Product Support Notice

PSN #	PSN027036u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 16-May-16. This is Issue #3, published date: 03-July-18.	Severity/risk level	Low	Urgency	Optional

Name of problem	PSN027036u – Limited use of VMware vSphere™ Client with Avaya Aura® Appliance Virtualization Platform

Products affected

Avaya Aura® Appliance Virtualization Platform 7.0.x – 8.0.x

Problem description

Solution Deployment Manager is the application that should be used when deploying Avaya applications onto Avaya Aura® Appliance Virtualization Platform (AVP).

However, there are some very limited troubleshooting and configuration cases where the VMware vSphere™ Client (for AVP 7.0.x) or the VMware Embedded Host Client can be utilized by people already experienced with those tools. These are limited to the following:

- Virtual console access is required to a VM for advanced trouble shooting:
  - A VM does not respond to pings or SSH after booting
    - The VM has a boot issue, it may be possible to connect to the console and resolve this issue, allowing the VM to boot normally, one example of this is if file system corruption is detected and a fsck needs permission to run
    - The VM has become incorrectly IP addressed. If the VM is not correctly addressed for its network, SDM will be unable to connect. It may be possible to console connect to a VM and use CLI networking commands to recover the VM to its correct IP address settings.
- Virtual console access is required for IP address changes for Session Manager or Avaya Aura Breeze:
  - IP address changes that require VM console access:
    - Changing the IP address of Session Manager or Avaya Aura Breeze (aka EDP). Currently Session Manager and Avaya Aura Breeze require console access when changing the IP address of the VM. After the IP address of the application is changed the IP address/FQDN value should be updated in the SDM local inventory.

  NOTE: This IP change process is not required for a new VM deployment, this is only required if you need to change the IP address after deployment, for example, if the server was staged with generic IP addresses, this is a ME 6.x migration to Avaya Aura® 7.x using pre-staged disks or the customer has decided to change the IP address of the system.

Critical Notes:

- Incorrect use of VMware vSphere™ Client or the Embedded Host Client with AVP may create deployment, networking or performance issues on the system. Only experienced technicians should use VMware vSphere™ Client or the Embedded Host Client with AVP and only in the way outlined in this PSN.
- Only the SDM client or SDM in Avaya Aura® System Manager should be used for deployment. The following is done automatically when deploying with SDM onto AVP:
  - CPU and Memory reservations for the VM will be automatically sized correctly for the Server
  - VM hard disk will be correctly sized if applicable
  - VM networking will be automatically configured
  - Correct VM disk format will be selected
  - A static route for the Services Port will be added to the VM
  - The VM will be registered to the Utility Services VM for Services Port connection
  - Will ensure Utility Services is present for security and alarm forwarding for the server
  - The VM will be set to automatically power on when the AVP server boots and automatically shutdown when the AVP server is shutdown

  The VMware vSphere™ Client or Embedded Host Client will not do the above so should not be used for deploying applications onto AVP. Use of VMware vSphere™ Client or Embedded Host Client for deployment may result in an unsupported configuration.
- Avaya does not provide support for the VMware vSphere™ Client or the Embedded Host Client
- With AVP, the following settings must not be changed on the host. AVP runs specific hypervisor and network settings to ensure the correct operation of the Avaya system. Changing settings on the hypervisor may result in the system experiencing issues and a re-installation being required. Settings that can normally be changed on VMware ESXi™ should not be change on AVP systems. Settings that should not be changed include:
  - Hypervisor Network or VM Network configuration
  - VM settings including CPU and Memory reservations

- If you do not wish to use the VMware vSphere™ Client or the Embedded Host Client in the cases mentioned in this document, contact Avaya Services for resolution of the issue of the Avaya application.

The Resolution section of this PSN also includes some additional troubleshooting tips.

Resolution

The VMware Embedded Host Client (AVP 7.1.x and higher)

Logon to the AVP host using the VMware Embedded Host Client via a web browser.

