Application Notes for Virsae Service Management with Avaya Breeze - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management R174 to interoperate with Avaya Breeze 3.8.

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 monitored Breeze 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 (herein after referred to as VSM) with Avaya Breeze (herein after referred to as Breeze). 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 uses Linux shell access connections to monitor Breeze statistics such as CPU, Memory and Disk Usage, Network Connectivity and SNMP for alarms and, display monitored data on web-based application.

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 Breeze.

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 enabled capabilities of encrypted SSH and non-encrypted SNMP 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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

- Verify that the server statistics information for BREEZE is populated on VSM dashboard such as CPU, Memory and Disk Usage and list of Software/Processes.
- Verify alarm capture were received and 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 and rebooting the VSM.

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 Breeze. In this compliance testing, Avaya Breeze is administered via Avaya Aura® System Manager. The system has H.323/SIP Deskphones and softphones configured for making and receiving calls. VSM was installed on a server running Microsoft Windows Server 2016. 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 contains Probe Service use to collect service management data. 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.

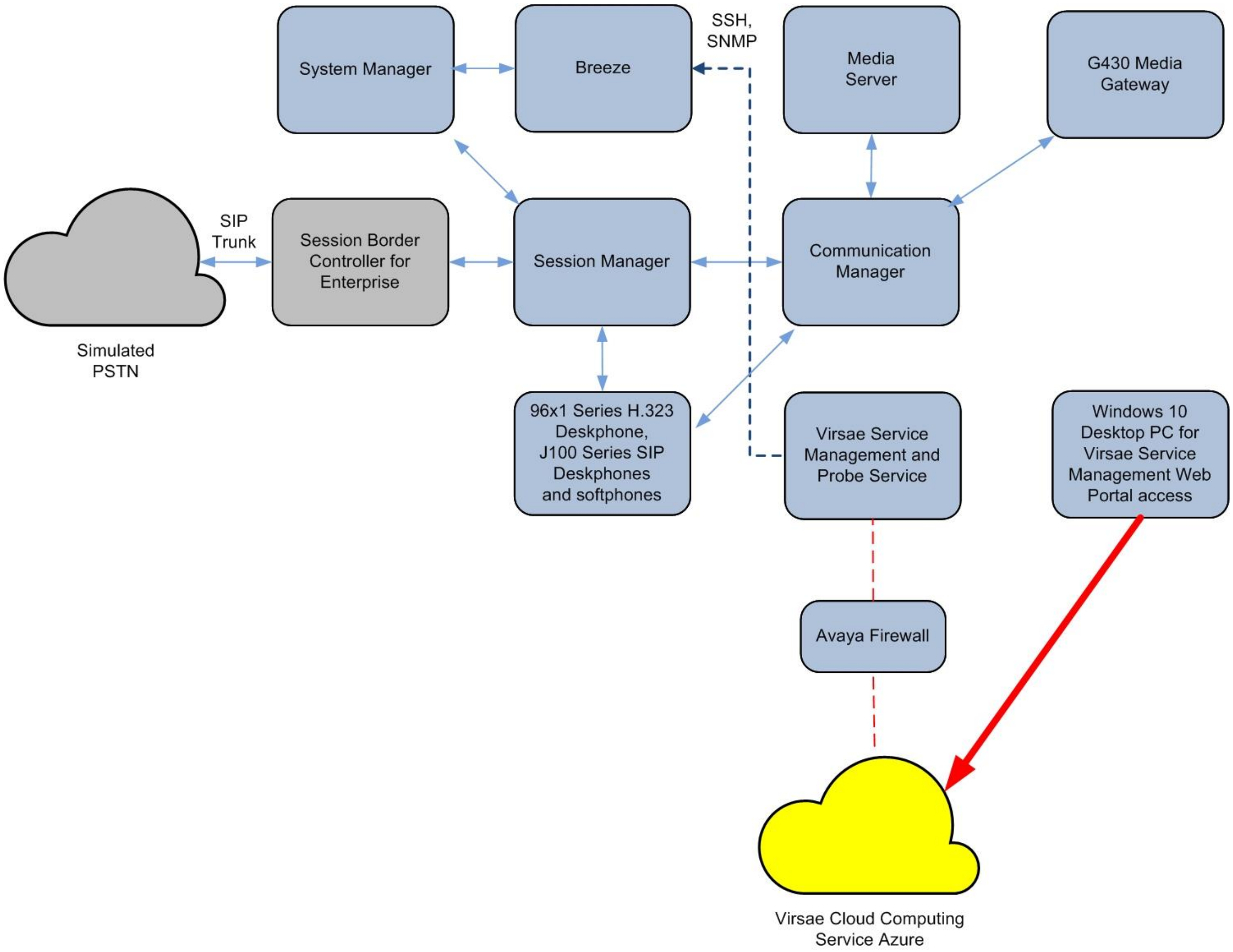


Figure 1: Test Configuration

4. Equipment and Software Validated

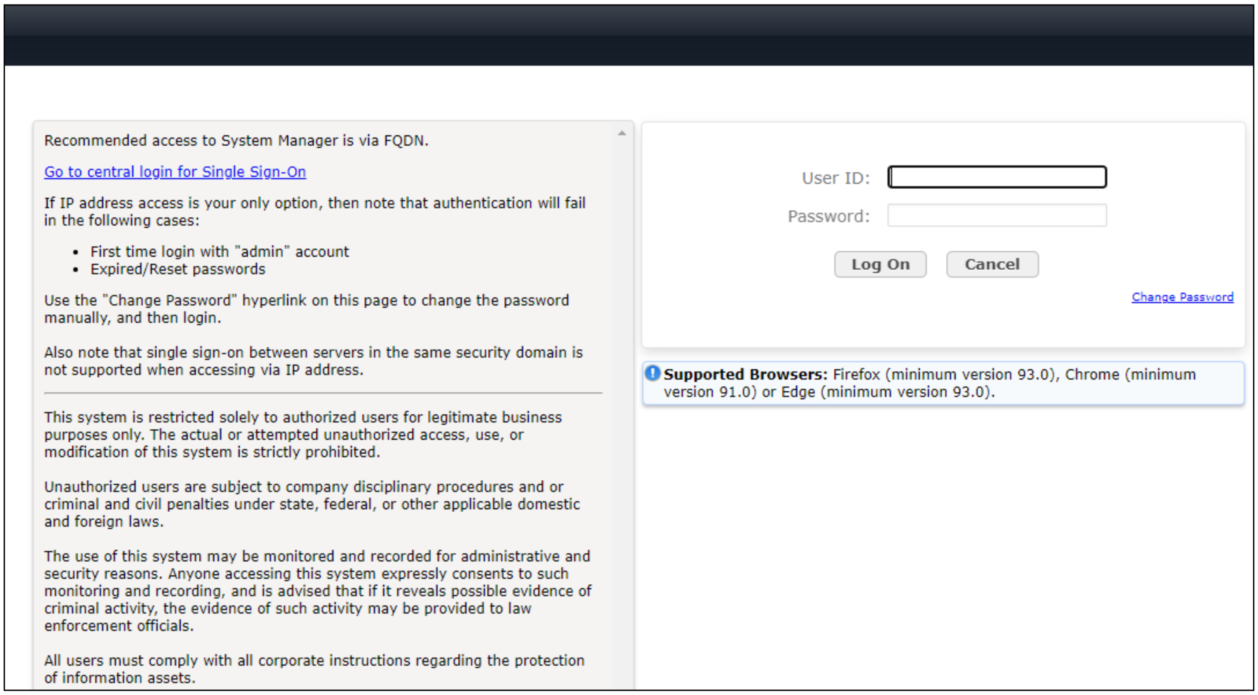
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Server	10.1 (10.1.0.0.0.974.27293)
Avaya G430 Media Gateway	42.4.0
Avaya Aura® Media Server running on Virtual Server	10.1.0.77
Avaya Breeze running on Virtual Server	3.8.1.1.381105
Avaya Aura® Session Manager running on Virtual Server	10.1 (10.1.0.0.1010019)
Avaya Aura® System Manager running on Virtual Server	10.1 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Avaya 96x1 Series (H.323)	6.8523
Avaya J100 Series (SIP)	4.0.11.0
Avaya Workplace Client for Windows (SIP)	3.27
Avaya Agent for Desktop (H.323)	2.0.6.22.3003
Virsae Service Management and Probe Service running on Windows 2016	174.1.2.268

5. Configure Avaya Breeze

The initial administration of Breeze 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.

Breeze is configured via the System Manager web interface. 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.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

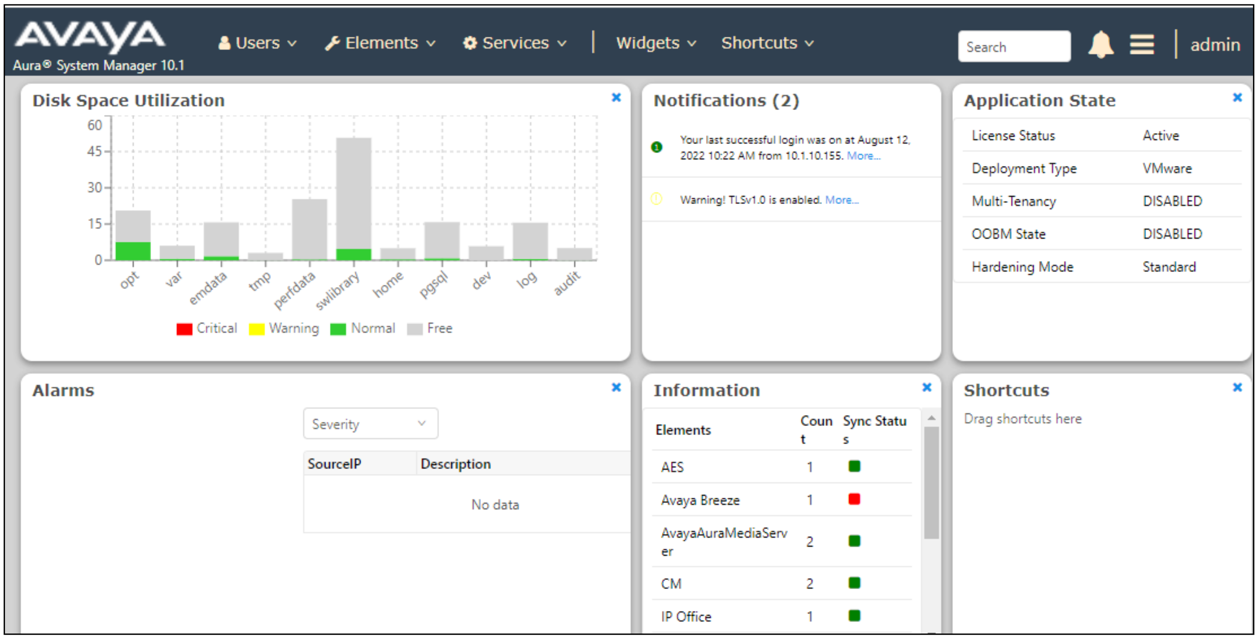
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

5.1. Configure SNMP Connection

The main System Manager dashboard page is shown below.



Notifications (2)

Your last successful login was on at August 12, 2022 10:22 AM from 10.1.10.155. More...

Warning! TLSv1.0 is enabled. More...

