



Avaya Solution & Interoperability Test Lab

Application Notes for Virsae Service Management for Unified Communications with Avaya Aura® System Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management for Unified Communications to interoperate with Avaya Aura® System Manager.

Virsae Service Management provides real-time monitoring and management solutions for IP telephony networks. Virsae Service Management provides visibility of Avaya and other vendor's IP Telephony solutions from a single console and enables a reduction in complexity when managing complex IP telephony environments.

Virsae Service Management integrates directly to System Manager using Secure Shell (SSH) or Telnet and uses Simple Network Management Protocol (SNMP) to query System Manager.

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® System Manager (herein after referred to as System Manager). 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.

The Virsae product uses SNMP and Linux shell access integration method to monitor System Manager.

- SNMP collection –Virsae uses SNMP to collect alarm and status information from System Manager.
- Telnet/SSH – Virsae establishes a Linux Shell connection to run the “sar” command and obtain system information. This command typically collects, reports and saves CPU, Memory, I/O usage in the Linux operating system.

2. General Test Approach and Test Results

The general test approach was to verify VSM using SNMP and SSH connection to monitor and display system status from System Manager.

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

For feature testing, VSM dashboard was used to view the configurations of System Manager such as the memory and CPU utilizations, disk usage and status from data collected via SSH and alarms via SNMP.

For serviceability testing, reboots were applied to the VSM and System Managers to simulate system unavailability. Loss of network connectivity to both VSM and System Managers were also performed during testing.

2.2. Test Results

All test cases passed successfully with the following observation.

- The “sar” command cannot be executed in the System Manager version used during this compliance testing since the “Sysstat” directory is not used in this version of Linux platform. By not able to execute this command, only the CPU occupancy information could not be obtained.

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 VSM interoperability with Communication Manager. The configuration consists of a Communication Manager system with an Avaya G450 Media Gateway. The system has Avaya H323, SIP, Equinox for Windows, digital and analog endpoints configured for making and receiving calls. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP endpoints. 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.

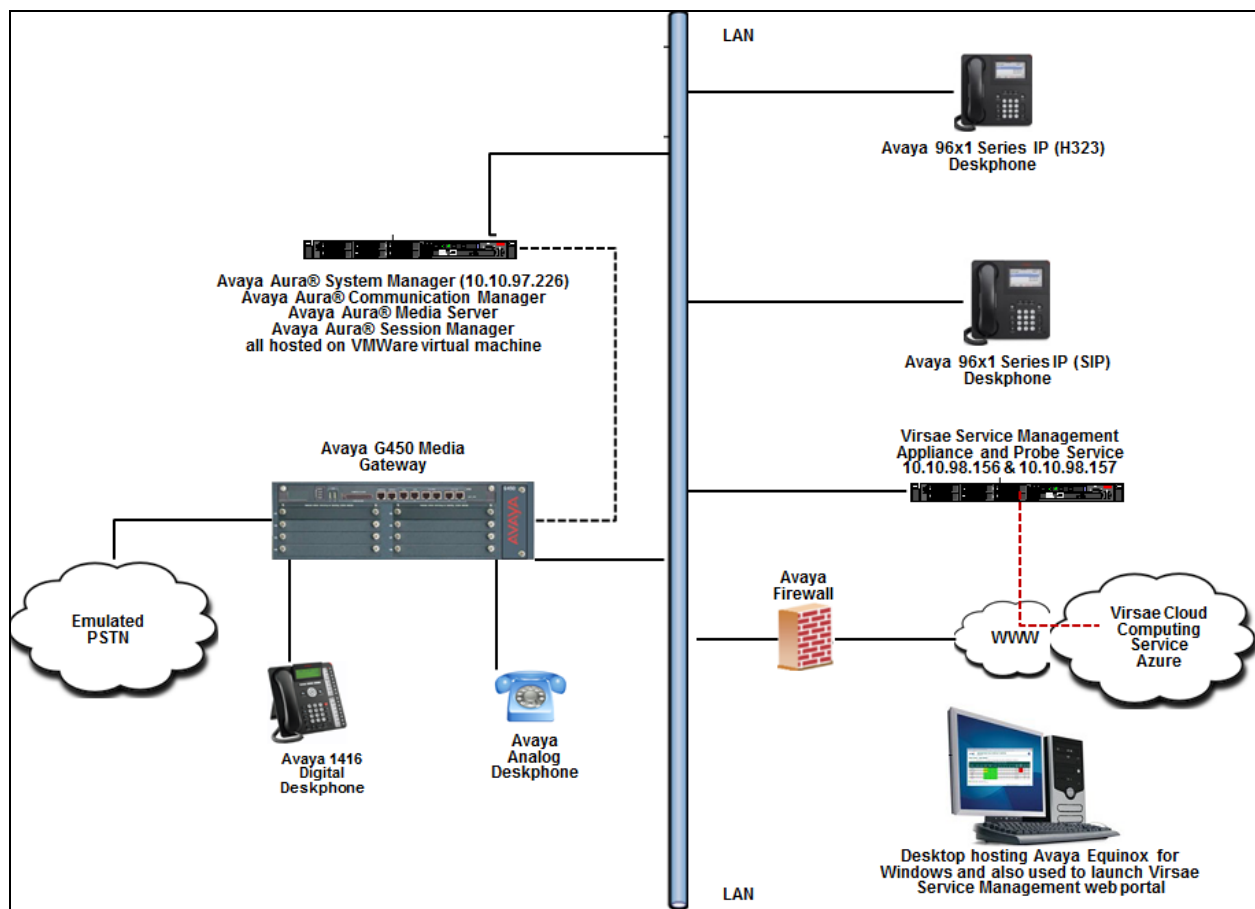


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on virtual server	7.1.2.0 (Feature Pack 2)
Avaya Aura® Session Manager running on virtual server	7.1.2.0.712004
Avaya Aura® Media Server running on virtual server	7.8.0.333
Avaya Aura® Communication Manager running on virtual server	7.1.2.0.0-FP2
Avaya G450 Media Gateway	38.21.0/1
Avaya IP Deskphones - 9641GS (H.323) - 9611G (SIP)	6.6506 7.1.1.0.9
Avaya Equinox for Windows	3.3.2.20
Avaya 1416 Digital Deskphone	15
Avaya 500 Analog Deskphone	N/A
Virsa Service Management for Unified Communications running on Windows 2012 R2 SP1	R79

5. Configure Avaya Aura® System Manager

This section describes the steps needed to configure System Manager to interoperate with VSM. This includes creating a login account for VSM to access System Manager and enabling SNMP.

