requirements, refer to **Section 9**. The configurations explained are:

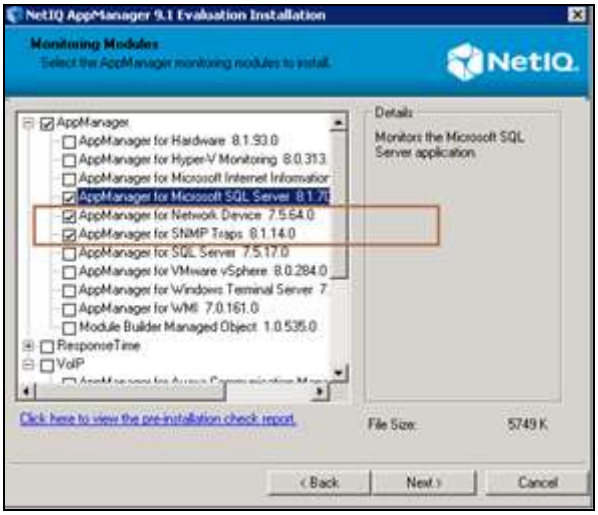
- AppManager Installation
- Activate the Netiq Trap Receiver Service
- Launch NetIQ Console
- Configure SNMPv2 Trap Monitoring
- Configure SNMPv3 trap Monitoring

6.1. AppManager Installation

In addition to the Core AppManager installation, the following product-specific AppManager modules should be installed:

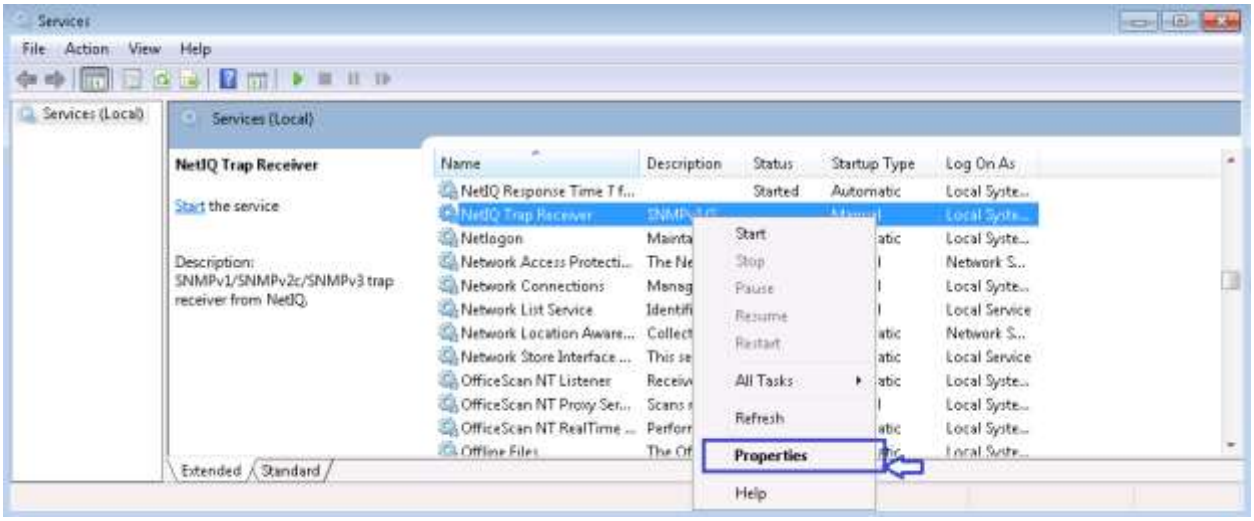
- AppManager for NetworkDevice
- AppManager for SNMPTraps

NetworkDevice and SNMPTraps modules are included in the AppManager 9.1 evaluation package available at https://www.netiq.com/products/appmanager/trial.html and may be selected during the installation of the AppManager 9.1 evaluation package.

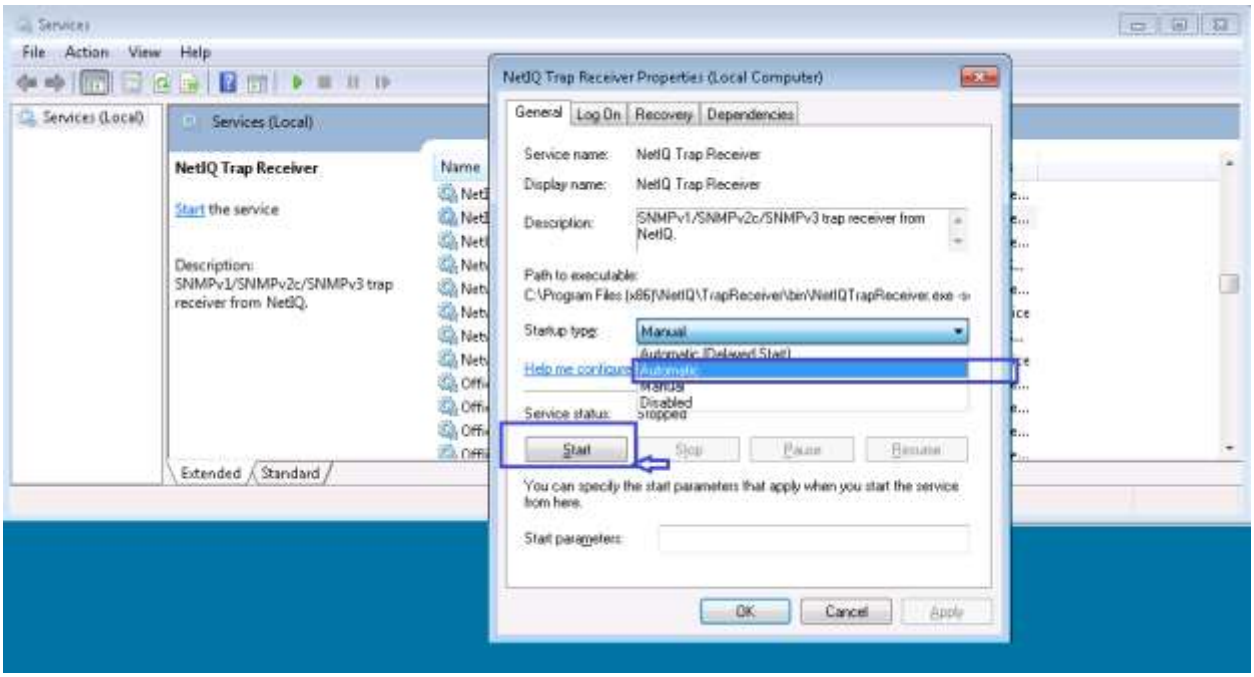


6.2. Activate the Netiq Trap Receiver Service

When AppManager for SNMPTraps is initially installed, the NetIQ trap receiver is not activated. To activate the NetIQ trap receiver: Click Start on the agent computer, click in the Start Search box, and type services.msc to access the windows services menu. Right click on NetIQ Trap Receiver service, select **Properties**.



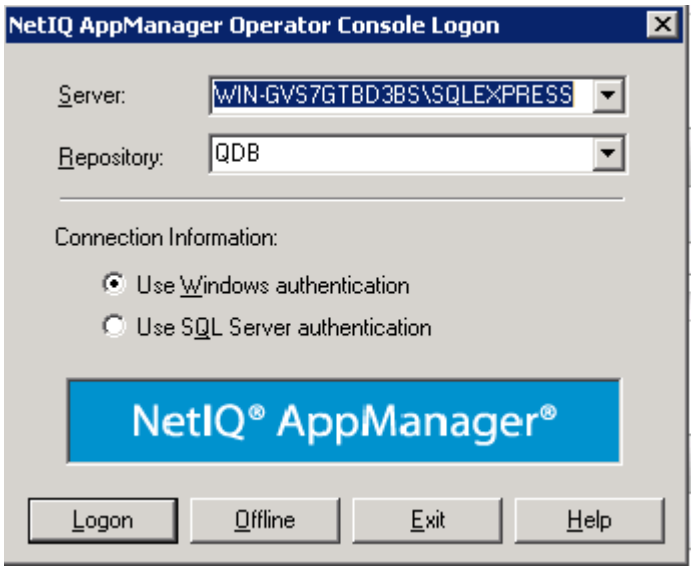
From the windows services menu as shown below and select “automatic” as the service start type. Click **OK** to save changes.



6.3. Launch NetIQ Console

In the NetIQ server navigate to **Start → All Programs → NetIQ → AppManager→ Operator Console** (not shown).

Select the required **Server** and **Repository** from the drop down menu and click on **Logon** as shown in below. During compliance testing **Use Windows authentication** was selected.



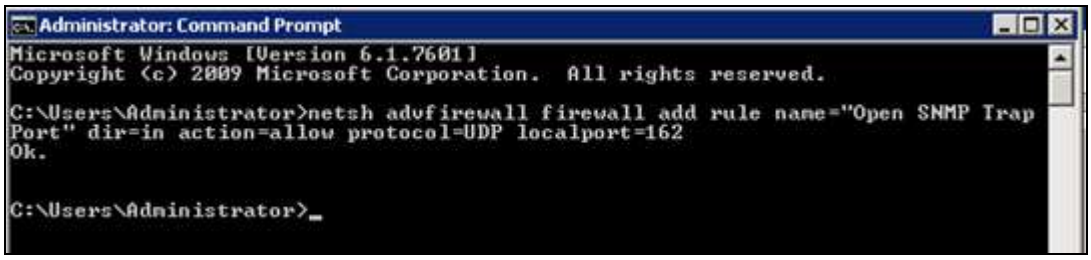
6.4. Configure SNMPv2 Trap Monitoring

While SNMPv3 trap sources must be explicitly configured, AppManager for SNMPTraps can discover SNMPv2 trap resources by monitoring for new incoming traps. No security manager entries are necessary, and while Discover_SNMPTraps may be used to provide trap sources with a customer-supplied name, it is not necessary as SNMPv2 trap sources can be created automatically.

