Avaya Solution & Interoperability Test Lab

Application Notes for Perspective Solutions Consolidated Service Experience with Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration procedures required for Perspective Solutions Consolidated Service Experience (CSE) to interoperate with Avaya Aura® Communication Manager. Perspective Solutions Consolidated Service Experience is an intelligent platform that converges monitoring and management of the different layers of a network and system infrastructure to provide a unified business service view of an entire application or its delivery system.

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 procedures required for Perspective Solutions Consolidated Service Experience (CSE) to interoperate with Avaya Aura® Communication Manager. The purpose of the testing was to verify that Perspective Solutions CSE recorded each phone call’s performance metrics.

The Perspective CSE™ (Consolidated Service Experience) network management solution is specifically designed for converged environments. With the ability to distribute the solution to key points within an infrastructure, Perspective CSE provides multi-protocol monitoring of Voice, Data and Video technical assets and offers real-time visibility into how these assets impact your business processes.

This intersection of these interrelationships between technology and business processes is called “Business Service Intelligence.” Perspective CSE’s Business Service Intelligence capability helps enterprises and their service providers manage issues that arise within the service delivery environment in the context of their specific business. This creates significant operational savings while augmenting technical staff with real-time automated monitoring functionality.

2. General Test Approach and Test Results

The general approach was to place various types of calls to and from stations, collect VoIP call quality data from Perspective Solutions CSE, and compare collected values with Avaya IP telephone’s Network Audio Quality values. For feature testing, the types of calls included internal calls, inbound trunk calls, outbound trunk calls, transferred calls, conferenced calls. During compliance testing, a VoIP impairment tool was utilized to simulate VoIP delay and packet drop. For serviceability testing, failures such as cable pulls and resets were applied.

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 interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of Perspective Solutions CSE to provide quality of calls placed to and from stations. The serviceability testing introduced failure scenarios to see if Perspective Solutions CSE can resume monitoring and recording after failure recovery. Hardware failures were generated in order to confirm the ability of Perspective Solutions CSE to collect SNMP alarms and use SAT commands to get further details about hardware outages.
2.2 Test Results
Perspective Solutions CSE successfully provided VoIP call quality data on various types of calls. For serviceability testing, Perspective Solutions CSE was able to resume collecting VoIP call quality data after restoration of connectivity to the Communication Manager processor, and after resets of Perspective Solutions CSE and the Avaya Media Gateway. Further, the Perspective Solutions CSE was able to discover and report on the configuration and health of components in the configured systems including media servers, gateways and boards using the SNMP capabilities of Communication Manager. Perspective Solutions CSE solution successfully reported alarms when resources were taken out of service including SNMP alarms and refined details provided by utilizing automated SAT terminal discovery methods.

2.3 Support
For technical support on Perspective Solutions CSE, contact Perspective Solutions via email at:

- **Email:** support@perspectivecorp.com
3. Reference Configuration

Figure 1 illustrates the network configuration used to verify Perspective Solutions CSE. The figure shows two separate communication systems, each running Avaya Aura® Communication Manager on separate Avaya servers. Site A was comprised of an S8300D Server with a G450 Media Gateway, which had 9600 Series IP Telephones registered to it. Site B was comprised of an S8300D with a G430 Media Gateway which had 9600 Series IP Telephones registered to it. Analog and digital phones were configured at both sites as additional endpoints. An IP trunk connected the two Avaya Aura® Communication Manager systems. A Perspective Solutions CSE server was located at Site A, and had IP connection to all devices. A Packet Storm network device was used in various places on the network during the tests in order to inject delays and packet loss to verify phone and Perspective Solutions CSE properly measured network performance. The primary focus of this test was to verify interoperability with Avaya Aura® Communication Manager at Site A. Site B was present primarily for the ability to connect external calls to the endpoints at Site A.