5.1. Configure Login Group

Create an Administrator account on System Manager since the VSM Probe requires access to System Manager with Administrative rights. Add an account that when used provides access to the Linux bash prompt.

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 System Manager account password to not expire.

5.2. Configure SNMP

SNMP is used to capture alarms raised by Session Manager. All configurations are done via Avaya Aura® System Manager (System Manager).

Using a web browser, enter `https://<IP address of System Manager>` to connect to the System Manager server and log in using appropriate credentials as shown below.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

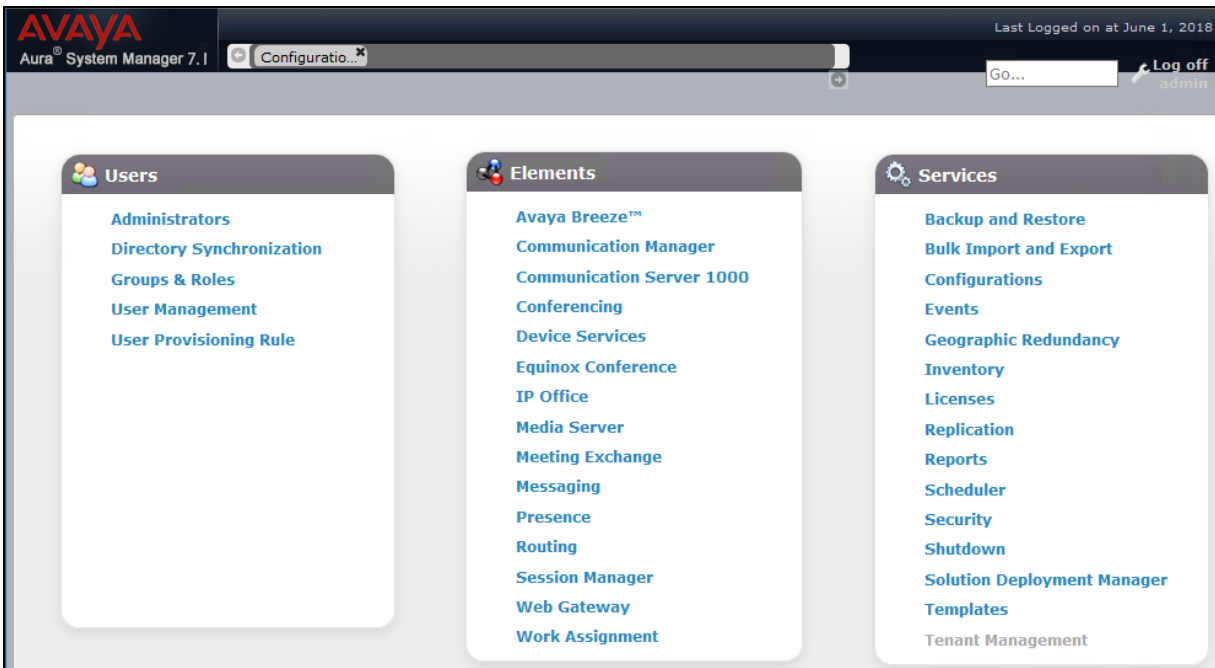
User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

The main System Manager dashboard page is shown below.



Navigate to **Services** → **Inventory** from the above shown dashboard. Then navigate to **Manage Serviceability Agents** → **SNMP Target Profiles** as shown in the screen below. Click on **New**.



From the **New Target Profile** window, under the **Target Details** tab, configure the following.

- **Name:** A descriptive name
- **IP Address:** The VSM probe IP address
- **Protocol:** Select **V2** from the drop-down menu

Retain default values for all other fields and click on the **Commit** button.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 7.1', and a search bar. The left sidebar contains a menu with options like 'Inventory', 'Manage Elements', 'Create Profiles and Discover SRS/SCS', 'Element Type Access', 'Subnet Configuration', 'Manage Serviceability Agents', 'SNMPv3 User Profiles', 'SNMP Target Profiles', 'Notification Filter Profile', 'Serviceability Agents', 'Synchronization', and 'Connection Pooling'. The main content area displays the 'New Target Profile' window. The 'Target Details' tab is selected, showing the following fields: 'Name' (Virsae), 'Description' (empty), 'IP Address' (10.10.98.157), 'Port' (162), 'Notification Type' (Trap), 'Protocol' (V2), and 'Community' (public). The 'Commit' button is located at the bottom right of the window. A legend at the bottom left indicates that fields marked with an asterisk (*) are required.

Then navigate to **Manage Serviceability Agents** → **Serviceability Agents** as shown in the screen below. Select an agent from the **Agent List** window, in this case the System Manager and click on the **Manage Profiles** button.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the version number, and a search bar. The left sidebar contains a navigation menu with the following items: Home, Inventory, Manage Elements, Create Profiles and Discover SRS/SCS, Element Type Access, Subnet Configuration, Manage Serviceability Agents, SNMPv3 User Profiles, SNMP Target Profiles, Notification Filter Profile, and Serviceability Agents. The main content area shows the 'Serviceability Agents' page. The breadcrumb trail is 'Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents'. The page title is 'Serviceability Agents'. Below the title is the 'Agent List' section, which includes buttons for 'Activate', 'Manage Profiles', 'Generate Test Alarm', and 'Repair Serviceability Agent'. The 'Agent List' table shows 3 items, with the first item selected. The table columns are Hostname, IP Address, System Name, System OID, and Status. The selected agent is 'devvmsmgr.bvwdev.com' with IP '10.10.97.226', System Name 'Avaya-Aura-System-Manager', System OID '1.3.6.1.4.1.6889.1.35', and Status 'active'. The 'Filter' is set to 'Enable'. The 'Select' options are 'All' and 'None'.

