DevConnect Program

Application Notes for Nectar Diagnostics with Avaya Session Border Controller 10.1 and Avaya Aura® Session Manager 10.1 − Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Nectar Diagnostics version 2023.0.0.3 with Avaya Session Border Controller 10.1 and Avaya Aura® Session Manager 10.1.

Nectar Diagnostics provides real-time service assurance for Unified Communications (UC) environments. It correlates real-time session (signaling), media (voice/video) streams, and topology paths and events for UC applications.

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 Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required to integrate Nectar Diagnostics (Diagnostics) version 2023.0.0.3 with Avaya Session Border Controller 10.1 (Avaya SBC) and Avaya Aura® Session Manager 10.1 (Session Manager).

In the reference configuration, Diagnostics collects and reports calls CDR data and Media Statistics from the Avaya SBC via RADIUS. Diagnostics also collects call setup SIP signaling information via Syslog messages, as configured on the Session Manager GUI. Diagnostics will then correlate the CDR/Media Statistics data with the SIP signaling to provide SIP and RTP analysis of each call traversing the Avaya SBC.

Nectar Diagnostics consists of the following components, which are collectively referred to as Unified Communications Diagnostics (UCD).

- Unified Communications Diagnostics Manager (UCD-M)
- Unified Communications Diagnostics Point (UCD-P)
- Unified Communications Diagnostics Analyzer (UCD-A).

In the reference configuration, the UCD software runs as a virtual machine on a VMware host located on the enterprise network.

2. General Test Approach and Test Results

The general test approach was to manually place inbound and outbound calls from the enterprise to the PSTN through a SIP trunk in Avaya SBC, to verify that Nectar Diagnostics collects the syslog and CDR/Media Statistics records, and properly classifies and reports the attributes of the calls.

Serviceability test cases focused on simulating a network outage and also a restart on the Diagnostics server. Calls records were verified to continue being received after the network was restored and the server came back in service.

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 this Application Notes, the interfaces between Avaya SBC and Avaya Session Manager to Nectar Diagnostics did not use encryption capabilities.

TLS/SRTP encryption was used internally on the enterprise between Avaya Aura® servers and endpoints.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. For the feature testing test cases, inbound and outbound PSTN calls were made to and from the enterprise site, being routed through the Avaya SBC to Session Manager and Communication Manager

Different SIP and H.323 IP endpoints at the enterprise were used to make inbound and outbound PSTN calls to generate useful Syslog/RADIUS traffic, sent to the Nectar Diagnostics server in the lab. Records were retrieved and analyzed on the Diagnostics GUI, and captures were taken to verify the accuracy of the data received.

The serviceability testing focused on verifying the ability of Nectar Diagnostics to recover from adverse conditions, such as a network outage and also a restart on the Diagnostics server

2.2. Test Results

All executed test cases were verified and completed successfully.

2.3. Support

For technical support and information on Nectar Diagnostics, 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 the sample configuration used for the compliance testing.

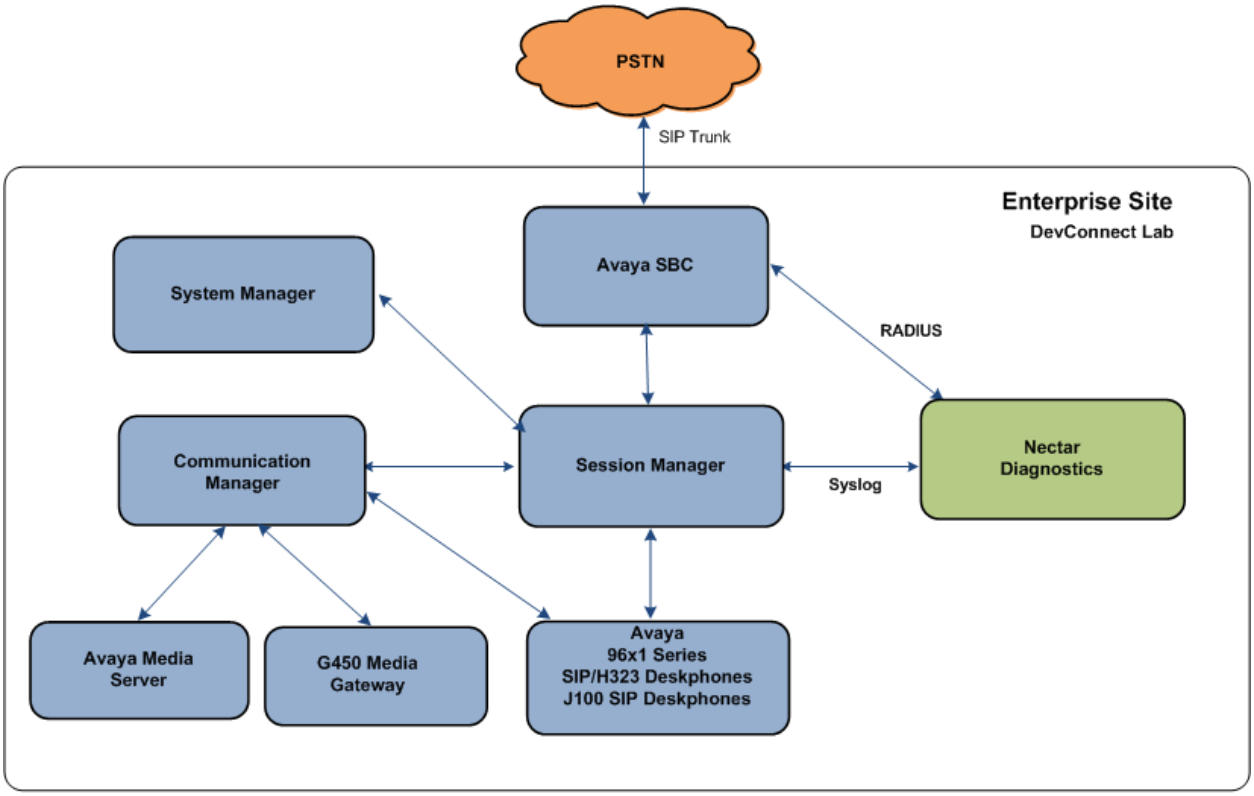


Figure 1: Test Configuration

A simulated enterprise site containing the Nectar Diagnostics server, Avaya SBC, Session Manager, Communication Manager and the rest of the Avaya Aura® infrastructure was installed at the DevConnect Lab. The Avaya SBC connected the enterprise site to a SIP trunk service provider, used to provide PSTN access to the enterprise.

Diagnostics collected real time CDR data and Media Statistics from the Avaya SBC via RADIUS. Diagnostics also collected real time SIP signaling information of call setup via Syslog messages from Session Manager, as configured on the Session Manager GUI. Diagnostics then correlated the CDR/Media Statistics data with the SIP signaling to provide SIP and RTP analysis of each call traversing the Avaya SBC.