Application State

License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

Alarms

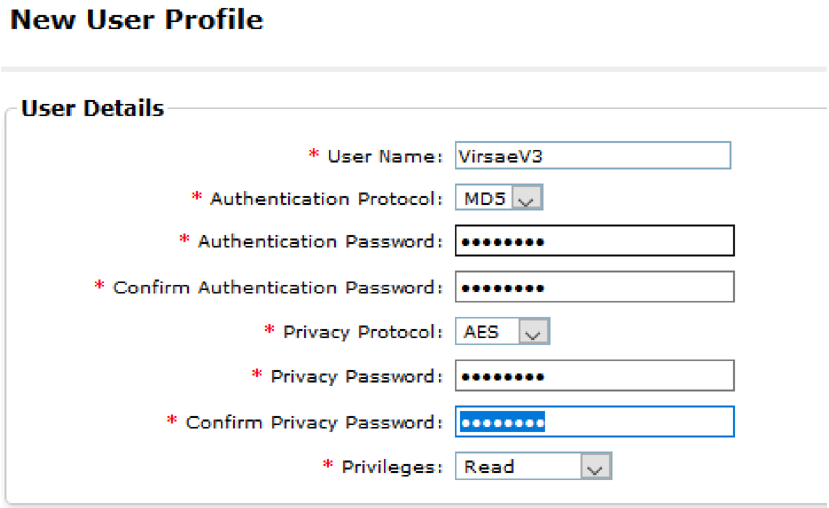
SourceIP	Description
No data	

Information

Elements	Count	Sync Status
AES	1	🟩
Avaya Breeze	1	🟥
AvayaAuraMediaServer	2	🟩
CM	2	🟩
IP Office	1	🟩

Then navigate to **Manage Servicability Agents → SNMPv3 User Profiles** and click **New** (not shown). Configure the following:

- **User Name**:	Descriptive name for SNMPv3.
- **Authentication Protocol**:	Select "MD5 or SHA".
- **Authentication Password** and **Confirm Authentication Password**:	Enter password.
- **Privacy Protocol**:	Select "AES, DES or none".
- **Privacy Password** and **Confirm Privacy Password:**	Enter password.

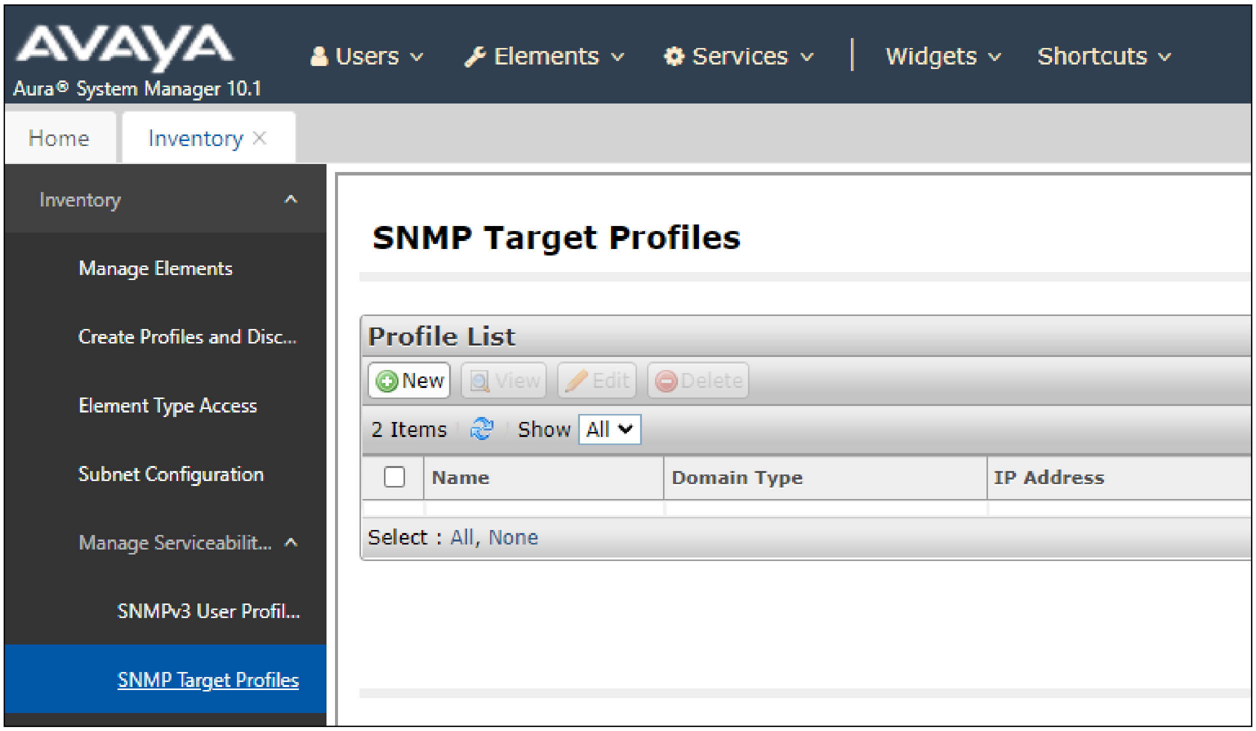


New User Profile

User Details

* User Name:	VirsaeV3
* Authentication Protocol:	MD5
* Authentication Password:	••••••••
* Confirm Authentication Password:	••••••••
* Privacy Protocol:	AES
* Privacy Password:	••••••••
* Confirm Privacy Password:	••••••••
* Privileges:	Read

Navigate to **Services → Inventory → Manage Servicability Agents → SNMP Target Profiles** as shown in the screen below. Click on **New**.



SNMP Target Profiles

Profile List

2 Items

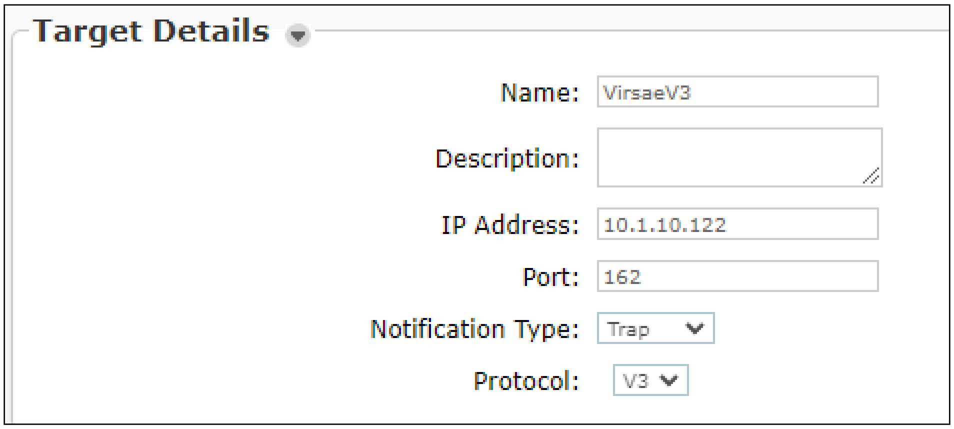
☐	Name	Domain Type	IP Address

Select : All, None

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

- **Name:** A descriptive name.
- **IP Address:** The VSM IP address.
- **Notification Type:** Select "Trap" from the drop-down menu.
- **Protocol:** Select **V3** from the drop-down menu.

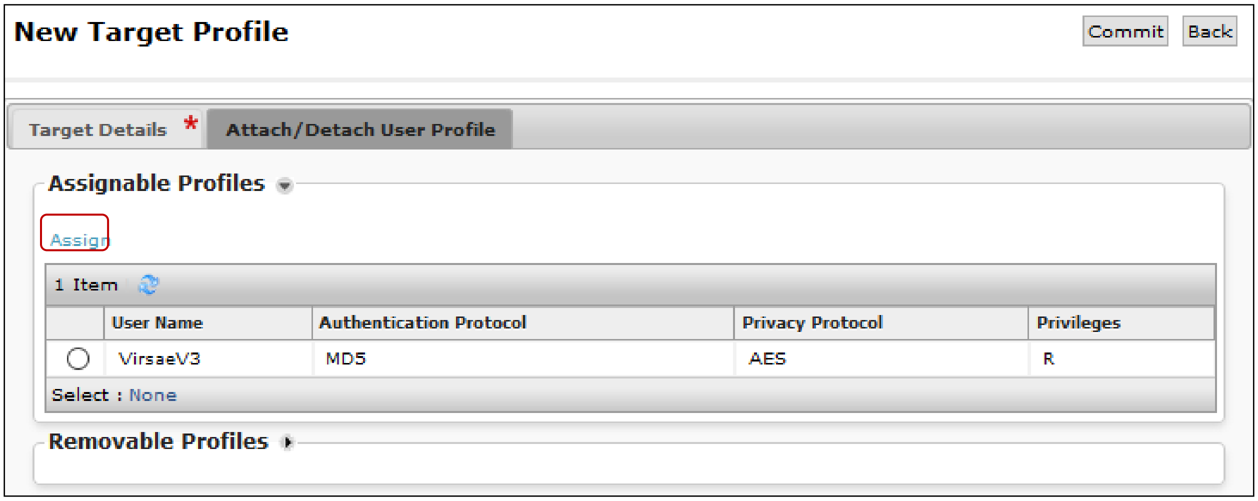
Retain default values for all other fields and click on the **Attach/Detach User Profile**.



Target Details

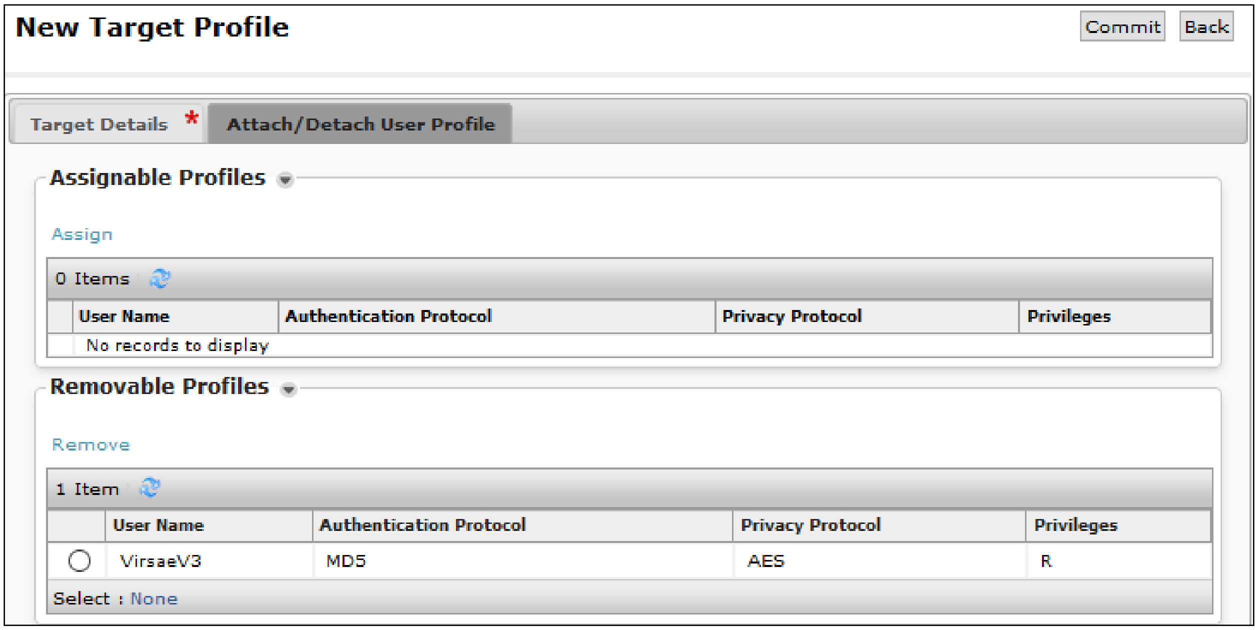
Name:	VirsaeV3
Description:	
IP Address:	10.1.10.122
Port:	162
Notification Type:	Trap
Protocol:	V3

Select the **VirsaeV3** user profile created earlier and click **Assign**.