	Hostname	IP Address	System Name	System OID	Status
<input checked="" type="checkbox"/>	devvmsmgr.bvwdev.com	10.10.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active

From the **Manage Profiles** window, under the **SNMP Target Profiles** tab, select the **Virsae** profile, click on **Assign** and then the **Commit** button.

The screenshot shows the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes 'Home', 'Inventory', and 'Routing'. The left sidebar lists various management options, with 'Serviceability Agents' selected under the 'Manage' section. The main content area is titled 'Manage Profile' and features three tabs: 'Selected Agents', 'SNMP Target Profiles' (which is active), and 'SNMPv3 User Profiles'. Within the 'SNMP Target Profiles' tab, there is a section for 'Assignable Profiles' containing an 'Assign' button. Below this is a table with 2 items. The table has columns for 'Name', 'Domain Type', 'IP Address', 'Port', and 'SNMP Version'. The first item, 'Virsae', is selected with a checkbox. Below the table is a 'Select : All, None' link. At the bottom of the 'Manage Profile' window, there is a 'Removable Profiles' section and 'Commit' and 'Back' buttons.

Avaya
Aura® System Manager 7.1

Configuration...

Go...

Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents

Manage Profile

Commit Back

Selected Agents SNMP Target Profiles SNMPv3 User Profiles

Assignable Profiles

Assign

2 Items

	Name	Domain Type	IP Address	Port	SNMP Version
<input checked="" type="checkbox"/>	Virsae	UDP	10.10.98.157	162	V2

Select : All, None

Removable Profiles

Commit Back

6. Configure Virsae Service Management

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

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® System Manager
- Configure Dashboard

6.1. 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.



