Abstract

These Application Notes describe the configuration steps required to integrate Nectar Foundation with Avaya Aura® System Manager and Avaya Aura® Session Manager. Nectar Foundation is a proactive health and performance monitor that provides enterprise customers and service providers with a comprehensive view of unified communications environments for monitoring, allowing service interruptions to be diagnosed and solved quicker. Nectar Foundation 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 Foundation with Avaya Aura® System Manager and Avaya Aura® Session Manager. Nectar Foundation is a proactive health and performance monitor that provides enterprise customers and service providers with a comprehensive view of unified communications environments for monitoring, allowing service interruptions to be diagnosed and solved quicker. Nectar Foundation 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 Foundation 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 Foundation collected the following data from Session Manager:

- Session Manager Status
- Session Manager Instances
- User Registrations

Nectar Foundation 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 Foundation 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 Foundation 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 Foundation came back into service after re-connecting the Ethernet cable (i.e., restoring network connectivity) and rebooting the Foundation 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note 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.

2.1. Interoperability Compliance Testing
Interoperability compliance testing covered the following Foundation features and functionality. Alarms/alerts, system inventory, resource utilization and status, and call quality metrics were displayed on the RIG client.

- 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, Session Manager Instances, 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 status changes made to Session Manager and SIP 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.
- Tracking the registration status of existing and new Avaya SIP Deskphones.
- Verifying proper system recovery after a restart of the Foundation server and loss of IP network connectivity.
2.2. Test Results
The compliance test passed with the following observations:

- Initially, the Session Manager Inventory data displays zeros in the RIG client when it is first started, click or select the inventory item again to display the actual data.

- The Session Manager Element Manager Web Service API returns incorrect field values for SIP Monitoring and CDR in the Session Manager administration. These field values are returned as false even when they are enabled.

- Currently, Nectar Foundation doesn’t support receiving SNMP traps from System Manager or Session Manager.

2.3. Support
For technical support and information on Nectar Foundation, contact Nectar Support at:

- Phone: 1-888-811-8647
- Website: http://nectarcorp.com/support
- Email: support@nectarcorp.com
3. Reference Configuration

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

Figure 1: Nectar Foundation with Avaya SIP-based Network
4. Equipment and Software Validated
The following equipment and software were used for the sample configuration provided:

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager</td>
<td>8.1.2.0.0-FP2</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>FW 41.24.0</td>
</tr>
<tr>
<td>Avaya Aura® Media Server</td>
<td>v.8.0.2.93</td>
</tr>
<tr>
<td>Avaya Aura® System Manager</td>
<td>8.1.2.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.2.0.0611167 Feature Pack 2</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>8.1.2.0.812039</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise</td>
<td>8.1.0.0-14-18490</td>
</tr>
<tr>
<td>Avaya 96x1 Series IP Deskphones</td>
<td>6.8304 (H.323) 7.1.9.0.8 (SIP)</td>
</tr>
<tr>
<td>Avaya J179 SIP Deskphone</td>
<td>4.0.5.0.10</td>
</tr>
<tr>
<td>Nectar Foundation</td>
<td>8.3.0.2-09317</td>
</tr>
<tr>
<td>Nectar Remote Intelligence Gateway (RIG) Client</td>
<td>8.3.0.2-09317</td>
</tr>
</tbody>
</table>
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 Foundation Access
- Verify System Manager Web Services
- Enable SNMP Polling

Configuration was performed by accessing the browser-based GUI of System Manager using the URL https://<ip-address>, where <ip-address> is the System Manager IP address, and logging in using the appropriate credentials.

5.1. Add New Administrator for Nectar Foundation Access

A user account is required by Foundation 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.
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**.
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:
  
  ```bash
  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.

```
--2020-05-04 11:31:35-- https://10.64.102.120/ws/grservice/getgrstate/test
Connecting to 10.64.102.120:443...connected.
WARNING: cannot verify 10.64.102.120's certificate, issued by '/CN=System Manager CA/OU=MGMT/O=AVAYA':
  Self-signed certificate encountered.
WARNING: certificate common name 'devcon-smgr.avaya.com' doesn't match requested host name '10.64.102.120'.
HTTP request sent, awaiting response... 200 OK
Length: 698 [application/octet-stream]
Saving to: 'test.4'

100%[==========================================] 698 --.-K/s in 0s

2020-05-04 11:31:35 (72.3 MB/s) - 'test.4' saved [698/698]
```

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 https://<ip-address>, 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 Foundation 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](image)

Finally, 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](image)
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.
6. Configure Nectar Foundation

This section covers the Foundation 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

6.1. Launch the RIG Client

In an Internet browser, enter the Foundation 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.
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 **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*).
- **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. Click **Add** to submit the form.
7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Foundation 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 can be retrieved using the System Manager Routing Web Service. The following screen displays the list of SIP entities.
2. Navigate to **Reports → Inventory → Avaya → System Manager (r7.1 or above)** and select either **Session Manager Status**, **Session Manager Instances**, 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.
3. 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.
4. 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.
8. Conclusion
These Application Notes described the configuration steps required to integrate Nectar Foundation 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.