	User Name	Authentication Protocol	Privacy Protocol	Privileges
○	VirsaeV3	MD5	AES	R

The **VirsaeV3** user profile is shown below as assigned to the Target.



New Target Profile

Assignable Profiles

0 Items

	User Name	Authentication Protocol	Privacy Protocol	Privileges
	No records to display			

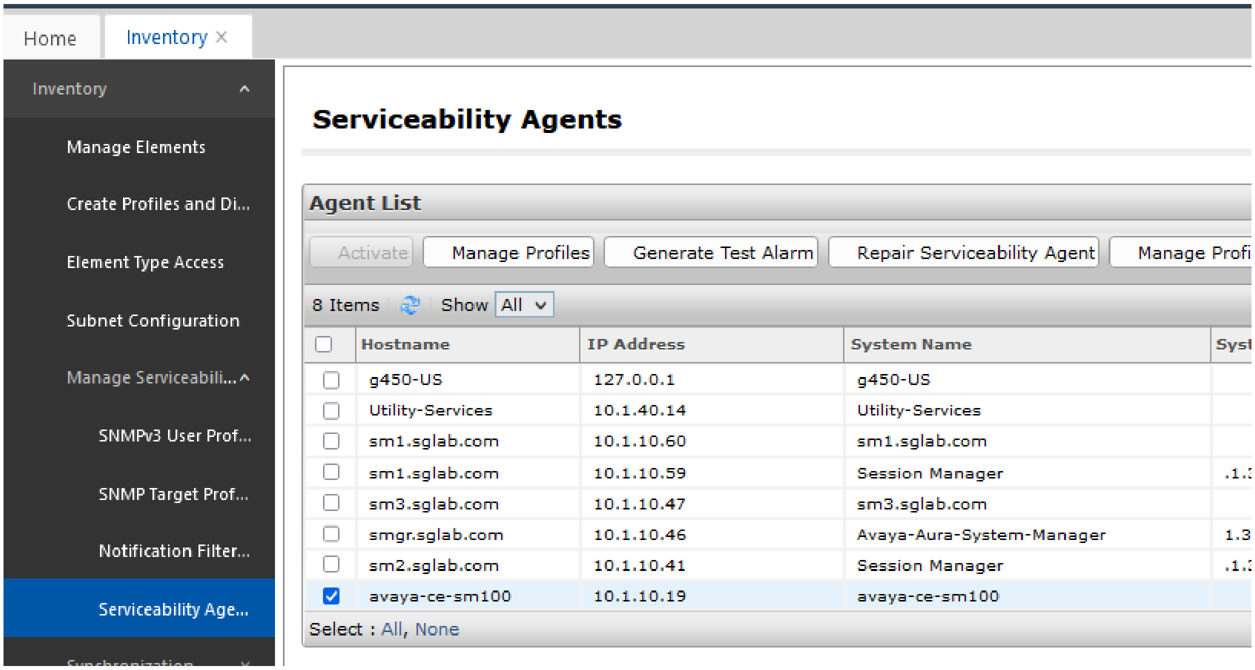
Removable Profiles

1 Item

	User Name	Authentication Protocol	Privacy Protocol	Privileges
○	VirsaeV3	MD5	AES	R

Select : None

Then navigate to **Manage Servicability Agents → Servicability Agents** as shown in the screen below. Select Breeze agent from the **Agent List** window, and click on the **Manage Profiles** button.



Serviceability Agents

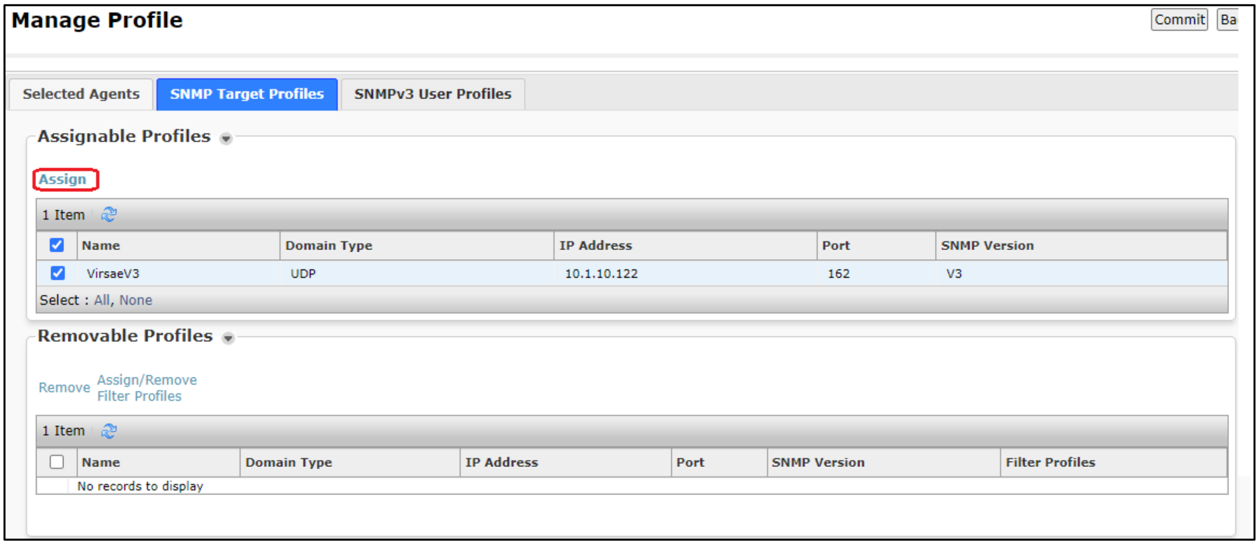
Agent List

8 Items Show All

□	Hostname	IP Address	System Name	Syst
□	g450-US	127.0.0.1	g450-US	
□	Utility-Services	10.1.40.14	Utility-Services	
□	sm1.sglab.com	10.1.10.60	sm1.sglab.com	
□	sm1.sglab.com	10.1.10.59	Session Manager	.1.:
□	sm3.sglab.com	10.1.10.47	sm3.sglab.com	
□	smgr.sglab.com	10.1.10.46	Avaya-Aura-System-Manager	1.3
□	sm2.sglab.com	10.1.10.41	Session Manager	.1.:
☑	avaya-ce-sm100	10.1.10.19	avaya-ce-sm100	

Select : All, None

From the **Manage Profile** window, under the **SNMP Target Profiles** tab, select the **VirsaeV3** profile, click on **Assign**. Then click the **Commit** button. Do the same for **SNMPv3 User Profiles** tab.



Assignable Profiles

1 Item

☑	Name	Domain Type	IP Address	Port	SNMP Version
☑	VirsaeV3	UDP	10.1.10.122	162	V3

Select : All, None

Removable Profiles

1 Item

□	Name	Domain Type	IP Address	Port	SNMP Version	Filter Profiles
	No records to display					

5.2. Configure Login Account

Create an Administrator account on Breeze since VSM requires access to Breeze with Administrative Rights. The new account should be like the default "**cust**" account. Log into Breeze console with root access and run the following command.

```
useradd <NAME>       ;Add User
passwd <NAME>        ;Enter password twice
chage -M 99999 <NAME>       ;Lengthen the expiry date of account
```

6. Configure Virsae Service Management

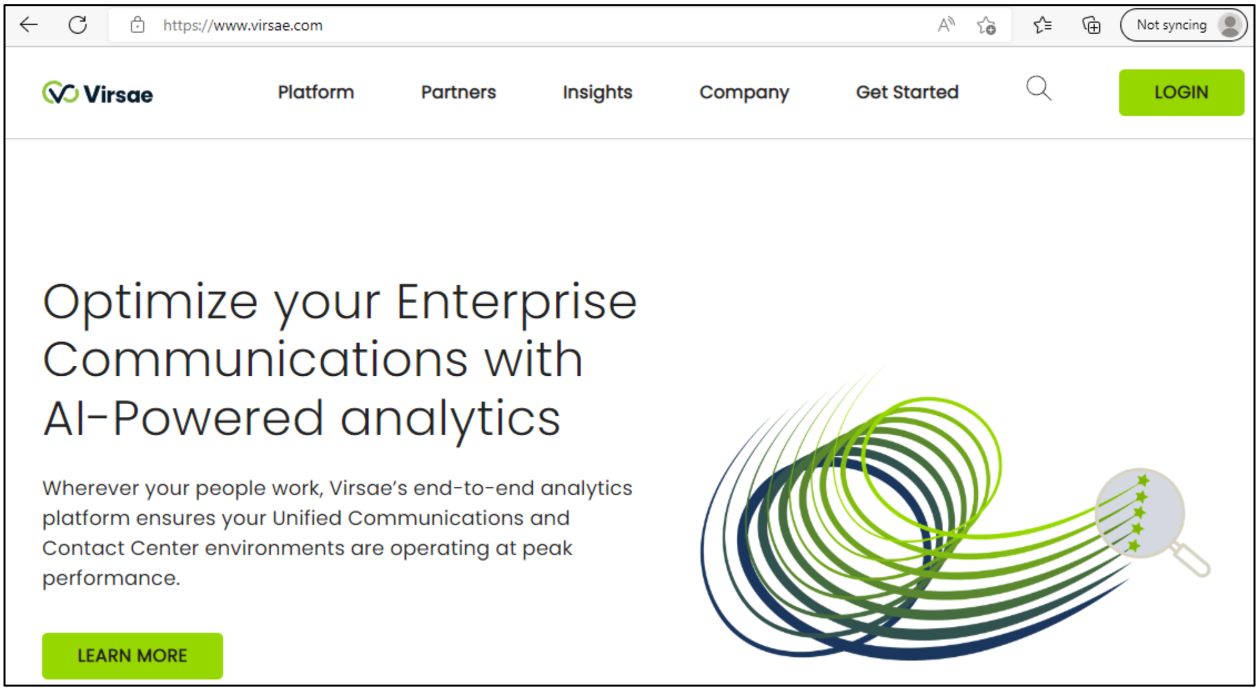
This section describes the configuration of VSM required to interoperate with Breeze.