AVAYA
DEVCONNECT

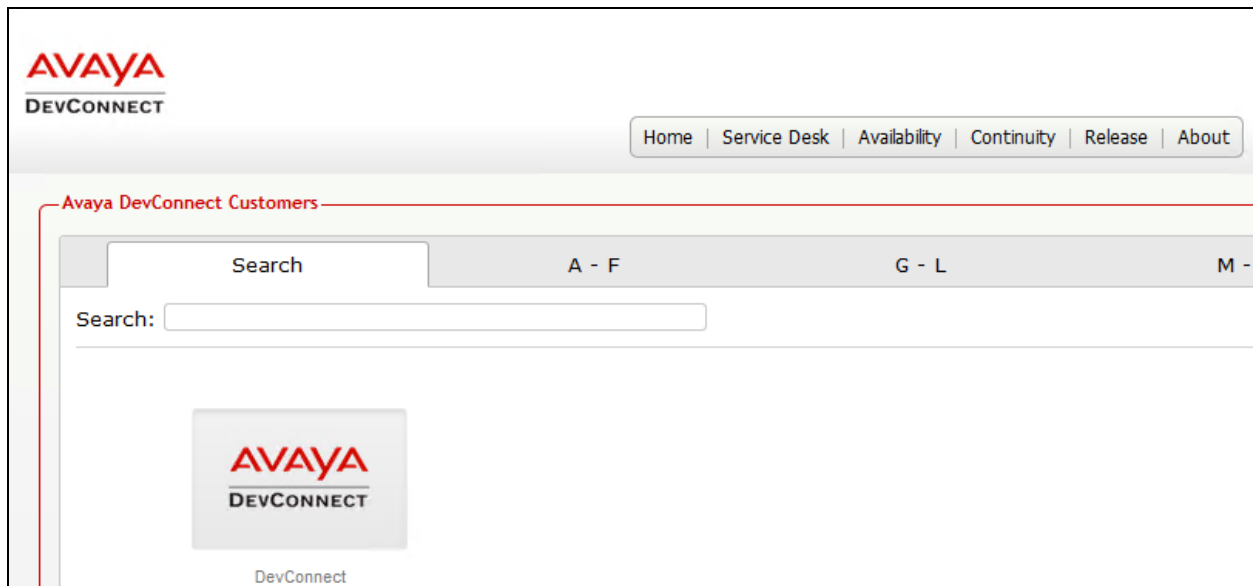
Email

Password

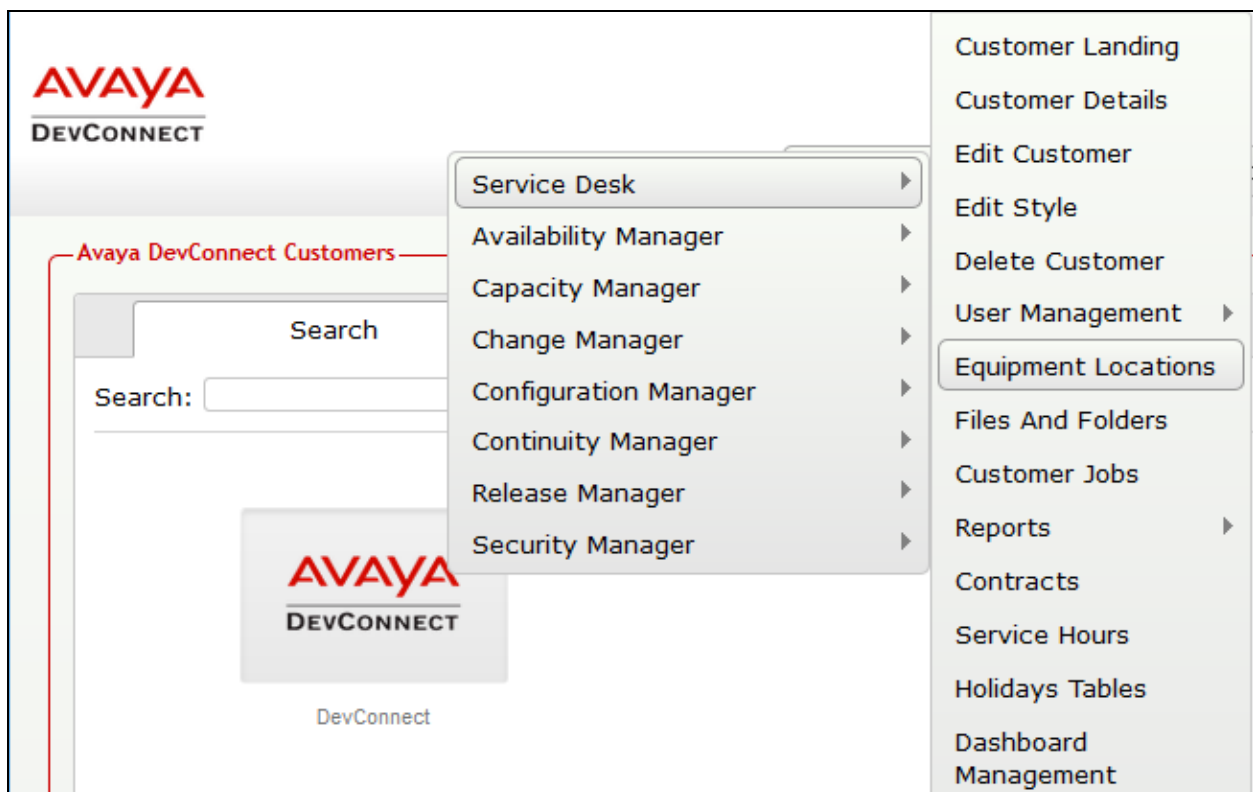
Log In

[Forgot your password?](#)

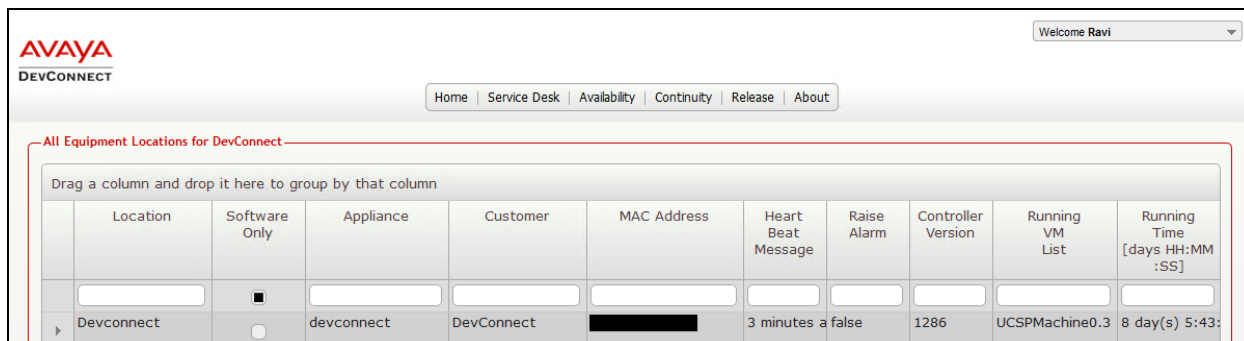
The customers belonging the business partner screen is shown. During compliance testing the customer created by Virsae is **Devconnect**.



Click on the customer icon and navigate to **Service Desk** → **Equipment Locations** as shown below.



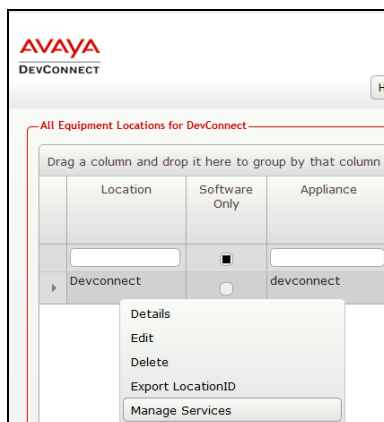
A **Location** called **Devconnect** is already configured as shown below.



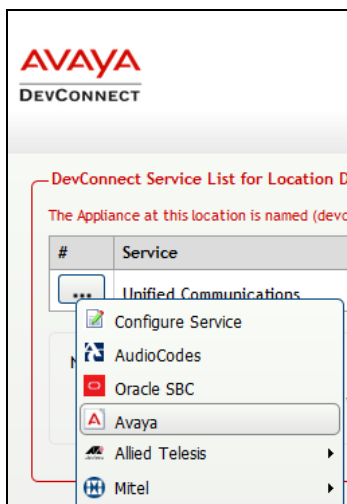
Location	Software Only	Appliance	Customer	MAC Address	Heart Beat Message	Raise Alarm	Controller Version	Running VM List	Running Time [days HH:MM:SS]
Devconnect	<input type="checkbox"/>	devconnect	DevConnect		3 minutes	false	1286	UCSPMachine0.3	8 day(s) 5:43:

6.2. Configuring Avaya Aura® System Manager

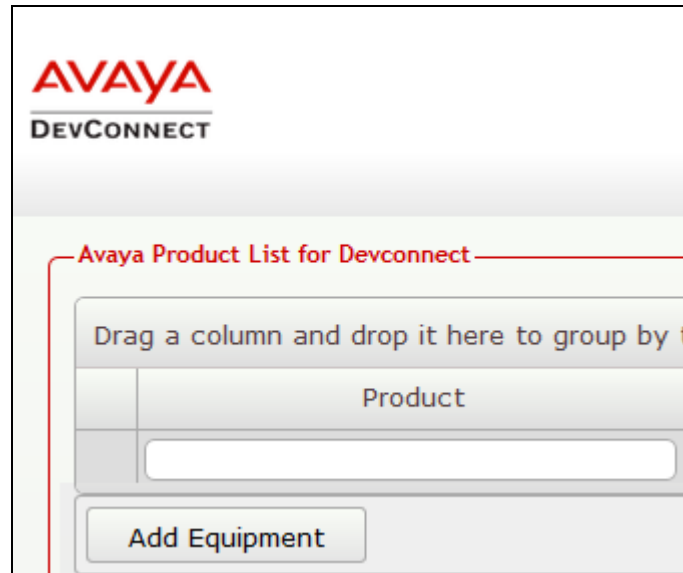
To add a System Manager to the Location created in **Section 6.1**, right click on the location **Devconnect** and select **Manage Services** as shown below.



