



Avaya Solution & Interoperability Test Lab

Application Notes for Nectar for Avaya with Avaya Aura® System Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Nectar for Avaya 2022 with Avaya Aura® System Manager 10.1 and Avaya Aura® Session Manager 10.1. Nectar for Avaya is a performance monitor that provides a comprehensive view of unified communications and contact center environments. It automatically captures Avaya Aura® System Manager and Avaya Aura® Session Manager inventory and provides resource utilization information using Avaya Aura® Routing Web Service, Avaya Aura® Session Manager Element Manager Web Service, and SNMP Polling.

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

These Application Notes describe the configuration steps required to integrate Nectar for Avaya with Avaya Aura® System Manager and Avaya Aura® Session Manager. Nectar for Avaya is a performance monitor that provides a comprehensive view of unified communications and contact center environments. It automatically captures Avaya Aura® System Manager and Avaya Aura® Session Manager inventory and provides resource utilization information using Avaya Aura® Routing Web Service, Avaya Aura® Session Manager Element Manager Web Service, and SNMP Polling.

The Routing Web Service and Element Manager Web Service are RESTful Web Services that are part of the Avaya Aura® System Manager Web Services. The Routing Web Service provides programmatic access to Routing administration data available from the **System Manager → Routing** GUI. Nectar for Avaya (hereafter referred to as Nectar) collected the following Routing data from System Manager:

- Locations
- SIP Entities
- Entity Links

The Session Manager Element Manager Web Service provides programmatic access to Session Manager Dashboard and User Registration status data. Nectar collected the following data from Session Manager:

- Session Manager Status
- User Registrations

Nectar captured the following resource utilization data from System Manager and Session Manager using SNMPv3 polls.

- CPU Utilization
- Linux Physical Memory Utilization

The frequency of data polling is configurable via Nectar or may be performed on-demand.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on the ability of Nectar to capture System Manager and Session Manager inventory data from the Routing Web Service and the Element Manager Web Service. In addition, SNMPv3 polling was used to capture the resource utilization data. The data was displayed on the Nectar Remote Intelligence Gateway (RIG) client.

The serviceability testing focused on verifying that the Nectar came back into service after re-connecting the Ethernet cable (i.e., restoring network connectivity) and restarting Nectar.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Nectar for Avaya utilized encryption capabilities of SNMPv3.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following Nectar features and functionality.

- Collecting System Manager Inventory (e.g., Locations, SIP Entities, and Entity Links) using the Routing Web Service and displaying the inventory on the RIG client.
- Collecting Session Manager Inventory (e.g., Session Manager Status and User Registrations) using the Element Manager Web Service and displaying the inventory on the RIG client.
- Verifying configuration changes made to the relevant data via the System Manager Web interface were updated on RIG client.
- Verifying Session Manager status, SIP user registration status, and SIP user configuration updates (e.g., adding/removing users) were updated on RIG client.
- Verifying resource utilization (e.g., CPU Utilization and Linux Physical Memory Utilization) captured from System Manager and Session Manager via SNMPv3 polling.
- Verifying proper system recovery after a restart of Nectar and loss of IP network connectivity.

2.2. Test Results

The compliance test passed with the following observations:

- Nectar throttles frequent data collections to System Manager using the Routing and Element Manager Web Services. If on-demand or scheduled data collections are requested too frequently, Nectar may suppress sending the requests to System Manager even though the Last Execution timestamp was updated in the Data Collections window. During the compliance test, on-demand and scheduled data collections were requested no more than once every 15 minutes.
- There may be up to an hour delay before Nectar updates and displays the latest data from System Manager and Session Manager retrieved using the Routing and Element Manager Web Services even though data collections are being requested periodically.
- Session Manager instances data is not supported by the Element Manager Web Service and should not be requested. Session Manager instances data collection should be disabled in Nectar as shown in **Section 6.3**. Nectar will remove Session Manager instances in the inventory report and the ability to poll for the data in a subsequent release.
- Currently, Nectar doesn't support receiving SNMP traps from System Manager or Session Manager.

2.3. Support

For technical support and information on Nectar for Avaya, contact Nectar Support at:

- Phone: +1 (888) 811-8647 (US)
+1 (631) 270-1077 (outside the US)
- Website: <https://support.nectarcorp.com>
- Email: support@nectarcorp.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Nectar with an Avaya SIP-based network, including Avaya Aura® System Manager and Avaya Aura® Session Manager. Nectar captured data from System Manager and Session Manager using System Manager Web Services and SNMP Polling. The RIG client was used to display system inventory and resource utilization data.