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 these Application Notes. The screen shots and partial configuration shown below, 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 Breeze
- Configure Dashboard

6.1. Login to the Web Portal

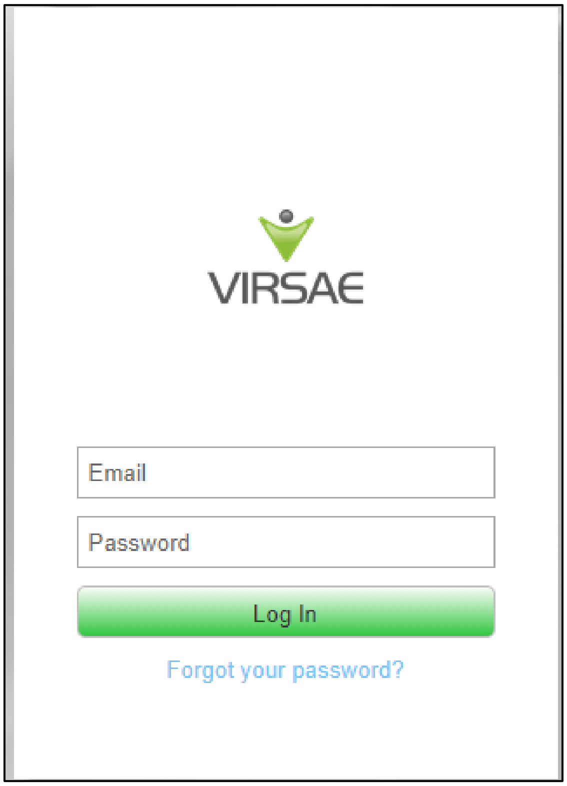
A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL *www.virsae.com* in a web browser. During compliance testing the same URL was used. Click on the **LOGIN** shown on the top right below.



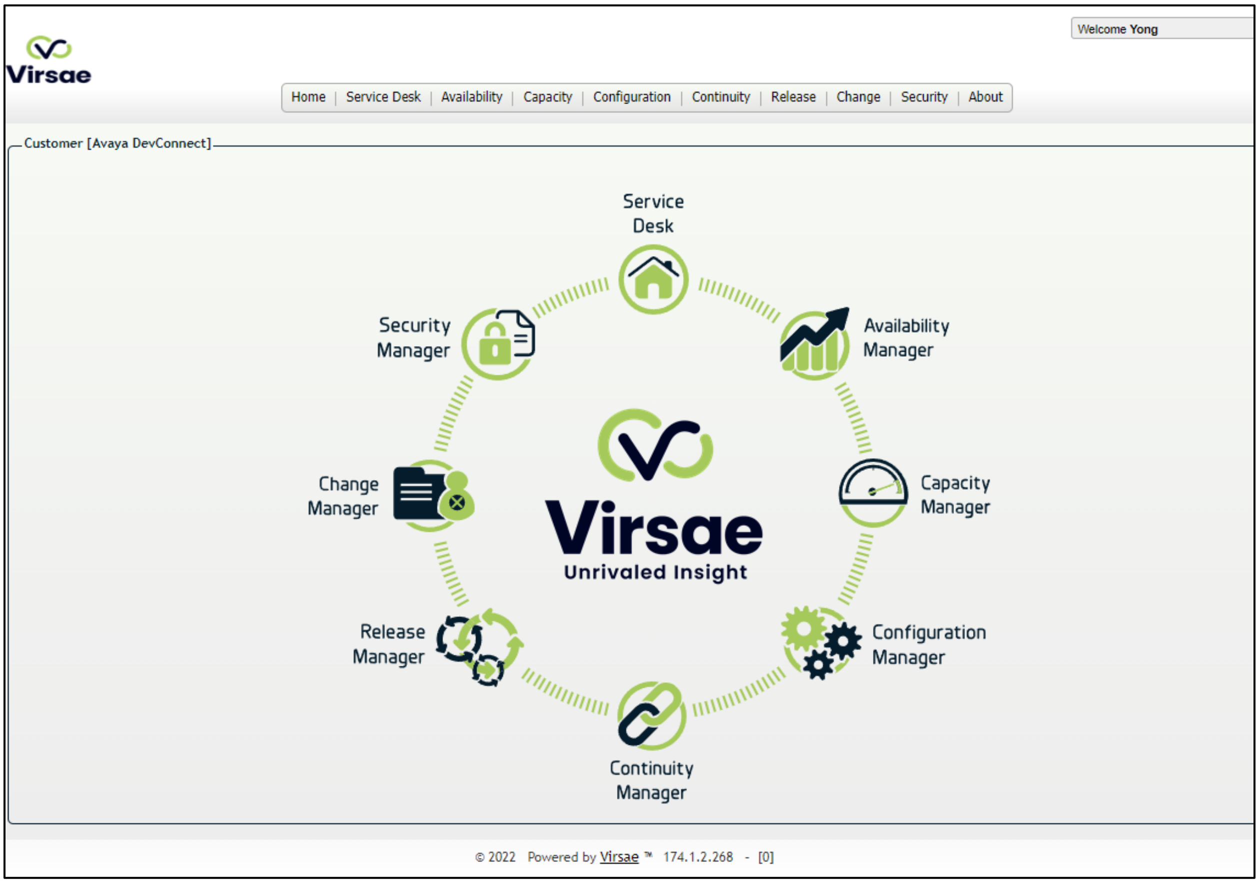
Optimize your Enterprise Communications with AI-Powered analytics

Wherever your people work, Virsae's end-to-end analytics platform ensures your Unified Communications and Contact Center environments are operating at peak performance.

Enter the **Email** and **Password** and click on the **Log In** button.

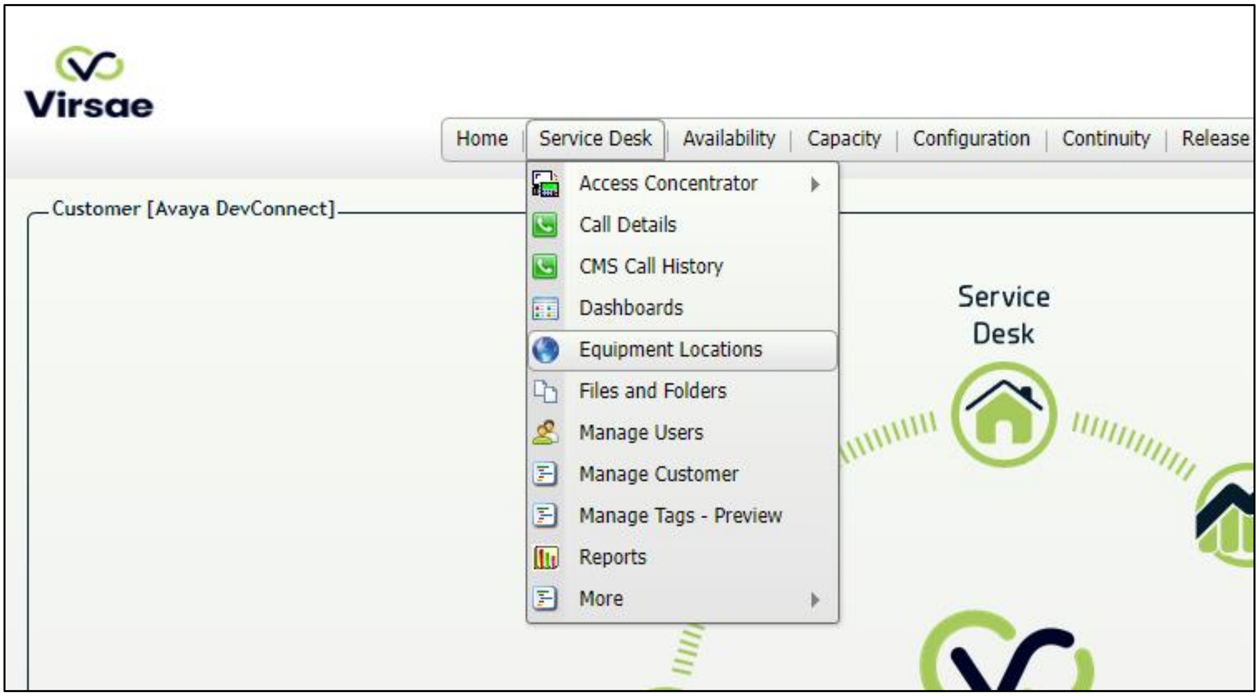


The customer screen is shown. During compliance testing the customer created by Virsae can be seen near the top right corner. Note the version running is shown at the bottom i.e., **174.1.2.268**.

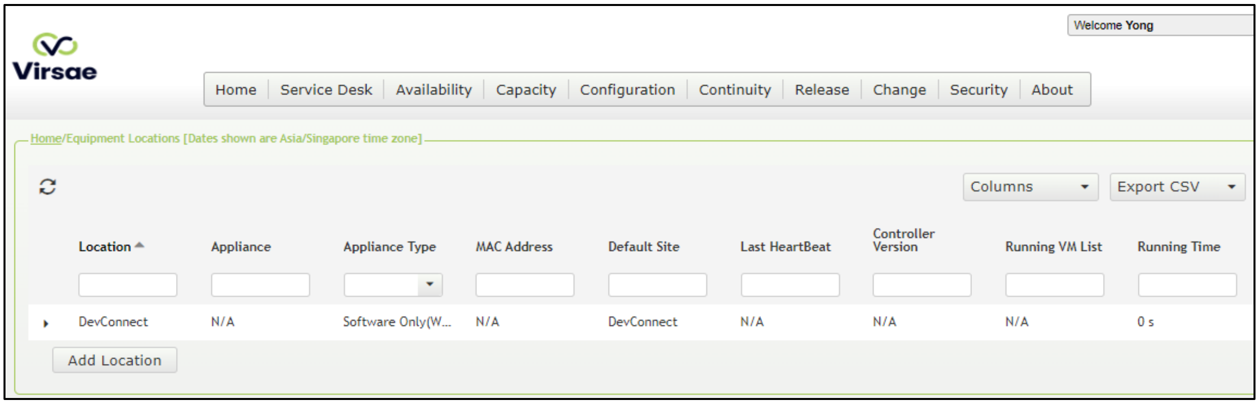


Welcome Yong
Virsae
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | About
Customer [Avaya DevConnect]
Service Desk
Availability Manager
Capacity Manager
Configuration Manager
Continuity Manager
Release Manager
Change Manager
Security Manager
Virsae
Unrivaled Insight
© 2022 Powered by Virsae ™ 174.1.2.268 - [0]

Navigate to **Service Desk → Equipment Locations** as shown below.