6.4.1. Configure firewall settings

To begin with, make sure that windows firewall on the agent does not block SNMP traps by applying the rule:

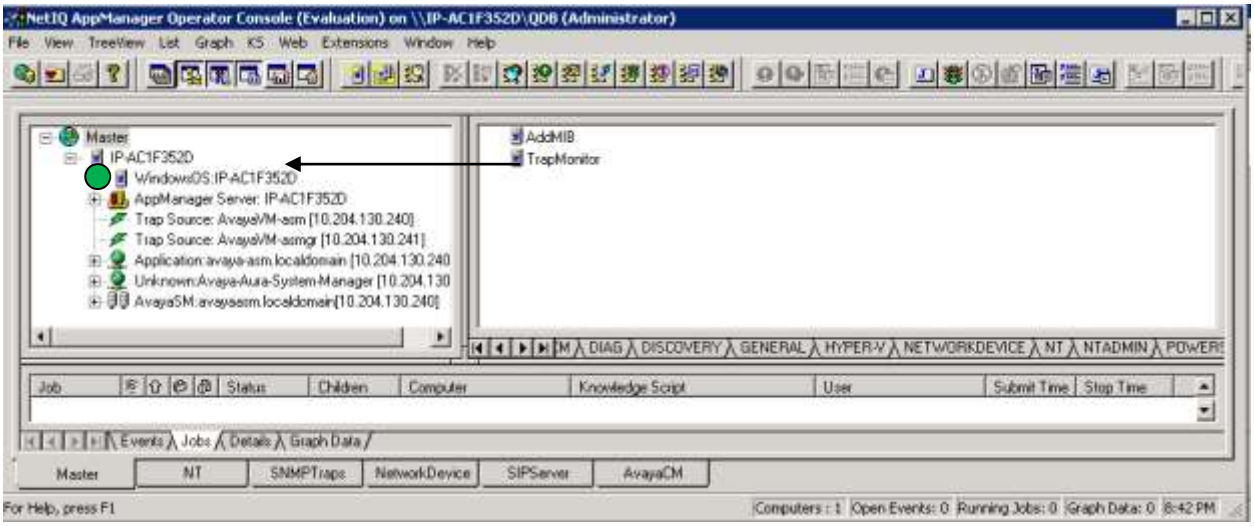
netsh advfirewall firewall add rule name="Open SNMP Trap Port" dir=in action=allow protocol=UDP localport=162



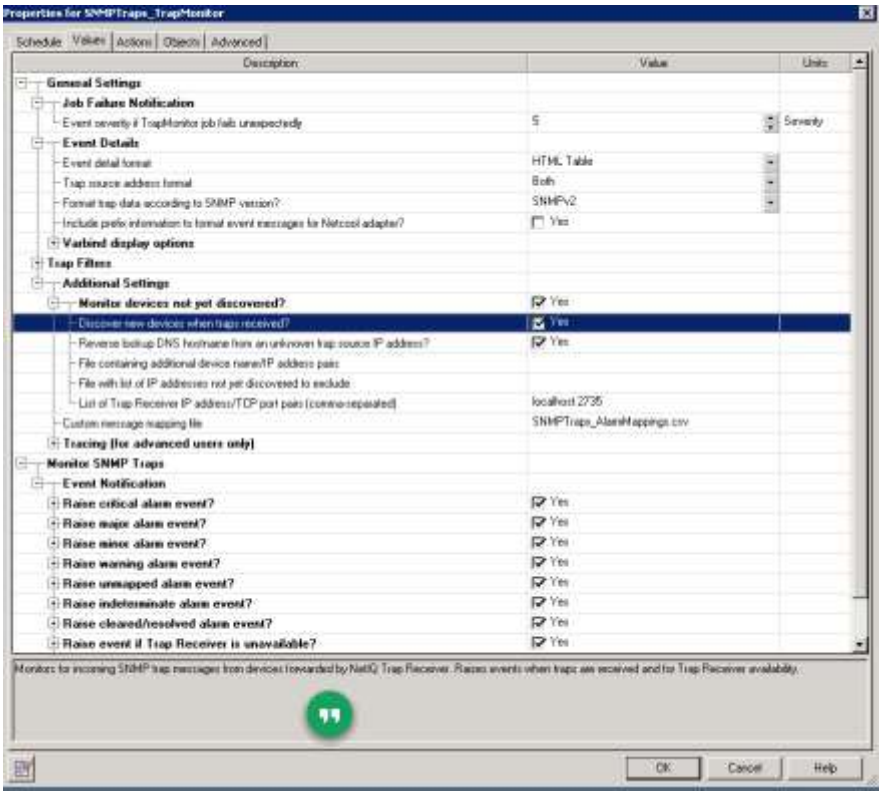
If there are any network firewalls which may block SNMP traps, a rule should be added there as well at this time.

6.4.2. Start Trap Monitoring

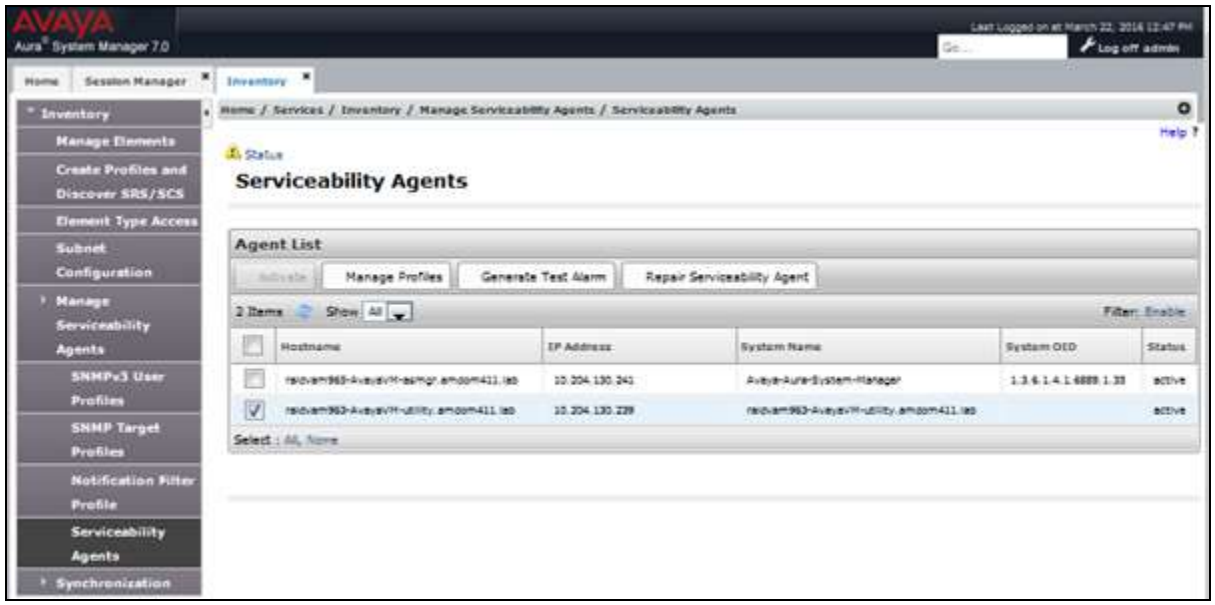
To start trap monitoring drop a copy of the SNMPTraps_TrapMonitor Knowledge Script on the agent computer.



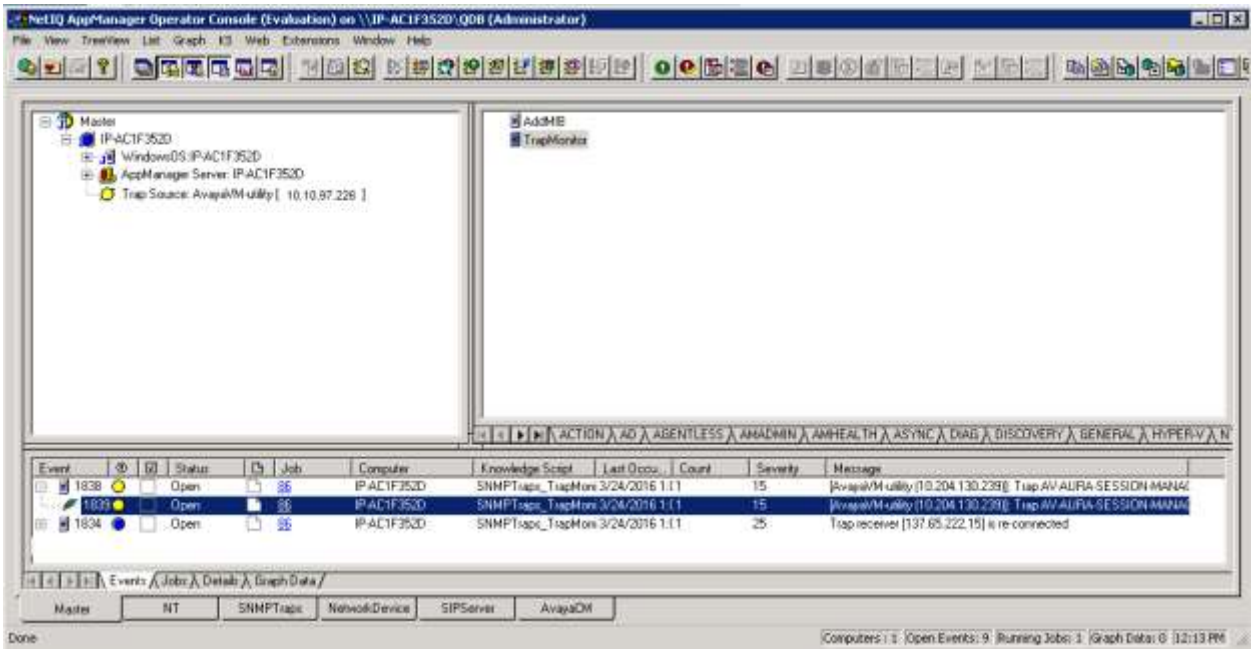
Make sure job detail with the “Monitor devices not yet discovered” and “Discover new devices when traps received” options checked:



On System Manager, send test trap from Session Manager to AppManager by select Session Manager in **Serviceability Agents** page, click on **Generate Test Alarm** button.