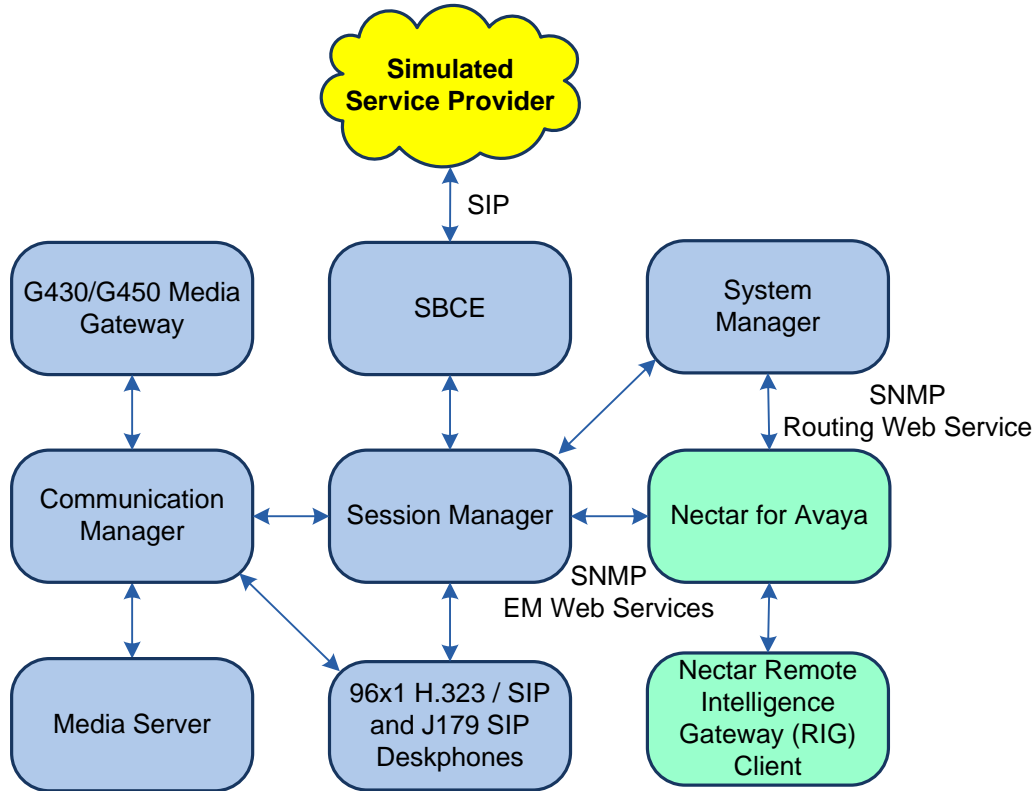


Figure 1: Nectar for Avaya with Avaya SIP-based Network

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.1.0.1.0-SP1
Avaya G430 Media Gateway	FW 42.4.0 Vintage 1
Avaya G450 Media Gateway	FW 42.7.0 Vintage 3
Avaya Aura® Media Server	10.1.0.77
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.0614394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series IP Deskphones	6.8.5.3.2 (H.323) 7.1.13.0.4 (SIP)
Avaya J100 Series SIP Deskphones	4.0.13.0.6
Nectar for Avaya	2022.1-21422
Nectar Remote Intelligence Gateway (RIG) Client	2022.1-20314

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

This section provides the procedure for providing access to System Manager Web Services and enabling SNMP polling on System Manager and Session Manager. The procedures include the following areas:

- Add New Administrator for Nectar
- Verify System Manager Web Services
- Enable SNMP Polling

Configuration was performed by accessing the browser-based GUI of System Manager using the URL **Error! Hyperlink reference not valid.**, where *<ip-address>* is the System Manager IP address, and logging in using the appropriate credentials.

5.1. Add New Administrator for Nectar

A user account is required by Nectar to retrieve SIP trunk and user registration information using System Manager Web Services.

From the main webpage, navigate to **Users → Administrators**. In the **Administrative Users** web page shown below, click **Add**.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'Administrative Users' and displays a table of users. The table has columns for 'User ID', 'Name', 'Roles', 'Type', and 'Account Status'. The 'nectar' user is highlighted in blue.

	User ID	Name	Roles	Type	Account Status
1	admin	Default security administrator	System Administrator	Local	Enabled
2	craft	craft	Avaya Services Maintenance and Support	External	Enabled
3	init	init	System Administrator	External	Enabled
4	nectar	Avaya DevConnect	Session Manager and Routing Administrator	Local	Enabled

In the **Add New Administrative User** web page, configure the following parameters:

- **User:** Provide a descriptive name (e.g., *nectar*).
- **Authentication Type:** Select **Local** radio button.
- **Full Name:** Provide full name (e.g., *Avaya DevConnect*).
- **Temporary Password:** Provide account password.
- **Re-enter Password:** Re-enter the password.