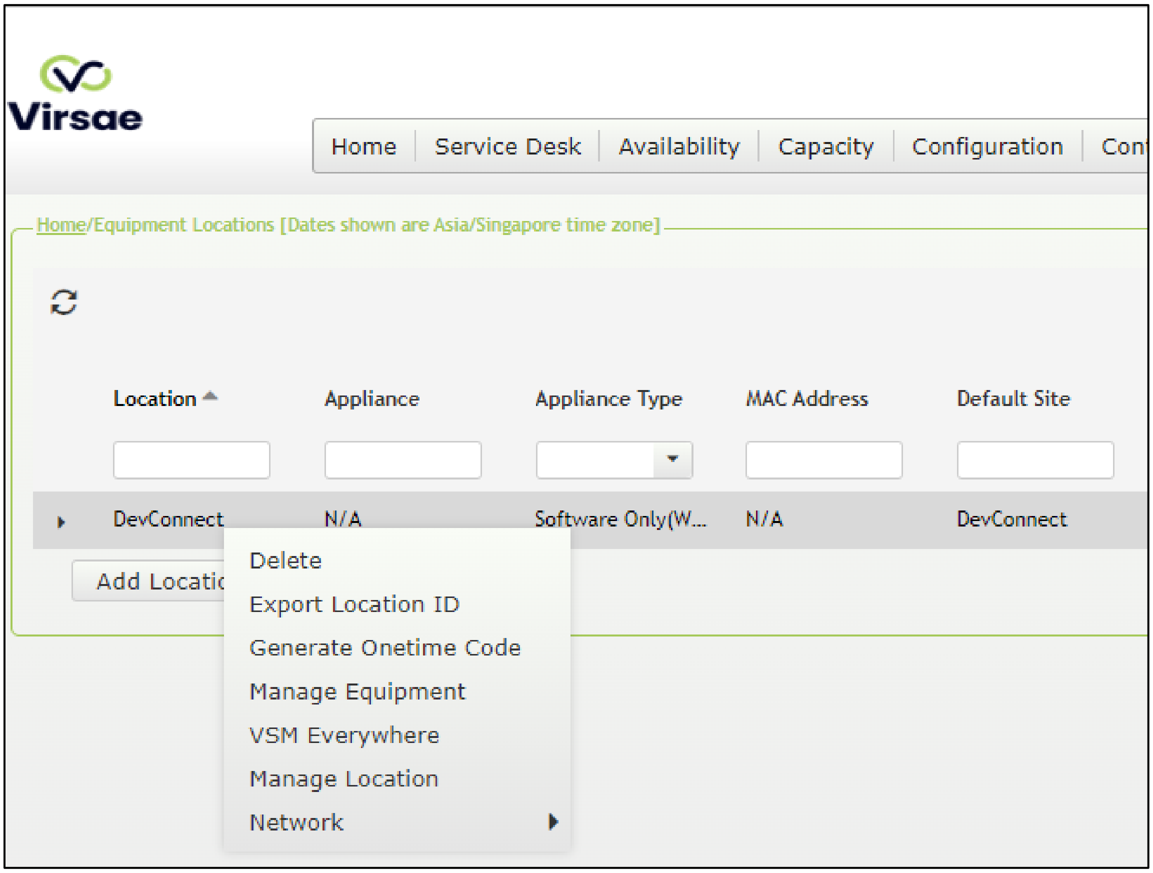
A **Location** called **DevConnect** is already configured as shown below.



Home/Equipment Locations [Dates shown are Asia/Singapore time zone]

Location	Appliance	Appliance Type	MAC Address	Default Site	Last HeartBeat	Controller Version	Running VM List	Running Time
DevConnect	N/A	Software Only(W...	N/A	DevConnect	N/A	N/A	N/A	0 s

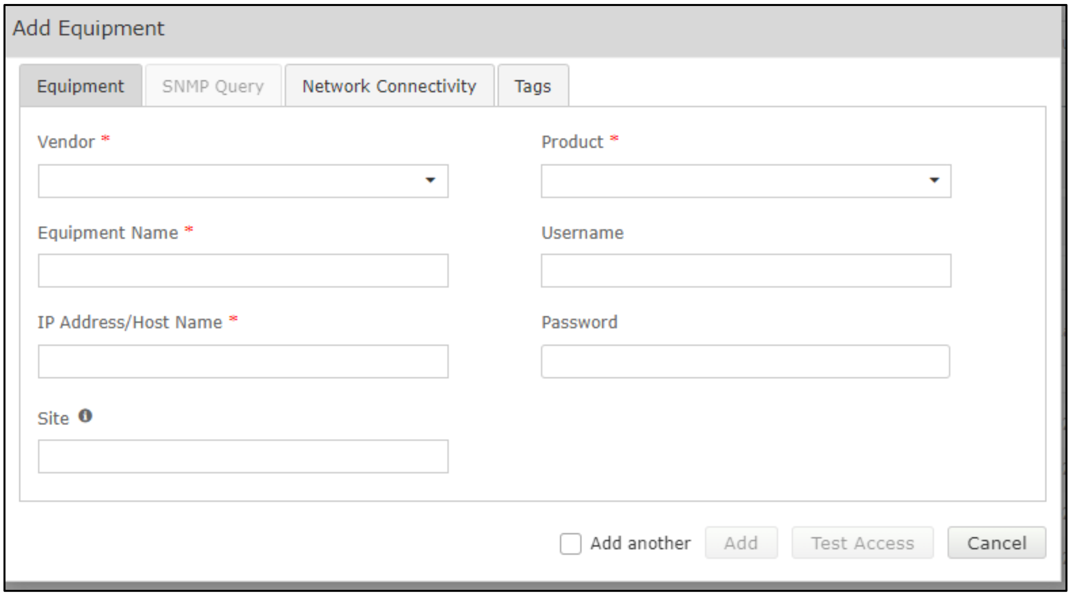
Right click on the **DevConnect** and select **Manage Equipment**.



Home/Equipment Locations [Dates shown are Asia/Singapore time zone]

Location	Appliance	Appliance Type	MAC Address	Default Site
DevConnect	N/A	Software Only(W...	N/A	DevConnect

Click **Add Equipment** (not shown) and the screen below pops up:



Add Equipment

Vendor *

Product *

Equipment Name *

Username

IP Address/Host Name *

Password

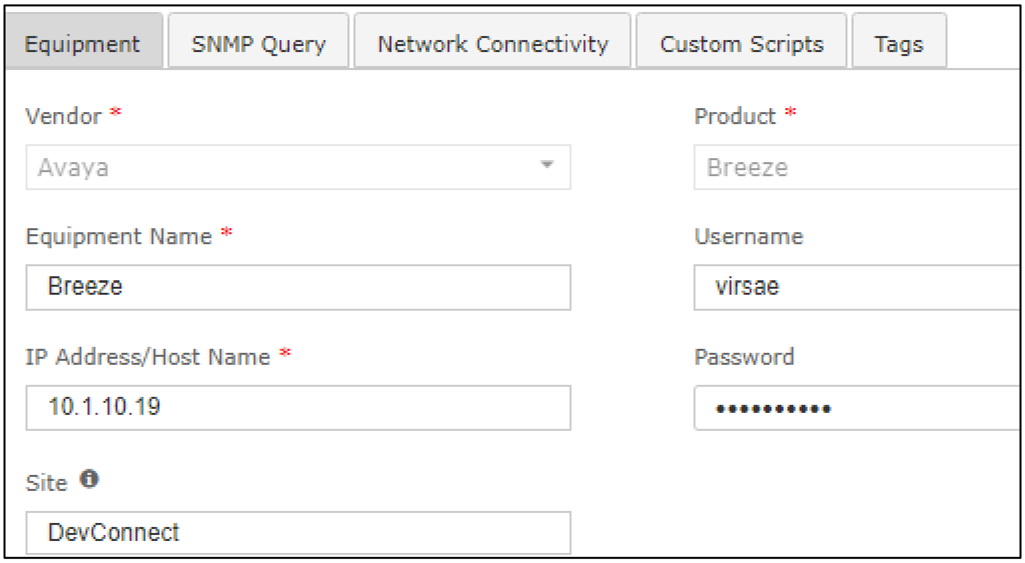
Site

6.2. Configuring Avaya Breeze

From the **Add Equipment** window, add Breeze to the Location. Select **Avaya** from the **Vendor** list. Select **Breeze** from the **Product** list. Configure the following values.

- **Equipment Name:** A descriptive name.
- **Username:** The username configured in **Section 5.2**.
- **Password:** The password configured in **Section 5.2**.
- **IP Address/Host Name:** Management IP address of Breeze.
- **Site:** A descriptive site name.

Below are the configured values of the Breeze.



Vendor * Avaya

Product * Breeze

Equipment Name * Breeze

Username virsae

IP Address/Host Name * 10.1.10.19

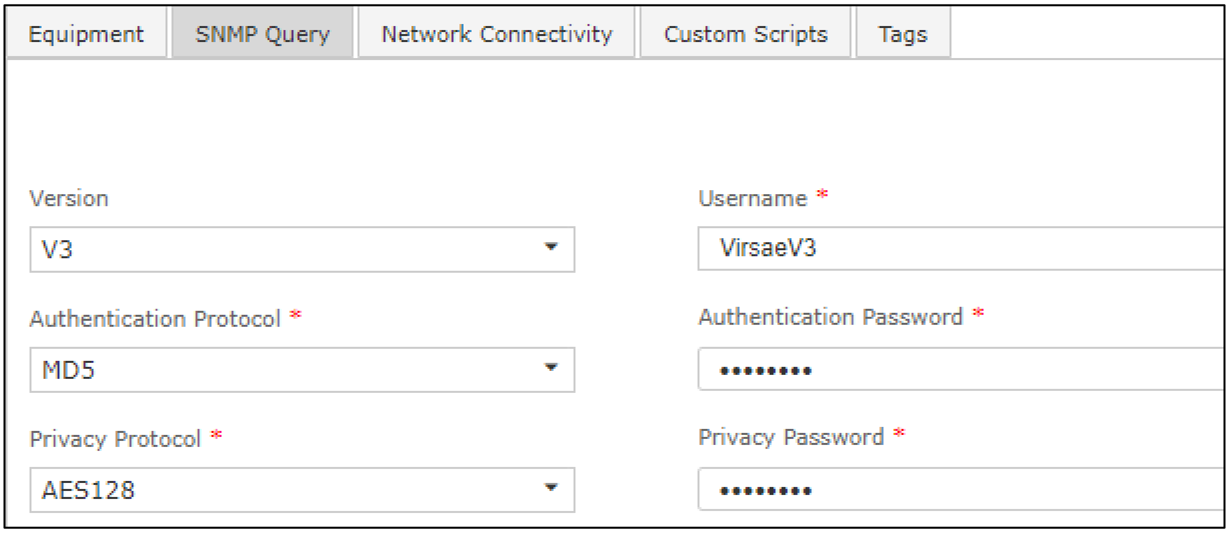
Password ••••••••••

Site DevConnect

In the **SNMP Query** tab, configure the following values.

- **Version:** Select **V3** from the drop-down menu.
- **Username:** Enter username configured in **Section 5.1**.
- **Authentication Protocol**: Protocol configured in **Section 5.1**.
- **Authentication Password**: Password configured in **Section 5.1**.
- **Privacy Protocol**: Protocol configured in **Section 5.1**.
- **Privacy Password**: Password configured in **Section 5.1**.

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



Version: V3

Username *: VirsaeV3

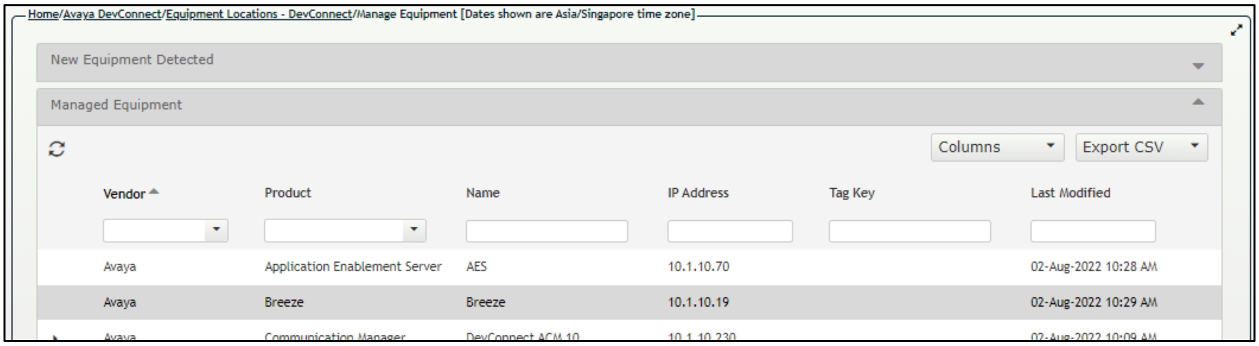
Authentication Protocol *: MD5

Authentication Password *: ••••••••

Privacy Protocol *: AES128

Privacy Password *: ••••••••

The screen below shows the added Breeze equipment.