Note – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

The following Avaya components were used in the reference configuration in the DevConnect Lab:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller
- Avaya G450 Media Gateway
- Avaya Media Server
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- Avaya J100 Series IP Deskphones using the SIP software bundle.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Session Border Controller	10.1.2.0-64-23285 HotFix-1
Avaya Aura® System Manager	10.1.3.1.0716418 Service Pack 1 Hotfix 1013116418
Avaya Aura® Session Manager	10.1.3.1.1013103
Avaya Aura® Communication Manager	10.1.3.0.1-FP3P1 Update ID 01.0.974.0-27893
Avaya Session Border Controller	10.1.2.0-64-23285 HotFix-1
Avaya Aura® Media Server	Media Server 10.1.0.154 Appliance Version 10.0.0.14
Avaya G450 Media Gateway	42.24
Avaya 96x1 Series IP Deskphone (H.323)	6.8.5.4.10
Avaya 96x1 Series IP Deskphone (SIP)	7.1.15.2.1
Avaya J100 IP Deskphones (SIP)	4.1.2.0.11
Nectar Diagnostics	2023.0.0.3

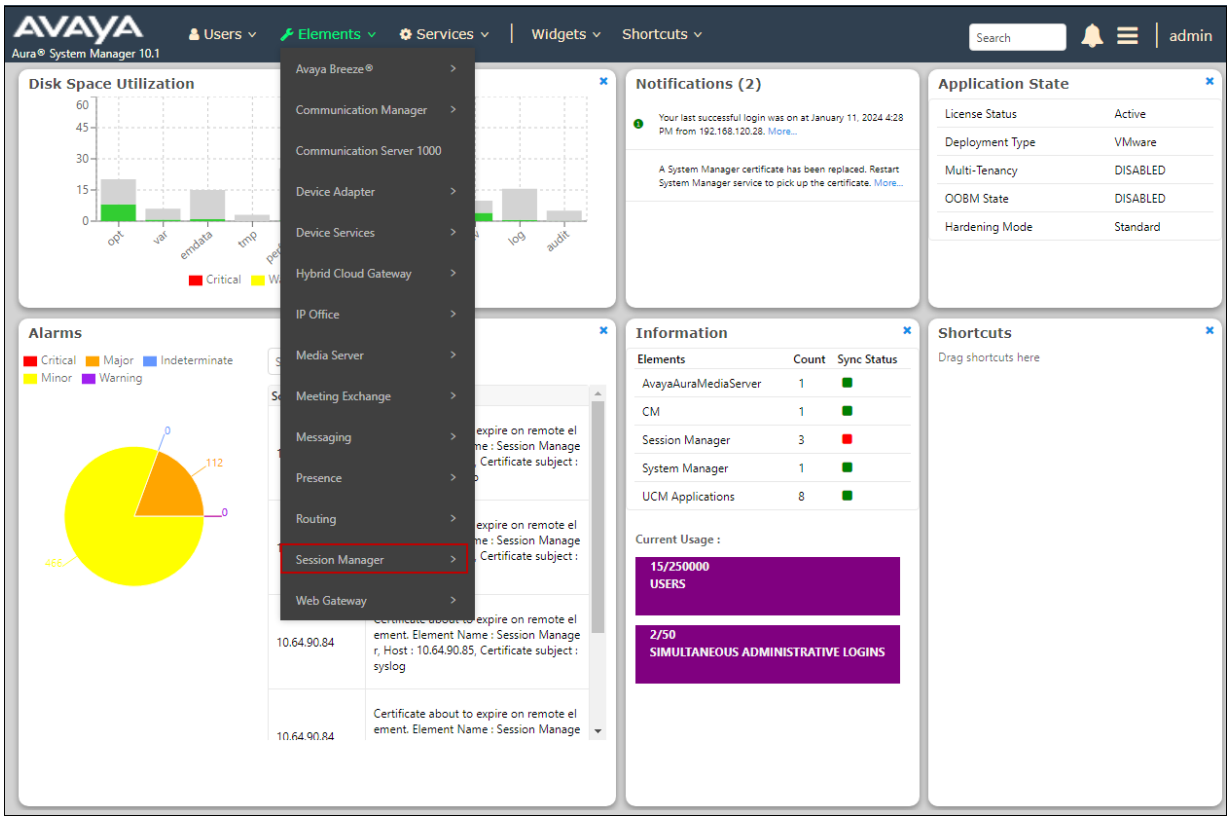
5. Configure Avaya Aura® Session Manager

Avaya Session Manager can be configured to send SIP signaling information to remote logging servers. The following section describes the configuration steps necessary to send SIP signaling data to Nectar Diagnostics via Syslog messages.

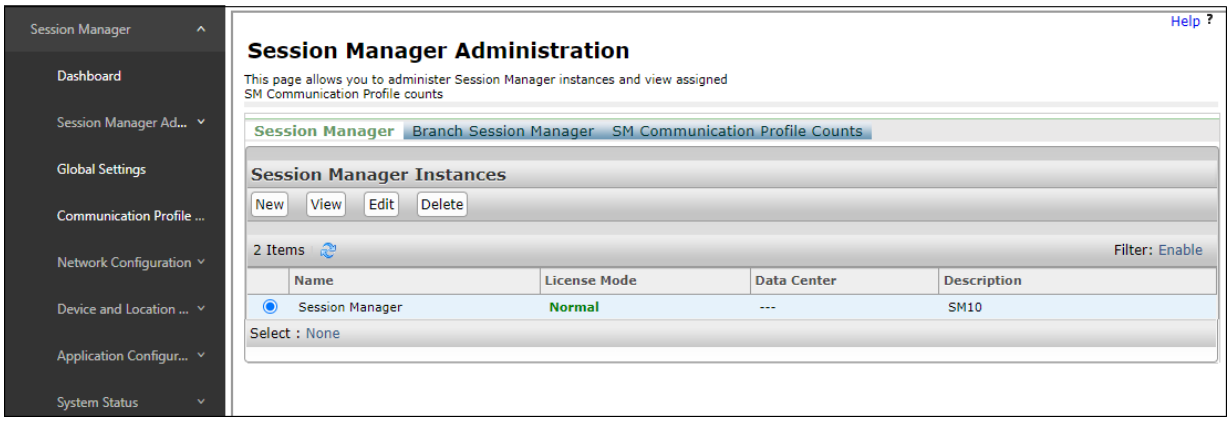
Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult the documentation in Additional References section for further details if needed.

5.1. Configure Remote Logging

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "**https://<ip-address>/SMGR**" where **"<ip-address>"** is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading, select **Session Manager**.

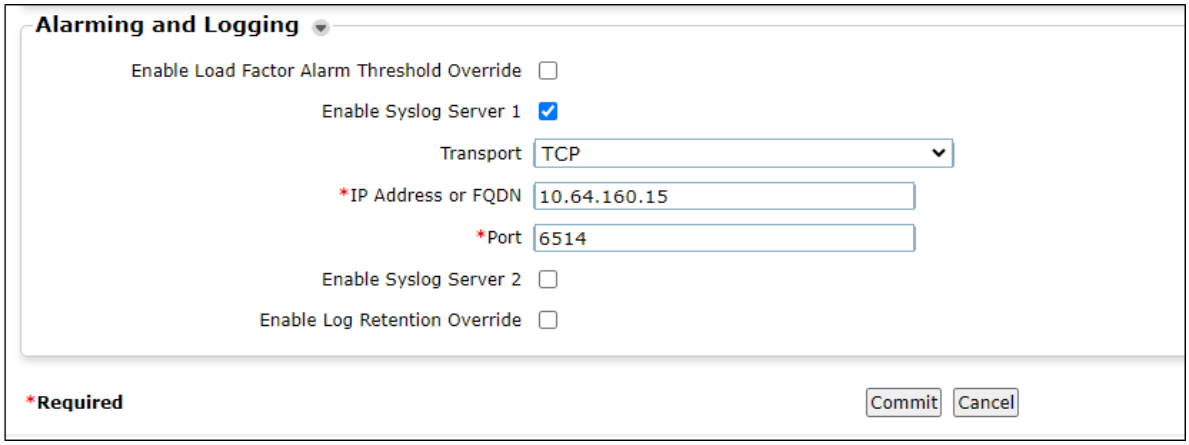


On the **Session Manager** tab, select **Session Manager Administration** from the menu on the left. Select the **Session Manager** instance and click **Edit**.