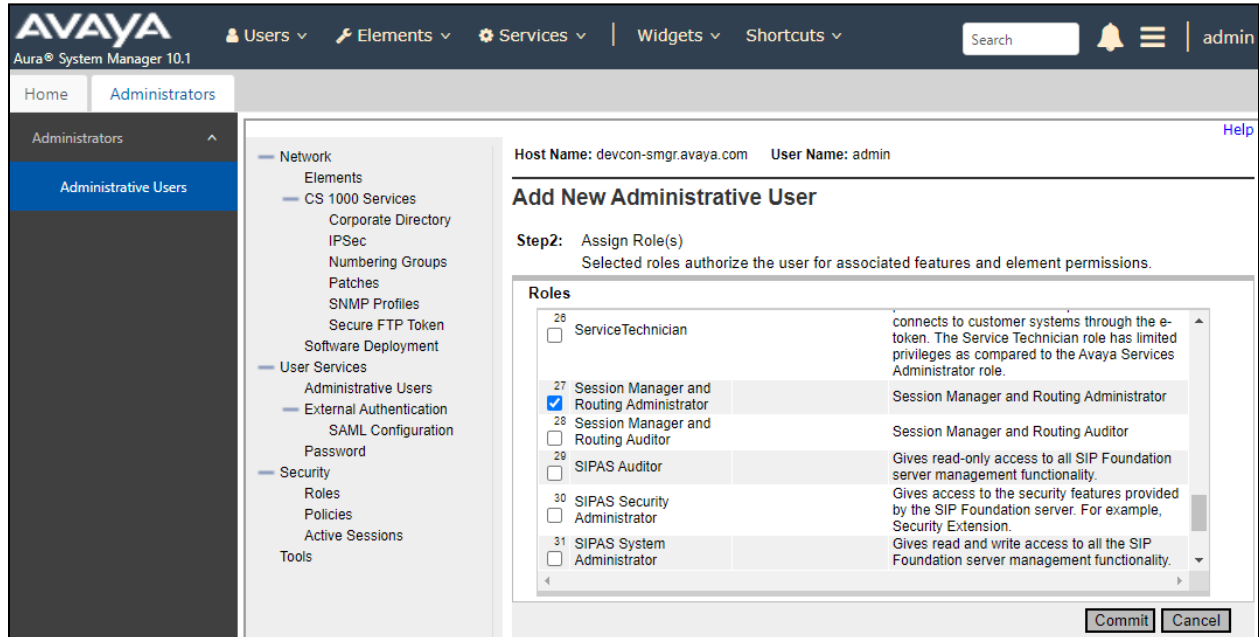
After completing the form, click **Commit and Continue**.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows a tree view with 'Administrative Users' selected. The main content area is titled 'Add New Administrative User' and contains the following form fields:

- User ID:** nectar (1-31) (Allowed characters are a-z, A-Z, 0-9, ., -, and _)
- Authentication Type:** Local (selected), External
- Full Name:** Avaya DevConnect
- E-Mail:** (empty)
- Temporary password:** (masked with asterisks)
- Re-enter password:** (masked with asterisks)

A 'Generate Password' button is located below the password fields. The page also shows a 'Host Name' of devcon-smgr.avaya.com and a 'User Name' of admin. At the bottom, there are 'Commit and Continue' and 'Cancel' buttons.

On the next web page, assign the role to the administrative user. Scroll down and select **Session Manager and Routing Administrator**. Click **Commit**.



Log out of the System Manager web interface. Log back into the System Manager web interface using the administrative user created above. During the first login attempt, the user must change the password using the **Change Password** link under the login prompt (not shown).

5.2. Verify System Manager Web Services

No additional configuration is required to enable the Routing Web Service or Element Manager Web Service. However, the steps in the following sections can be performed to verify that System Manager Web Services are running and that data can be retrieved using the Routing Web Service and Element Manager Web Service.

5.2.1. Verify System Manager Web Services is Running

To verify System Manager Web Services is running, perform the following steps:

- Log into System Manager using SSH.
- At the Linux prompt, enter the following command:
`wget --no-check-certificate https://SMGR-IP/ws/grservice/getgrstate/test`, where SMGR-IP is the System Manager IP address.
- A similar output to the one below should be displayed indicating that the HTTP request was successful.

```
cust >wget --no-check-certificate https://10.64.102.120/ws/grservice/getgrstate/test
--2022-08-18 12:02:16-- https://10.64.102.120/ws/grservice/getgrstate/test
Connecting to 10.64.102.120:443... connected.
WARNING: The certificate of '10.64.102.120' is not trusted.
WARNING: The certificate of '10.64.102.120' hasn't got a known issuer.
The certificate's owner does not match hostname '10.64.102.120'
HTTP request sent, awaiting response... 200 OK
Length: 700 [application/octet-stream]
Saving to: 'test.2'

test.2          100%[=====>]          700  --.-KB/s   in 0s

2022-08-18 12:02:16 (37.2 MB/s) - 'test.2' saved [700/700]
```

5.2.2. Test Routing Web Service

Verify that data can be accessed from the System Manager Routing Web Service by requesting for SIP entity data using a web browser. Enter the following URL in the web browser: <https://SMGR-IP/NRP/admin/sipentities>, where SMGR-IP is the System Manager IP address. Enter the appropriate login credentials, from **Section 5.1**, when prompted. System Manager should respond with a list of SIP entities in the web browser.