![Figure 1: Avaya Network with Perspective Solutions CSE](image-url)
## 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 S8300D Server with an Avaya G450 Media Gateway</td>
<td>Avaya Aura® Communication Manager 6.2 (R016x.02.0.238.0-19926)</td>
</tr>
<tr>
<td>Avaya 9600 Series IP Telephones</td>
<td>Avaya one-X® Deskphone Edition SIP 2.6.7</td>
</tr>
<tr>
<td>96x0 (H.323)</td>
<td>Avaya one-X® Deskphone Edition SIP 6.1</td>
</tr>
<tr>
<td>96x1 (H.323)</td>
<td></td>
</tr>
<tr>
<td>Perspective Solutions CSE</td>
<td>CSE 2.1 (REP Version 2.1_25113x64)</td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager

Perspective Solutions REP utilizes a combination of the following three methods to collect data for generating a report on VoIP devices.

- **System Access Terminal (SAT)** – Perspective Solutions REP utilizes a SAT connection to collect resource information in Avaya Aura® Communication Manager. In order for Perspective Solutions REP to perform the resource collection, credentials were provided.
- **RTCP Monitor Server** – Perspective Solutions REP receives RTCP reports from endpoints or media processor (medpro) boards to provide VoIP path and call quality information.
- **SNMP/TRAP** – Perspective Solutions REP queries Avaya Aura® Communication Manager utilizing SNMP walk, to collect status information. Perspective Solutions REP was set up as a trap receiver, and thus received alarms from Avaya Aura® Communication Manager.

This section provides the procedures used for configuring the above mentioned methods in Avaya Aura® Communication Manager.

5.1 Configuring System Access Terminal (SAT) Access

This section describes how to create credentials for Perspective Solutions Remote Experience Platform (REP) to login to a Communication Manager.

There are two steps to creating a user within Communications Manager for use by the Perspective Solutions REP system. The first part is within the Server Maintenance of the Web Administration system for Communication Manager. The second part is conducted using the Communication Manager SAT interface to propagate the login amongst the Main processor and any survivable processors distributed throughout the system (e.g. ESS and LSP processors).
For the first step, launch a web browser and connect to the Communication Manager by entering https://<IP address>. Supply proper credentials.
Click on the **Administration / Server (Maintenance)** link.
Click on the **Administrator Accounts** link under the **Security** section on the left pane.

On the **Administrator Accounts** page, select the **Add Login** radio button. Select the **Privileged Administrator** radio button under **Add Login** section. Click on the **Submit** button.
**Note:** It is important that a Privileged Administer account (also known as a “Profile 18 Account”) is established for the REP. The REP does not issue any “write” or “change” commands. However this level of access is required to review the status of standby processors and to login to the Linux shell where additional review commands are issued against the system.

- Provide a **Login name**.
- Select ‘**prof18**’ for the **Additional groups** option.
- Do not check **Lock this Account**.
- Do not enter any dates within the **Date after which account is disabled-blank to ignore field**.
- Use a **Password** setting for **Select Type of Authentication**.
- Provide a password for the new account in the **Enter password or key** and **Re-enter password or key** fields
- Select the **No** option for **Force password/key change on next login**.

Click on the **Submit** button. Default values may be used in the remaining fields.
For the second step, leave the Web Administration interface up and start a SAT session against the Communication Manager to access the SAT command line. Enter the `save translation` command.

This will immediately perform one of the nightly synchronization routines of pushing translations from the Main processor to all survivable processors that are part of the system. The UID/PWD combinations are contained within the Translation set. This will immediately “push” the newly administered Profile 18 login for the REP to all processors within the system. The push is necessary to enable regular interrogation by the REP for the survivable processors and to complete the next step in preparation of the processors.

<table>
<thead>
<tr>
<th>Command Completion Status</th>
<th>Error Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>0</td>
</tr>
</tbody>
</table>

Command successfully completed

5.2 Creating the RTCP Monitor Server

Within Communication Manager, enable VoIP quality metrics to be sent to a collector for each IP voice stream associated with a DSP resource within a Avaya G-Series Gateway (e.g. G450), serviced by a Media Processing Board or the VoIP terminals themselves. These quality metrics come from the RTCP protocol (the sister protocol of RTP which handles statistics mediation between and amongst DSP resources). To turn on RTCP forwarding, enter the `change system-parameters ip-options` command. Provide the following information:

- **Enable Voice/Network Stats?** – Set to `y` to enable RTCP
- **Server IPV4 Address** - Enter the REP IP address used for RTCP collection
- **IPV4 Server Port** – Keep default value of **5005**
- **RTCP Report Period (secs)** – Keep default value of **5**

Default values may be used in the remaining fields. Submit the form.
5.3 Configuring SNMP / TRAP Agents

This section describes the configuration steps required to administer SNMP access and alarm destination settings for interaction with the REP system. During the administration, it will be required to restart the SNMP Master Agent twice. While this is not a user impacting event, it is recommended to make all such changes within the platform during off-peak business hours for the target environment.