Confirm that the SNMPv2 trap source, Session Manager at 10.10.97.226, is now discovered and appears in the treeview.

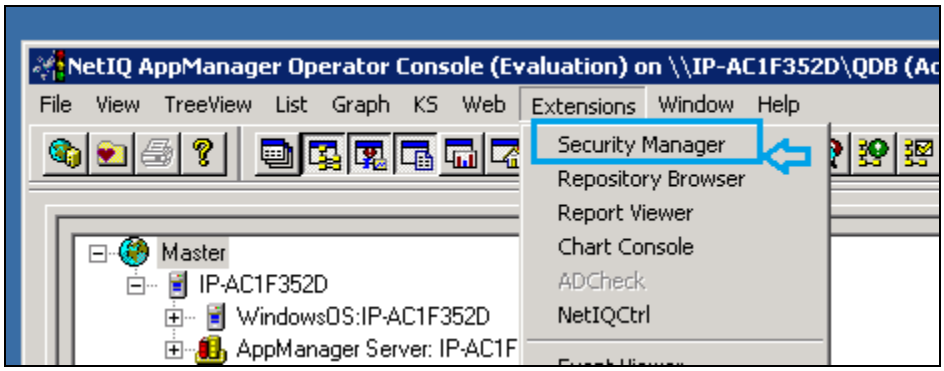


6.5. Configure SNMPv3 trap Monitoring

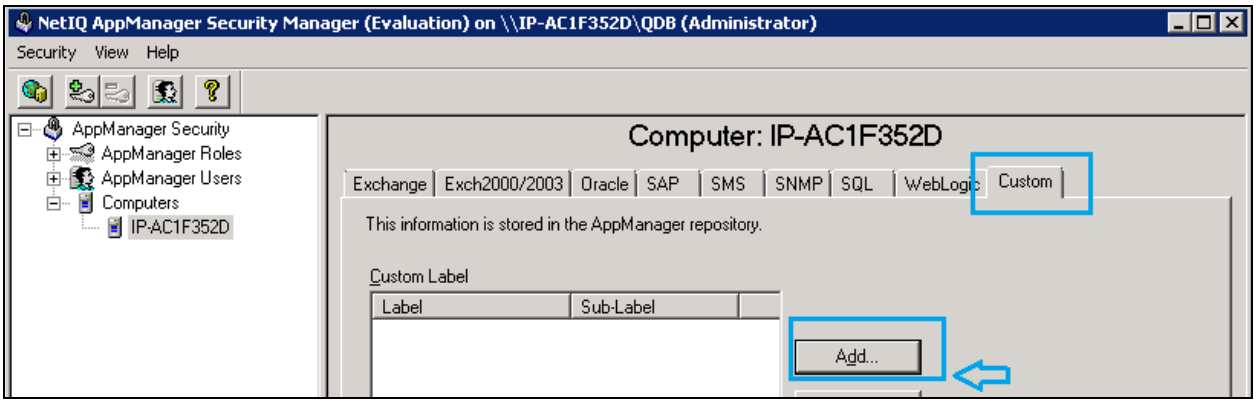
6.5.1. Configure Security Manager

To enable AppManager to use SNMP to access Session Manager and System Manager devices, the SNMP community strings are required to be configured in the AppManager Security Manager.

From the AppManager Operator Console window navigate to **Extensions → Security Manager** as shown in below.



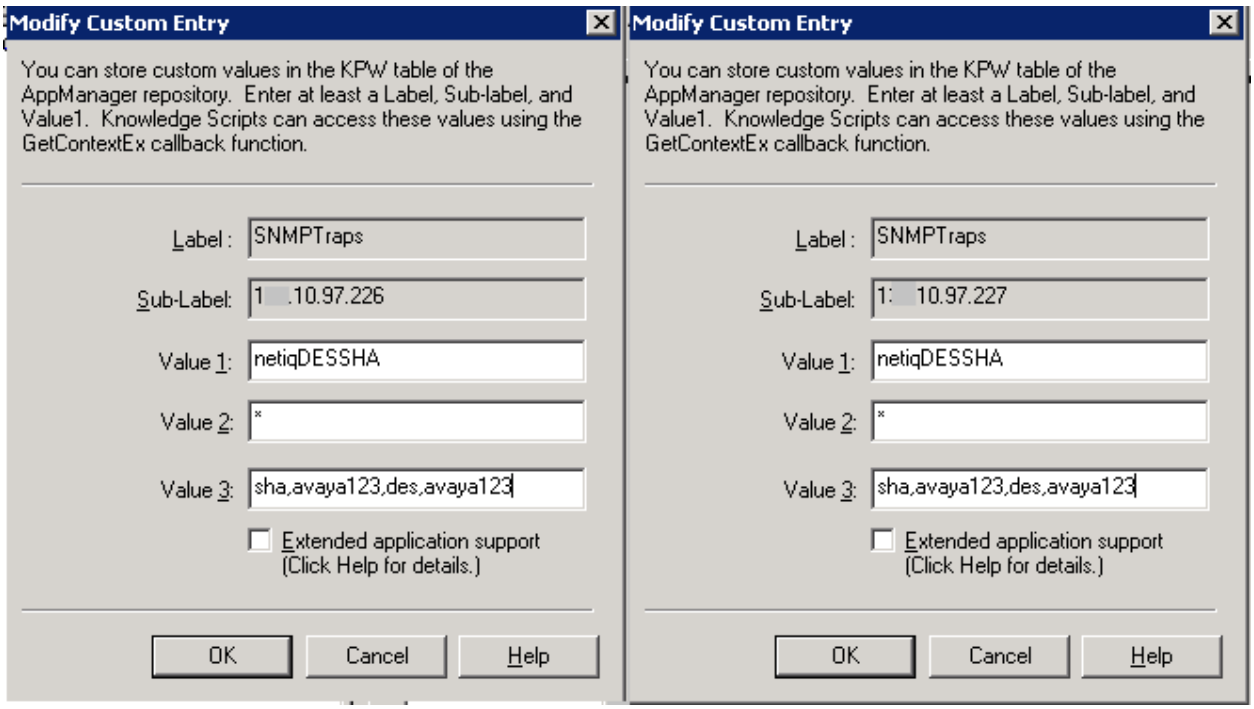
Add a custom profile:



Enter the System Manager SNMPv3 User Profile created in **Section 5.3** as example display below used during compliance test for Security Manager:

- **Label**: Enter any descriptive name, ex: SNMPTraps.
- **Sub-Label**: Enter System manager's IP Address, ex:10.10.97.226.
- **Value 1**: Enter user name created in Section 5.3.
- **Value 2**: Enter *.
- **Value 3**: Enter user created in Section 5.3 passwords, ex: sha,avaya123,des,avaya123.

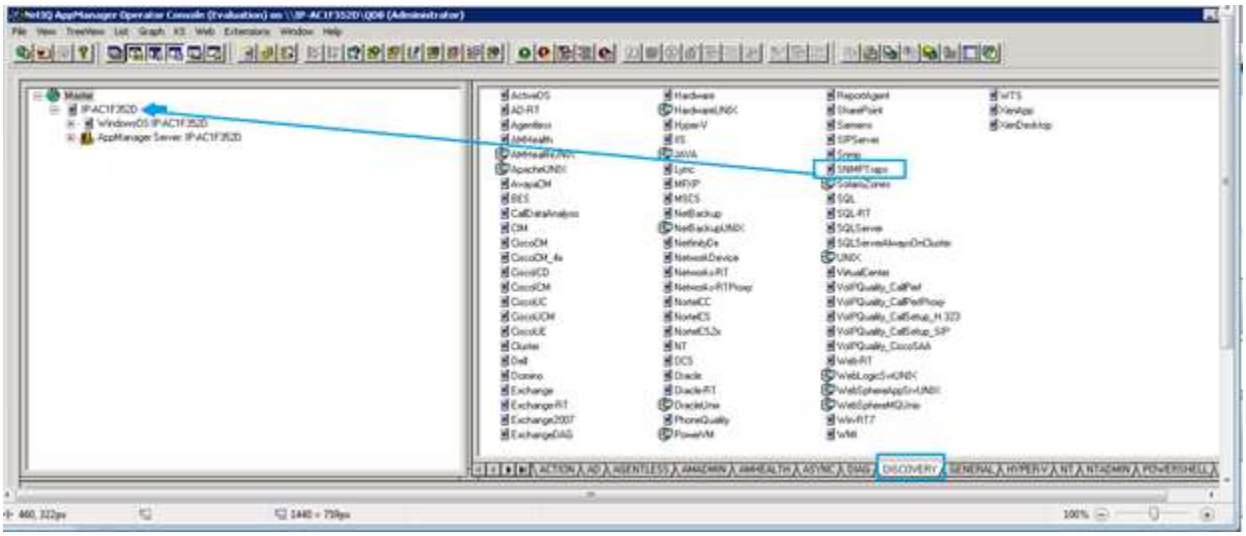
Create the same entry with Sub-Label is Session Manager's IP address, ex: 10.10.97.227 as display below:



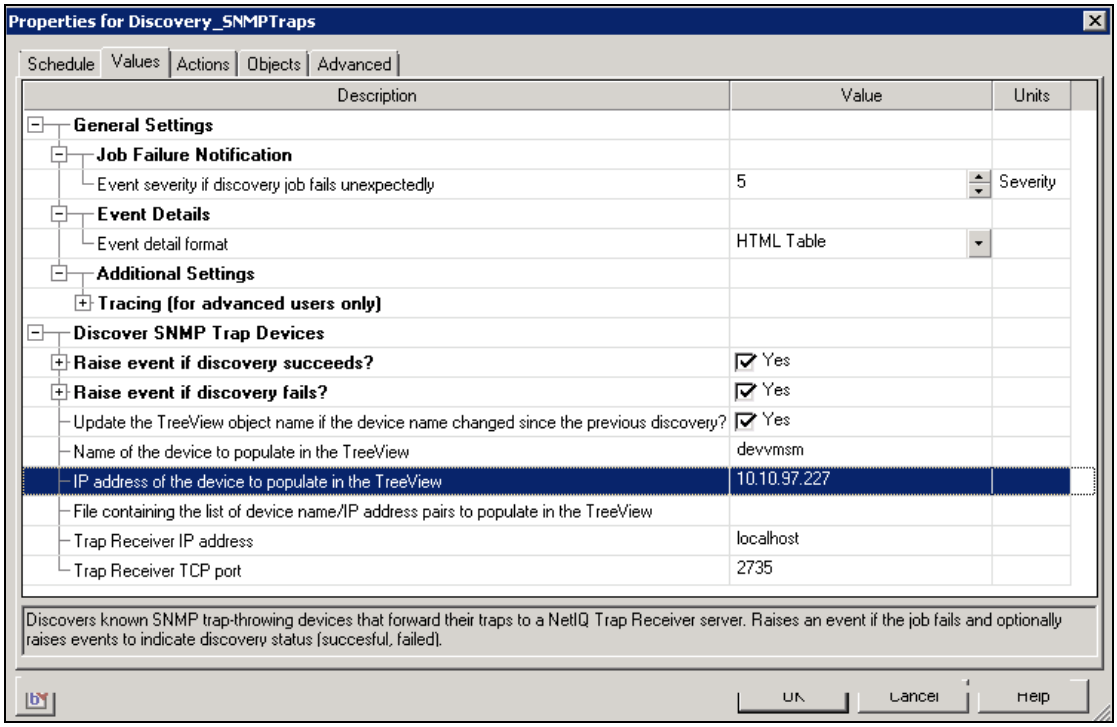
6.5.2. Discover the Device

To monitor SNMP trap source devices that require the use of SNMP v3, run the Discovery_SNMPTraps Knowledge Script on the agent computers which monitor those source devices.

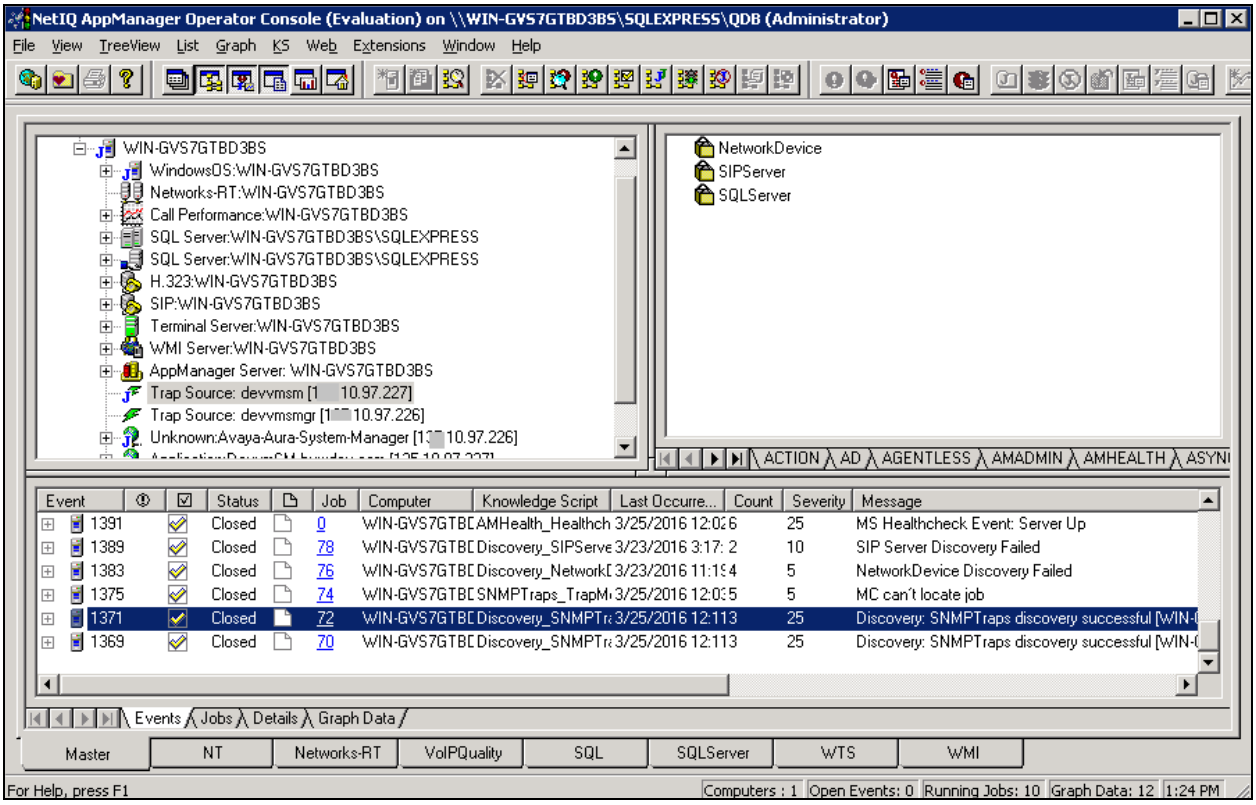
Navigate to the "**Discovery**" tab and drop the "SNMPTraps" Discovery KS (Knowledge Script) on the agent machine in the treeview to create the discovery job.



On the job creation panel, enter the name and IP address of the Session Manager.

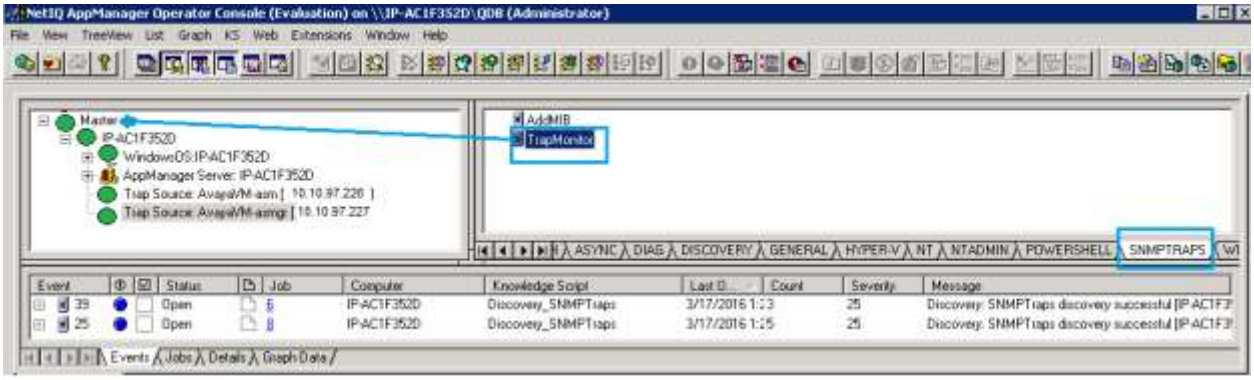


Confirm that Session Manager appears in the treeview (which confirms the SNMPv3 credentials are valid and the NetIQ trap receiver service is available on the agent), in this case, it is Trap Source: devvmsm[10.10.97.226] and Trap Source: devsmgr[10.10.97.227]