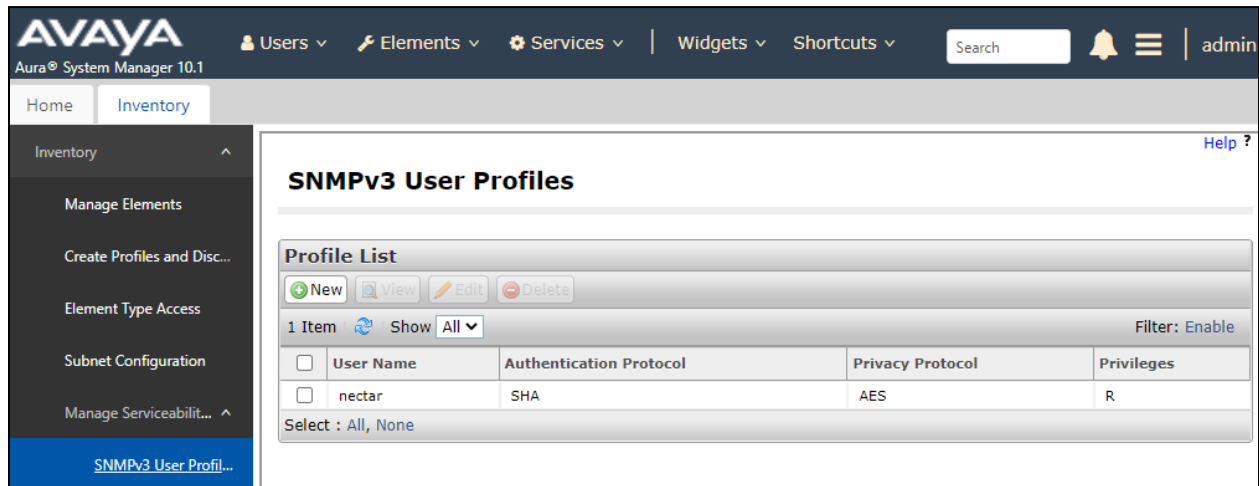
5.2.3. Test Element Manager Web Service

Verify that data can be accessed from the Session Manager Element Manager Web Service by requesting for Session Manager status using a web browser. Enter the following URL in the web browser: <https://SMGR-IP/ASM/ws/asmstatuses>, where SMGR-IP is the System Manager IP address. Enter the appropriate login credentials, from **Section 5.1**, when prompted. System Manager should respond with the Session Manager status in the web browser.

5.3. Configure SNMP

This section provides the procedure for enabling SNMP polls on System Manager and Session Manager. Configuration was performed by accessing the browser-based GUI of System Manager using the URL **Error! Hyperlink reference not valid.**, where *<ip-address>* is the System Manager IP address. Log in using the appropriate credentials.

From the main webpage above, navigate to **Services → Inventory**. In the subsequent webpage, select **SNMPv3 User Profiles** under **Manage Serviceability Agents** in the left pane to display the webpage below. Click **New**.



Configure the **User Details** for SNMPv3 polls to be used for System Manager and Session Manager. Nectar requires that the SNMPv3 credentials match for System Manager and Session Manager. The following user profile will be used by System Manager and Session Manager.

New User Profile Commit Back

User Details

* User Name:

* Authentication Protocol:

* Authentication Password:

* Confirm Authentication Password:

* Privacy Protocol:

* Privacy Password:

* Confirm Privacy Password:

* Privileges:

*Required Commit Back

Under **Manage Serviceability Agents** in the left pane, select **Serviceability Agents**. Select the serviceability agents, which should include System Manager and Session Manager, by selecting both checkboxes as shown below. This step selects the serviceability agents to which the SNMP user profile configured above will be attached. Click on **Manage Profiles**.

Serviceability Agents Help ?

Agent List

Activate Manage Profiles Generate Test Alarm Repair Serviceability Agent Manage Profile Job Status Reset Table Advanced Search

3 Items Show All Filter: Enable

<input type="checkbox"/>	Hostname	IP Address	System Name	System OID	Status
<input checked="" type="checkbox"/>	devcon-smgr.avaya.com	10.64.102.120	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
<input checked="" type="checkbox"/>	devcon-sm.avaya.com	10.64.102.116	Session Manager	.1.3.6.1.4.1.6889.1.36	active
<input type="checkbox"/>	devcon-util.avaya.com	10.64.102.100	devcon-util.avaya.com		active

Select : All, None

In the **SNMPv3 User Profiles** tab, select the entry in the **Assignable Profiles** section and click **Assign** to push the SNMP details to System Manager and Session Manager. Click **Commit** to submit the changes.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). The main content area is titled "Manage Profile" and features three tabs: "Selected Agents", "SNMP Target Profiles", and "SNMPv3 User Profiles". The "SNMPv3 User Profiles" tab is active, showing an "Assignable Profiles" section with a table containing one row. The table has columns for "User Name", "Authentication Protocol", "Privacy Protocol", and "Privileges". The row shows "nectar" as the user name, "SHA" as the authentication protocol, "AES" as the privacy protocol, and "R" as the privilege. Below the table is a "Removable Profiles" section. The interface includes "Commit" and "Back" buttons at the top right and bottom right of the main content area.

<input checked="" type="checkbox"/>	User Name	Authentication Protocol	Privacy Protocol	Privileges
<input checked="" type="checkbox"/>	nectar	SHA	AES	R