Enabling the SNMP service is configured through the Communication Manager’s web interface. From the Communication Manager web System Management Interface, Click on the SNMP Agents link under the Alarms section, on the left pane, to display the SNMP Agents page.

On the SNMP Agents page, select the Following IP addresses radio button under the IP Addresses for SNMP Access section. Note, Any IP address implies that any device can perform SNMP request to the Communication Manager. Enter the IP Address of the interface on the REP designated to interface with CM.

Enable SNMP Version 1 and SNMP Version 2c by selecting enabled from the list in each of these sections. The community name strings configured here must match entries on the REP configuration.

Click on the Submit button at the bottom of the page.
SNMP Agents

The SNMP Agents SMI page allows modification of SNMP properties. SNMP allows the active server to monitor the SNMP port for incoming requests and commands (gets and sets).

Note:
- Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before starting the Master Agent. Please use the Agent Status page to start or stop the Master Agent.

Master Agent status: UP

View G3-AVAYA-MIB Data

IP Addresses for SNMP Access

- No Access
- Any IP address

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Add</th>
<th>Delete</th>
<th>Delete</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.64.21.201</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SNMP Users / Communities

SNMP Version 1

- Community Name (read-only): repro
- Community Name (read-write): repro

SNMP Version 2c

- Community Name (read-only): repro
- Community Name (read-write): repro

SNMP Version 3

- User (read-only): 
  - User Name:
  - Authentication Protocol:
  - Authentication Password:
  - Min. 8 characters. (for authentication and privacy)
  - Privacy Protocols:
  - Privacy Password:
  - Min. 8 characters. (for privacy)

- User (read-write):
  - User Name:
  - Authentication Protocol:
  - Authentication Password:
  - Min. 8 characters. (for authentication and privacy)
  - Privacy Protocols:
  - Privacy Password:
  - Min. 8 characters. (for privacy)
A highlighted message at the top of the main navigation pane will appear confirming the success of the operation.
Restart the Master SNMP Agent so that the administered changes to the SNMP Agents are bound to the running system. Click on the Agent Status link in the Alarms section on the navigation panel. Stop the SNMP Master Agent by clicking the Stop Master Agent button.
After the Master Agent status shows **down**, the **Stop Master Agent** button will now display **Start Master Agent**. Click on the **Start Master Agent** button to start the Master Agent.
5.3.1 Confirming SNMP / TRAP Firewall Services
The firewall in the Avaya server must allow SNMP on UDP port 161 and SNMPTRAP on UDP port 162. REP utilizes this service to obtain health statistics about the Media Server hardware that hosts the Communication Manager software.

In Communication Manager 6 and later, Firewall rules are configured by a privileged user (root for example) as operating system modifications. For this test, no modifications were required to the default configuration. Modifications would be documented in Linux operating system guides and are beyond the scope of these Application Notes.

5.3.2 Configure SNMP TRAP Destination
This section describes how to create a trap destination. Navigate to the SNMP Traps link under the Alarms section. Click on the Add/Change button to configure or modify the SNMP traps.
In the **Add Trap Destination** section, in the **SNMP Version 1** section, select **enabled** for the **Status** selection and enter the trap destination **IP address** (the REP IP address). Also enter the **Community Name** (**public** was used in the test).

In the **SNMP Version 2c** section, select **enabled** for the **Status** selection and enter the trap destination **IP address** (the REP IP Address). Select **trap** for the **Notification** option, and enter the **Community Name** (**public** was used in the test). Click **Submit** to commit these entries.
5.3.3 Configure Alarm Filters

Navigate to the Filters link under the Alarms section. Click on the Add button to add filter associated to the trap message.
On the **Add Filter** page, all Severity check boxes were checked during the compliance test. Select **All** for the **Category** field. Click on the **Add** button.
6. Configure Perspective Solutions REP

The steps in this section describe the configuration of Perspective Solutions REP that receives RTCP packets from the VoIP endpoint, and recording performance metrics. Additionally, the Communication Manager, and other servers must be administered.