Scroll down to **the Alarming and Logging** section and set the following:

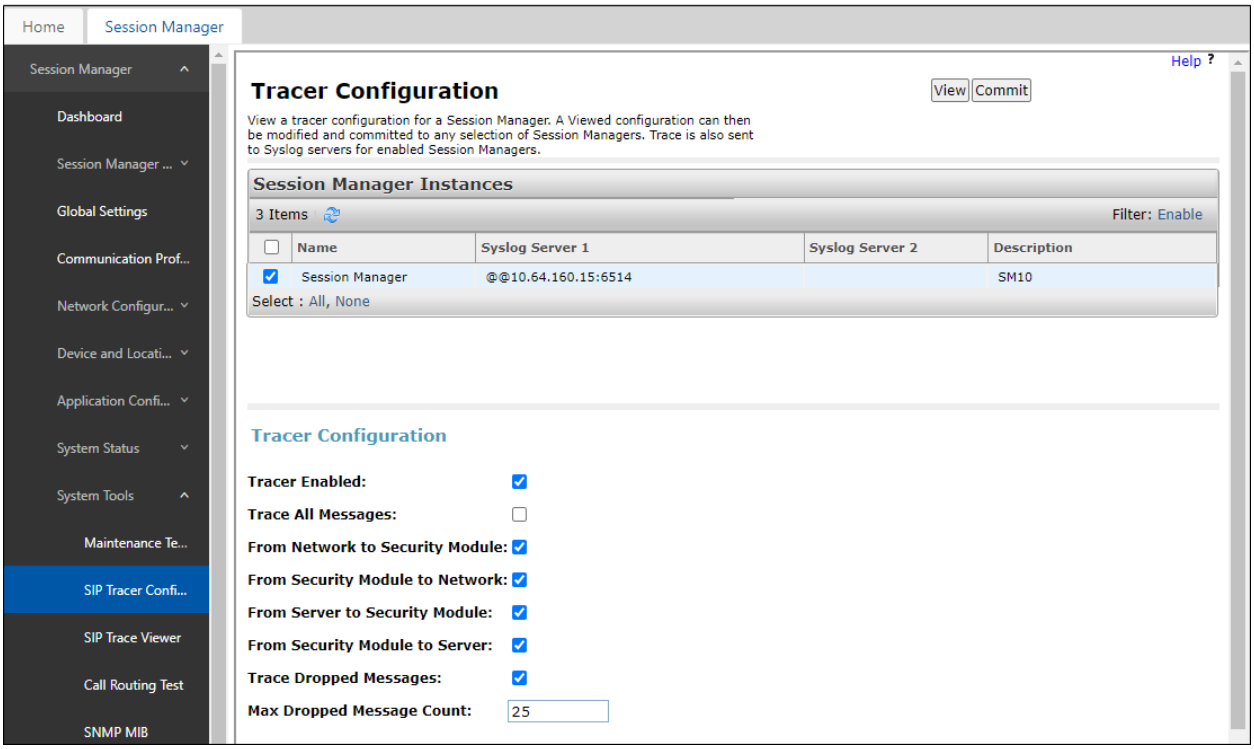
- Check the **Enable Syslog Server** 1 box.
- **Transport**: select **TCP**.
- **IP Address or FQDN** and **Port**: enter the IP address and port of the Nectar Diagnostics (UCD-P) server interface.
- Click on **Commit.**



5.2. SIP Tracer Configuration

The SIP Tracing feature is used to define the type of messages to be traced by the capturing engine in the Session Manager security module.

On the **Session Manager** tab, select **System Tools → SIP Tracer Configuration** from the menu on the left. Select the **Session Manager** instance and click **View**. Check the **Tracer Enabled** box. Configure the remaining fields as shown on the screen below. Select **Commit**.

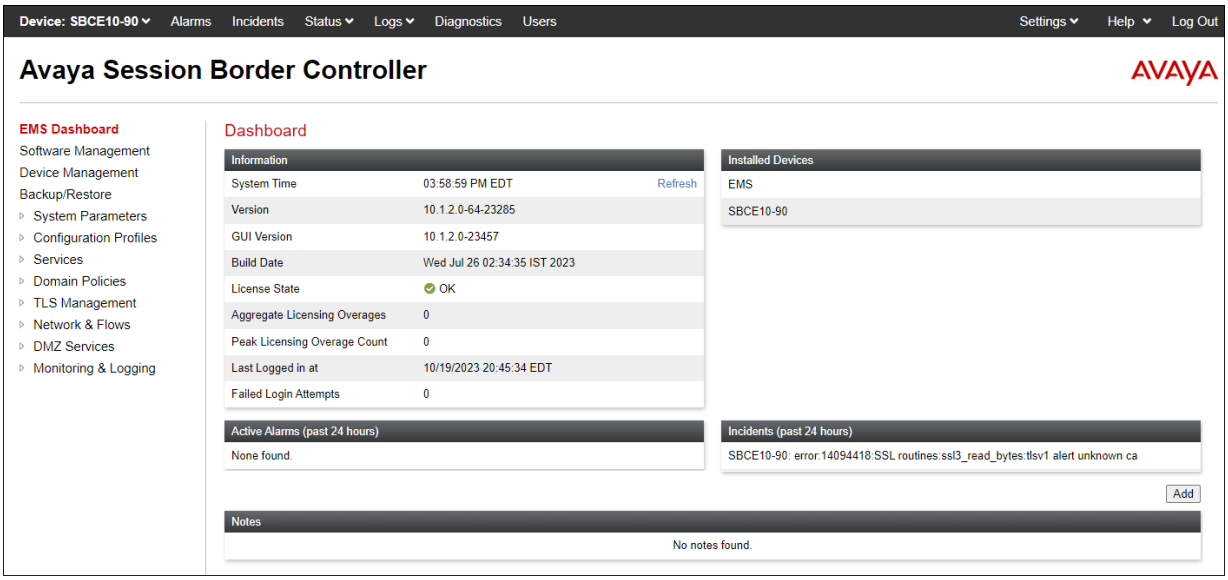


6. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBC to send CDR data and Media Statistics via RADIUS to Nectar Diagnostics. It is assumed that the initial provisioning of the Avaya SBC, including license installation and SIP trunking configuration has already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBC consult the documentation in the **Additional References** section.

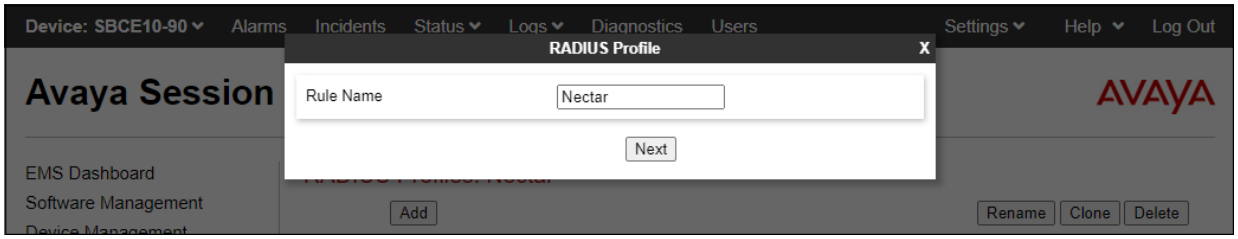
Use a WEB browser to access the Element Management Server (EMS) web interface, and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBC. Log in using the appropriate credentials.

