

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 Section 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: <u>Support@netiq.com</u>
- Web Site: <u>https://www.netiq.com/support/default.asp</u>

## 3. Reference Configuration

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

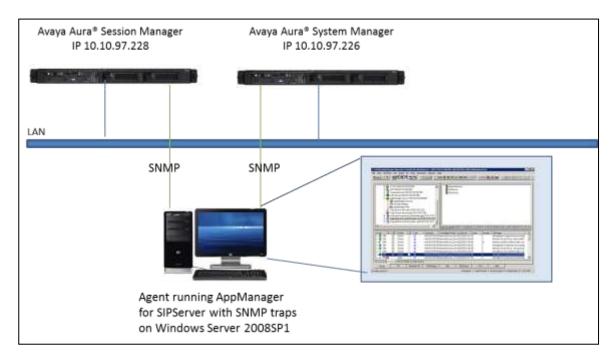


Figure 1: Test Solution Configuration

## 4. Equipment and Software Validated

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

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

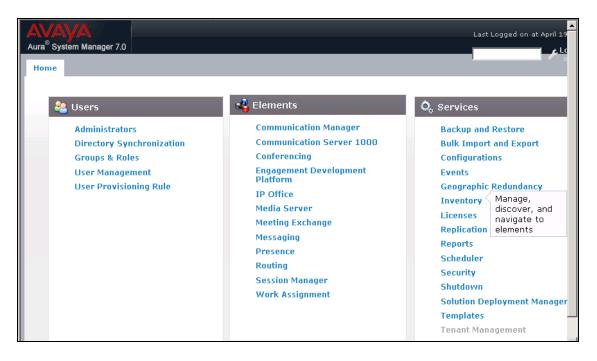
This section describes the steps to configure Session Manager and System Manager to work with AppManager.

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**  $\rightarrow$  **Inventory** as show below:



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

os://devvmsmgr.bvwdev.com/SMGi								
Element Type Access	Pro	Profile List						
Subnet Configuration								
Manage	2 Ite	2 IteCreate New SNMP Target Profile Filter: Enable						
Serviceability Agents		Name	Domain Type	IP Address	Port	SNMP Version		
SNMPv3 User		netiqSNMPv2	UDP	1 5.10.98.27	162	V2		
Profiles		netiqDESSHAtraps	UDP	1.0.98.27	162	V3		
SNMP Target	Selec	t : All, None						
Profiles								
Notification Filter								
Profile								
Serviceability								
Agents								
Synchronization								

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.

<pre>//devvmsmgr.bvwdev.com/SMGR/</pre>		🚹 🔹 🔊 👻 📇 🖶 🔹 Page 🔹 Safety 🔹 Tools 🔹 🌘
Manage Elements Create Profiles and Discover SRS/SCS	View Target Profile	Edit Done
Element Type Access	Target Details * Attach/Detach User Profile	
Subnet Configuration	Target Details 👳	
Manage Serviceability Agents	Name: hetiqSNMPv2	
SNMPv3 User	Description:	
Profiles	IP Address: 100.10.98.27	
SNMP Target Profiles	Port: 162	
Notification Filter	Notification Type: Trap 🗾	
Profile	Protocol: V2 💌	
Serviceability	Community: public	
Agents		
Synchronization	*Required	Edit Done

#### 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.

Attps://devvmsmgr.bvwdev.com/SMGF					🖃 🖶 👻 Page 👻 Safety	→ Tools →
Tinventory	Home	/ Services / Inventory /	Manage Serviceabilit	y Agents / Serviceability	Agents	
Manage Elements						Help ?
Create Profiles and Serviceability Agents						
Discover SRS/SCS						
Element Type Access	Age	nt List				
Subnet Configuration	A	ctivate Manage Profile	es 👘 Generate Test /	Alarm Repair Serviceab	ility Agent	
▼ Manage	2 Iter	ms   🍣   Show All 🗾 🛄	here to manage the profiles		Filter	:Enable
Serviceability Agents		Hostname	IP Address	System Name	System OID	Status
SNMPv3 User		devvmsmgr.bvwdev.com	1 .10.97.226	Avaya-Aura-System- Manager	1.3.6.1.4.1.6889.1.35	active
Profiles		DevvmSM.bvwdev.com	1.10.97.227	DevvmSM		active
SNMP Target	Selec	t : All, None				_
Profiles						
Notification Filter						
Profile						
Serviceability						
Agents						

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.

					Last Logged on at A
Aura <sup>®</sup> System Manager 7.0 Home Inventory ×					
Tinventory	Home / Services / Inv	entory / Manage Servicea	bility Agents / Servicea	bility A	gents
Manage Elements	Manage Prof	file			Commit Back
Create Profiles and	manaye rivi				Commic Back
Discover SRS/SCS					
Element Type Access	Selected Agents	SNMP Target Profiles	SNMPv3 User Profile	s	
Subnet Configuration	Assignable Pro	ofiles 💂			
▼ Manage	<b></b>				
Serviceability Agents	Assign				
SNMPv3 User	1 Iter <mark>Click to Assign</mark>				
Profiles	✓ Name	Domain Type	IP Address	Port	SNMP Version
SNMP Target	netiqSNMPv2	2 UDP	110.98.27	162	V2
Profiles	Select : All, None				

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**  $\rightarrow$  **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 Passw	vord: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.

AvayA Aura <sup>®</sup> System Manager 7.0		Last Logged	l on at A
Home Inventory ×			
Tinventory 4	Home / Services / Inventory / Manage Serviceability Agents / SNMPv3 User Profiles		
Manage Elements Create Profiles and	New User Profile	Commit	Back
Discover SRS/SCS Element Type Access Subnet Configuration	User Details * User Name: netiqDESSHA		
Manage Serviceability Agents	<ul> <li>* Authentication Protocol: SHA </li> <li>* Authentication Password: •••••••</li> </ul>		
SNMPv3 User Profiles	* Confirm Authentication Password: •••••••• * Privacy Protocol: DES 🔽		
SNMP Target Profiles Notification Filter	* Privacy Password:     •••••••      * Confirm Privacy Password:     •••••••		
Profile	* Privileges: Read/Write		
Agents	*Required	Commit	Back

#### 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.

AVAVA Aura <sup>®</sup> System Manager 7.0		
Home Inventory ×		
Tinventory	Home / Services / Inventory / Manage Serviceability Agents /	SNMP Target Profil
Manage Elements	Now Target Profile	Commit Back
Create Profiles and	New Target Profile	Commit Back
Discover SRS/SCS		
Element Type Access	Target Details * Attach/Detach User Profile	
Subnet Configuration	Target Details 👻	
▼ Manage	* Name: netiqDESSHAtraps	
Serviceability Agents		
SNMPv3 User	Description: V3 SNMP trap	
Profiles	* IP Address: 10.10.98.27	
SNMP Target	* Port: 162	
Profiles	* Notification Type: Trap	
Notification Filter	* Protocol: V3 V	
Profile		
Serviceability		
Agents	*Required	Commit Back

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.