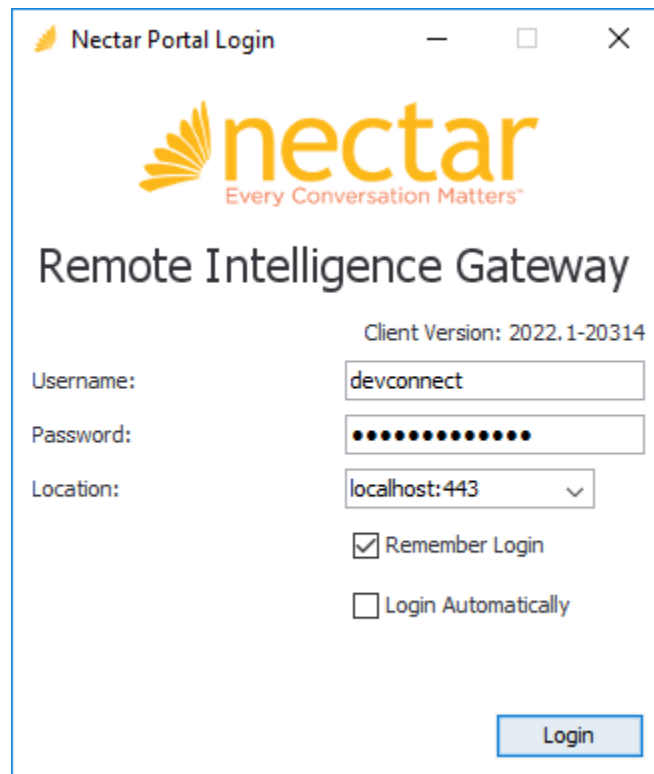
6. Configure Nectar for Avaya

This section covers the Nectar configuration to collect Session Manager Inventory and resource utilization data from System Manager and Session Manager using SNMPv3 polling. The configuration was performed via the **RIG client**. The procedure covers the following areas:

- Launch the RIG Client
- Configure System Manager Web Services and SNMP Polling Access
- Disable ASM Instance Data Collection

6.1. Launch the RIG Client

In an Internet browser, enter the Nectar IP address in the URL field. The RIG client software is downloaded. Install and run the RIG client. In the **Nectar Portal Login** screen, enter the user credentials and click **Login**.



Nectar Portal Login

nectar
Every Conversation Matters™

Remote Intelligence Gateway

Client Version: 2022.1-20314

Username: devconnect

Password: ●●●●●●●●●●

Location: localhost:443

Remember Login

Login Automatically

Login

6.2. Configure System Manager Web Services and SNMP Polling Access

Navigate to **Modules** → **Avaya** → **System Manager** and right-mouse click on the screen and select **Add** from the pop-up menu shown below to add a System Manager and Session Manager connection.

The screenshot shows the Nectar System Manager web interface. The top navigation bar includes the Nectar logo and the text "Every Conversation Matters". The main navigation menu contains icons for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. A status bar below the navigation menu displays "Primary: 2022.1-21422", "RTD: 4 ms", and "Users: 0".

The main content area is titled "Avaya System Manager Setup :". It has two tabs: "Configurations" and "VKM Options". Below the tabs is a "Connections" section with a search bar. A table with the following columns is visible: "Name", "Ip", "Port", "Description", and "Version". The table is currently empty, and a context menu is open over it, showing the following options: "Add...", "Edit...", "Remove", "View Collections...", "Session Manager", "Collect User Registrations", "Collect SIP Entities and Configure Monitoring", and "Copy to Clipboard".

At the bottom left of the table area, it says "1 row".

The **Add System Manager** dialog box is displayed as shown below. This configuration allows the System Manager Web Services access credentials and the SNMPv3 polling credentials for both System Manager and Session Manager to be specified.

Configure the following fields:

- **Version:** Select *r7.1 or above*.
- **Name:** Provide a descriptive name (e.g., *System Manager*).
- **IP:** Specify the System Manager IP address (e.g., *10.64.102.120*).
- **Port:** Specify HTTPS port 443.
- **Username:** Specify the user name configured in **Section 5.1**.
- **Password:** Specify the password configured in **Section 5.1**.
- **Description:** Provide an optional description (e.g., *DevConnect Test*).

In the **Community** section, specify the SNMPv3 polling credentials from **Section 5.3**. Click **Test** to test the connection and verify the credentials. Click **Add** to submit the form.

Add System Manager

Version: r7.1 or above

Name: SMGR

IP: 10.64.102.120

Port: 443

Username: nectar

Password: ●●●●●●●●●●

Description: DevConnect Test

Community

SNMP Version: V1 V2 V3

Port: 161

Community: [Redacted]