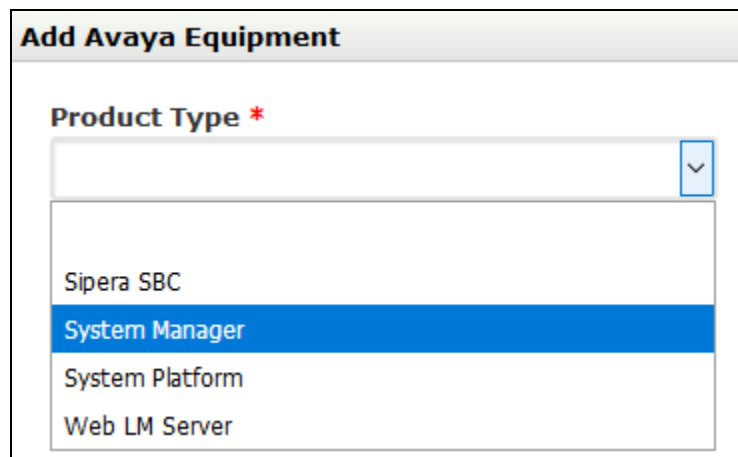
From the **Unified Communications Service**, select **Avaya**.



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 **System Manager** 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 5.1**
- **Password:** The password configured in **Section 5.1**
- Check the **Use SSH** box
- **IP Address/Host Name:** IP address of System Manager
- **Default Site:** A descriptive site name
- **Command Set:** Select **Linux Server** from the drop-down menu

Add Avaya Equipment

Product Type *
System Manager

Configure Equipment

Configure SNMP

Equipment Name *
Devconnect SMGR

IP Address/Host Name *
10.10.97.226

Username *
virsae

Default Site
Belleville

Password *
●●●●●●●●

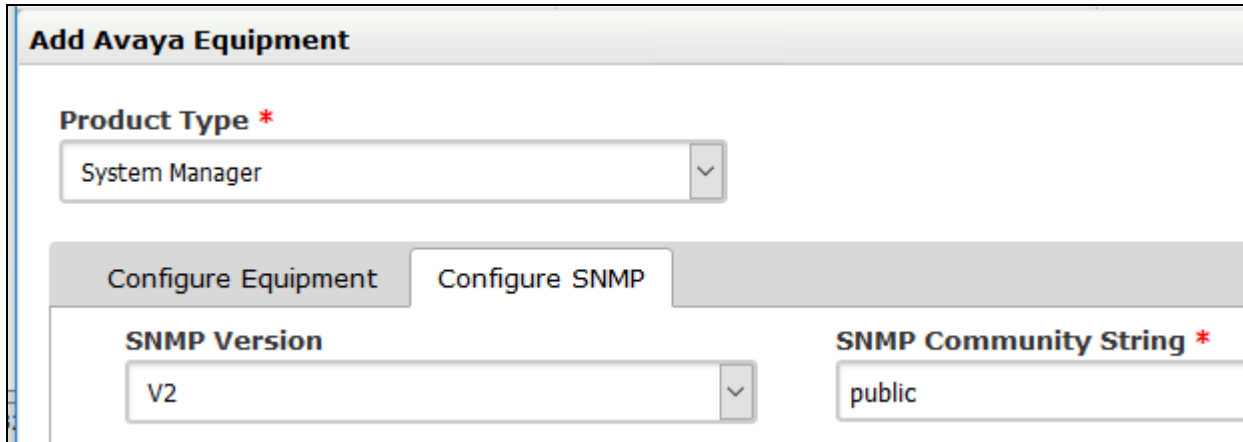
Command Set *
Linux Server

☒ **Use SSH**

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 5.2**

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



Add Avaya Equipment

Product Type *

System Manager

Configure Equipment | **Configure SNMP**

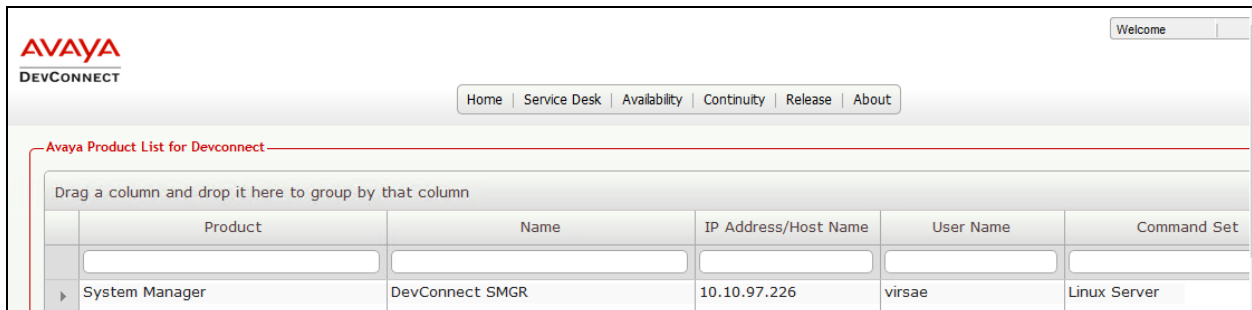
SNMP Version

V2

SNMP Community String *

public

The screen below shows the added System Manager equipment.