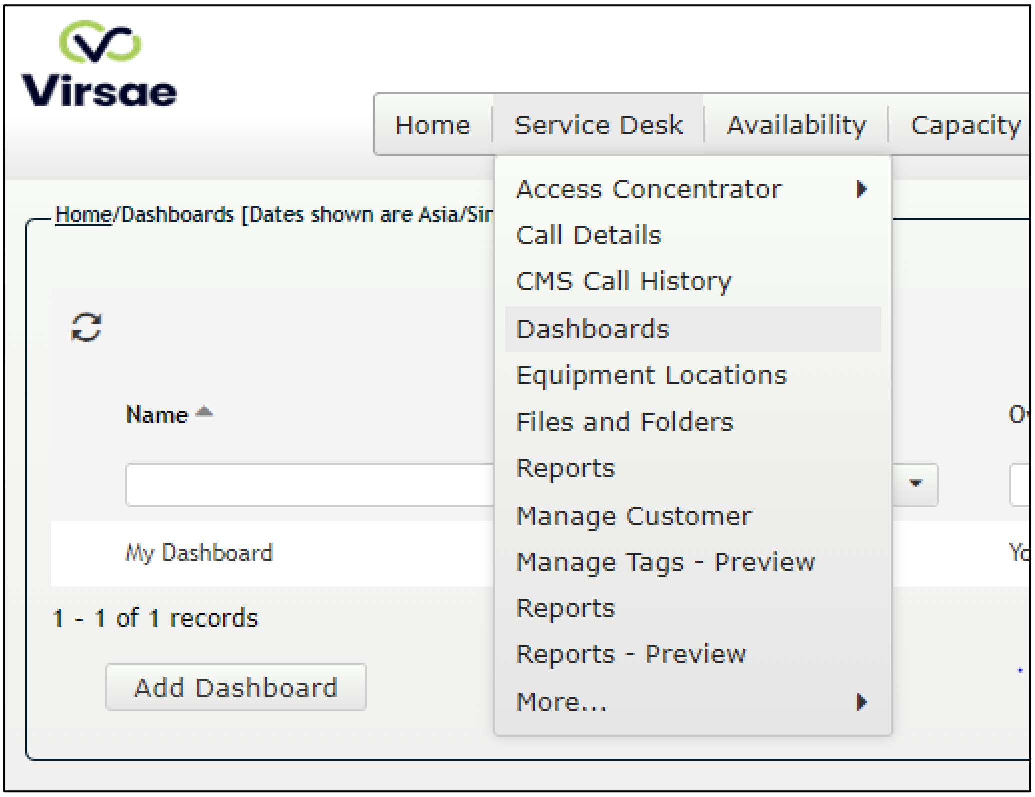

Home/Avaya DevConnect/Equipment Locations - DevConnect/Manage Equipment [Dates shown are Asia/Singapore time zone]
New Equipment Detected
Managed Equipment
Columns
Export CSV

Vendor	Product	Name	IP Address	Tag Key	Last Modified
Avaya	Application Enablement Server	AES	10.1.10.70		02-Aug-2022 10:28 AM
Avaya	Breeze	Breeze	10.1.10.19		02-Aug-2022 10:29 AM
Avaya	Communication Manager	DevConnect ACM 10	10.1.10.230		02-Aug-2022 10:09 AM

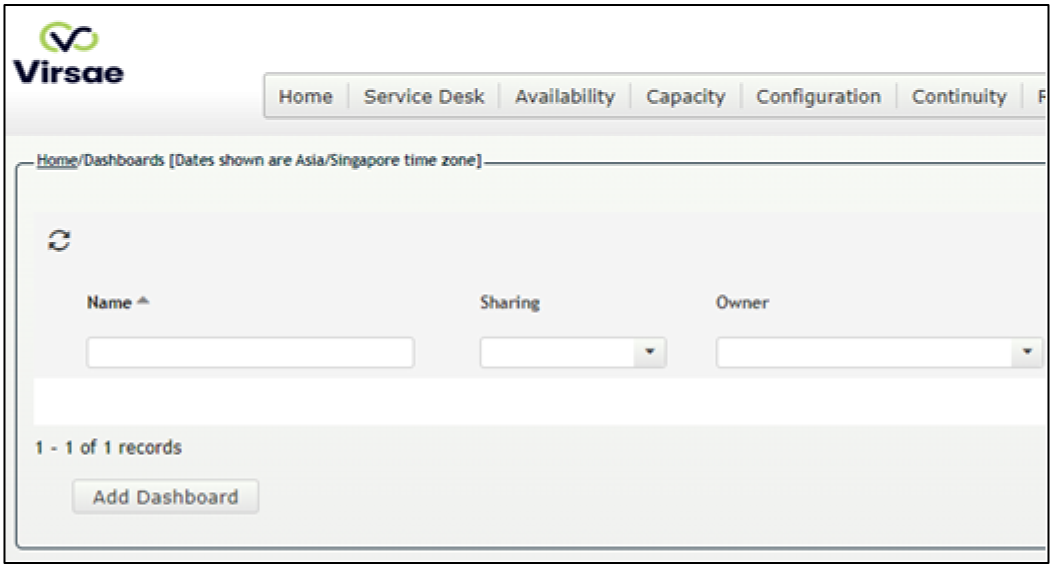
6.3. Configure Dashboard

This section shows the steps to configure Breeze on the dashboard.

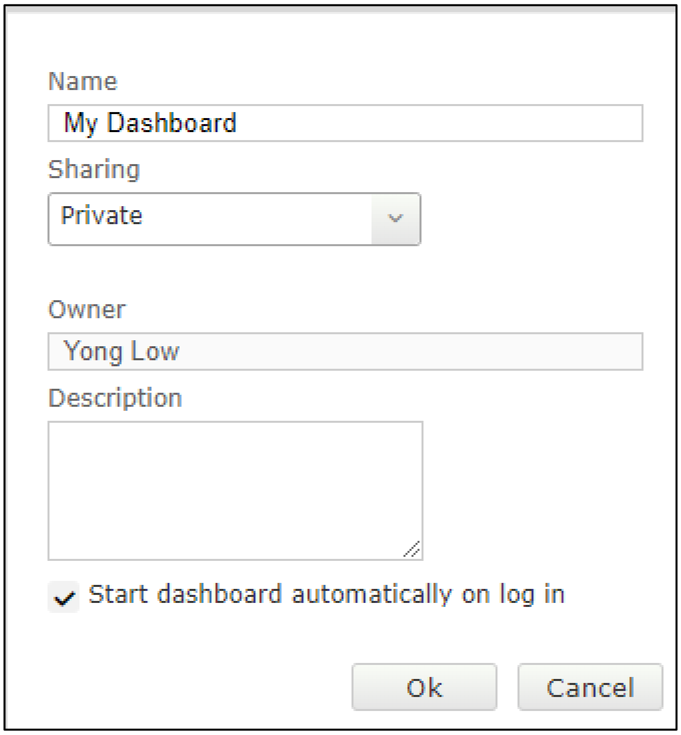
From the home screen, navigate to **Service Desk → Dashboards** as shown below.



From the **Available Dashboards** window, click on the **Add Dashboard** button.



In the **Add Dashboard** window, type a descriptive name for **Name** field as shown below. Retain default values for all other fields. Click on **Start dashboard automatically on log in** box and then click on **Ok** to submit**.**



Name

My Dashboard

Sharing

Private

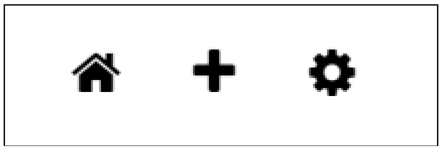
Owner

Yong Low

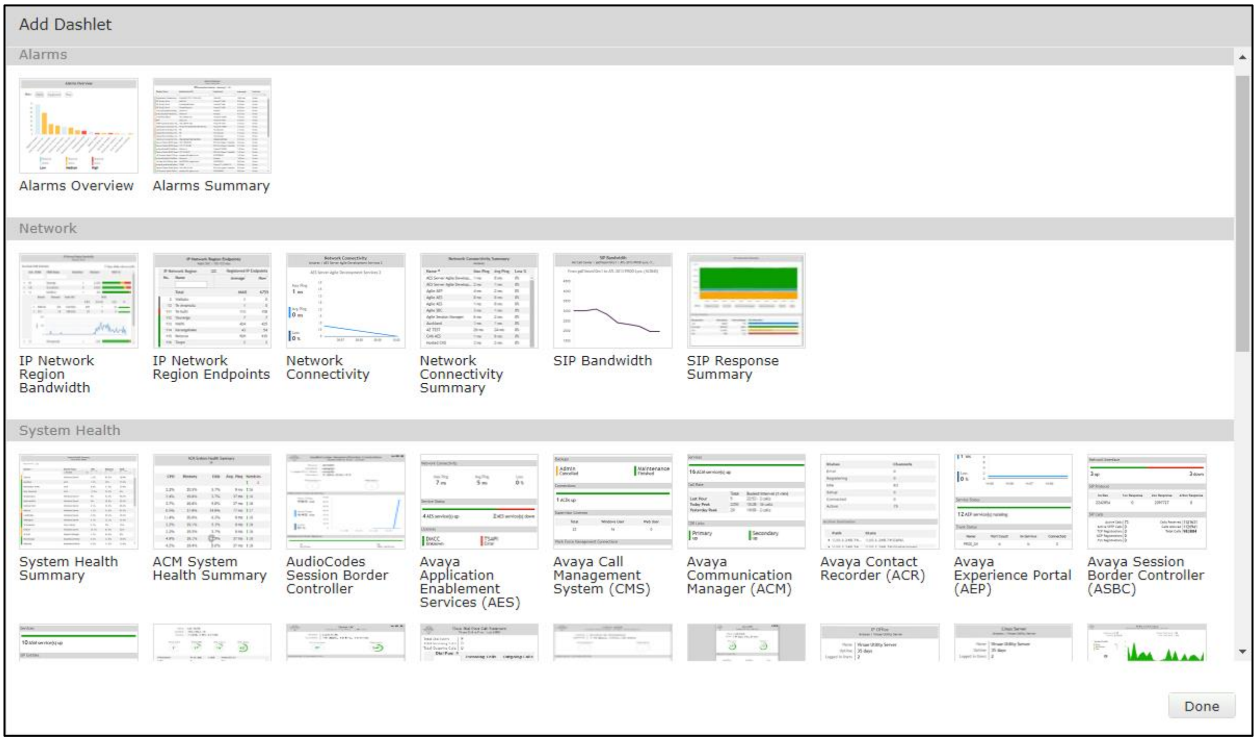
Description

☑ Start dashboard automatically on log in

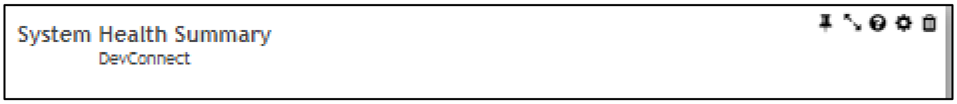
In the dashboard window bottom shown below, click on "+" sign at the bottom.