Authentication: None MD5 SHA

User ID: nectar

Password: ●●●●●●●●●●

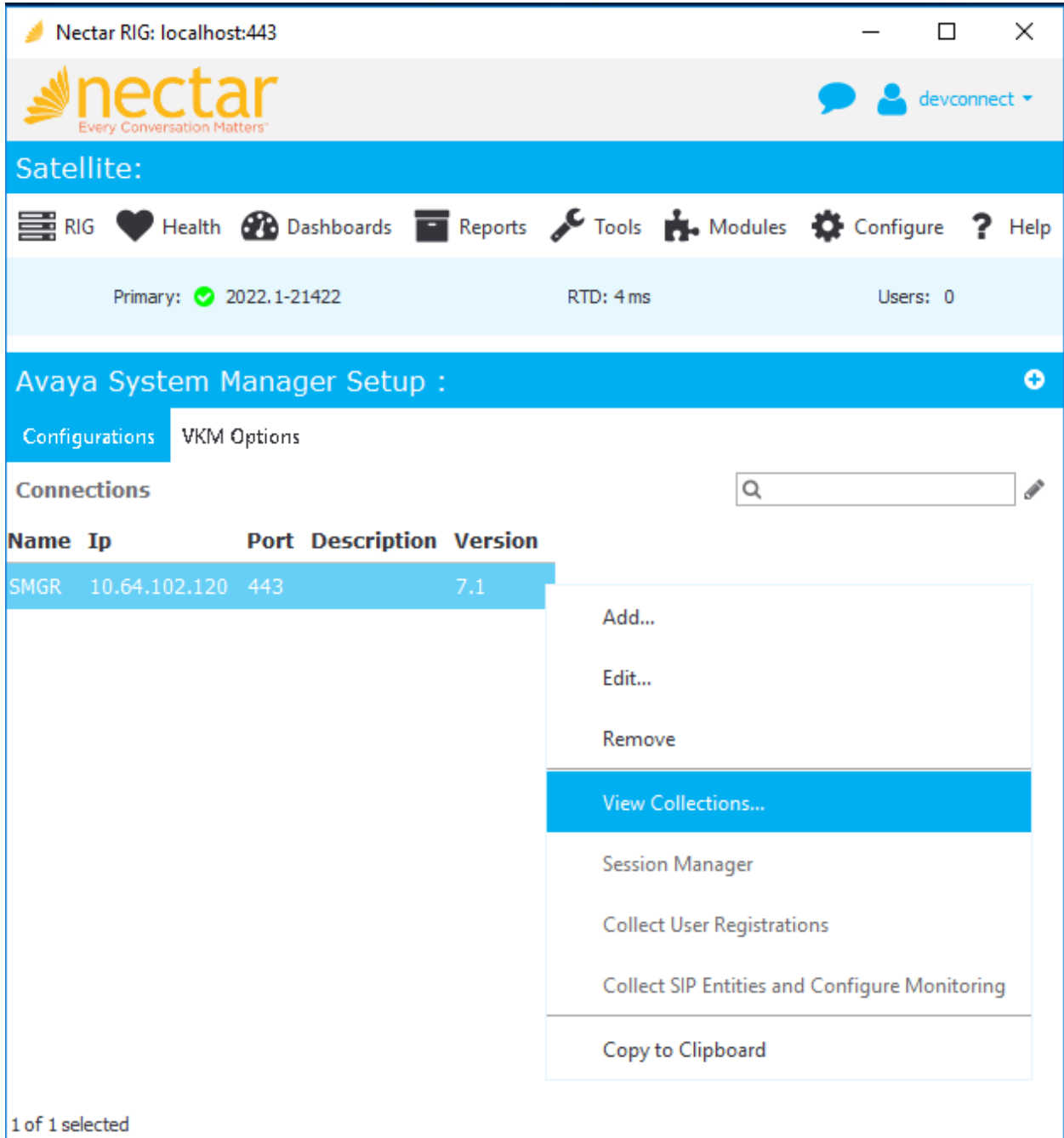
Privacy Protocol: AES

Privacy Password: ●●●●●●●●●●

Test **Cancel** **Add**

6.3. Disable ASM Instance Data Collection

Navigate to **Modules** → **Avaya** → **System Manager** and right-mouse click on the System Manager connection and select **View Collections...** from the pop-up menu as shown below. ASM Instance data collection is not supported.



The screenshot shows the Nectar RIG interface. At the top, the title bar reads "Nectar RIG: localhost:443". Below it is the Nectar logo with the tagline "Every Conversation Matters". A navigation bar contains icons for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. A status bar shows "Primary: 2022.1-21422", "RTD: 4 ms", and "Users: 0". The main content area is titled "Avaya System Manager Setup" and has two tabs: "Configurations" and "VKM Options". Under "Configurations", there is a "Connections" section with a search bar. A table lists connections with columns for Name, Ip, Port, Description, and Version. One connection is selected: SMGR, 10.64.102.120, 443, 7.1. A context menu is open over this row, listing options: Add..., Edit..., Remove, View Collections... (highlighted), Session Manager, Collect User Registrations, Collect SIP Entities and Configure Monitoring, and Copy to Clipboard. The bottom left of the table area says "1 of 1 selected".

Name	Ip	Port	Description	Version
SMGR	10.64.102.120	443		7.1

In **Collections**, right-mouse click on **ASM Instance for agent 0** and select *Disable* from the pop-up menu as shown below.