Create Profiles and	Serviceability Age	ents			
Discover SRS/SCS Element Type Access	Agent List				
Subnet Configuration	Activate Manage Profi	iles Generate Test Ala	rm Repair Serviceability Ag	ent	
▼ Manage	2 Items 🛛 🍣 🗆 Show 🛛 🖬 🖃 👘	Click here to manage the profiles		Filter:	Enable
Serviceability Agents SNMPv3 User	✓ Hostname	IP Address	System Name	System OID	Status
Profiles	DevvmSM.bvwdev.com	1.10.97.227	DevvmSM		active
SNMP Target	devvmsmgr.bvwdev.com Select : All, None	1: .10.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
Profiles	Select : All, None				
Notification Filter					
Profile					
Serviceability					
Agents					

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

* loventory	Home / Services / Inventory	/ Manage Service:	bility Agents / Serviceability Ag	ents			
Manage Elements	Managa Basfila			14000	mit Bad		
Create Profiles and Discover SRS/SCS	Manage Profile			Com	niti bao		
Element Type Access	Selected Agents SNMP	Target Profiles	SNMPv3 User Profiles				
Subnet Configuration	Selected Agents +						
<ul> <li>Manage</li> <li>Serviceability Agents.</li> </ul>	2 Items 2 Filter: Enable						
SNMPv3 User	Hostname	IP Address	System Name	System OID	Status		
Profiles	DevvmSM.bvwdev.com	10.97.227	DevvmSM		active		
SNMP Target	devymsmgr.bywdev.com	1=.10.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active		
Profiles							
Notification Filter				Com	mit Bad		
Profile				- Abbarran			
Serviceability							
Agents							

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:

Manage Elements Create Profiles and Discover SRS/SCS	Manage	e Profile		Commit B			
Element Type Access	Selected A	gents SNMP Ta	rget Profiles	SNMPv3	3 User Profiles		
Subnet Configuration " Manage Serviceability Agents	Assign	able Profiles 🔹					
SNMPv3 User Profiles	2 10 Cid	to Assign	Domain	Type	IP Address	Port	SNMP Version
SNMP Target Profiles	E n	etiqSNMPv2 etiqDESSHAtraps	UDP		105.10.98.27	162 162	V2 V3
Notification Filter Profile	Select : /	All, None					2.00
Serviceability	Remov	able Profiles 🔹					

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

- Inventory	Home / Servi	ces / Invent	ory / Manage Service	ability Agents / 9	Serviceability Agents		
Manage Elements	Manage	. Drafil				Commit Back	
Create Profiles and Discover SRS/SCS	Manage	e Profile	3			Commit Back	
Element Type Access	Selected	Selected Agents SNMP Target Profiles SNMPv3 User Profiles					
Subnet Configuration	Assian	able Profi	les =				
* Monage Serviceability Agents	Assign						
SNMPv3 User	1 1t Cld.	to Assign					
Profiles	1 U	ser Name	Authentication	Protocol	Privacy Protocol	Privileges	
SNMP Target	n 14	etiqDESSHA	SHA		DES	R.	
Profiles	Select :	Ail, None					
Notification Filter Profile	Remo	vable Prof	iles 🔹				
Serviceability	Remove						
Agents	0 Items	2					

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

lected Agents	SNMP Target Prof	iles SNMPv3 Use		
	SNMP Target Prof	ilos SNMDu3 Hee		
			er Profiles	
Assignable Pr	ofiles 🔹			
···· <b>·</b>				
Assign				
0 Items I 🍣				
🔲 User Name	Authenticati	on Protocol	Privacy Protocol	Privileges
No records t	o display			
Removable P	rofiles 💿			
Remove				
1 Item   🍣				
User Name	e Authenti	cation Protocol	Privacy Protocol	Privileges
netiqDESSI	HA SHA		DES	R
Select : All, None				
				Commit Bac
	D Items 2 User Name No records to Removable P Remove 1 Item 2 User Name netiqDESS	D Items       D Items     Image: Constraint of the second s	D Items 💝 User Name Authentication Protocol No records to display Removable Profiles • Remove I Item 😌 User Name Authentication Protocol netiqDESSHA SHA	D Items     Image: Constraint of the state o

## 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:

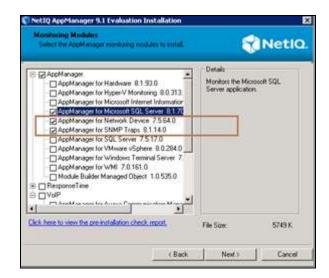
- AppManager Installation
- Activate the Netiq Trap Receiver Service
- Launch NetIQ Console
- Configure SNMPv2 Trap Monitoring
- Configure SNMPv3 trap Monitoring

#### 6.1. AppManager Installation

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

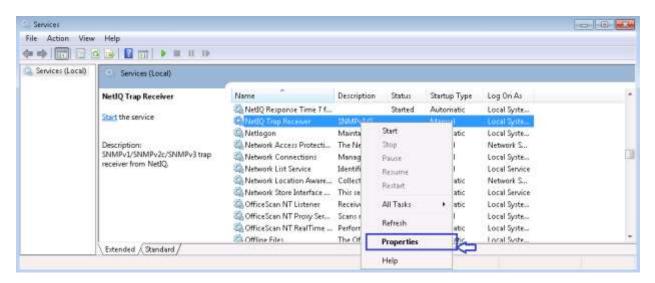
- <u>AppManager for NetworkDevice</u>
- <u>AppManager for SNMPTraps</u>

NetworkDevice and SNMPTraps modules are included in the AppManager 9.1 evaluation package available at <u>https://www.netiq.com/products/appmanager/trial.html</u> 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.

(a a)		NetlQ Trap Receiver Properties (Local Computer)	
🔍 Services (Local)	Start the service Description: SNMPv1/SNMPv2c/SNMPv3 trap receiver from NetQ.	General         Log On         Recovery         Dependencies           me         Service name:         NetQ Trap Receiver           NetZ         Display name:         NetQ Trap Receiver           NetZ         Description:         SNMPv1/SNMPv2c/SNMPv3 trap receiver from *           NetZ         Description:         Snmpro:           NetS         C-Vhogsam Files (x86)/NetIQ\TrapReceiver\bin\NetIQTrapReceiver.exx to *           NetS         Starbup typg:         Martual           Offic         Martual         *           Offic         Displayed         *	
		Office Start Store Permitter Bernaties That apply when you start the service from here.  Start paragretees  OK Cancel Apple	

#### 6.3. Launch NetlQ Console

In the NetIQ server navigate to Start  $\rightarrow$  All Programs  $\rightarrow$  NetIQ  $\rightarrow$  AppManager $\rightarrow$  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.