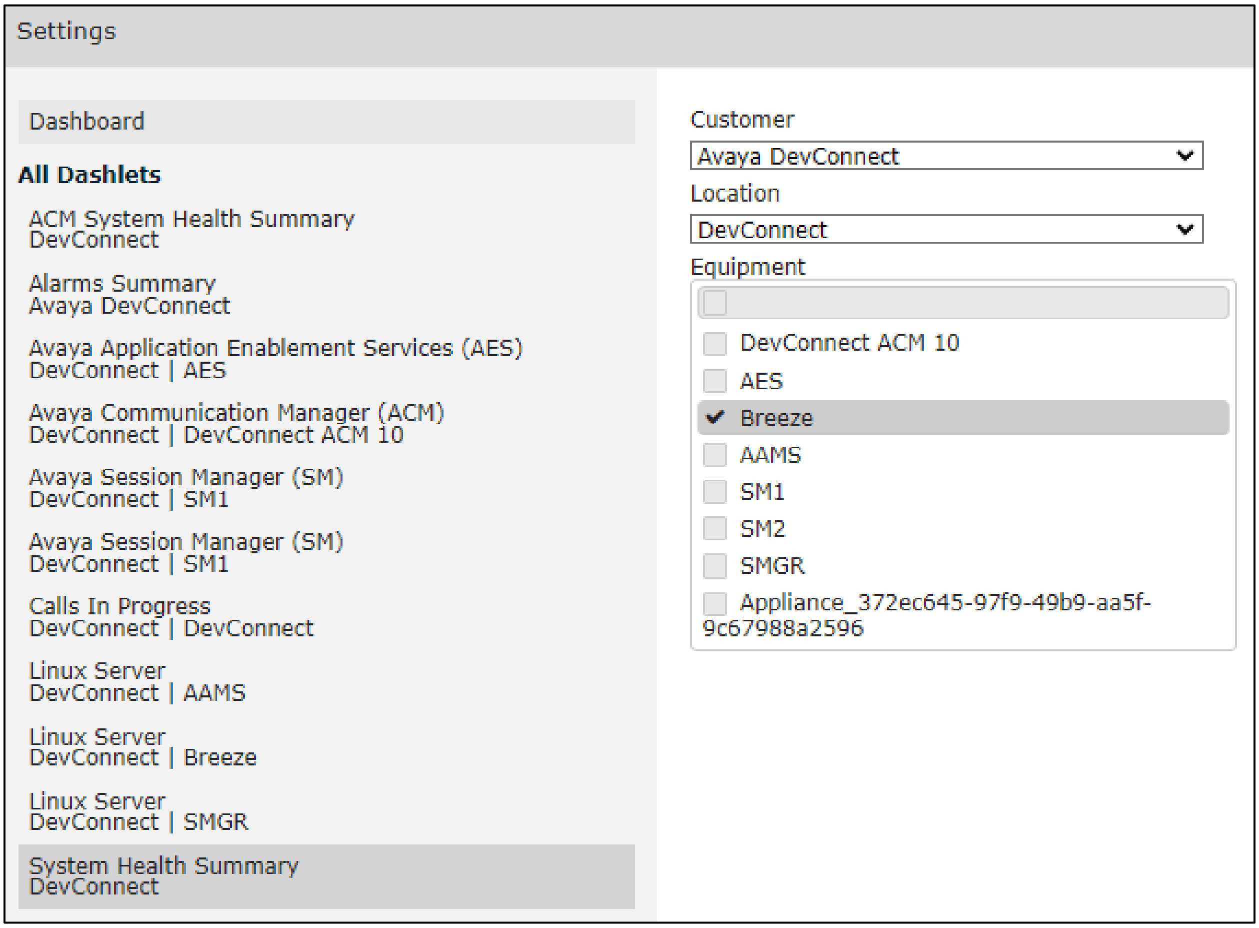
In the **Add Dashlet** window that pops up, select the **System Health Summary** from the available dashlet by hovering the "+" image over it and click **Done**.


Add Dashlet
Alarms
Alarms Overview
Alarms Summary
Network
IP Network Region Bandwidth
IP Network Region Endpoints
Network Connectivity
Network Connectivity Summary
SIP Bandwidth
SIP Response Summary
System Health
System Health Summary
ACM System Health Summary
AudioCodes Session Border Controller
Avaya Application Enablement Services (AES)
Avaya Call Management System (CMS)
Avaya Communication Manager (ACM)
Avaya Contact Recorder (ACR)
Avaya Experience Portal (AEP)
Avaya Session Border Controller (ASBC)
Done

From the **System Health Summary** window, select the **setup cog** on the top right corner of the box.



Select the correct **Location** i.e., **DevConnect** and the appropriate **Equipment** i.e., **Breeze** and click **Done** (not shown) to complete.



Settings

Dashboard

All Dashlets

ACM System Health Summary
DevConnect

Alarms Summary
Avaya DevConnect

Avaya Application Enablement Services (AES)
DevConnect | AES

Avaya Communication Manager (ACM)
DevConnect | DevConnect ACM 10

Avaya Session Manager (SM)
DevConnect | SM1

Avaya Session Manager (SM)
DevConnect | SM1

Calls In Progress
DevConnect | DevConnect

Linux Server
DevConnect | AAMS

Linux Server
DevConnect | Breeze

Linux Server
DevConnect | SMGR

System Health Summary
DevConnect

Customer: Avaya DevConnect

Location: DevConnect

Equipment

□

□ DevConnect ACM 10

□ AES

☑ Breeze

□ AAMS

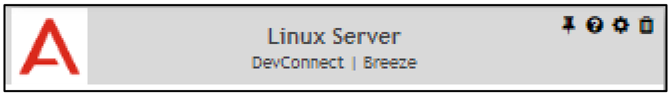
□ SM1

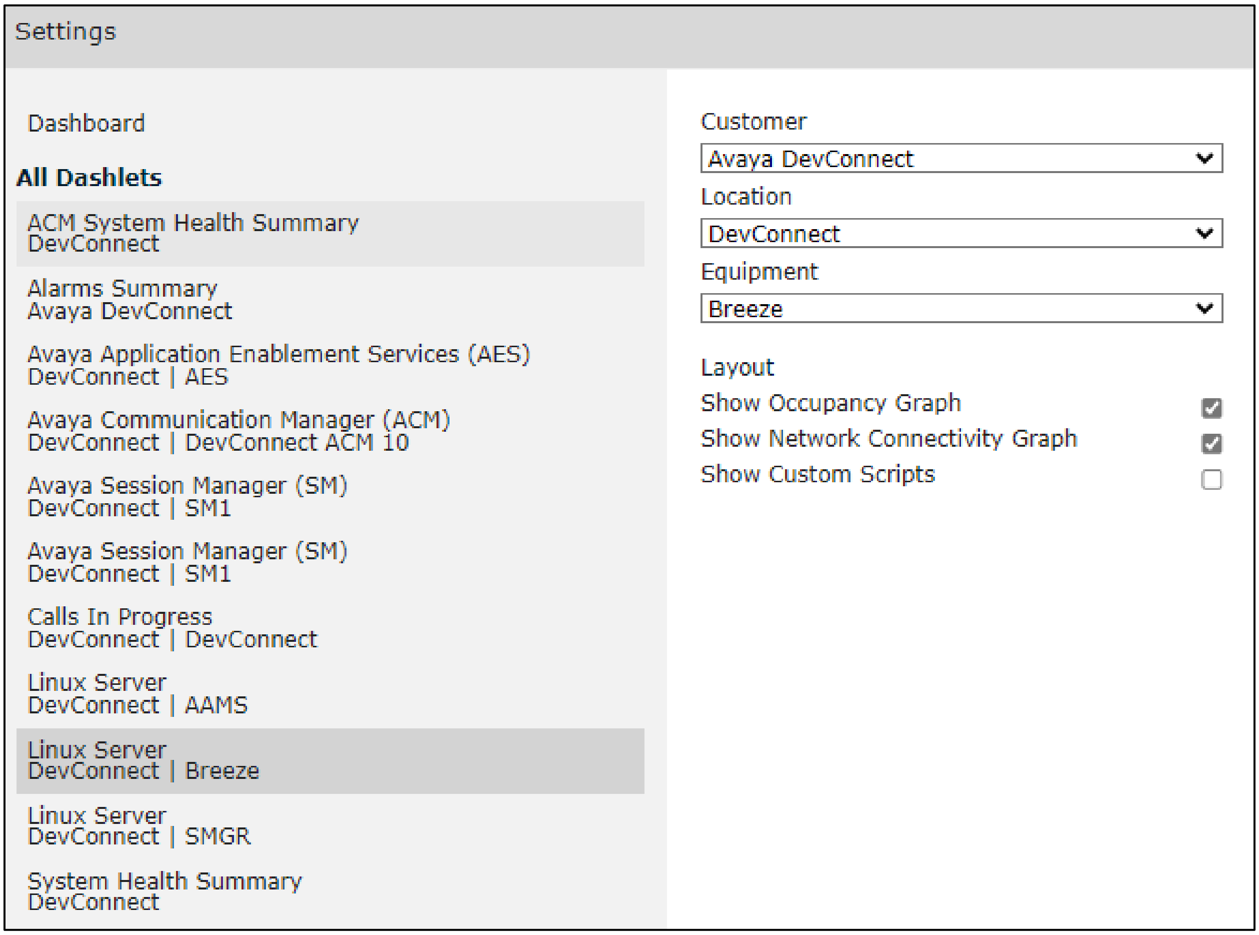
□ SM2

□ SMGR

□ Appliance_372ec645-97f9-49b9-aa5f-9c67988a2596

Repeat the same for the **Linux Server** dashlet and in addition select the desired **Layout**.