The EMS Dashboard page of the Avaya SBC will appear. All configuration screens of the SBC are accessed by navigating the menu tree in the left pane.



6.1. Add RADIUS Profile

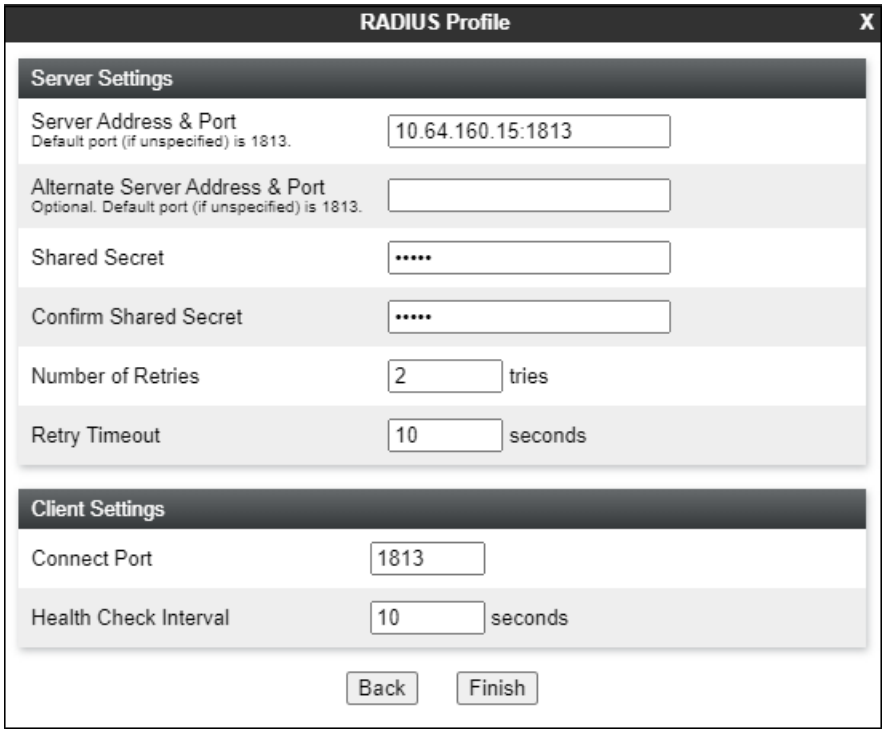
To create the RADIUS profile for the Nectar Diagnostics server, navigate to **Services → RADIUS** on the menu on the left pane and select **Add**. Enter a name under **Rule Name** (e.g., **Nectar**) and click **Next**.



On the **RADIUS Profile** screen enter the following:

- **Server Address & Port**: IP address and port of the Nectar Diagnostics (UCD-P) server (e.g., **10.64.160.15:1813**)
- **Shared Secret**: The shared password for Avaya SBC and RADIUS server.
- **Confirm Shared Secret**: Re-enter the shared password above.

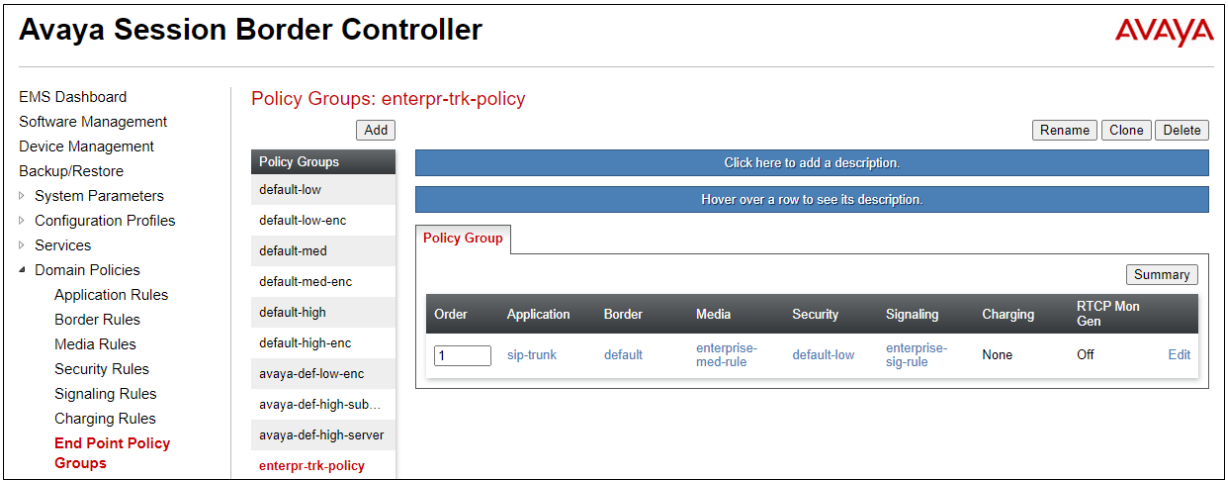
The remaining fields can be set as shown on the screen below, as set in the reference configuration. Select **Finish** after all entries are made.



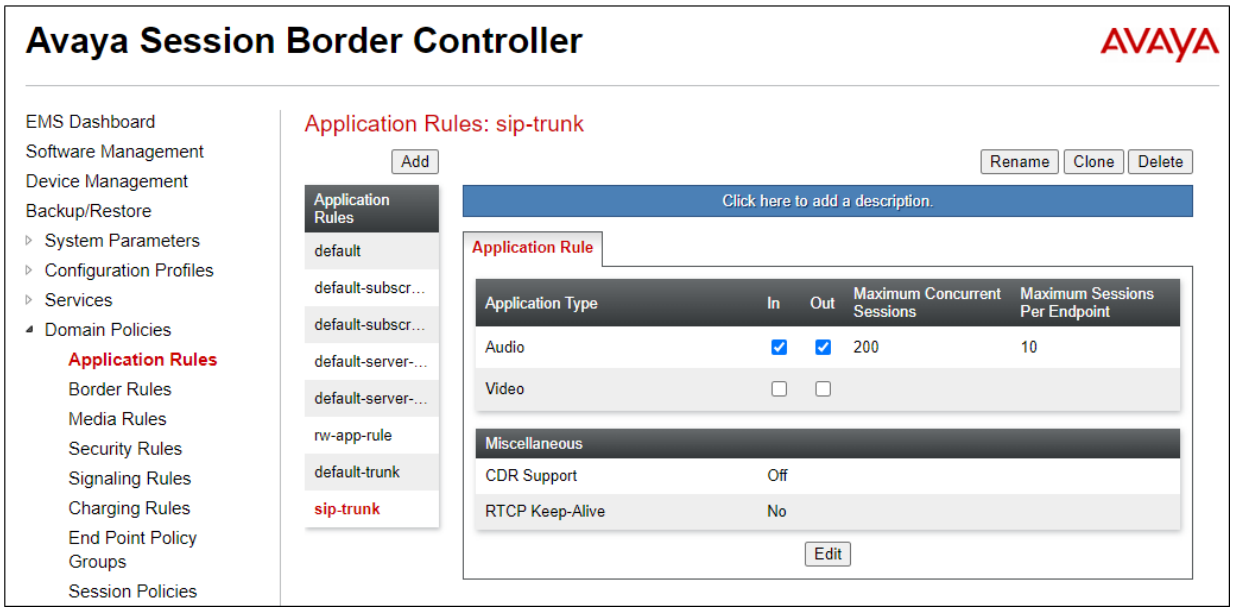
6.2. Enable CDR Support in Application Rule

CDR support must be enabled in the Application Rule used by the End Point Policy Group associated with the SIP trunk, so the CDR data is sent to the RADIUS server configured in the previous section.