6.1 Configure Perspective Solutions REP to receive RTCP Packets

Log into the Perspective Ubiquity system associated with the on-premises REP system. Refer to the Ubiquity Service Delivery Cloud Login Procedures provided by Perspective Solutions. If working directly on a REP system, launch a Java-enabled browser and point the URL to the IP address of the REP system.

The REP system will send a client via the Web browser’s JNLP (Java Network Launch Protocol) capability to the desktop. During this phase, a “Java” splash screen will be displayed and then a download completion bar.

A login screen will appear once the download has completed. Refer to the monitoring plan for the user ID and password for the particular REP system.

The rest of the instructions assume that the user is already connected to their designated Service Delivery Cloud and the user has administrator or setup equivalent privileges for the REP being configured.
Use the Ubiquity Bar at the top of the screen to perform a quick-find of the System Display Name to be administered, locate the REP on the Endpoints list, and click on it (not shown). The following screen is displayed.
Once the REP Bar appears beneath the Ubiquity Bar, perform the following:

- Navigate to the **Avaya** menu option on the left navigation bar and click on it. This display the Avaya module screen.
- On the bottom right hand portion of the screen find the grey **Setup Avaya…** link and click it.
More than one Avaya domains may be monitored from the same REP platform. An Avaya Domain can mean a single stand-alone server or an entire FCE system (flat-consolidated-extend). From the bottom of the Avaya module page find and click on Add Avaya Domain.

The Add Avaya Domain dialog box will appear. Enter the nick-name of the Avaya Domain desired within the system and click Next.
The **Define Main Processor** dialog box will appear next. Enter the following information:

- **Auto Include Elements**: check this checkbox
- **Processor Name**: Enter a descriptive name
- **IP address**: IP Address of Main processor (Communication Manager)
- **SAT Port**: (typically 5022)
- **BASH Port**: Enter 22
- **Connection type**: Choose SSH
- **Profile 18 Username** and **Password** for user created for REP software
- **Use SAT1 Login Quantity** of 2
- **Use SAT2 Login Quantity** of 1
- **Use BASH Login Quantity** of 1

Press **Add** to continue.
The domain will appear on the Avaya Module page. Confirm that the REP is in fact communicating with the Main processor by selecting the Avaya Domain on the left and clicking on the Processors tab in the center of the screen.

Repeat the above procedure to add any domains desired. Two domains were monitored during compliance tested. The screens below show the second domain that was added.
Next, enter the SNMP read-only community string for the Media Gateways within each Communication Manager domain administered in the Perspective Software. The community string used should be defined as part of the monitoring plan and is expected to be the same for all of the gateways within the system.

Notice that the system ships with the Avaya SNMP default community string of “public”. If this is accurate, there is no need to configure anything else. If the monitoring plan calls for a different SNMP read-only community string then perform the following:

Go to the **MG Communities** tab on the Avaya Setup screens and press **Change**.
On the **Set Default MG Community** pop-up screen, enter the SNMP community called for by the monitoring plan and press **Update**.

![Set Default MG Community](image)

### 7. Verification Steps

The following steps were used to verify the configuration.

1. Use the **ping** command to verify connectivity from Perspective Solutions REP to all devices.
2. Verify that calls can be successfully completed between the IP telephones and telephones.
3. Within Perspective Solutions RPE, click on the **RTCP** menu option on the left navigation bar to display the Quality overview screen. Confirm that traffic is being received.

![Perspective](image)
4. Compare VoIP quality data from the following sources:
   - A VoIP impairment tool
   - Avaya IP telephone’s Network Audio Quality data
   - Perspective Solutions REP

8. Conclusion
These Application Notes illustrate the procedures for configuring Perspective Solutions CSE to monitor and correctly provide VoIP call quality statistics on various types of calls. During compliance testing, Perspective Solutions successfully monitored call streams, correctly provided VoIP call quality data, and received traps from VoIP devices and media servers.

9. References
This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at http://support.avaya.com.


Contact Perspective Solutions to obtain product documentation.