Abstract

These Application Notes describe the procedures for configuring Virsa Service Management for Unified Communications to interoperate with Avaya Aura® Application Enablement Services.


Virsae Service Management monitored Application Enablement Services using SNMP and Linux shell access and displayed monitored data on a web-based application.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as any 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 compliance tested configuration used to validate Virsae Service Management for Unified Communications (herein after referred to as VSM) with Avaya Aura® Application Enablement Services (herein after referred to as AES). VSM is a cloud-based service management platform that brings visibility, service transparency and cost savings to Unified Communications environments over the short, medium and long term.

VSM used SNMP and Linux shell access connection to monitor AES statistics such as CPU, Memory and Disk Usage, License information and AE Services links status detail and display monitored data on web-based applications.

2. General Test Approach and Test Results

The general test approach was to verify VSM using SNMP and Linux shell access connections to monitor and display system status from AES.

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 VSM utilized capabilities of SSH as requested by Virsae.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third-party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.
Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third-party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager or the Telnet/SSH interface to interact with other Avaya products. While this solution has successfully completed Compliance Testing for the specific release levels as described in these Application Notes, Avaya does not generally recommend use of these interfaces as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the interfaces in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using these interfaces. Using these interfaces in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real-time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in these Application Notes explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Avaya Product Releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing
The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying proper display of AES monitored data on VSM.

- Verify that the server statistics information for AES is populated on VSM dashboard such as CPU, Memory and Disk Usage and list of Software/Processes.
- Verify proper display of AES server status and link information included SNMP Availability, Raised Alerts, Link Status, TSAPI Client Connections and DMCC Sessions.
- Verify that the list of AES links is visible in VSMs: ASAI Link, DLG CTI Link, TSAPI CTI Link and TSAPI TLink, along with utilization details.
- Verify License, DMCC and TSAPI Status were displayed correctly.

The serviceability testing focused on verifying the ability of VSM to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to VSM appliance.

2.2. Test Results
All test cases passed successfully.

2.3. Support
For technical support on Virsae Service Management, contact the Virsae Support Team at:

- Tel: +1 800 248 7080 (Americas)
  +44 0808 234 2729 (UK and Europe)
  +64 9 477 0696 (Asia Pacific)
- Email: support@virsae.com
3. Reference Configuration

Figure 1 illustrates the test configuration used to verify the VSM application with AES. For compliance testing Communication Manager with a G450 Media Gateway connected to an AES using the CTI link. The system has Avaya H323, SIP, Equinox for Windows, digital and analog endpoints configured for making and receiving calls. VSM was installed on a server running Microsoft Windows Server 2012 R2 with Service Pack 1. Architecturally the VSM Service relies on an appliance being placed on a corporate LAN and being configured to connect to a Unified Communication platform as well as the Microsoft Azure cloud via the internet. The VSM appliance acts as a collector and compresses, encrypts then forwards data from all sources to the Virsae cloud computing service. A PC/Laptop is used to access the Virsae portal to manage VSM services, add additional users and view reporting data on the equipment being managed.

Figure 1: Test Configuration
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® Application Enablement Services running on virtual server</td>
<td>7.1.2.0.0.3-0</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager running on virtual server</td>
<td>7.1.2.0.0-FP2</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>38.21.0/1</td>
</tr>
<tr>
<td>Avaya IP Deskphones</td>
<td></td>
</tr>
<tr>
<td>- 9641GS (H.323)</td>
<td>6.6506</td>
</tr>
<tr>
<td>- 9611G (SIP)</td>
<td>7.1.1.0.9</td>
</tr>
<tr>
<td>Avaya Equinox for Windows</td>
<td>3.3.2.20</td>
</tr>
<tr>
<td>Avaya 1416 Digital Deskphone</td>
<td>15</td>
</tr>
<tr>
<td>Avaya 500 Analog Deskphone</td>
<td>N/A</td>
</tr>
<tr>
<td>Virsae Service Management for Unified Communications running on Windows 2012 R2 SP1</td>
<td>R79</td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager
The configuration of Communication Manager and AES is assumed to be in place and will not be discussed in this document. For more information of how to configure Communication Manager and AES, please refer to Section Errors! Reference source not found..

6. Configure Avaya Aura® Application Enablement Services
The initial administration of AES and the connection to Communication Manager is assumed to be in place and will not be covered here. This section covers the configuration of SNMP that is required for integration with VSM.

AES is configured via the AES Management web interface. To access the web interface, enter http://<ip-addr>/ as the URL in an internet browser, where<ip-addr> is the IP address of AES. Log in using the appropriate login credential. The screen shown below is displayed.

Note: All screens in this section are shown after AES had been configured. Click Save button to save the screen parameters configured on AES if needed.
6.1. Configure SNMP Connection

To configure SNMP Connection, navigate to Utilities → SNMP → SNMP Agent. The SNMP Agent page is displayed in the right. Configure the following parameters as shown below.