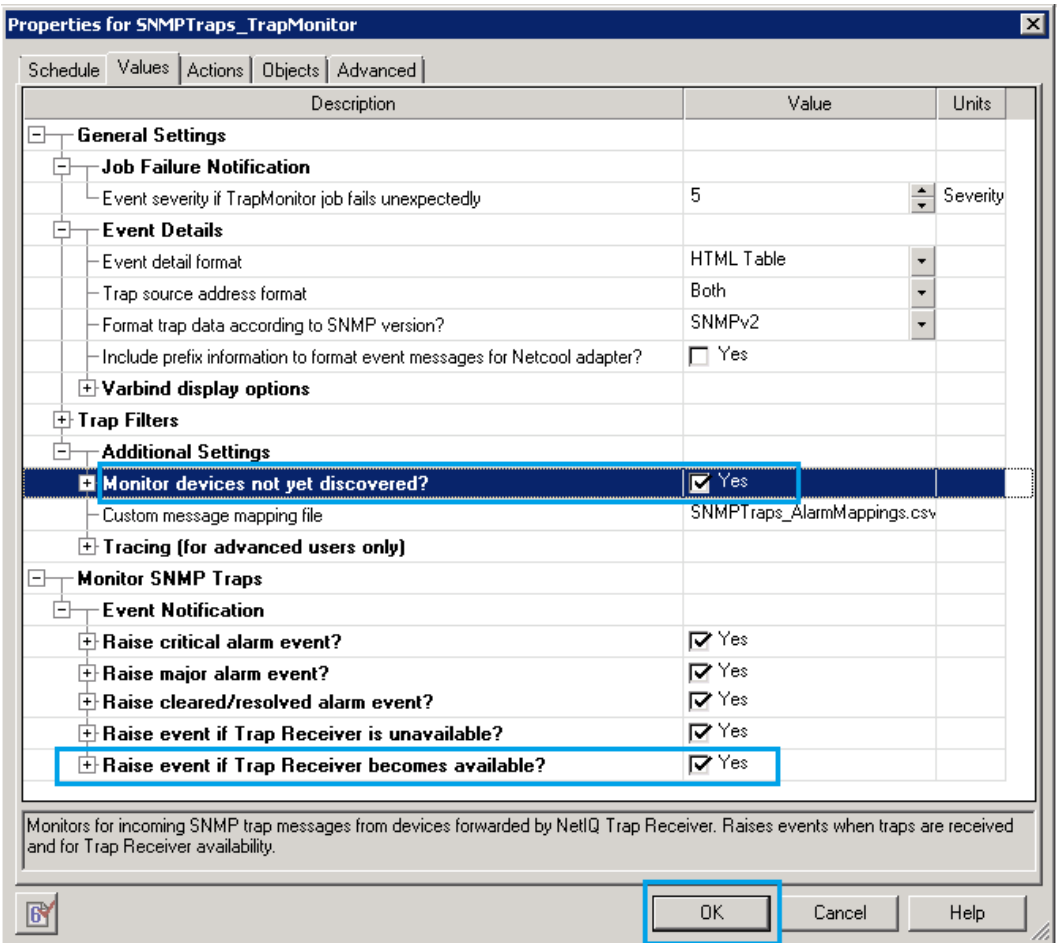


6.5.3. Start Trap Monitoring

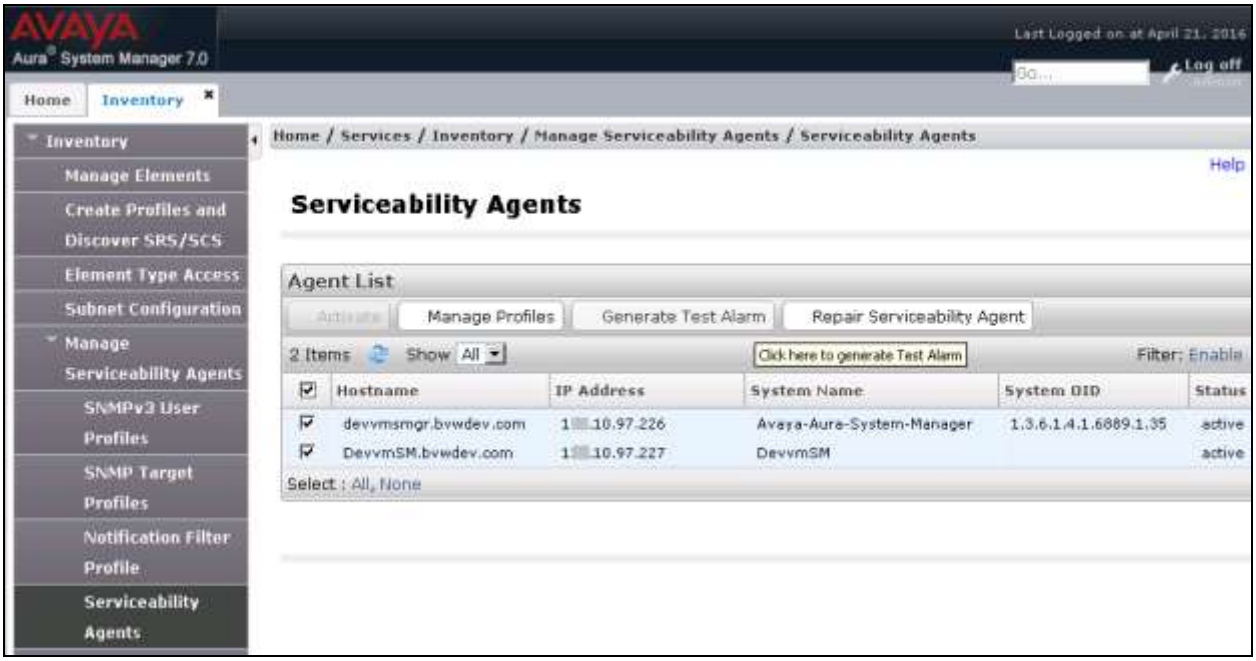
Next, run the SNMPTraps_TrapMonitor Knowledge Script on the agent computer and any SNMPv3 trap sources discovered in the treeview:



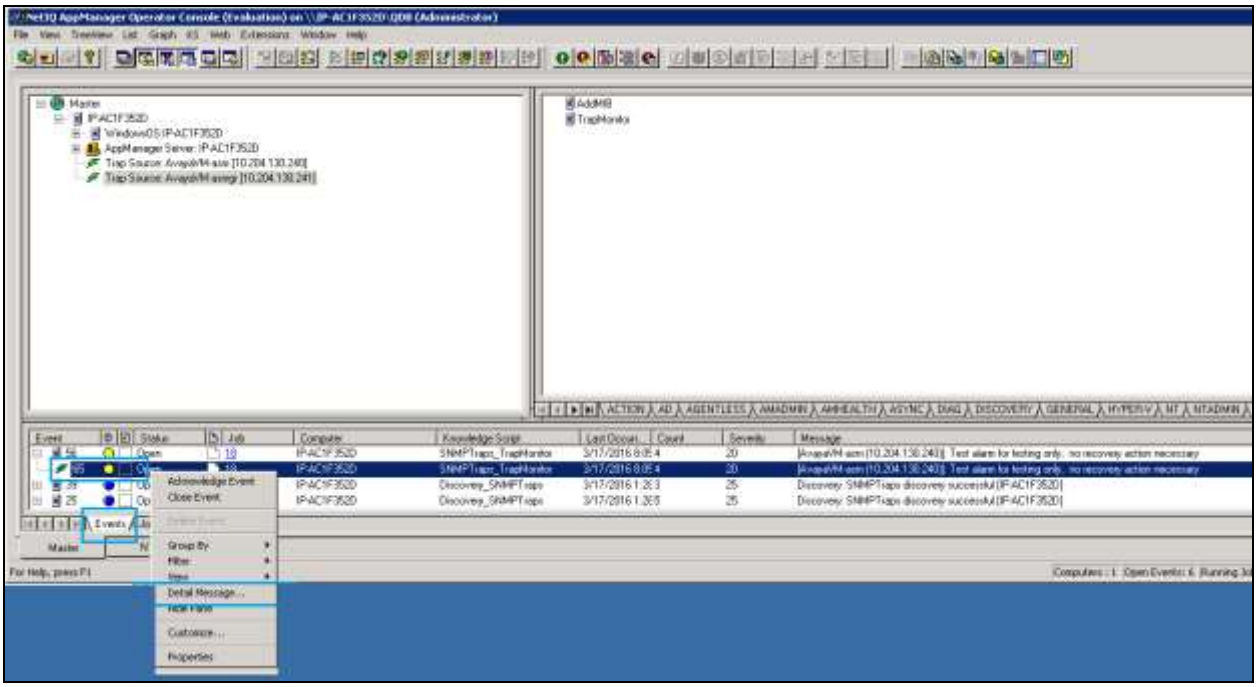
In the job detail make sure **Monitor devices not yet discovered?** and **Raise event if Trap Receiver become available**? options are checked.



Finally, generate a test trap from the System Manager by select system to send trap, in this case they are Session Manager and System Manager, then click on **Generate Test Alarm** button as display in below screenshot:

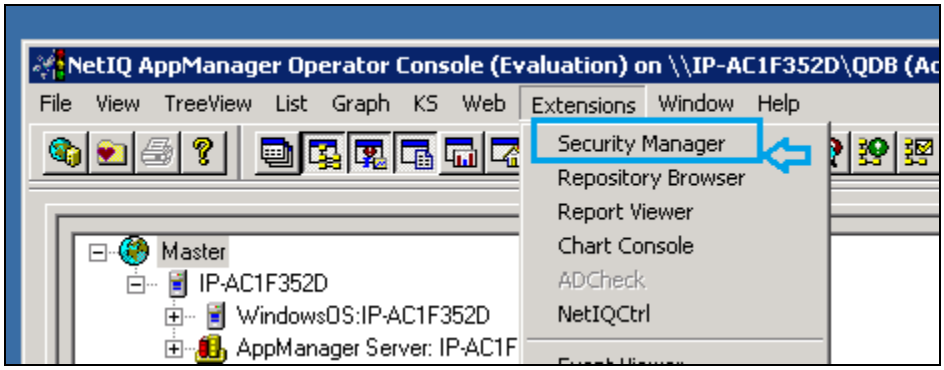


The test trap and any subsequent traps received will be reported in the AppManager console as events:

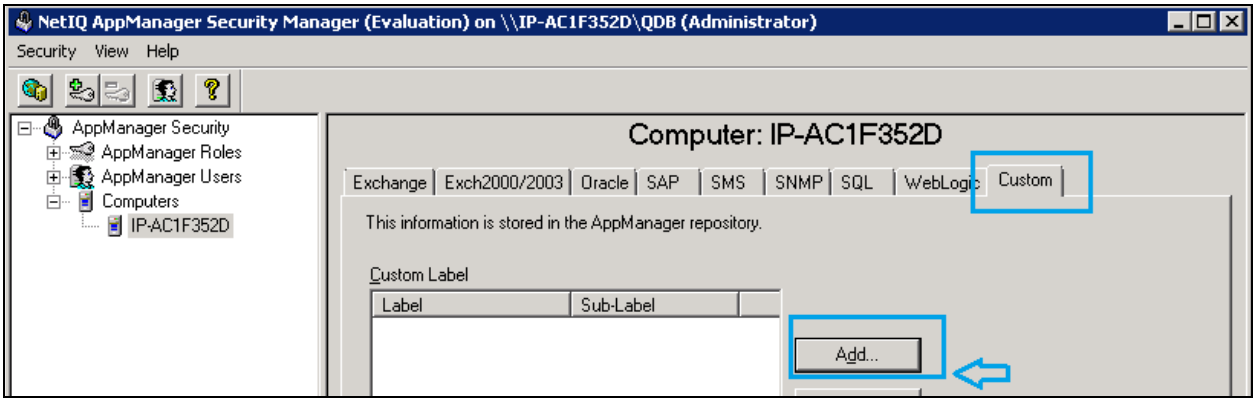


6.5.4. Administer Network Device

AppManager for NetworkDevice discovers the session and system manager using SNMP to query the device characteristics. To use SNMP, create the SNMP access credentials as follows: First, create an SNMP profile for the session manager. Note that this is different from the "AppManager for SNMPTraps" profile created in **Section 6.5.1** because it is for snmp-get requests from the networkDevice module. Here we are entering SNMPv3 profile for session manager and system manager by select security manager:



Add a custom profile:

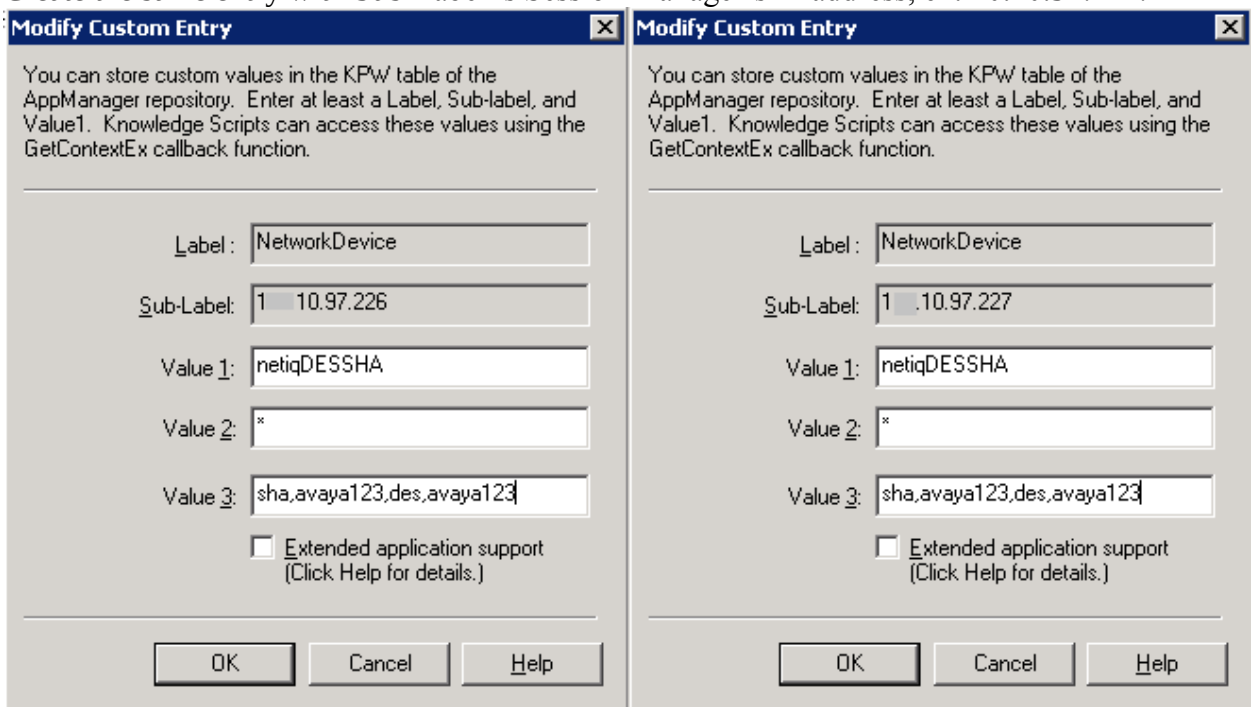


Enter the System Manager SNMP profile into security manager. If all devices on your network will use the same SNMP configuration, enter "default" as the label2 string. If they are each different, enter the active IP address of the device as the label2 string:

Enter the System Manager SNMPv3 User Profile created in **Section 5.3** as example display below used during compliance test for Security Manager:

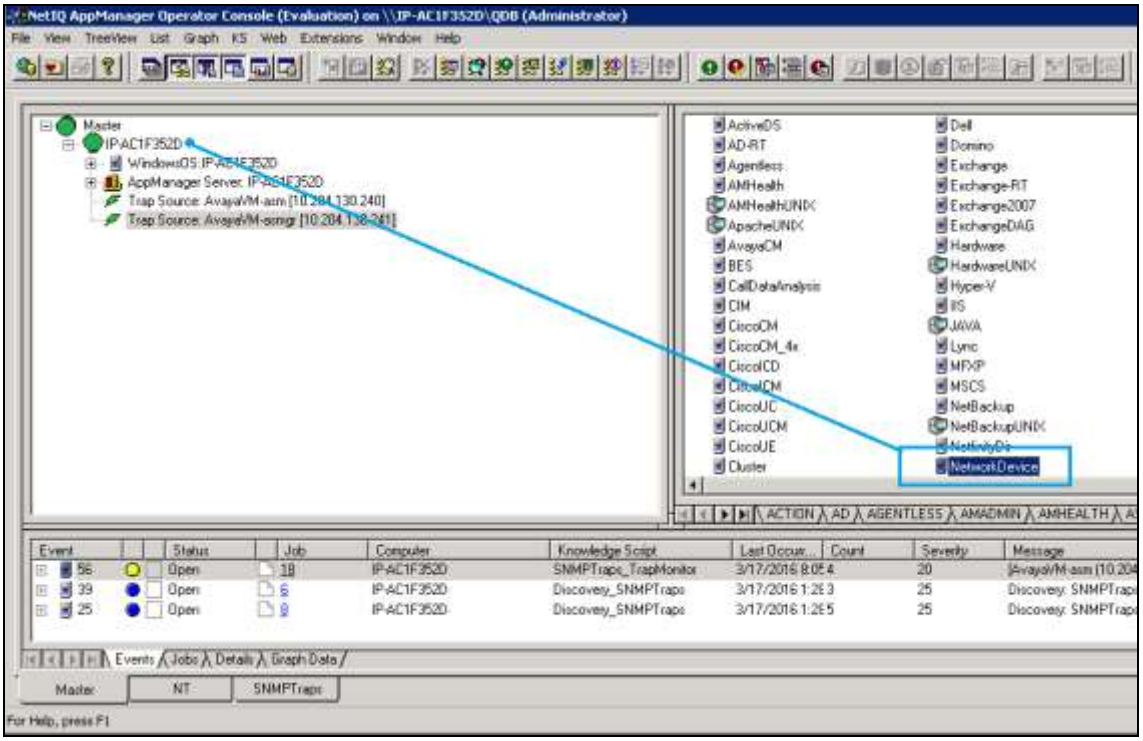
- **Label**: Enter any descriptive name, ex: NetworkDevice.
- **Sub-Label**: Enter System manager's IP Address, ex:10.10.97.226.
- **Value 1**: Enter user name created in Section 5.3, ex: netiqDESSHA.
- **Value 2**: Enter *.
- **Value 3**: Enter user created in Section 5.3 passwords, ex: sha,avaya123,des,avaya123.

Create the same entry with Sub-Label is Session Manager's IP address, ex: 10.10.97.227.