NetIQ AppManaq	ger Operator Console Logon	×
<u>S</u> erver: <u>R</u> epository:	WIN-GVS7GTBD3BS\SQLEXPRESS	
	formation: ⊻indows authentication : <u>Q</u> L Server authentication	
Net	tlQ® AppManager®	
Logon	<u>O</u> ffline <u>E</u> xit <u>H</u> elp	

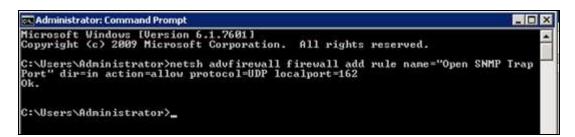
## 6.4. Configure SNMPv2 Trap Monitoring

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.

	C1F352D WindowsDS.IP.AC1F352D AppManager Server, IP.AC1 Trap Soucce: AvayaVM-an Trap Soucce: AvayaVM-an Application: avaya/asm.local Unknown/Avaya-Aua-Syste AvayaSM.avayasm.locald	1F3520 n [10.204.130.240] ngr [10.204.130.241] Idomain [10.204.130.240 em-Manager [10.204.130	TrepManitor		
			did to have a process of the	ENERAL \$ MARED 1/ 3 ME	THE PROPERTY AND A DESCRIPTION OF THE PROPERTY AND A DESCRIPTION OF A DESC
1			A A DIAG & DISCOVERY & G	CHENNE & HIVELDA VIAC	I WORKDEVICE A NI A NTADMIN A POW

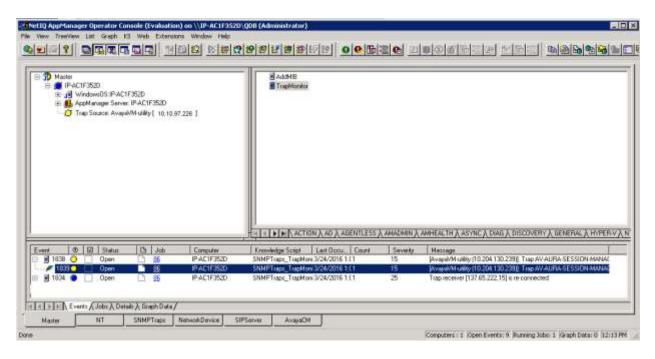
Make sure job detail with the "Monitor devices not yet discovered" and "Discover new devices when traps received" options checked:

Description	Value		Units	
- General Settings				
C Job Faihare Notification				
L Event seventy if TrapMonitor job faits unexpectedly	5		Seventy	
- Event Details				
- Event detail format	HTML Table			
- Tsap mucce addem firmal	Both	-		
- Format trap data according to SNMP version?	SNHPv2	-		
- Irichade prefix information to termat event meccages for Netcool adapte/?	IT Yes			
🗄 Varbind display options				
🗄 Trap Filters				
- Additional Settings				
- Monitor devices not pet discovered?	P Yes			
Discover new devices when traps received?	1 🔁 Yes			
- Reverse ballup DNS hostname him an unknown hap source IP address?	12 Yes			
- File containing additional device manw/IP address pairs				
- File with hit of IP addresses not per discovered to exclude				
List of Trap Receiver IP address/TDP part pairs (commonspecialed)	localhort 2735			
- Custom reescage mapping He	SNMPTraps_AlamMappings.cov			
F Tracing (for advanced users only)				
Manitor SNMP Traps				
🗄 — Event Notification				
Baise critical alarm event?	P Yes			
🗄 Raise major alarm event?	P Yei			
🔅 Raise minor alarm event?	R Yes			
🗄 Raise warning alars event?	I⊋ Yei			
Baise unsupped alarm event?	P Yes			
Raise indeterminate alarm event?	P Yes			
Faise cleared/resolved alarm event?	P Yei			
Baise event if Trap Receiver is unavailable?	P Yes			

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.

AVAVA Aura <sup>®</sup> System Manager 7.0			Ge	art Logged on at March 22, 201	
Home Session Hanaper	Inventory *				
* Inventory	. Nome / Services / Inventory / Manage Serviceation	tity Agents / Serviceabili	ty Againts		0
Manage Elements	I. Salar				Help 7
Create Profiles and Discover SRS/SCS	Serviceability Agents				
Element Type Access					
Subnet Configuration	Agent List Manage Profiles General	e Test Alarm   Repair	r Servicesbilty Agent		_
• Manage Serviceability	2 Itams 📚 Shaw Al	anarese word homoroom		Filer	n Enable
Agents	Hostname	LP Address	System Rame	Systam OED	Status
SNMPv3 User	reiovem965-Ave; eVM-exitig: emoom413, les	10 204 130 243	Aveya-Aura-System-Haragar	1341414009133	active
Profiles	V recvam963-AvaysVII-utility amoon411.180	10.204 130.229	reckam963-4veyev#rutRty.ampom411.las		active.
SNMP Target Profiles	Select : 44, Nove				-
Notification Filter Profile					
Serviceability Agents					
* Synchronization					

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. Confirm that the SNMPv2 trap source, Session Manager at 10.10.97.226, is now discovered and appears in the treeview.

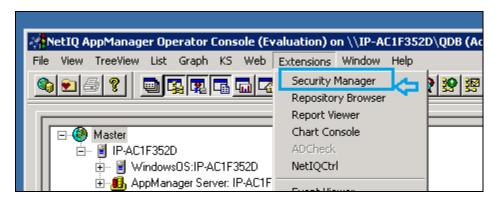


#### 6.5. Configure SNMPv3 trap Monitoring

#### 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**  $\rightarrow$  **Security Manager** as shown in below.



Add a custom profile:

🐥 NetIQ AppManager Security Mana	ager (Evaluation) on \\IP-AC1F352D\QDB (Administrator)	
Security View Help		
🎕 📚 🕵 🤶		
	Computer: IP-AC1F352D	
AppManager Users	Exchange Exch2000/2003 Oracle SAP SMS SNMP SQL WebLogic Custom	
i⊟ 🔋 Computers	This information is stored in the AppManager repository.	
	<u>Custom Label</u>	
	Label Sub-Label	

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:

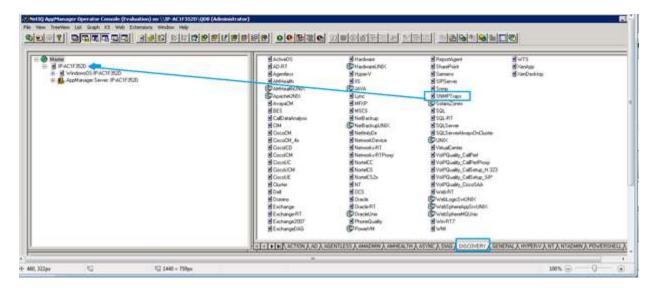
Modify Custom Entry 🛛 🛛 🗙	Modify Custom Entry
You can store custom values in the KPW table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.	You can store custom values in the KPW table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.
Label: SNMPTraps	Label : SNMPTraps
Sub-Label: 1 .10.97.226	Sub-Label: 1: 10.97.227
Value <u>1</u> : netiqDESSHA	Value <u>1</u> : netiqDESSHA
Value <u>2</u> : *	Value <u>2</u> :
Value <u>3</u> : sha,avaya123,des,avaya123	Value <u>3</u> : sha,avaya123,des,avaya123
Extended application support (Click Help for details.)	<u>Extended application support</u> (Click Help for details.)
OK Cancel <u>H</u> elp	OK Cancel <u>H</u> elp

#### 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.

Properties for Discovery_SNMPTraps		×
Schedule Values Actions Objects Advanced		
Description	Value	Units
General Settings		
Job Failure Notification		
Event severity if discovery job fails unexpectedly	5	Severity
Event Details		
Event detail format	HTML Table 🗸	
+ Tracing (for advanced users only)		
Discover SNMP Trap Devices		
+ Raise event if discovery succeeds?	🔽 Yes	
+ Raise event if discovery fails?	🔽 Yes	
- Update the TreeView object name if the device name changed since the previous discovery?	🔽 Yes	
-Name of the device to populate in the TreeView	devvmsm	
IP address of the device to populate in the TreeView	10.10.97.227	
-File containing the list of device name/IP address pairs to populate in the TreeView		
- Trap Receiver IP address	localhost	
Trap Receiver TCP port	2735	
Discovers known SNMP trap-throwing devices that forward their traps to a NetIQ Trap Receiver serv raises events to indicate discovery status (succesful, failed).	rer. Raises an event if the job fails and	optionally
<b>M</b>	UN Lancei	нер

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. 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]

🚧 NetIQ AppManager Operator Console (Evaluation) on \\\WIN-GVS7GTBD3	3B5\SQLEXPRES5\QDB (Administrator)
Eile <u>V</u> iew TreeView List Graph KS Web Extensions <u>W</u> indow Help	
	9 29 29 29 29 29 20 20 20 20 20 20 20 20 20 20 20 20 20
⊡j∰ WIN-GVS7GTBD3BS	NetworkDevice
😥 🚽 WindowsOS:WIN-GVS7GTBD3BS	SIPServer
	🚹 🕐 SQLServer
🗈 🔛 Call Performance: WIN-GVS7GTBD3BS	
SQL Server: WIN-GVS7GTBD38S\SQLEXPRESS	
SQL Server:WIN-GVS7GTBD3BS\SQLEXPRESS	
⊕-     ⊕     H.323:WIN-GVS7GTBD3BS     ⊕-     ⊕     SIP:WIN-GVS7GTBD3BS	
Terminal Server:WIN-GVS7GTBD3BS	
🗄 🚛 AppManager Server: WIN-GVS7GTBD3BS	
🖉 Trap Source: devvmsmgr [111 10.97.226]	
⊕	
	→ H ACTION AD AGENTLESS AMADMIN AMHEALTH ASYNI
Event 🔍 🗹 Status 🗅 Job Computer Knowledge Scrip	ot Last Occurre Count Severity Message
🗄 🖻 1391 🧭 Closed 🗋 🔮 WIN-GVS7GTBEAMHealth_Health	nch 3/25/2016 12:026 25 MS Healthcheck Event: Server Up
🗄 🗄 🗃 1389 🛛 🧭 Closed 🗋 <u>78</u> WIN-GVS7GTBEDiscovery_SIPSe	rve 3/23/2016 3:17: 2 10 SIP Server Discovery Failed
🗄 🗄 1383 🧭 Closed 🗅 <u>76</u> WIN-GVS7GTBEDiscovery_Netwo	-
🗄 🗄 1375 🧭 Closed 🗅 <u>74</u> WIN-GVS7GTBESNMPTraps_Trap	
🗄 🗄 🚺 1371 🛛 🖌 Closed 🗋 <u>72</u> WIN-GVS7GTBEDiscovery_SNMF	
🔢 🗄 🗃 1369 🛛 🧭 Closed 🗋 <u>70</u> WIN-GVS7GTBEDiscovery_SNMF	PTrk 3/25/2016 12:113 25 Discovery: SNMPTraps discovery successful [WIN-(]
Events / Jobs / Details / Graph Data /	
Master NT Networks-RT VolPQuality SG	QL SQLServer WTS WMI
For Help, press F1	Computers : 1 Open Events: 0 Running Jobs: 10 Graph Data: 12 1:24 PM //

#### 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:

e Wew Tree	eview List Graph	KS Web Exte	nsions Window Help	20\008 (Administrator) 연양 왕 왕 왕 동 동 동	000			
	P-AC1F3520 Windows05:IP4 AppManager Ser Tiap Source: Av		0.97.226 1		AG 入 DISCOVERI	() GENERA	L), HYPER-V)	(NT ), NTADMIN ), POWERSHELL SNMPTRAPS (N
Event	@ 🖾 Status	D Job	Computer	Knowledge Script	Last D.	Count	Seventy	Message
0 39 0 25	Open     Open	00	IP-AC1F352D IP-AC1F352D	Discovery_SNMPTraps Discovery_SNMPTraps	3/17/2016 3/17/2016		25 25	Discovery: SNMPTraps discovery auccessful (IP ACTF) Discovery: SNMPTraps discovery successful (IP ACTF)
de plat	Events & Jobs & C	letals A Graph D a	ia/					

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

ML Table	<ul> <li>Severity</li> <li>I</li> </ul>
ML Table in the second	
ML Table in the second	
h · · · · · · · · · · · · · · · · · · ·	
h · · · · · · · · · · · · · · · · · · ·	
MPv2 /	
Yes	
Yes	
	au
	~
MPTraps_AlarmMappings.c	~
	24
162	
	Yes Yes Yes Yes

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. 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:

AVAVA Aura <sup>®</sup> System Menager 7.0				Last Logged on at April	1 21. 2014 Log off
Home Inventory *					
Tinventory 4	Home / Services / Inventory / M	lanage Serviceability A	gents / Serviceability Agents		
Manage Elements					Help
Create Profiles and Discover SRS/SCS	Serviceability Age	nts			
Element Type Access	Agent List				
Subnet Configuration	Manage Profile	Generate Test A	arm Repair Serviceability A	gent	
Manage Serviceability Agents	2 Items 🤰 Show All 🔳		Click here to generate Test Alarm	Filter	; Enable
SNMPv3 User	I Hostname	IP Address	System Name	5ystem 010	Statu
Profiles	devvmsmgr.bvwdev.com     DevvmSM.bvwdev.com	1 10.97.226	Avaya-Aura-System-Manager DevvmSM	1.3.6.1.4.1.6889.1.35	active
SNMP Target Profiles	Select : All, None	1	Detrinian		
Notification Filter Profile					
Serviceability Agents					

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

Harter Harter H Marter H Marter		0.240]		AddMB Trightonia	1010121	
			्वार	▶ [₩] ACTON & AD & AD	NTLESS & AND	рана У маначици У милис У раз У разодици. У опривант У ни цели АУ на У памър
Event DE	In Los	Computer	Knowledge Strat	and the second se		
		Lance Methods		Lan Occur. Court	Several	Messaje
0 44 010	gen 1112	IPAC% 500	SNMPTraps_TrapMontol	3/17/2016 8:05 4	20	(Anage/VM ears (10.204.130.240)). Test elem for festing only. No recovery estim necessary
	Advendelige Event	PAC#350 PAC#350 PAC#350			20 20	[Angel/M-scn(10.204.130.242] Test alarm for lesting only. To recovery action recomany [Angel/M-scn(10.204.130.242] Test alarm for testing only. Increasively action recovery.
B 44 000	Advendadge Event	IPAC#3520 IPAC#3520	SNMPTract_Trackforder SNMPTract_Trackforder	3/17/2016 0:0E 4 3/17/2016 0:0E 4	20	(Anage/VM ears (10.204.130.240)). Test elem for festing only. No recovery estim necessary
	Admonifiedge Event Close Event	PAC97520 PAC97520 PAC97520	SNMPTraps_TrapHonton SNMPTraps_TrapHonton Choovery_SNMPTraps	3/17/2016/6/8/8 4 3/17/2016/9/05/4 3/17/2016/1/201	20 20 25	(Assay-WH ears (10.2013) 2020) Test sizes for horizing only, no recovery estima recentary (Proposition desc) (10.2014) 805 (2013) Fest sizes for horizing only, increasing editors increasing Discovery, SMM <sup>2</sup> Tapa discovery, successful (24.4215) 3201
	Admonifiedge Event Close Event	PAC97520 PAC97520 PAC97520	SNMPTraps_TrapHonton SNMPTraps_TrapHonton Choovery_SNMPTraps	3/17/2016/6/8/8 4 3/17/2016/9/05/4 3/17/2016/1/201	20 20 25	(Assay-WH ears (10.2013) 2020) Test sizes for horizing only, no recovery estima recentary (Proposition desc) (10.2014) 805 (2013) Fest sizes for horizing only, increasing editors increasing Discovery, SMM <sup>2</sup> Tapa discovery, successful (24.4215) 3201
	Advansedge Divert Oktor Divert Original Divert Original Divert	PAC97520 PAC97520 PAC97520	SNMPTraps_TrapHonton SNMPTraps_TrapHonton Choovery_SNMPTraps	3/17/2016/6/8/8 4 3/17/2016/9/05/4 3/17/2016/1/201	20 20 25	Josephil and (10.204.130.201) Test alies to histogrady, an ancorea, where exercises Received and (10.204.130.201) Test alies to histogrady, in an exercise, where exercises Decrements SMMPFTage decovery successful (IP-4C1F38.20) Decovery SMMPFTage decovery successful (IP-4C1F38.20)
	Adventidige Event Close Event Close Event Proge By Here Here Lings	PAC97520 PAC97520 PAC97520	SNMPTraps_TrapHonton SNMPTraps_TrapHonton Choovery_SNMPTraps	3/17/2016/6/8/8 4 3/17/2016/9/05/4 3/17/2016/1/201	20 20 25	(Assay-WH ears (10.2013) 2020) Test sizes for horizing only, no recovery estima recentary (Proposition desc) (10.2014) 805 (2013) Fest sizes for horizing only, increasing editors increasing Discovery, SMM <sup>2</sup> Tapa discovery, successful (24.4215) 3201
	Advansedge Divert Oktor Divert Original Divert Original Divert	PAC97520 PAC97520 PAC97520	SNMPTraps_TrapHonton SNMPTraps_TrapHonton Choovery_SNMPTraps	3/17/2016/6/8/8 4 3/17/2016/9/05/4 3/17/2016/1/201	20 20 25	Josephil and (10.204.130.201) Test alies to histogrady, an ancorea, where exercises Received and (10.204.130.201) Test alies to histogrady, in an exercise, where exercises Decrements SMMPFTage decovery successful (IP-4C1F38.20) Decovery SMMPFTage decovery successful (IP-4C1F38.20)
	pan 1018 Admandadige Scient Core Event Core Event Core Scient Research Detail Message Tear 1999	PAC97520 PAC97520 PAC97520	SNMPTraps_TrapHonton SNMPTraps_TrapHonton Choovery_SNMPTraps	3/17/2016/6/8/8 4 3/17/2016/9/05/4 3/17/2016/1/201	20 20 25	Josephil and (10.204.130.201) Test alies to histogrady, an ancorea, where exercises Received and (10.204.130.201) Test alies to histogrady, in an exercise, where exercises Decrements SMMPFTage decovery successful (IP-4C1F38.20) Decovery SMMPFTage decovery successful (IP-4C1F38.20)
	Addresivelige Event Close Event Group By How How Detail Message	PAC97520 PAC97520 PAC97520	SNMPTraps_TrapHonton SNMPTraps_TrapHonton Choovery_SNMPTraps	3/17/2016/6/8/8 4 3/17/2016/9/05/4 3/17/2016/1/201	20 20 25	Josephil and (10.204.130.201) Test alies to histogrady, an ancorea, where exercises Received and (10.204.130.201) Test alies to histogrady, in an exercise, where exercises Decrements SMMPFTage decovery successful (IP-4C1F38.20) Decovery SMMPFTage decovery successful (IP-4C1F38.20)

#### 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:

2	NetIQ AppManager Operator Console (Ev	aluation) on \\IP-AC1F352	D\QDB (Ac
File	e View TreeView List Graph KS Web	Extensions Window Help	
6	) •   #   <b>*   •   •   •</b>   •   •   •   •   •   •	Security Manager	> :0 :2
		Repository Browser	
L r		Report Viewer	<u> </u>
	🖃 🛞 Master	Chart Console	
	🗄 🖷 📓 IP-AC1F352D	ADCheck	
	🗓 🔋 Windows0S:IP-AC1F352D	NetIQCtrl	
	🗄 🦺 AppManager Server: IP-AC1F		

Add a custom profile:

🗳 NetIQ AppManager Security Mana	ager (Evaluation) on \\IP-AC1F352D\QDB (Administrator)	
Security View Help		
🎕 📚 🕵 🙎		
⊡ 🥵 AppManager Security ⊡ 🐋 AppManager Roles	Computer: IP-AC1F352D	
in the set of the set	Exchange Exch2000/2003 Oracle SAP SMS SNMP SQL WebLogic Custom	
IP-AC1F352D	This information is stored in the AppManager repository.	
	<u>C</u> ustom Label	
	Label Sub-Label	

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:

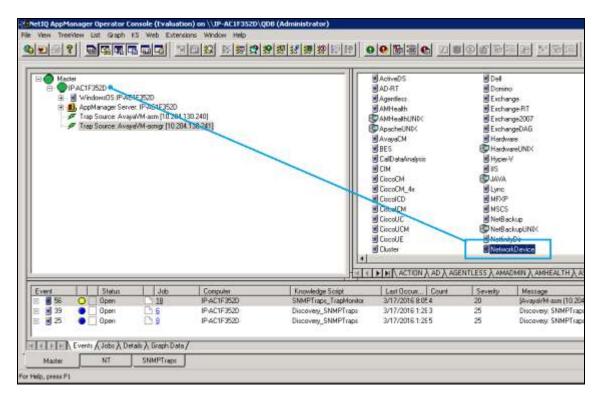
- Label: Enter any descriptive name, ex: NetworkDevice.
- Sub-Label: Enter System manager's IP Address, ex:10.10.97.226.
- Value 1: Enter user name created in Section 5.3, ex: netiqDESSHA.
- Value 2: Enter \*.
- Value 3: Enter user created in Section 5.3 passwords, ex: sha,avaya123,des,avaya123.

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

Modify Custom Entry	×	Modify Custom Entry	×
You can store custom values in the KPW table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.		You can store custom values in the KPW table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.	
Label: NetworkDevice		Label : NetworkDevice	
<u>S</u> ub-Label: 1 10.97.226		Sub-Label: 1 .10.97.227	
Value <u>1</u> ; netiqDESSHA		Value <u>1</u> ; netiqDESSHA	
Value <u>2</u> : ×		Value <u>2</u> : ×	
Value <u>3</u> : sha,avaya123,des,avaya123		Value <u>3</u> : sha,avaya123,des,avaya123	
Extended application support (Click Help for details.)		Extended application support (Click Help for details.)	
OK Cancel <u>H</u> elp		OK Cancel <u>H</u> elp	

#### 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.

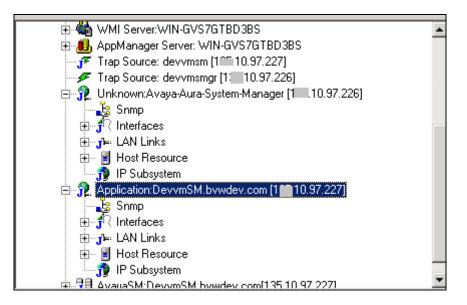
Description	Value	Units
Auto Discovery		
- Default gateway router		
- Maximum number of hops	1	Hops
- CAUTION: Enabling can negatively impact network performance		
Walk subnets for layer-2 devices? (y/n)	n	
List of network devices (comma-separated)	10.10.97.226,10.10.97.227	
List of network device ranges (comma-separated)		
Full path to file with list of network devices		
Discovery Details		
Discovery timeout	10	Minutes
Raise event when discovery succeeds? (y/n)	2	
Event severity when discovery succeeds	25	Severity
Event severity when discovery fails	5	Severity
scovers network devices: routers, switches, gateways, etc. You can specify a co iddresses, a gateway router for auto-discovery, or the name of a file that contains i scause only one computer should act as a proxy for a given network device, drop anager with SNMP version and security information (community string for SNMPv fore you can discover network devices.	levice names on separate lines. Specify at least this script on only one computer at a time. You	one remote comp must update Secu