Customer

Avaya DevConnect

Location

DevConnect

Equipment

Breeze

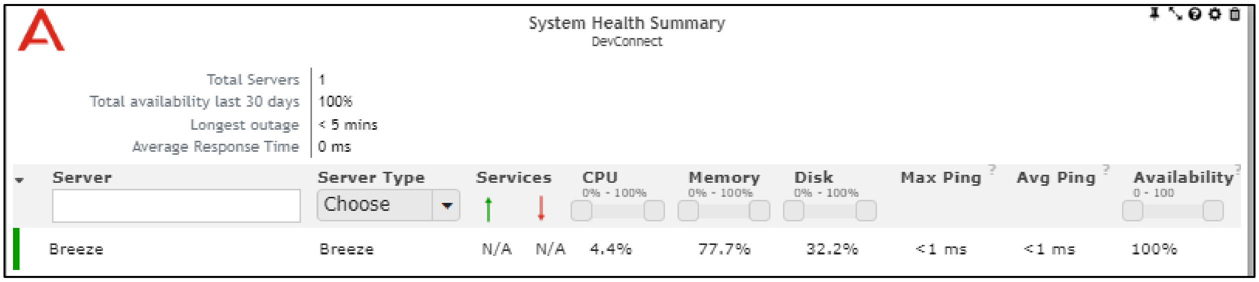
Layout

Show Occupancy Graph ☑

Show Network Connectivity Graph ☑

Show Custom Scripts □

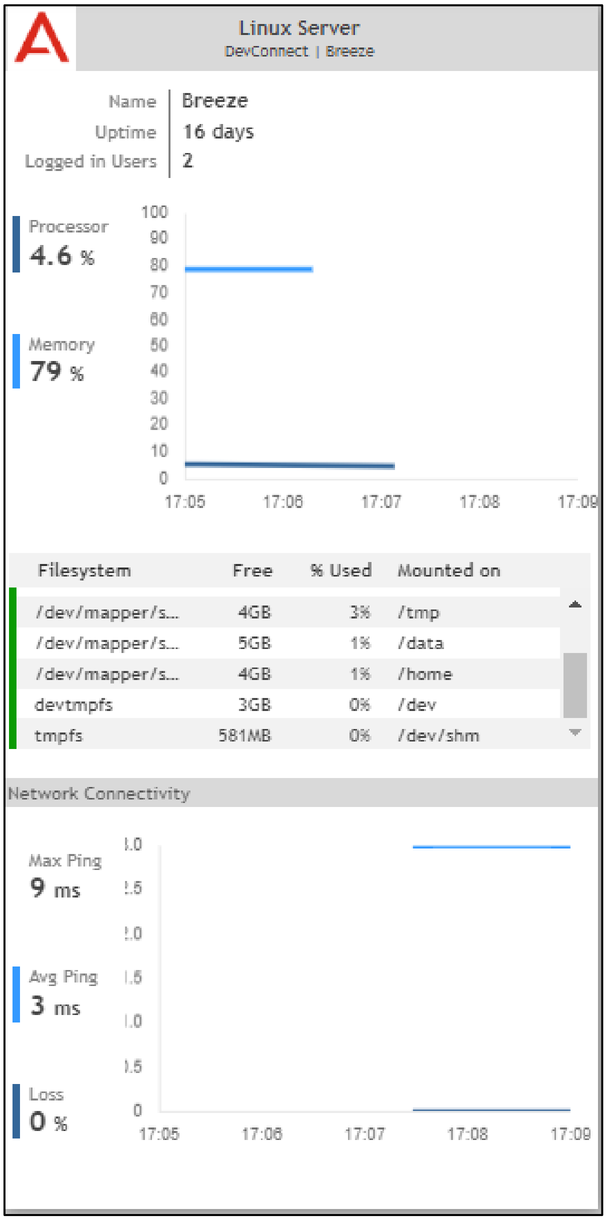
The dashboard with the configured equipment is shown below. The above steps can be repeated to configure other equipment or/and dashboard parameters.



System Health Summary
DevConnect

Total Servers	1
Total availability last 30 days	100%
Longest outage	< 5 mins
Average Response Time	0 ms

Server	Server Type	Services		CPU 0% - 100%	Memory 0% - 100%	Disk 0% - 100%	Max Ping	Avg Ping	Availability 0 - 100
	Choose	↑	↓						
Breeze	Breeze	N/A	N/A	4.4%	77.7%	32.2%	<1 ms	<1 ms	100%



Linux Server
DevConnect | Breeze

Name	Breeze
Uptime	16 days
Logged in Users	2

Processor
4.6 %

Memory
79 %

Filesystem	Free	% Used	Mounted on
/dev/mapper/s...	4GB	3%	/tmp
/dev/mapper/s...	5GB	1%	/data
/dev/mapper/s...	4GB	1%	/home
devtmpfs	3GB	0%	/dev
tmpfs	581MB	0%	/dev/shm

Network Connectivity

Max Ping
9 ms

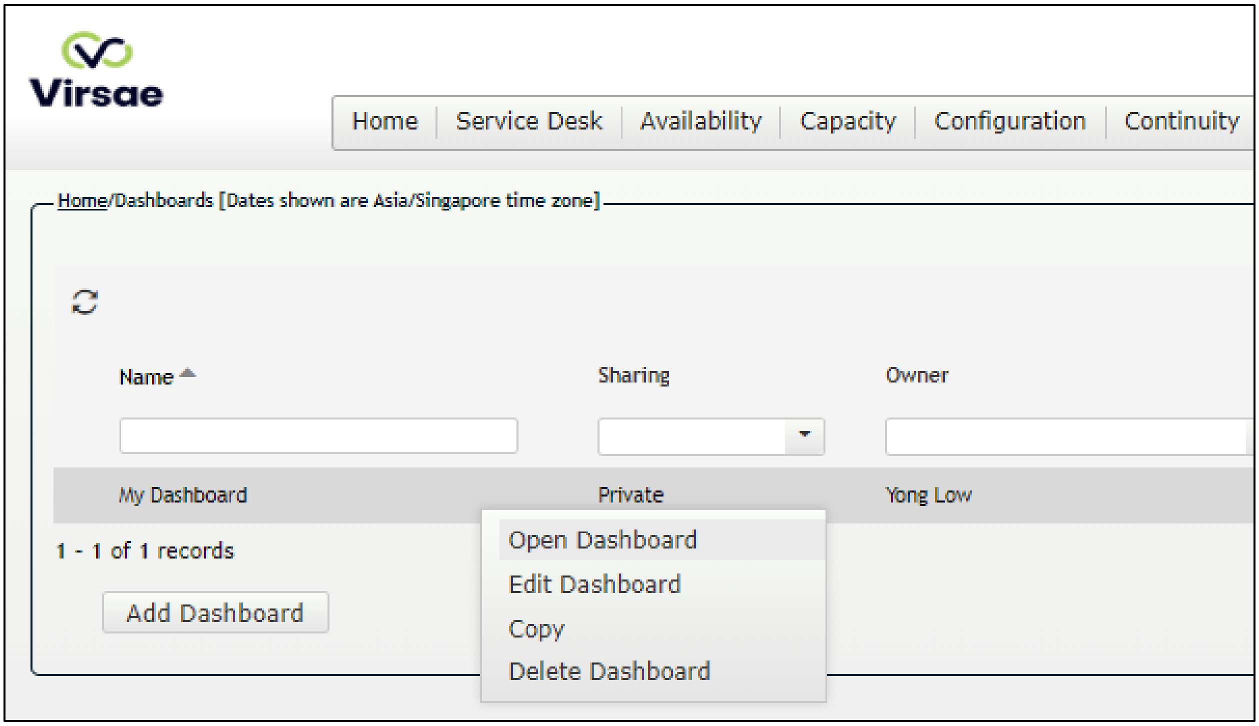
Avg Ping
3 ms

Loss
0 %

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Breeze 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 → Dashboards** (not shown) and the screen is shown as below. Right click "My Dashboard" and select "Open Dashboard".

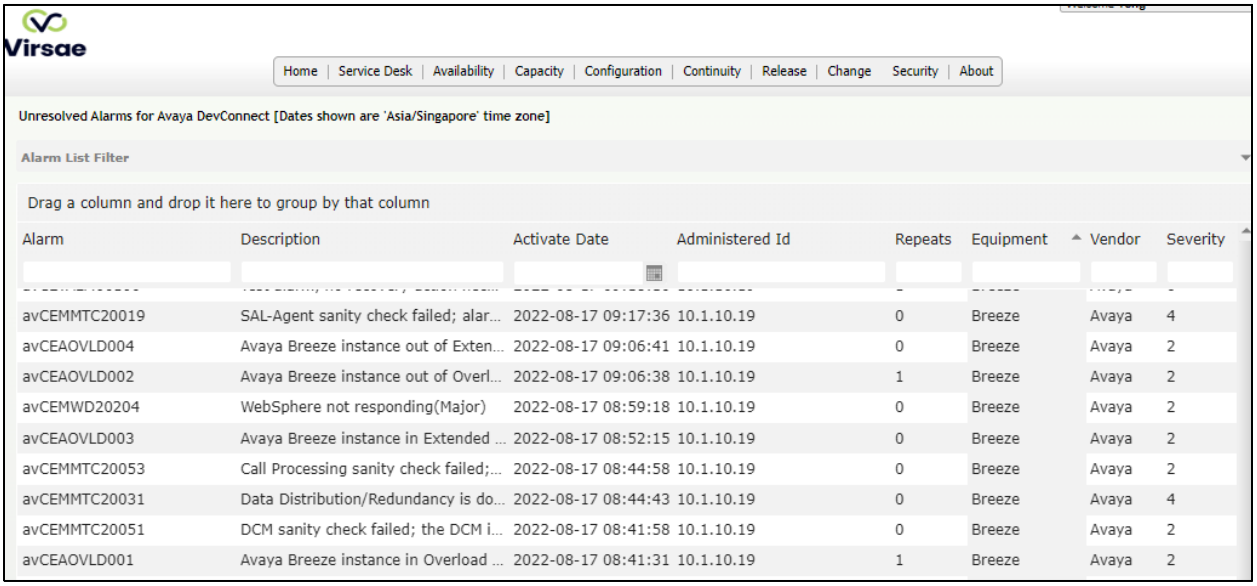


Name	Sharing	Owner
My Dashboard	Private	Yong Low

1 - 1 of 1 records

Whatever is configured during setup will be shown here. However, if the dashboard is configured to open automatically on startup in **Section 6.3**, once logged in, all the dashboards last configured at the end of **Section 6.3** will be populated in a new tab on the browser.

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


Virsae
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | About
Alarm List Filter
Drag a column and drop it here to group by that column

Unresolved Alarms for Avaya DevConnect [Dates shown are 'Asia/Singapore' time zone]

Alarm	Description	Activate Date	Administered Id	Repeats	Equipment	Vendor	Severity
avCEMMTC20019	SAL-Agent sanity check failed; alar...	2022-08-17 09:17:36	10.1.10.19	0	Breeze	Avaya	4
avCEAOVLD004	Avaya Breeze instance out of Exten...	2022-08-17 09:06:41	10.1.10.19	0	Breeze	Avaya	2
avCEAOVLD002	Avaya Breeze instance out of Overl...	2022-08-17 09:06:38	10.1.10.19	1	Breeze	Avaya	2
avCEMWD20204	WebSphere not responding(Major)	2022-08-17 08:59:18	10.1.10.19	0	Breeze	Avaya	2
avCEAOVLD003	Avaya Breeze instance in Extended ...	2022-08-17 08:52:15	10.1.10.19	0	Breeze	Avaya	2
avCEMMTC20053	Call Processing sanity check failed;...	2022-08-17 08:44:58	10.1.10.19	0	Breeze	Avaya	2
avCEMMTC20031	Data Distribution/Redundancy is do...	2022-08-17 08:44:43	10.1.10.19	0	Breeze	Avaya	4
avCEMMTC20051	DCM sanity check failed; the DCM i...	2022-08-17 08:41:58	10.1.10.19	0	Breeze	Avaya	2
avCEAOVLD001	Avaya Breeze instance in Overload ...	2022-08-17 08:41:31	10.1.10.19	1	Breeze	Avaya	2

8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R174 to interoperate with Avaya Breeze 3.8. During compliance testing, all test cases were completed successfully.

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 Breeze® platform,* Release 3.8.1, Issue 2, Nov 2021.
2. *Administering Avaya Breeze® platform*, Release 3.8.1, Issue 3, Nov 2021.
3. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 10.1, Issue 2, Mar 2022.
4. *Administering Avaya Aura® System Manager*, Release 10.1, Issue 3, Feb 2022.

Product documentation for Virsae products may be found at https://documentation.virsae.com.

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.