In the reference configuration, since the SIP signaling data is retrieved from Session Manager via Syslog, CDR was enabled on the Application Rule called **sip-trunk**, used by End Point Policy Group **enterpr-trk-policy** associated to the trunk between Session Manager and the Avaya SBC.

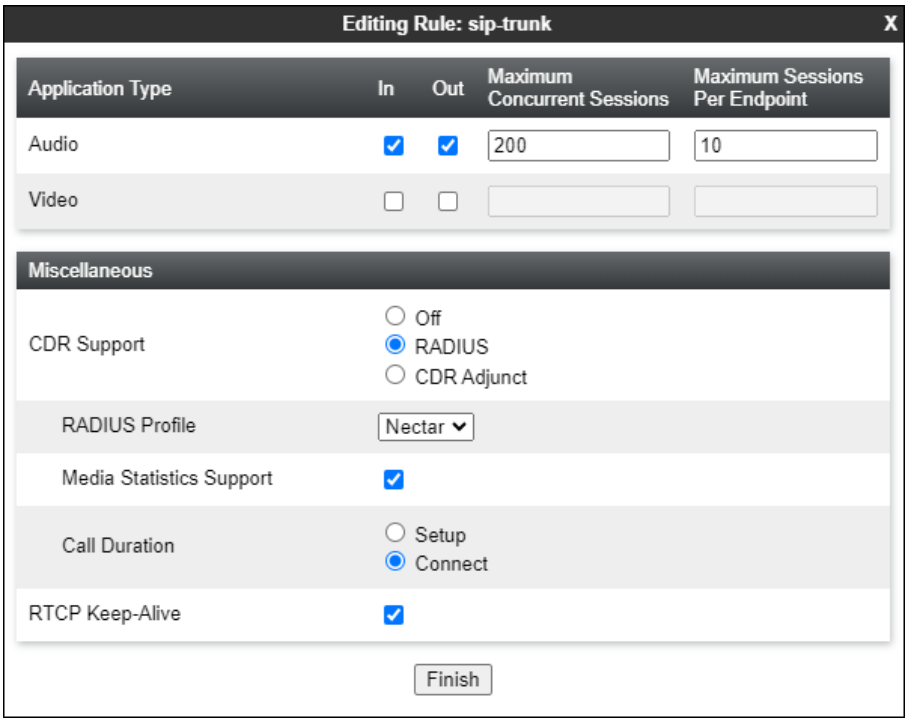


In the left navigation pane, select **Domain Policies → Application Rules**. Select the Application Rule to be modified (e.g., **sip-trunk**) and click **Edit**.



On the Miscellaneous section:

- **CDR Support**: Select **RADIUS**
- **RADIUS Profile**: Select the **Nectar** profile created in **Section 6.1**.
- Check the box for **Media Statistic Support,** to specify call media statistics data to be made available in the CDR file.
- **Call Duration**: Set to **Connect**. With this setting data in the CDR file is stored from the time the Avaya SBC receives a 200 OK message for connecting the call.
- Check the box for **RTCP Keep-Alive**.
- Click **Finish**.



Note: It may be necessary to restart the Avaya SBC application before CDR data starts to be collected. Navigate to **Device Management → Restart Application** to perform the restart. Note that this step will be service affecting.

7. Configure Nectar Diagnostics

Configuration of the Nectar Diagnostics solution, including installation, licensing and initial provisioning of the server at the customer's enterprise is assumed to be in place and it is not discussed in these Application Notes. . For more information on the installation and provisioning of these task consult the Nectar documentation in the **Additional References** section.

This section covers the configuration command needed on Nectar Diagnostics to receive Syslog messages from Session Manager, and CDR messages via RADIUS from Avaya SBC.

7.1. Enable Syslog Messages

Perform the following steps to configure Diagnostics (UCD-P) to receive Syslog messages from Session Manager. Open a SSH connection to the Diagnostics management IP address and log in with the appropriate credentials. At the prompt, enter the following commands:

 # configure terminal
*# listen-voip-msg-backhaul syslog port **6514** platform avayasm*
 # session-sip-identity avaya callid-fromip
 # end
 # copy running-config startup-config

Note that *syslog port* must match the value for the remote Syslog server configuration in Session Manager (**Section 5.1**). In the reference configuration port **6514** is used.

7.2. Enable RADIUS messages

Perform the following steps to configure Diagnostics (UCD-P) to receive RADIUS messages from Avaya SBC. Open a SSH connection to the Diagnostics management IP address and log in with the appropriate credentials. At the prompt, enter the following commands:

 # configure terminal
*# listen-voip-msg-backhaul radius-acct port **1813***
*# radius-acct client **10.64.90.90** key **avaya123***
 # end
 # copy running-config startup-config

Note the following:

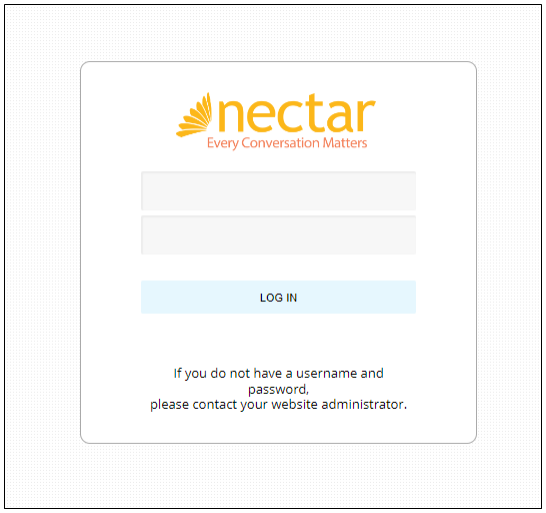
- The *radius-acct port* must match the value configured for the RADIUS profile on the Avaya SBC (**Section 6.1**). In the reference configuration port **1813** is used.
- *radius-acct client* corresponds to the IP address of the management interface of the Avaya SBC, **10.64.90.90** in the example.
- *key* is the shared password (Shared Secret) configured on the Avaya SBC RADIUS profile (**Section 6.1**), **avaya123** in the example.

8. Verification Steps

The following steps may be used to verify the configuration.

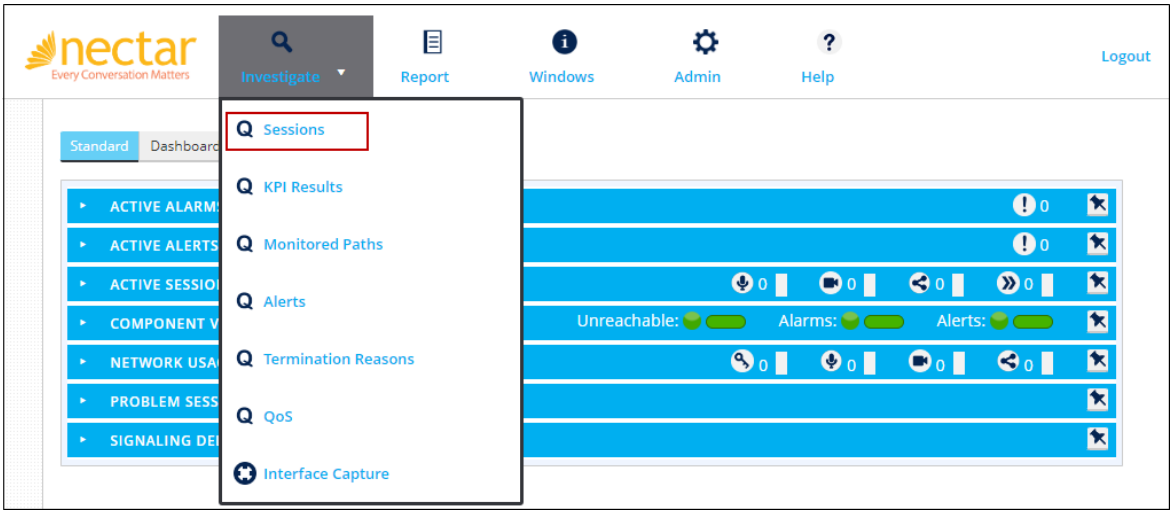
8.1. Verify Data Collection

Log in to the Nectar Diagnostics GUI interface (UCD-M) using the proper credentials.