- Check the **Enable SNMP Version 2c** box
- **Community Name**: Configured as **virsae** during compliance testing
- Select the radio button for **Any IP Addresses**
- **IP Address 1**: Enter the IP address of the VSM probe

Retain default values for all other fields and click on the **Apply Changes** button.
6.2. Configure Login Account

The VSM Probe requires access to AES with Administrative rights. Add an account that when used, provides access to the Linux bash prompt. The new account should be like the default “cust” account.

SSH connect to the AES and log in using your ‘cust’ credentials or a ‘super user’ account. At the command prompt type su root. When prompted enter the ‘root’ user password.

Use the command useradd NAME; where NAME is the account name to create and hit enter.

Use the command passwd NAME; where NAME is the account name created above and hit enter. Enter the password then hit enter (need to do this twice).

Enter the command chage –M 99999 NAME; where NAME is the account created above and hit enter to set the AES account password to not expire.
7. Configure Virsae Service Management

This section describes the configuration of VSM required to interoperate with AES.

This section provides a “snapshot” of VSM configuration used during compliance testing. Virsae creates the business partner portal in the cloud environment and is beyond the scope of this Application Notes. The screen shots and partial configuration shown below, supplied by Virsae, are provided only for reference. These represent only an example of the configuration GUI of VSM, available through the web Portal. Contact Virsae for details on how to configure VSM. The configuration operations described in this section can be summarized as follows:

- Login to the Web Portal
- Configuring Avaya Aura® Application Enablement Services
- Configure Dashboard

7.1. Login to the Web Portal

A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL <business partner name>.virsae.com in a web browser. During compliance testing the URL used was devconnect.virsae.com. The Login screen is shown as below. Enter the Email and Password and click on the Log In button.
The customers belonging the business partner screen is shown. During compliance testing the customer created by Virsae is **Devconnect**.

Click on the customer icon and navigate to **Service Desk → Equipment Locations** as shown below.
A Location called Devconnect is already configured as shown below.

7.2. Configuring Avaya Aura® Application Enablement Services
To add a AES to the Location created in Section 7.1, right click on the location Devconnect and select Manage Services as shown below.

From the Unified Communications Service, select Avaya.
The product list for the configured location is shown as seen below. Click on the Add Equipment button.

From the Add Avaya Equipment window, select Application Enablement Services (AES) from the Product Type drop-down menu.
In the **Configure Equipment** tab, configure the following values.

- **Equipment Name:** A descriptive name
- **Username:** The username configured in Section 6.2
- **Password:** The password configured in Section 0
- Check the **Use SSH** box
- **IP Address/Host Name:** IP address of AES
- **Default Site:** A descriptive site name
- **Command Set:** Select **Avaya AES** from the drop-down menu
In the **Configure SNMP** tab, configure the following values.

- **SNMP Version:** Select V2 from the drop-down menu
- **SNMP Community String:** Enter the value configured in Section Error! Reference source not found.

Click on the **Add** (not shown) button to complete the configuration.

The screen below shows the added AES equipment.
7.3. Configure Dashboard
This section shows the steps to configure Communication Manager on the dashboard.

From the customer icon, navigate to Service Desk → Dashboard Management as shown below.

From the Available Dashboards window, click on the Add Dashboard button.
In the Create Dashboard window, type a descriptive name for Name and Title fields as shown below. Retain default values for all other fields. Click on Layout button and then click on Submit (not shown) button.

![Create Dashboard window](image)

Screen below shows the above created Dashboard. Right click on it and select Start.

![Dashboard list](image)
In the dashboard window shown below, click on **System Health** and drag the **AES System Health** icon from the left to the right column.

![System Health](image1)

From the drop-down menu for **AES System Health** window, select the **Edit Settings** button as shown below.

![Edit Settings](image2)
In the **Edit Settings** window shown below, select the required **Location** and **Equipment** from the drop-down menu and click on the **Save** button.

The dashboard with the configured equipment is shown below. The above steps can be repeated to configure other equipment or/and dashboard parameters.
8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of AES and VSM. The following steps are done by accessing the VSM web portal for the Business partner.

After login to the web portal, navigate to Service Desk → Dashboard Management (not shown). Start the dashboard and the screens below shows the System Health of the already configured AES for various parameters.
To view alarms using historical reporting, navigate to **Availability Manager → Manage Alarms** (not shown). A list of all unresolved alarms for all equipment is shown. Screen below shows the alarm for AES equipment.

9. **Conclusion**
These Application Notes describe the procedures for configuring the Virsae Service Management to interoperate with Avaya Aura® Application Enablement Services. During compliance testing, all test cases were completed successfully.

10. **Additional References**
This section references the product documentation relevant to these Application Notes.

Product documentation for Avaya products may be found at [http://support.avaya.com](http://support.avaya.com).

2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.1.2, Issue 4 January 2018

Product documentation for Virsae products can be obtained directly from Virsae.

1. *Virsae Service Management - Implementation Guide*
2. *Virsae Service Management – Technical Requirements*