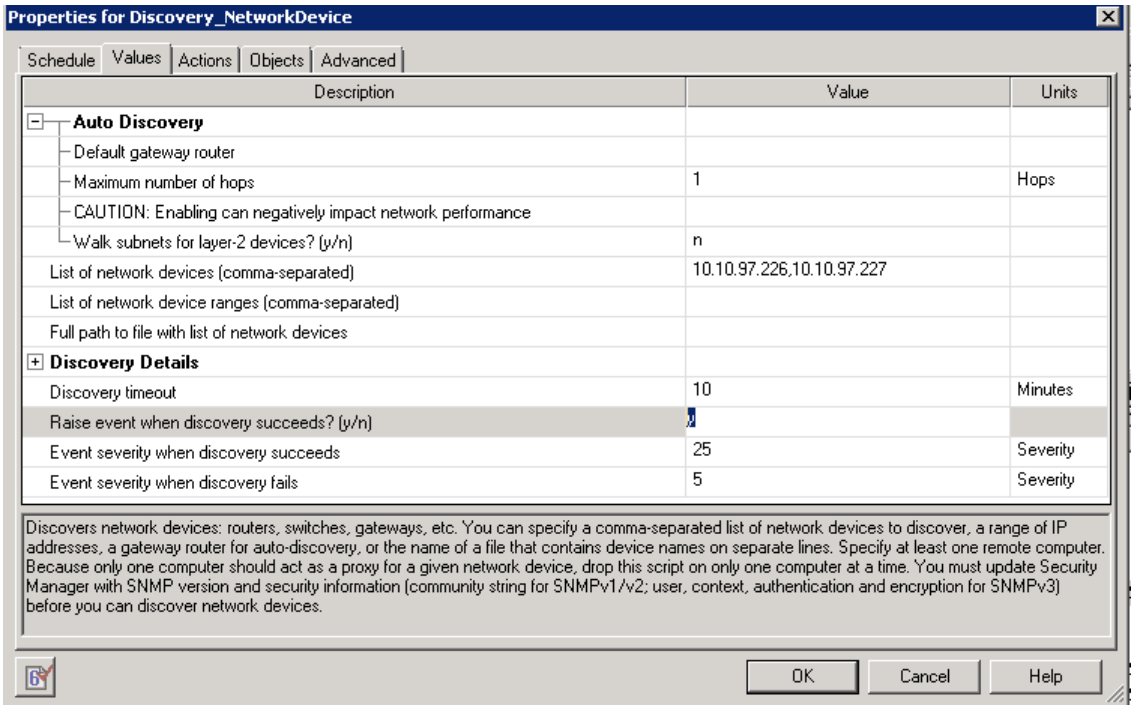


6.5.5. Discover the Device

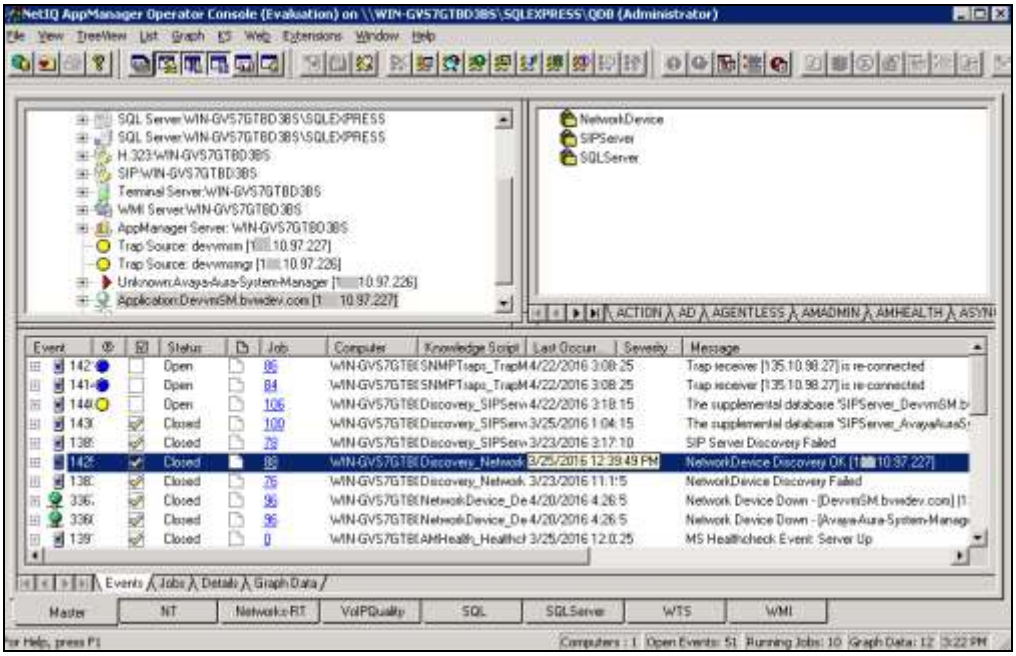
Navigate to the “Discovery” tab and drop the “NetworkDevice” Discovery KS on the agent machine in the treeview to create the discovery job for the devices.



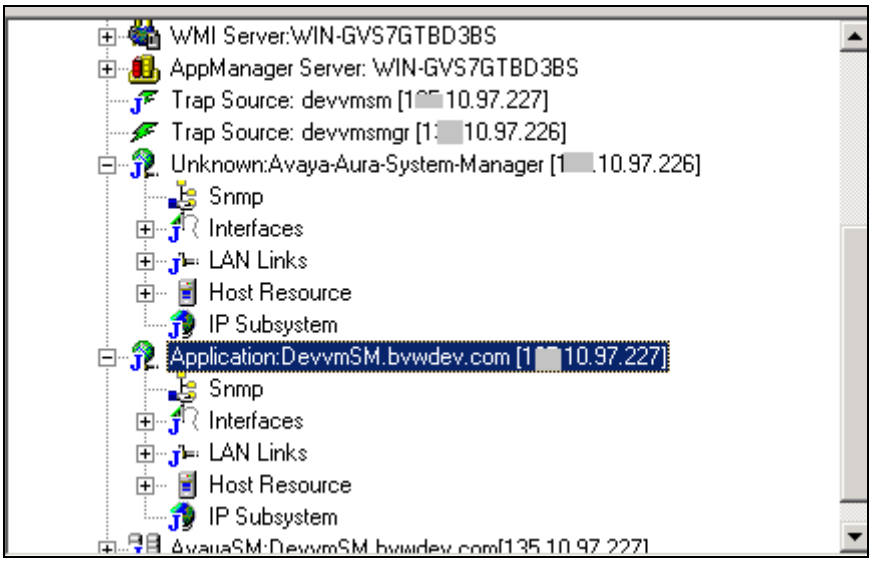
Enter the IP address of Session Manager and system manager in the job properties for **List of network devices (comma-separated),** in this case 10.10.97.226,10.10.97.227.



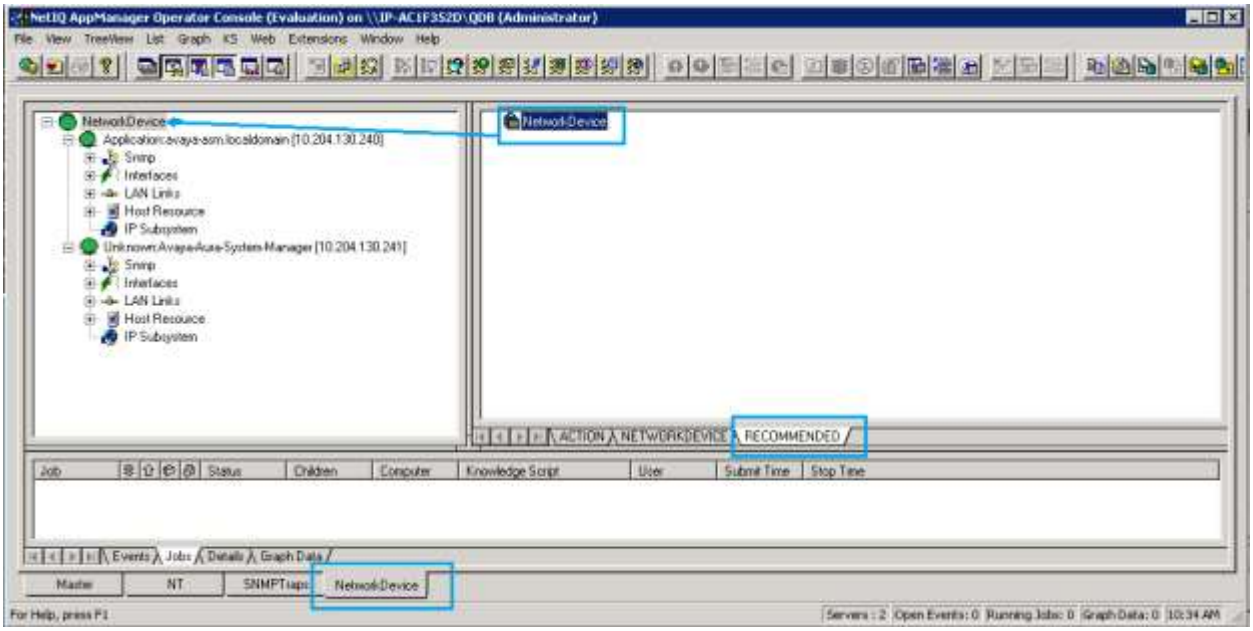
Discovery will create treeview objects for the Session Manager and System Manager using SNMP
Unknown: Avaya-Aura-System-Manager [10.10.97.226] and Application: DevvnSM.bvwdev.com[10.10.97.227] Discovery Network OK



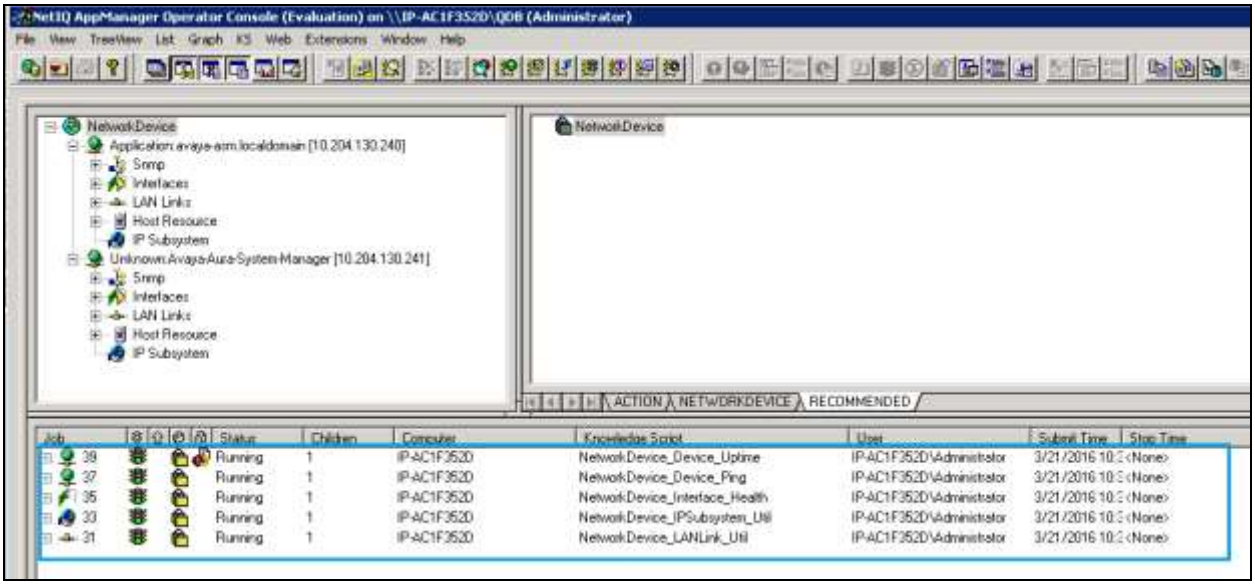
Click on the treeview object to verify that platform details are available for both session and system manager are listed such as Snmp, Interfaces, LAN links, Host Resource and IP Subsystem.