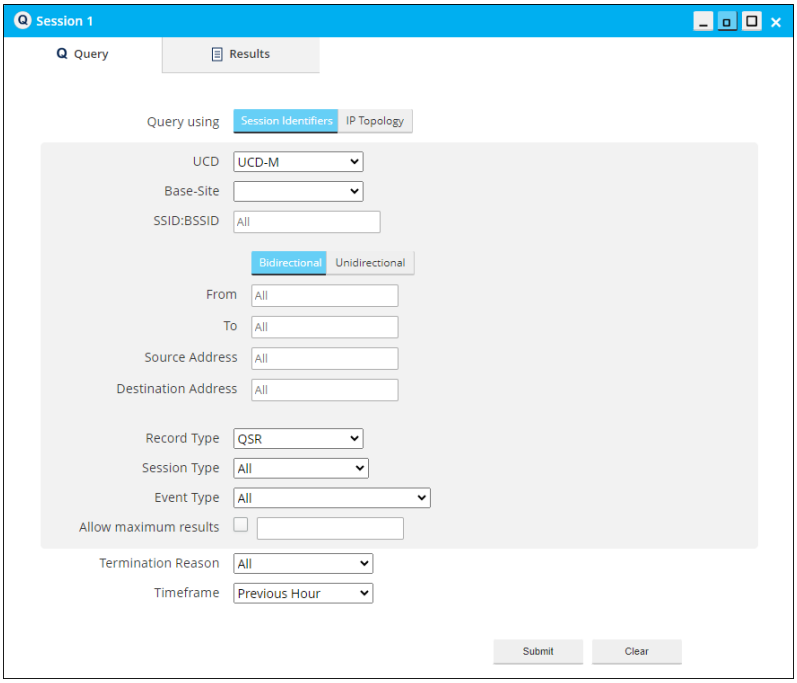


Make several inbound and outbound SIP trunk calls via Avaya SBC and Session Manager to generate Syslog and CDR traffic.

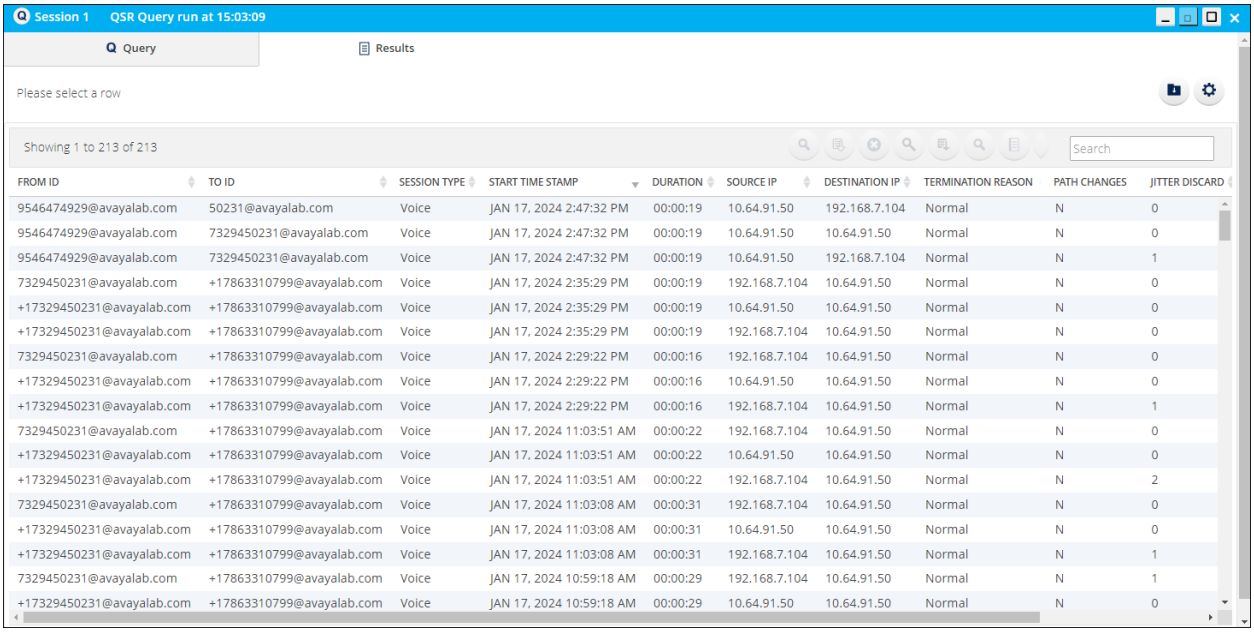
On the UCD-M Dashboard, select **Investigate → Sessions.**



Select the desired **Timeframe** and click **Submit**.

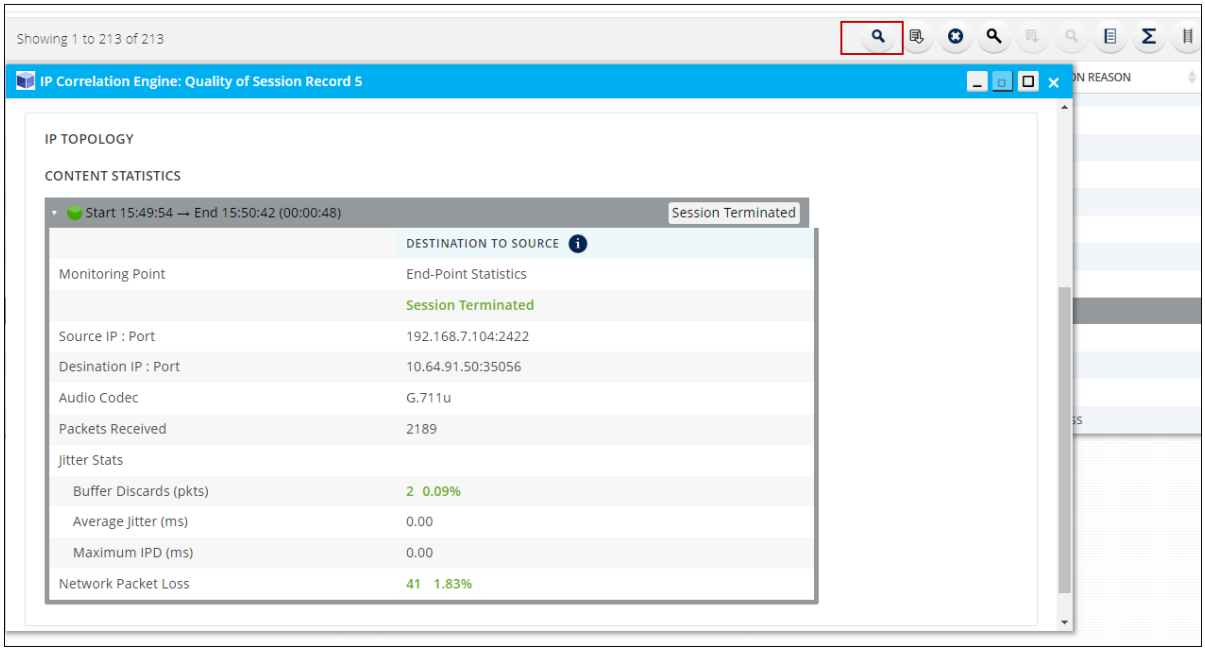


The resulting screen should show the calls records received.