AVAYA
DEVCONNECT

Welcome

Home | Service Desk | Availability | Continuity | Release | About

Avaya Product List for Devconnect

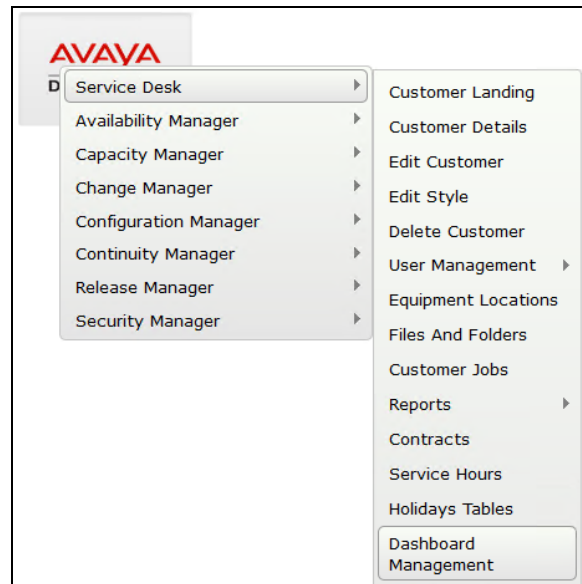
Drag a column and drop it here to group by that column

	Product	Name	IP Address/Host Name	User Name	Command Set
▶	System Manager	DevConnect SMGR	10.10.97.226	virsa	Linux Server

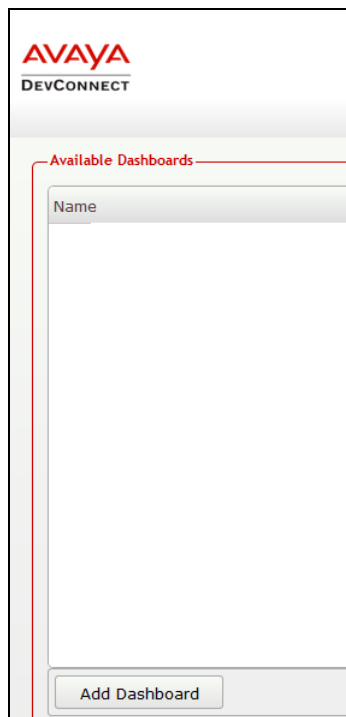
6.3. Configure Dashboard

This section shows the steps to configure Communication Manager on the dashboard.

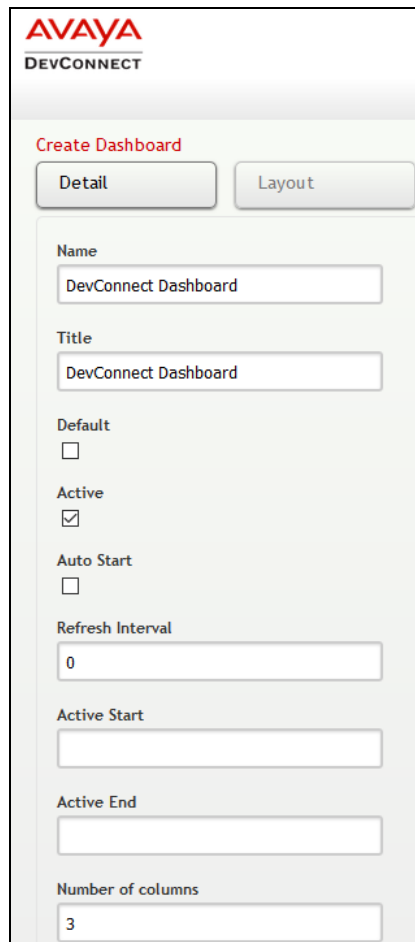
From the customer icon, navigate to **Service Desk → Dashboard Management** as shown below.



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.