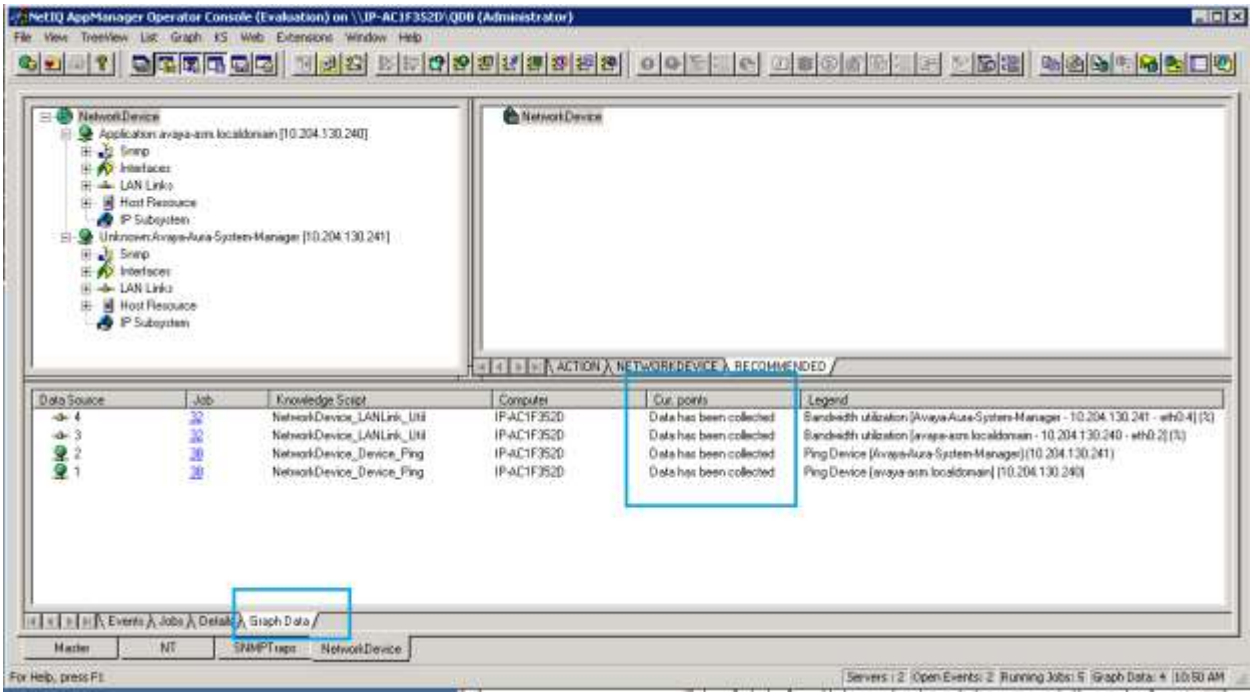
Start the **NetworkDevice** recommended knowledge script group for monitoring each device.



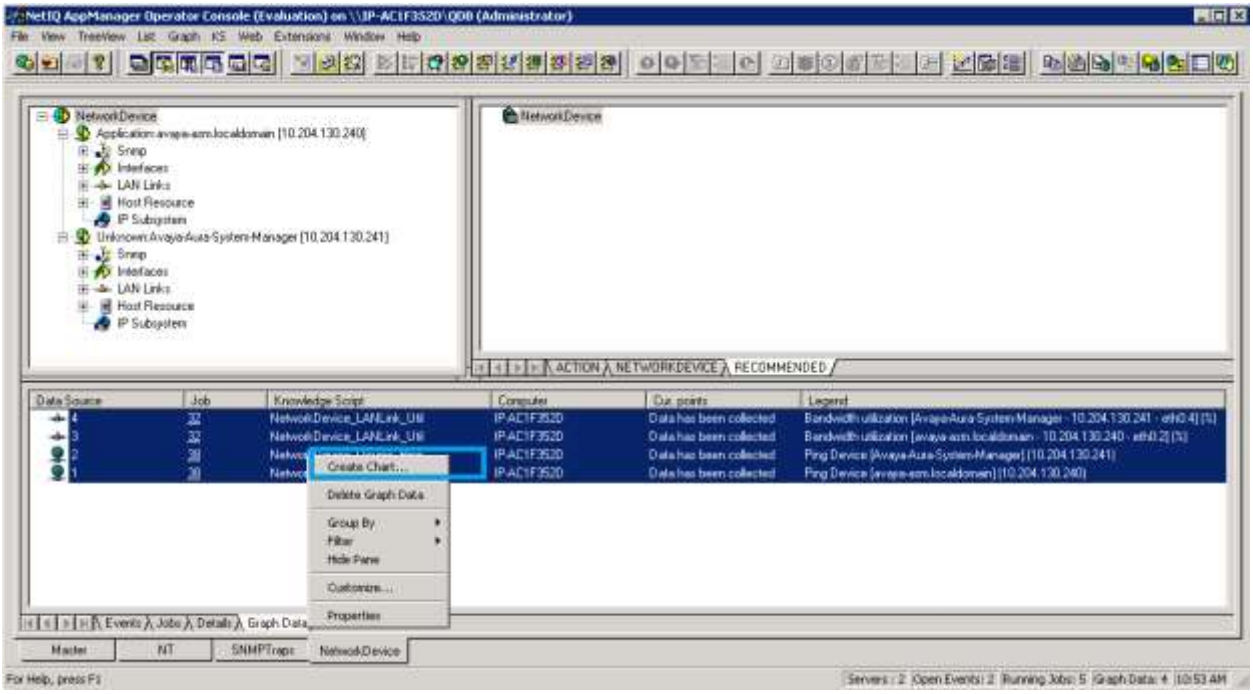
Confirm that the following device monitoring jobs have started: NetworkDevice_Device_Uptime, NetworkDevice_Device_Ping, NetworkDevice_Interfaces_Health, NetworkDevice_IPSubsystem_Ulti and NetworkDevice_LANLink_Ulti as shown in below screenshot.



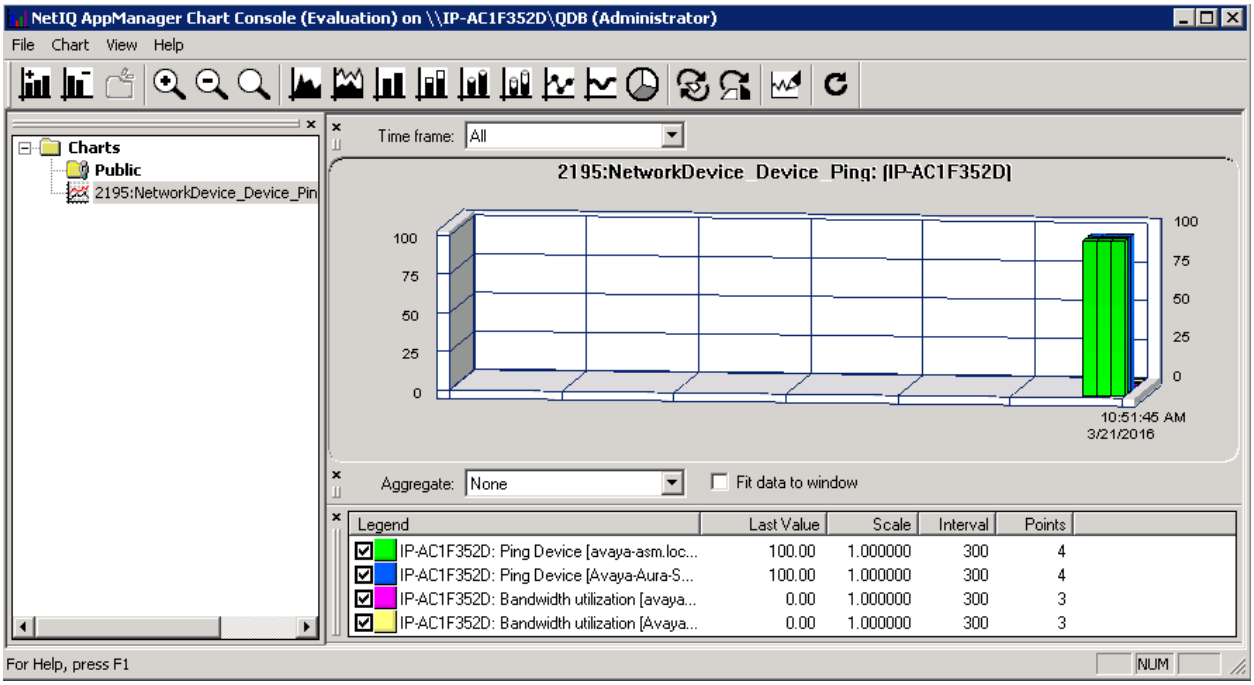
After a monitoring interval has been completed, data streams will be visible in the Graph Data pane as shown in below screenshot.



This data may be displayed as a graph using “Create Chart” as display in below screenshot.



Below display the NetworkDevice_Device_Ping data in graphic chart.



7. Verification Steps

The following tests were conducted to verify the solution between the Session Manager, System Manager and AppManager Application.

- Ensure AppManager can discover Session Manager via SNMPv2 as display in last part of **Section 6.4**.
- Ensure AppManager can discover Session Manager and System Manager and their devices detail via SNMPv3 as displayed throughout in **Section 6.5**.

8. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 2**. The NetIQ AppManager 9.1 is considered compliant with Avaya Aura® Session Manager and Avaya Aura® System Manager 7.0.

9. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at http://support.avaya.com.

1. *Administering Avaya Aura® Session Manager Release 7.0 Issue 1 August 2015*
2. *Administering Avaya Aura® System Manager for Release 7.0 Issue 1 January 2016*

Product documentation for NetIQ AppManager may be found at:

1. *Administrator Guide NetIQ® AppManager® April 2016 on https://www.netiq.com/documentation/appmanager-9/pdfdoc/administratorguide/administratorguide.pdf*
2. *Net IQ online documents:*

NetIQ AppManager for SIP Server Management Guide March 21 https://www.netiq.com/documentation/appmanager-modules/appmanagerforsipserver/data/b19cptxp.html
SNMP Traps Knowledge Scripts https://www.netiq.com/documentation/appmanager-modules/appmanagerforsnmptraps/data/snmptraps_trapmonitor.html