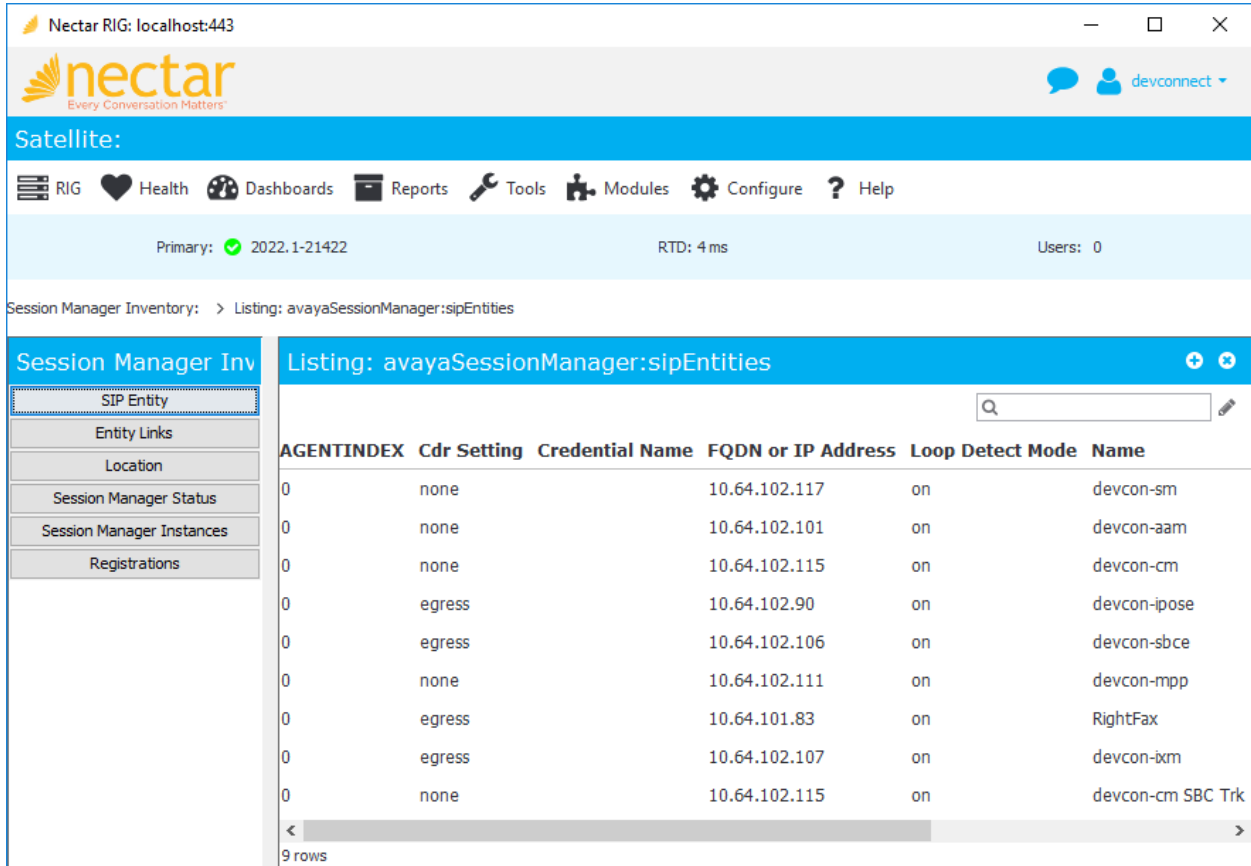
The screenshot shows the Nectar RIG interface for localhost:443. The top navigation bar includes links for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. Below the navigation bar, system status is shown: Primary: 2022.1-21422, RTD: 5 ms, Users: 0. The main content area is titled 'Collections' and contains a table of collection items. The 'ASM Instance for agent 0' row is highlighted in blue, and a context menu is open over it, showing options: Enable, Disable (highlighted), Change Cron String, Execute Now, and Copy to Clipboard. The bottom left of the table area shows '1 of 7 selected'.

Name	Enabled	Status	Schedule	Last Execution	Last Execution Duration
Session Manager Status for agent 0	Yes	Success	0 0 0 ? * *	08/18/22 12:00:...	0 min 0 sec
Registrations for agent 0	Yes	Success	0 0/15 * ...	08/18/22 12:15:...	0 min 0 sec
SIP Entity Links for agent 0	Yes	Success	0 0 0 ? * *	08/18/22 12:00:...	0 min 0 sec
SIP Entities for agent 0	Yes	Success	0 0 0 ? * *	08/18/22 12:00:...	0 min 0 sec
Locations for agent 0	Yes	Success	0 0 0 ? * *	08/18/22 12:00:...	0 min 0 sec
Users for agent 0	Yes	Success	0 0 0 ? * *	08/18/22 12:00:...	0 min 0 sec
ASM Instance for agent 0	Yes	Success	0 0 0 ? * *	08/18/22 12:00:...	0 min 0 sec

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Nectar with System Manager and Session Manager.

1. Navigate to **Reports** → **Inventory** → **Avaya** → **System Manager (r7.1 or above)** and select either **SIP Entity**, **Entity Links**, or **Location** to verify that Session Manager Inventory was retrieved using the System Manager Routing Web Service. The following screen displays the list of SIP entities.



The screenshot shows the Nectar RIG interface. The top navigation bar includes the Nectar logo and the text "Every Conversation Matters". Below the navigation bar, there is a "Satellite:" section with a menu of options: RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. The main content area displays the "Session Manager Inventory" page, which is titled "Listing: avayaSessionManager:sipEntities". The page shows a table of SIP entities with the following columns: AGENTINDEX, Cdr Setting, Credential Name, FQDN or IP Address, Loop Detect Mode, and Name. The table contains 9 rows of data.

AGENTINDEX	Cdr Setting	Credential Name	FQDN or IP Address	Loop Detect Mode	Name
0	none		10.64.102.117	on	devcon-sm
0	none		10.64.102.101	on	devcon-aam
0	none		10.64.102.115	on	devcon-cm
0	egress		10.64.102.90	on	devcon-ipose
0	egress		10.64.102.106	on	devcon-sbce
0	none		10.64.102.111	on	devcon-mpp
0	egress		10.64.101.83	on	RightFax
0	egress		10.64.102.107	on	devcon-ixm
0	none		10.64.102.115	on	devcon-cm SBC Trk

- Navigate to **Reports** → **Inventory** → **Avaya** → **System Manager (r7.1 or above)** and select either **Session Manager Status** or **Registrations** to verify that Session Manager Inventory can be retrieved using the Session Manager Element Manager Web Service. The following screen displays the user registrations.