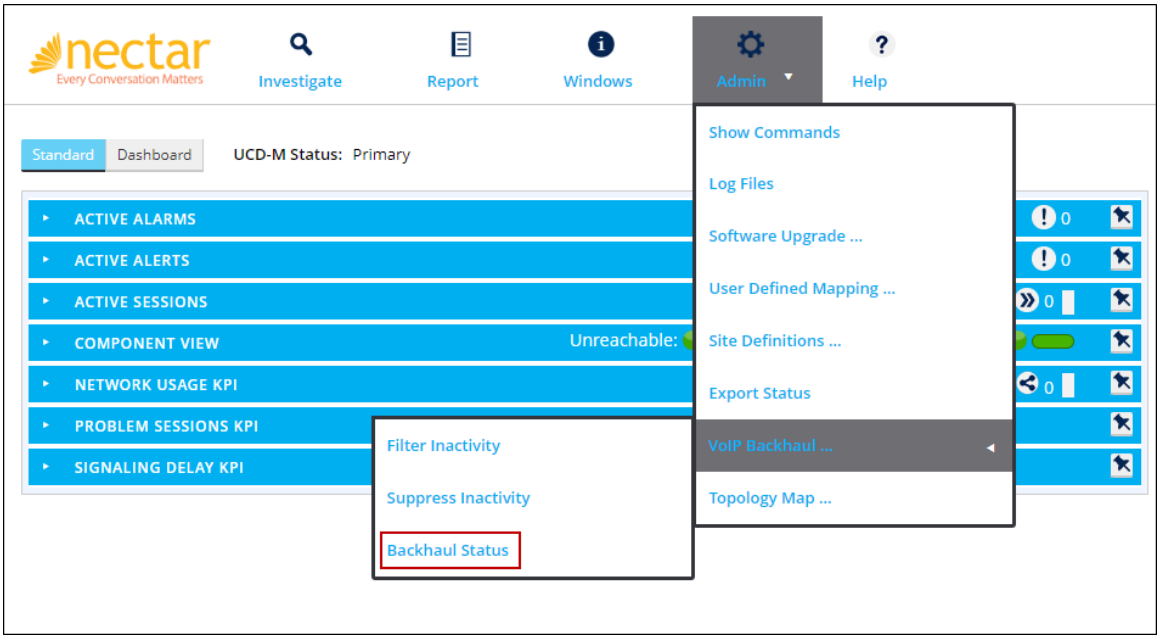
FROM ID	TO ID	SESSION TYPE	START TIME STAMP	DURATION	SOURCE IP	DESTINATION IP	TERMINATION REASON	PATH CHANGES	JITTER DISCARD
9546474929@avayalab.com	50231@avayalab.com	Voice	JAN 17, 2024 2:47:32 PM	00:00:19	10.64.91.50	192.168.7.104	Normal	N	0
9546474929@avayalab.com	7329450231@avayalab.com	Voice	JAN 17, 2024 2:47:32 PM	00:00:19	10.64.91.50	10.64.91.50	Normal	N	0
9546474929@avayalab.com	7329450231@avayalab.com	Voice	JAN 17, 2024 2:47:32 PM	00:00:19	10.64.91.50	192.168.7.104	Normal	N	1
7329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 2:35:29 PM	00:00:19	192.168.7.104	10.64.91.50	Normal	N	0
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 2:35:29 PM	00:00:19	10.64.91.50	10.64.91.50	Normal	N	0
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 2:35:29 PM	00:00:19	192.168.7.104	10.64.91.50	Normal	N	0
7329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 2:29:22 PM	00:00:16	192.168.7.104	10.64.91.50	Normal	N	0
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 2:29:22 PM	00:00:16	10.64.91.50	10.64.91.50	Normal	N	0
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 2:29:22 PM	00:00:16	192.168.7.104	10.64.91.50	Normal	N	1
7329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 11:03:51 AM	00:00:22	192.168.7.104	10.64.91.50	Normal	N	0
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 11:03:51 AM	00:00:22	10.64.91.50	10.64.91.50	Normal	N	0
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 11:03:51 AM	00:00:22	192.168.7.104	10.64.91.50	Normal	N	2
7329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 11:03:08 AM	00:00:31	192.168.7.104	10.64.91.50	Normal	N	0
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 11:03:08 AM	00:00:31	10.64.91.50	10.64.91.50	Normal	N	0
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 11:03:08 AM	00:00:31	192.168.7.104	10.64.91.50	Normal	N	1
7329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 10:59:18 AM	00:00:29	192.168.7.104	10.64.91.50	Normal	N	1
+17329450231@avayalab.com	+17863310799@avayalab.com	Voice	JAN 17, 2024 10:59:18 AM	00:00:29	10.64.91.50	10.64.91.50	Normal	N	0

Select one of the records and click the magnifier icon on the taskbar to show session details and media statistics. Note that the **Monitoring Port** line shows "End-Point Statistics", a key verbiage that indicates when those statistics are received via RADIUS. This verbiage also points out that the statistics seen below are from an End-Point (in this case the Avaya SBC).

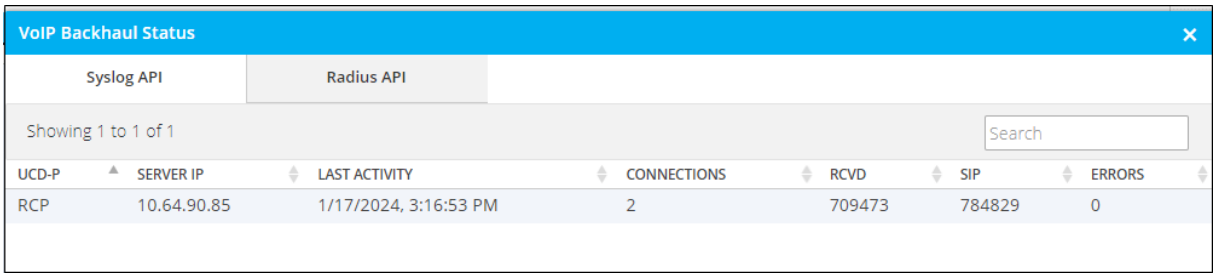


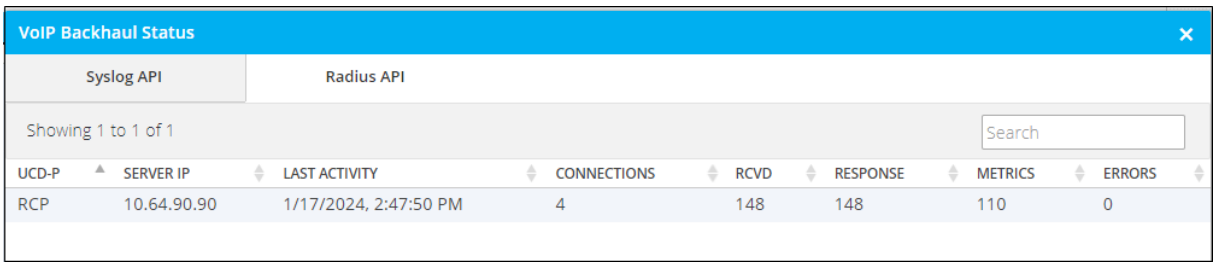
8.2. VoIP Backhaul Status

The following steps may be used to troubleshoot the configuration.
On the UCD-M Dashboard, select **Admin → VoIP Backhaul → Backhaul Status**.