AVAYA
DEVCONNECT

Create Dashboard

Detail Layout

Name
DevConnect Dashboard

Title
DevConnect Dashboard

Default
☐

Active
☒

Auto Start
☐

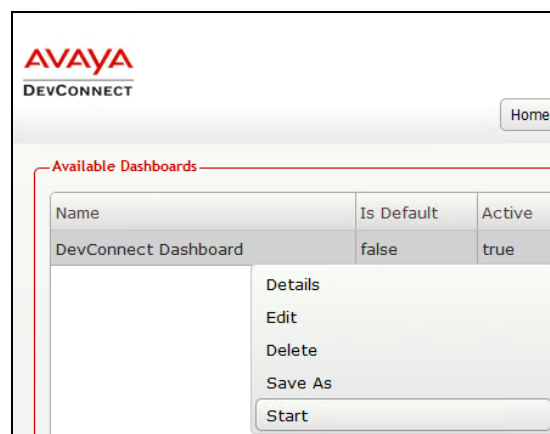
Refresh Interval
0

Active Start

Active End

Number of columns
3

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



AVAYA
DEVCONNECT

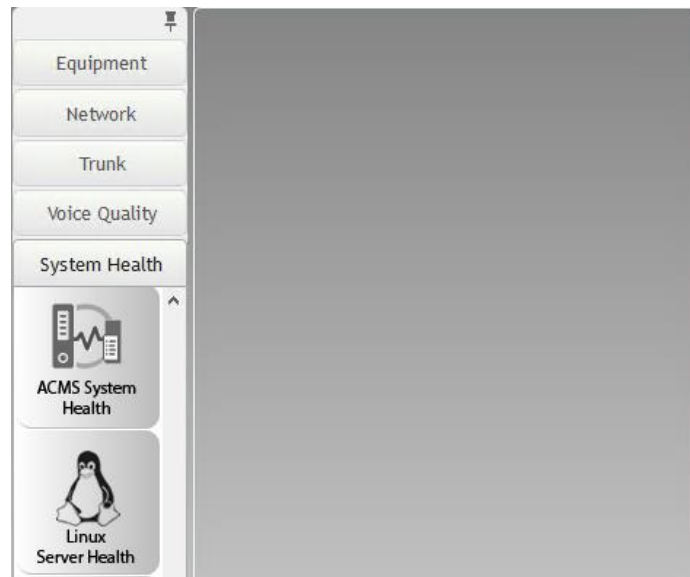
Home

Available Dashboards

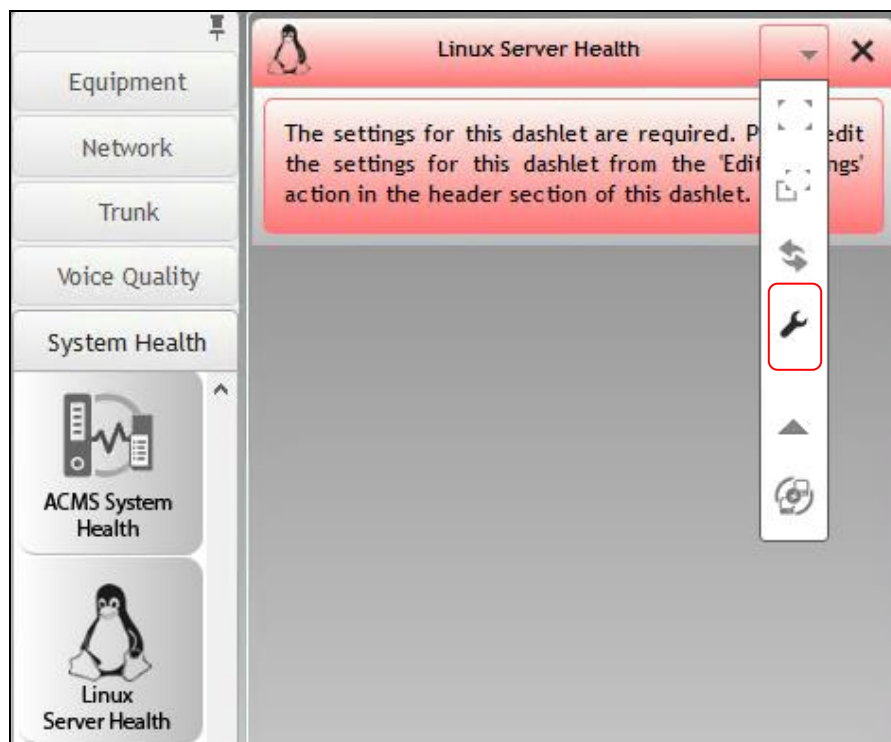
Name	Is Default	Active
DevConnect Dashboard	false	true

Details
Edit
Delete
Save As
Start

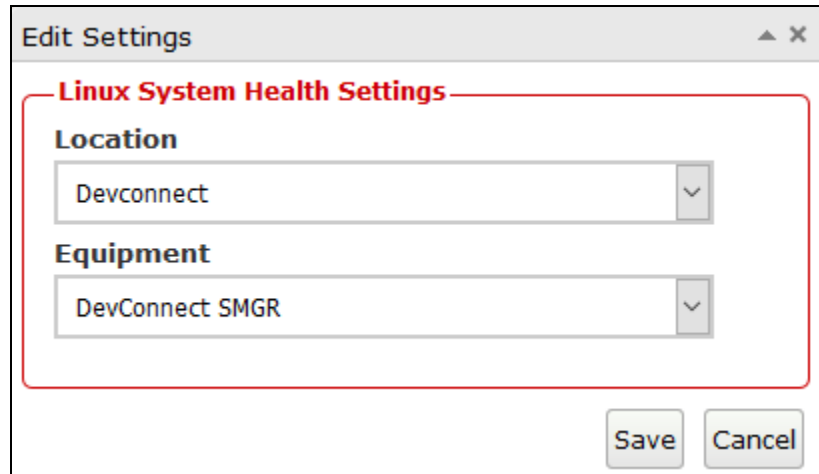
In the dashboard window shown below, click on **System Health** and drag the **Linux Server Health** icon from the left to the right column.