The screenshot shows the Nectar RIG interface. The top navigation bar includes 'RIG', 'Health', 'Dashboards', 'Reports', 'Tools', 'Modules', 'Configure', and 'Help'. The main content area displays 'Session Manager Inventory' with a sub-section for 'Listing: avayaSessionManager:registrations'. A table lists registration details for Avaya devices.

Controller	MAC	Model	Type	Vendor	Version	First Name	Handle	Ip Address	Last Name	Login
0						SIP			78001	78001@avaya.com
0						SIP			78000	78000@avaya.com
0	devcon-sm	3c:b1:5b:5f:97:af	96x1	Avaya	7.1.15.0.14	Agent	78030@avaya.com	192.168.100.49:34273	78030	78030@avaya.com
0						SIP			78002	78002@avaya.com
0	devcon-sm	2c:f4:c5:f6:69:a5	96x1	Avaya	7.1.13.0.4	SIP	78003@avaya.com	192.168.100.64:34176	78003	78003@avaya.com

22 rows

- Navigate to **Health** → **Elements** and select **Agents** in the leftmost pane. In the **All Agents** pane, select the System Manager agent. In the **Poll Functions** tab, the *CPU Utilization* and *Linux Physical Memory Utilization*, derived from SNMPv3 polls, should be displayed.

The screenshot shows the Nectar RIG interface for localhost:443. The 'Elements' section is active, showing a list of agents under 'All Agents'. The 'SMGR' agent is selected. The 'Poll Functions' tab is active, displaying a table of system metrics. Two rows are highlighted with a red border: 'CPU Utilization' and 'Linux Physical Memory Utilization'.

Description	Function	Sub Function	Enabled	Current Value	Max V...
Disk Usage /var/opt/nortel/cnd	snmpDiskUsage		true	7.798	100
Disk Usage /swlibrary	snmpDiskUsage		true	4.184	100
Disk Usage /boot	snmpDiskUsage		true	32.632	100
Disk Usage /boot/efi	snmpDiskUsage		true	1.127	100
Disk Usage /var/lib/pgsqldata	snmpDiskUsage		true	5.469	100
Disk Usage /var/log	snmpDiskUsage		true	3.446	100
Disk Usage /var/log/audit	snmpDiskUsage		true	1.33	100
Disk Usage /tmp	snmpDiskUsage		true	1.764	100
Disk Usage /var/tmp	snmpDiskUsage		true	1.764	100
Disk Usage /home	snmpDiskUsage		true	7.723	100
Disk Usage /run/user/0	snmpDiskUsage		true	0	100
Disk Usage /run/user/779	snmpDiskUsage		true	0	100
CPU Utilization	cpuUtilizationSNMP		true	2	100
Linux Physical Memory Utilization	SNMPLinuxPhysMemory		true	72	100
Disk Usage Swap space	snmpDiskUsage		true	11.768	100

- Navigate to **Health** → **Elements** and select **Agents** in the leftmost pane. In the **All Agents** pane, select the Session Manager agent. In the **Poll Functions** tab, the *CPU Utilization* and *Linux Physical Memory Utilization*, derived from SNMPv3 polls, should be displayed.

The screenshot shows the Nectar RIG interface for localhost:443. The 'Elements' pane is active, showing the 'All Agents' list on the left and the 'Poll Functions' table on the right. The 'devcon-sm' agent is selected, and its poll functions are displayed in a table. Two rows are highlighted in red: 'CPU Utilization' and 'Linux Physical Memory Utilization'.

Description	Function	Sub Function	Enabled	Current Value	Max V...
Ping 10.64.102.116	ping		true	1	
Current Registrations	AvayaComStruc		true	4	100
CPU Utilization	cpuUtilizationSNMP		true	3	100
Linux Physical Memory Utilization	SNMPLinuxPhysMemory		true	71	100
Disk Usage Swap space	snmpDiskUsage		true	9.443	100
Disk Usage /dev/shm	snmpDiskUsage		true	0.001	100
Disk Usage /run	snmpDiskUsage		true	9.428	100
Disk Usage /sys/fs/cgroup	snmpDiskUsage		true	0	100
Disk Usage /	snmpDiskUsage		true	31.226	100
Disk Usage /boot	snmpDiskUsage		true	8.251	100
Disk Usage /boot/efi	snmpDiskUsage		true	2.879	100
Disk Usage /tmp	snmpDiskUsage		true	1.016	100
Disk Usage /data	snmpDiskUsage		true	1.379	100
Disk Usage /home	snmpDiskUsage		true	21.513	100
Disk Usage /var	snmpDiskUsage		true	6.47	100

8. Conclusion

These Application Notes described the configuration steps required to integrate Nectar for Avaya with Avaya Aura® System Manager and Avaya Aura® Session Manager using Avaya Aura® System Manager Web Services and SNMP polling. The compliance test passed with observations noted in **Section 2.2**.

9. Additional References

This section references the Avaya documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022.
- [2] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022.
- [3] *Avaya Routing Web Service API Programming Reference*, Release 8.1, Issue 1, June 2019, available at <http://support.avaya.com>.
- [4] *Avaya Aura® Session Manager Element Manager Web Service API Programming Reference*, Release 7.1.1, Issue 1.0, August 2017, available at <http://support.avaya.com>.

©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ 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 devconnect@avaya.com.