The resulting screen and tabs provide information on the status and activity of the Diagnostics Syslog and RADIUS connections to Session Manager and the Avaya SBC.

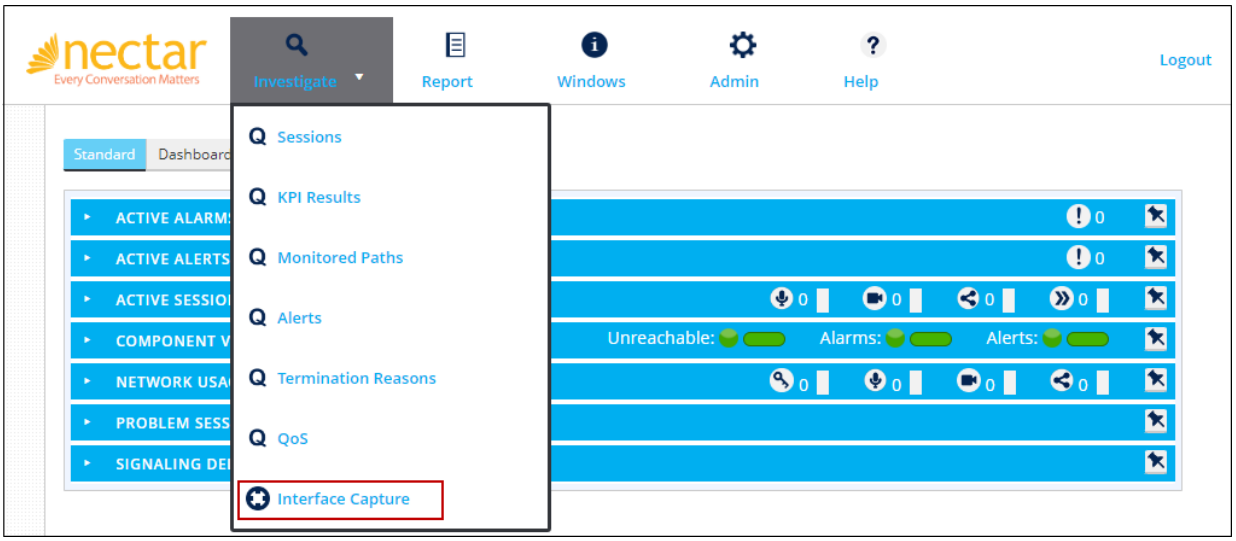




8.3. Interface Capture

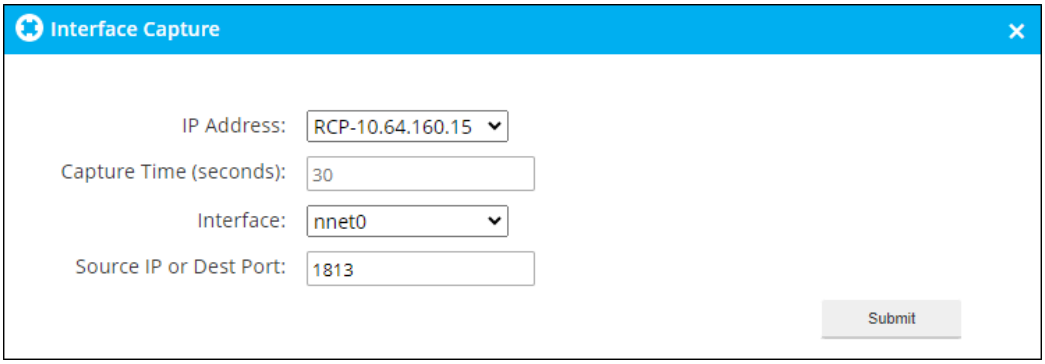
The Interface Capture tool allows for the capturing of pcap data from any interface on the UCD-P, and may be useful in troubleshooting the configuration.

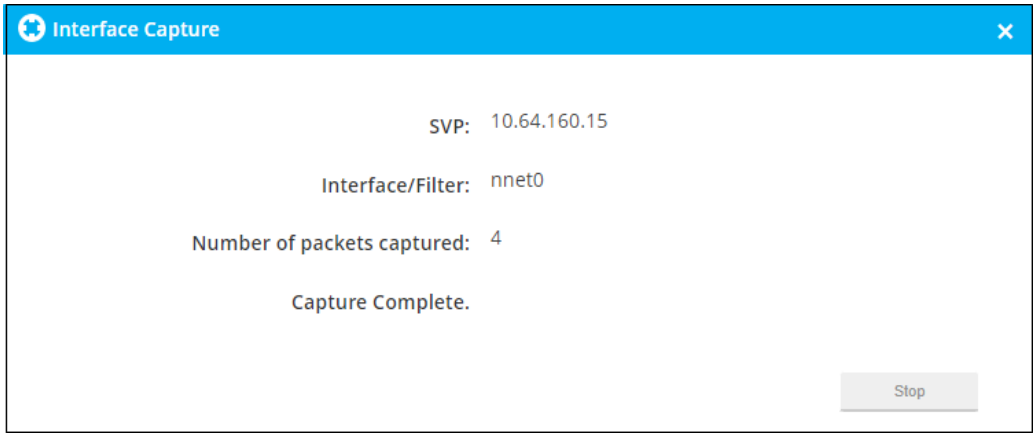
On the UCD-M Dashboard, select **Investigate → Interface Capture**.



On the next screen:

- **Capture Time (seconds)**: Adjust as needed.
- **Interface**: Select **nnet0**.
- **Source IP or Dest Port**:
  - To capture Syslog traffic, enter the IP address of the Session Manager management interface, or the destination port (**6514** in the reference configuration, **Section 5.1**)
  - To capture CDR/media statistics traffic, select the IP address of the management interface of the Avaya SBC, or the destination port (**1813** in the reference configuration, **Section 6.1**) as shown on the sample screen below.





When the capture completes, the browser automatically download the file to the local PC, where it can be opened with an application such as Wireshark.

9. Conclusion

These Application Notes described the configuration steps required to integrate Nectar Diagnostics version 2023.0.0.3 with Avaya Session Border Controller 10.1 and Avaya Aura® Session Manager 10.1. All test cases completed successfully.

10. Additional References

Avaya product documentation, including the following, is available at http://support.avaya.com

[1] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 12, September 2023.
[2] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023.
[3] *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 5, October 2023.

Nectar Diagnostics product documentation, including the following, can be obtained at the Nectar Knowledge Center at https://support.nectarcorp.com/

[4] *Nectar Diagnostics VMWare Installation Guide*, Release 22.2, Version 5.1, February 2023.
[5] *Nectar Diagnostics Configuration Guide*, Release 23.0, Version 7.2, November 2023.
[6] *Nectar Diagnostics Monitoring of Avaya SBC Feature Guide*, Release 22.2, Version 1.2, September 2023.

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.