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



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



Edit Settings

Linux System Health Settings

Location

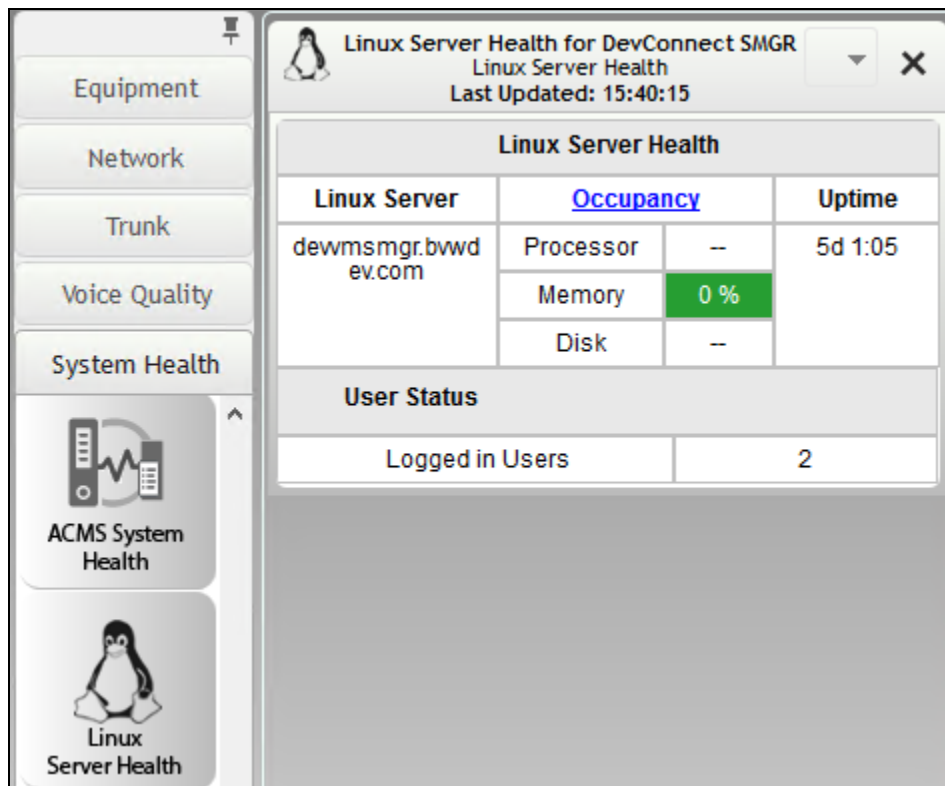
Devconnect

Equipment

DevConnect SMGR

Save Cancel

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



Linux Server Health for DevConnect SMGR
Linux Server Health
Last Updated: 15:40:15

Linux Server Health			
Linux Server	Occupancy		Uptime
dewmsmgr.bwwd.ev.com	Processor	--	5d 1:05
	Memory	0 %	
	Disk	--	

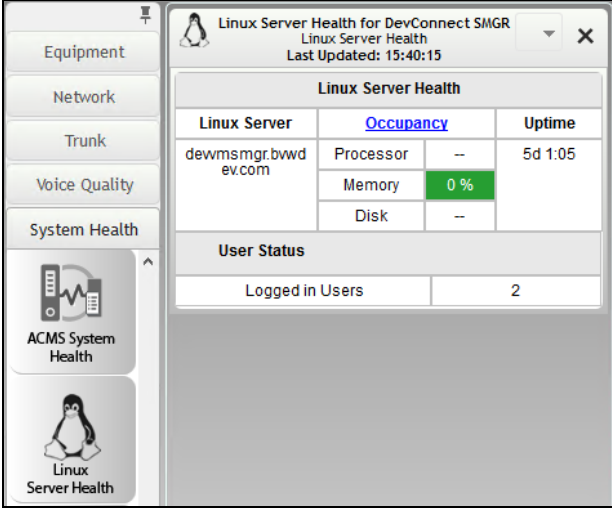
User Status

Logged in Users	2
-----------------	---

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of System Manager 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 System Manager for various parameters.

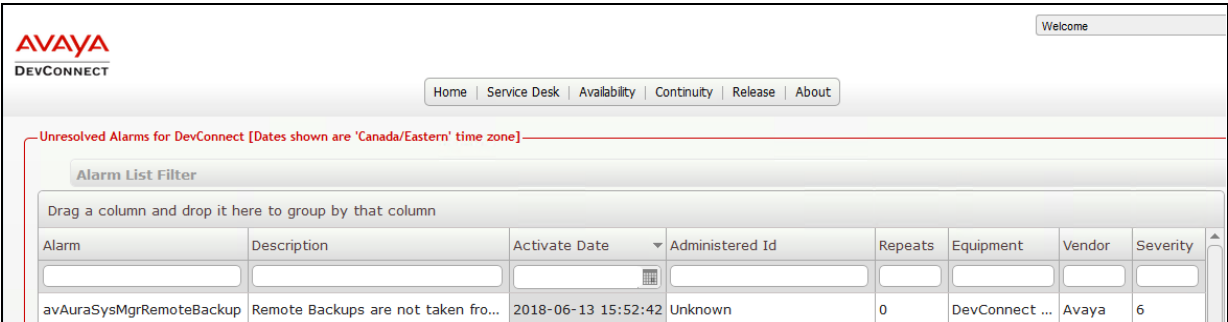


The screenshot displays the 'Linux Server Health for DevConnect SMGR' dashboard. On the left, a sidebar contains navigation links: Equipment, Network, Trunk, Voice Quality, System Health, ACMS System Health, and Linux Server Health. The main content area is titled 'Linux Server Health' and includes a table for 'Linux Server' health metrics. The table shows the server name 'dewmsmgr.bwwd.ev.com', its occupancy (0%), and its uptime (5d 1:05). Below this, a 'User Status' section indicates that there are 2 logged-in users.

Linux Server	Occupancy	Uptime
dewmsmgr.bwwd.ev.com	0 %	5d 1:05

User Status	
Logged in Users	2

To view alarms via historical reporting, navigate to **Availability Manager → Manage Alarms** (not shown). A list of all unresolved alarms for all equipment is shown. Screen below shows an alarm for System Manager equipment.



The screenshot shows the 'Unresolved Alarms for DevConnect' page in the Avaya DevConnect interface. The page includes a navigation bar with links to Home, Service Desk, Availability, Continuity, Release, and About. Below the navigation bar, there is a section for 'Unresolved Alarms for DevConnect [Dates shown are 'Canada/Eastern' time zone]'. This section contains an 'Alarm List Filter' and a table of unresolved alarms.

Alarm	Description	Activate Date	Administered Id	Repeats	Equipment	Vendor	Severity
avAuraSysMgrRemoteBackup	Remote Backups are not taken fro...	2018-06-13 15:52:42	Unknown	0	DevConnect ...	Avaya	6

8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management to interoperate with Avaya Aura® System Manager. During compliance testing, all test cases were completed successfully with observations noted in **Section 2.2**.

9. 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>.

1. *Deploying Avaya Aura® Communication Manager*, Release 7.1.2, Issue 2 December 2017
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.1.2, Issue 4 January 2018
3. *Deploying Avaya Aura® Session Manager*, Release 7.1.2, Issue 4 December 2017
4. *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 4 March 2018
5. *Deploying Avaya Aura® System Manager*, Release 7.1.2, Issue 6 March 2018
6. *Administering Avaya Aura® System Manager for Release 7.1.2*, Release 7.1.2, Issue 11 March 2018

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

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

©2018 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.