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

TO THE REPORT	H 323-WIN-GVS70 SIP-WIN-GVS70 Teminal Server/V WMI Server/WIN AppManager Ser Trap Source: dev	GVS7GTBD3BS GTBD3BS	SQLEXPRESS 05 180.305 227)	-	SOLServer		
	Unknown Avaya		ager [110.97.226]	-			
	Application Devv	nSM bywdev.cor	a († 10.97.227)	-		IX AD X AGENTLESS X AMADMIN X AM	MHEALTH \ AS
vert @	🛛 🗐 🗍 Stetur	D lab	Computer	یر ۱ ۲. rowledge Script	Last Occur   Severa	y Message	-
+ ♀ } vent 00 142 ●	😥 Stetur		Computer WIN-GVS7GTEC	SNMPTreps_Trep	I Last Gocur   Sever M 4/22/2016 3:08:25	v Message Trap lecever (135:10.98:27) is re-con	nected
(vent 00 142 € 141-€	Dpen		Computer WIN-GV57GTBC WIN-GV57GTBC	SNMPTieps_Trep SNMPTieps_Trep	Lait Occur Sever M4/22/2016 3:08:25 M4/22/2016 3:08:25	<ul> <li>Message</li> <li>Trap teceiver [125.10.98.27] is re-cons</li> <li>Trap teceiver [125.10.98.27] is re-cons</li> </ul>	nected nected
9 142 0 1 142 0 1 141 0 1 141 0 1 144 0	21 Stetur Dpen Dpen Open	D 100	Computer WIN-GVS7GTBC WIN-GVS7GTBC WIN-GV57GTBC	SNMPTieps_Trep SNMPTieps_Trep Discovery_SIPSer	Lait Occur Sever M4/22/2016 3:08:25 M4/22/2016 3:08:25 M4/22/2016 3:18:15	<ul> <li>Message Trap lecever (125:10.98:27) is re-com Trap lecever (125:10.98:27) is re-com Trap lecever (125:10.98:27) is re-com The supplemental database SIPServe</li> </ul>	nected nected s_DevymSM.br
₩ Q 3 ₩ 142 Φ ₩ 142 Φ ₩ 141-Φ ₩ 144.Q ₩ 143	20 Stetur Open Open Open Se Closed	D 84 D 85 D 106 D 109	Computer WIN-GVS7GTBC WIN-GVS7GTBC WIN-GV57GTBC WIN-GV57GTBC	SNMPTieps_Trep SNMPTieps_Trep Discovery_SIPSer Discovery_SIPSer	Last Occur Seven M 4/22/2016 3:08:25 M 4/22/2016 3:08:25 m 4/22/2016 3:18:15 m 3/25/2016 1:04:15	<ul> <li>Message Trap tecesive (125:10.98.27) is re-com Trap tecesive (125:10.98.27) is re-com Trap tecesive (125:10.98.27) is re-com The supplemental database SIPServe The supplemental database SIPServe</li> </ul>	nected nected s_DevymSM.br
(verit 0) ■ 142 ● ■ 142 ● ■ 141 ● ■ 144 ○ ■ 143 ■ 143 ■ 138	Bit         Stetur           Open         Open		Computer WIN-GVS7GTELS WIN-GVS7GTELS WIN-GV57GTELS WIN-GV57GTELS WIN-GV57GTELS	SNMPTieps_Trep SNMPTieps_Trep Discovery_SIPSer Discovery_SIPSer Discovery_SIPSer	Last Occur Served M 4/22/2016 3:08:25 M 4/22/2016 3:08:25 M 4/22/2016 3:08:25 m 4/22/2016 3:18:15 m 3/25/2016 1:04:15 m 3/23/2016 3:17:10	Message     Trap tecesive [135:10:99:27] is re-com     Trap tecesive [135:10:99:27] is te-com     Trap tecesive [135:10:98:27] is te-com     The supplemental database SIPS arve     SIP Server Discovery Failed	nected nected 9_DevvmSM.b #_AvayaAuaeSt
(142) ■ 142 ■ 142 ■ 141 ■ 144 ■ 144 ■ 148 ■ 138 ■ 138 ■ 138	Bit         Stetur           Open         Open           Open         Open		Computer WIN-GVS7GTBLS WIN-GVS7GTBLS WIN-GV57GTBLC WIN-GV57GTBLC WIN-GV57GTBLC WIN-GV57GTBLC	SNMPTieps_Trep SNMPTieps_Trep Discovery_SIPSer Discovery_SIPSer Discovery_SIPSer Discovery_SIPSer	Lad Occur Sevel M 4/22/2016 308 25 M 4/22/2016 3:08 25 M 4/22/2016 3:18 15 m 3/25/2016 3:18 15 m 3/25/2016 10 15 m 3/25/2016 3:17 10	Message Tags tecesive [135:10:99.27] is re-com Tags tecesive [135:10:98.27] is re-com The supplemental database SIPServe The supplemental database SIPServe SIP Serve Discovery Failed NetworkDevice Discovery Failed	nected nected 9_DevvmSM.b #_AvayaAuaeSt
	1         Stetur           Open         Open           Open         Closed           Closed         Closed           Closed         Closed		Computer WIN GVS7GTBIS WIN GVS7GTBIS WIN GVS7GTBIS WIN GVS7GTBIS WIN GVS7GTBIS WIN GVS7GTBIS WIN GVS7GTBIS	SNMPTraps_Trap SNMPTraps_Trap Discovery_SIPSer Discovery_SIPSer Discovery_SIPSer Discovery_Networ Discovery_Networ	Last Occur Server M4/22/2016 308 25 M4/22/2016 308 25 M4/22/2016 318 15 m3/25/2016 1 04 15 m3/25/2016 1 04 15 m3/25/2016 31 15 M3/25/2016 32 944 PM 4.3/23/2016 11 115	<ul> <li>Message Trap tecesive [135:10.98.27] is re-com Trap tecesive [135:10.98.27] is te-com The supplemental database SIPServe The supplemental database SIPServe SIP Servet Discovery Failed NetworkDavice Discovery Failed</li> </ul>	nected nected s_DevmSM.tb g_AvayaAuteSt 137,227
	1         Stetur           Open         Open           Open         Closed           Closed         Closed           Closed         Closed		Computer WIN-GVS7GTBC WIN-GVS7GTBC WIN-GVS7GTBC WIN-GVS7GTBC WIN-GVS7GTBC WIN-GVS7GTBC WIN-GVS7GTBC WIN-GVS7GTBC	SNMPT rept_Trept SNMPT rept_Trept Discovery_SIPSer Discovery_SIPSer Discovery_SIPSer Discovery_Network Discovery_Network Discovery_Network Network Device_D	Last Occur Sevel M4/22/2016 3:08:25 M4/22/2016 3:08:25 m4/22/2016 3:18:15 m3/25/2016 1:08:15 m3/25/2016 1:2:39:49 PM 4:3/22/2016 1:2:39:49 PM 4:3/22/2016 1:2:39:49 PM 4:3/22/2016 1:2:39:49 PM	Message     Tap receiver [135:10:39.27] is re-com     Tap receiver [135:10:39.27] is re-com     Tap receiver [135:10:39.27] is re-com     The supplemental database SUPS erve     SIP Server Dacovery Faled     NetworkDarkse Discovery OK (166:10     NetworkDarkse Discovery Faled     NetworkDarkse Discovery Faled     NetworkDarkse Discovery Faled	nected nected 5. DevvmSM b 6. AvageActeS 1997/227
	20         Stetur           Open         Open           Open         Open           Ø         Closed           Ø         Closed           Ø         Closed           Ø         Closed		Computer WIN-GVS7GTBCS WIN-GVS7GTBCS WIN-GVS7GTBCS WIN-GVS7GTBCS WIN-GVS7GTBCS WIN-GVS7GTBCS WIN-GVS7GTBCS WIN-GVS7GTBCS	SNMPT rept_Trept_ SNMPT rept_Trept Discovery_SIPSer Discovery_SIPSer Discovery_SIPSer Discovery_Network Discovery_Network Device_D Network Device_D	Last Occur Server M4/22/2016 308 25 M4/22/2016 308 25 M4/22/2016 318 15 m3/25/2016 1 04 15 m3/25/2016 1 04 15 m3/25/2016 31 15 M3/25/2016 32 944 PM 4.3/23/2016 11 115	<ul> <li>Message Trap tecesive [135:10.98.27] is re-com Trap tecesive [135:10.98.27] is te-com The supplemental database SIPServe The supplemental database SIPServe SIP Servet Discovery Failed NetworkDavice Discovery Failed</li> </ul>	nected nected 5. DevvmSM b 6. AvageActeS 1997/227

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. 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.



E Statest Devce	ience
Application: exays-esm localdomein (10.204.130.240)	
19: - An Links 19: - 📓 Host Resource	
P Subsystem     P Subsystem     Proceedings Acae System Manager [10:204.130.243]     A Singe	
er og strong er ∲ Enhertsons er ok LAN Links	
<ul> <li>Host Recource</li> <li>IP Subsystem</li> </ul>	
64**) S	
op [8]Ω[Φ]@]Status [Dridden [Computer Knowledge Script	TION A NETWORKDEVICE A RECOMMENDED /
06. 10-10-10-10-0000 Cuedau Coldon Automode 20-01	and and and and the
[ ∈ ] ⊨ [ ] [ ] Events λ Jobs Λ Denats λ Graph Data /	
Image: Street State         Comparison         Comparison         Comparison         Network         Details         Comparison         Details         Details	Servers 2 Open Events: 0 Running Jobs: 0 Graph Data: 0 10:34

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.

n 🥊 29 🕷 🏠 🖓 Running 1 IP-4C1F3520 Network Device, Device, Uptime IP-4C1F352D/Administrator 3/21/2016.10.3 9 9 9 7 🕷 🏟 Running 1 IP-4C1F352D Network Device Ping IP-4C1F352D/Administrator 3/21/2016.10.3		Smip Interfaces An LAN Links Host Resour P Subsystem	ce 1 Aura-System+ 2e	mein (10,204,130 Manager (10,204	40.01			
2 9 8 6 6 6 Plunning 1 IP-4C1F3520 NetworkDevice_Device_Uptime IP-4C1F352D/Administrator 3/21/201610.2 ■ 9 27 8 6 Running 1 IP-4C1F3520 NetworkDevice Device Ping IP-4C1F352D/Administrator 3/21/201610.3	1	18/0/0/0	T films	1000	,f	spandadada da	and the second se	Suberi Time Stop Time
n 👷 27 🐮 🏠 Running 1 IP-AC1F352D Network/Device_Pring IP-AC1F352D/Administrator 3/21/2016.10.5 n 🗗 35 🐮 🏠 Running 1 IP-AC1F352D Network/Device_Interface_Health IP-AC1F352D/Administrator 3/21/2016.10.5	and the second	8 04		1		and the second se	A STATISTICS OF A STATISTICS AND A STATI	3/21/2016 10/2 (None)
🖌 35 🐻 Running 1 IP-AC1F352D Network/Device_Interface_Health IP-AC1F352DVAdministrator 3/21/2016 10.0	9 39	19K A	Bunning	1	IP-AC1F3520		IP-AC1F352D\Administrator	3/21/2016 10 S (None)
				1	IP-AC1F352D	NetworkDevice_Interface_Health	IP-AC1F352DVAdministrator	3/21/2016 10.3 (None>
n 🧑 33 🐻 🚔 Running 1 IP-AC1F3520 Network Device_JPSubaysten_Uki IP-AC1F3520 Administrator 3/21/2016.10.3 1 🛥 31 🐻 🏟 Running 1 IP-AC1F3520 Network Device_UANLink_Util IP-AC1F3520 Administrator 3/21/2016.10.3	1 35		Burining					

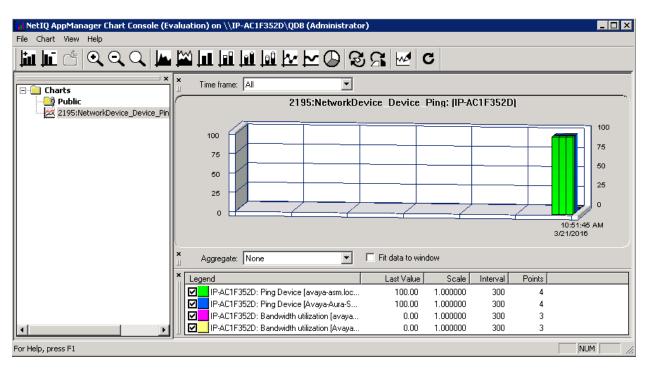
After a monitoring interval has been completed, data streams will be visible in the Graph Data pane as shown in below screenshot.

H & Somo H & Landa H & Land H & Land H & Heat B	avaga-anni kocal nko escolarce eputen Anaga-Aura Syste cen reto escolarce	kkonain (10.304.330.240) en-Maniager (10.204.130.241)	Anterest Device		
Data Source	Jab	Knowledge Script	Computer	Cur. ports	Legend
	22	NetworkDevice_LANLink_Util NetworkDevice_LANLink_Util NetworkDevice_Device_Ping NetworkDevice_Device_Ping	IPACIF5520 IPACIF3520 IPACIF3520 IPACIF3520	Data has been collected Data has been collected Data has been collected Data has been collected	Bandheidh Udizaton (Avaya-Ause-System-Manager - 10.204.130.241 - eth2.4[[3 Bandheidh Udizaton (Avaya-aum localdonain - 10.204.130.240 - eth2.2[[3] Ping Device (Avaya-aum localdonain[[10.204.130.241] Ping Device (avaya-aum localdonain][10.204.130.240]

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

E Srep E A Interfe E A LAN L E B Host F P Sub	n avaga azmilocak into into teopace ogstam Avayo Auso Syste icos into Teopurce			tietworkDewsee		
	agestern.				and an and a second	
Data Source	Job 32	Network	ndge Scief «Device LANLerk_Util	Computer IP AC1F2520	NETWORKDEVICE A RECOMME Data points Data has been collected	Legent Bandwidt Hulkaation (Avage-Aure System Manager - 10.204.130.241 - eth0.4)
Data Source	Job II II II II	Network	(Device_LANLink_UN) (Device_LANLink_UN)	Computer	Die points	Legent
Data Source	Job 22 32	Network	Device, LANLAN, UN Device, LANLAN, UN Create Chart	Computer IP.AC1F2520 IP.AC1F2520	Dix points Data has been collected Data has been collected	Logant Bardwollt ulkator (Anapekus Suten Manage - 10.204.130.241 - eH0.4) Bardwollt ulkator (avays son localdanae - 10.204.130.240 - eH0.2)(1)
Data Source	Job II II II II	Network Network Network	(Device_LANLink_UN) (Device_LANLink_UN)	Computer IP ACTE252D IP ACTE252D IP ACTE252D	Ox points Data has been collected Data has been collected Data has been collected	Legant Bandwidth uikzaton (Anaper-Kura System Manager - 10.204.130.241 - orbit 4) Bandwidth uikzaton (awaya aun koatdonaan - 10.204.130.240 - erbit 2) (h) Ping Device (Awaya Aura System Manager) (10.204.130.241)
)wa Source 	Job II II II II	Network Network Network	Device LAALAA UN Device LAALAA UN Create Chart Debte Graph Data Group By Hitsy	Computer IP ACTE252D IP ACTE252D IP ACTE252D	Ox points Data has been collected Data has been collected Data has been collected	Legard Bandwidth uikzation (Avapet-Kura System Manager - 10.204.130.241 - edis0.4) Bandwidth uikzation (avaya aust koakdonaan - 10.204.130.240 - edis0.2(15) Ping Device (Avaya Ause System-Manager) (10.204.130.241)

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved.



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 <u>http://support.avaya.com</u>.

- 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 <u>https://www.netiq.com/documentation/appmanager-</u> <u>9/pdfdoc/administratorguide/administratorguide.pdf</u>
- 2. Net IQ online documents:

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

#### ©2016 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and <sup>TM</sup> are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at <u>devconnect@avaya.com</u>.