Use the local management IP address of the AVP host in the following URL: https://<AVP host IP address>/ui

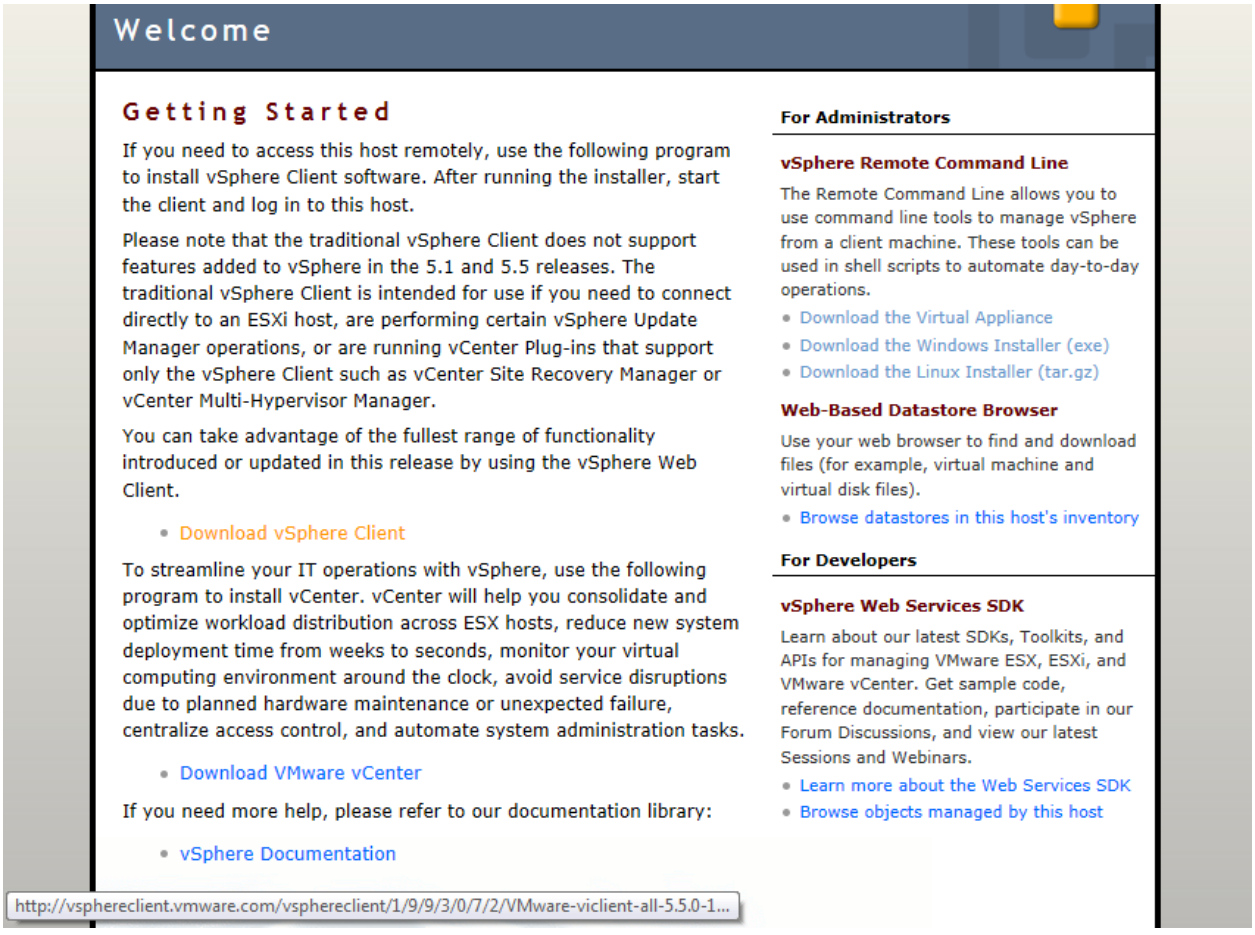
Installing the VMware vSphere™ Client (AVP 7.0.x only)

VMware vSphere™ Client 5.5 supported Operating Systems includes the following:

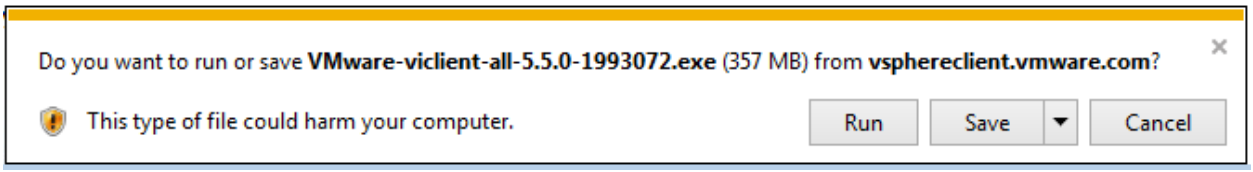
- Microsoft Windows 8.1 (32-bit and 64-bit)
- Microsoft Windows 8 (32-bit and 64-bit)
- Microsoft Windows 7 Service Pack 1 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows Server 2012 R2 64-bit
- Microsoft Windows Server 2012 64-bit
- Microsoft Windows Server 2008 Service Pack 2 (32-bit and 64-bit)
- Microsoft Windows Server 2008 R2 Service Pack 1 64-bit
- Microsoft Windows Server 2008 R2 64-bit

Using a web browser, browse to the AVP IP address and accept any security warnings.

The following page will display:



If you are connected to the internet from the computer viewing the web page you will be prompted to download the VMware vSphere™ Client 5.5 exe file.



If your PC is not connected to the Internet cut and paste the shortcut to the computer that is connected to the internet and download the file.

Copy the file to the PC where VMware vSphere™ Client is to be installed.

NOTE: None of the other links are supported with AVP. They must not be used and attempted use of them may place the AVP system into an unsupported state.

Select Save and download the file.

Minimum installation requirements are list in the following VMware knowledge base article

https://kb.vmware.com/kb/2005083

Right click on the VMware vSphere™ Client executable and run the file as administrator.

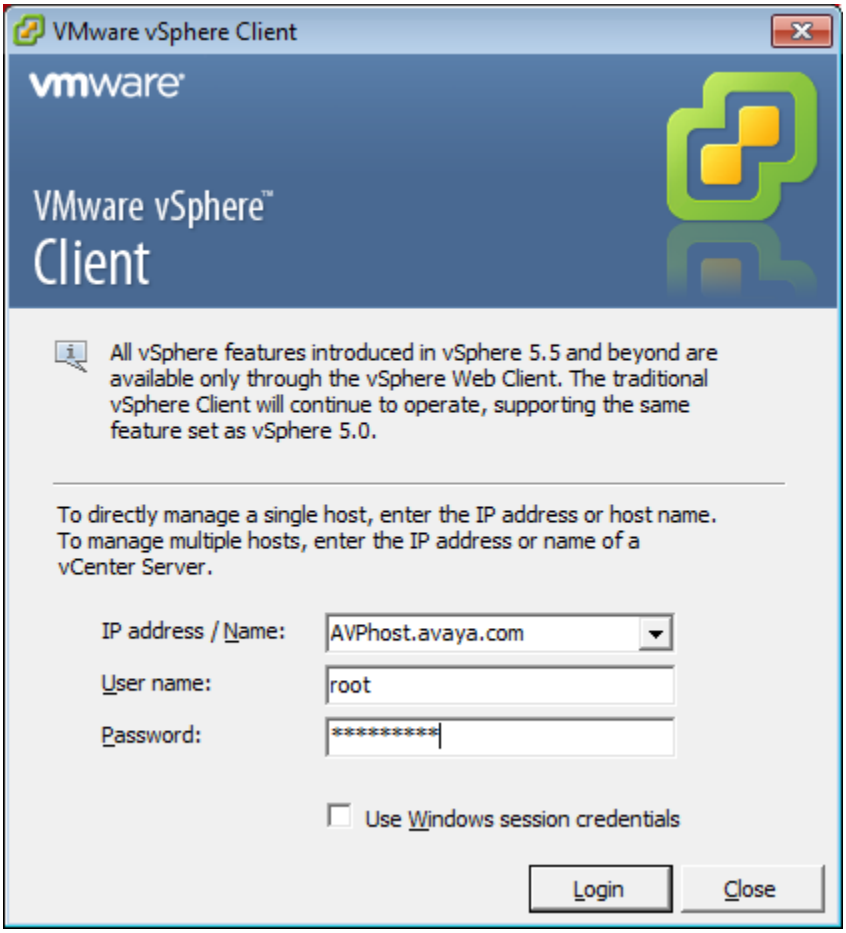
Accept the options presented in the VMware EULA and click install.

The installation will proceed to install the VMware vSphere™ Client.

Launch the VMware vSphere™ Client.

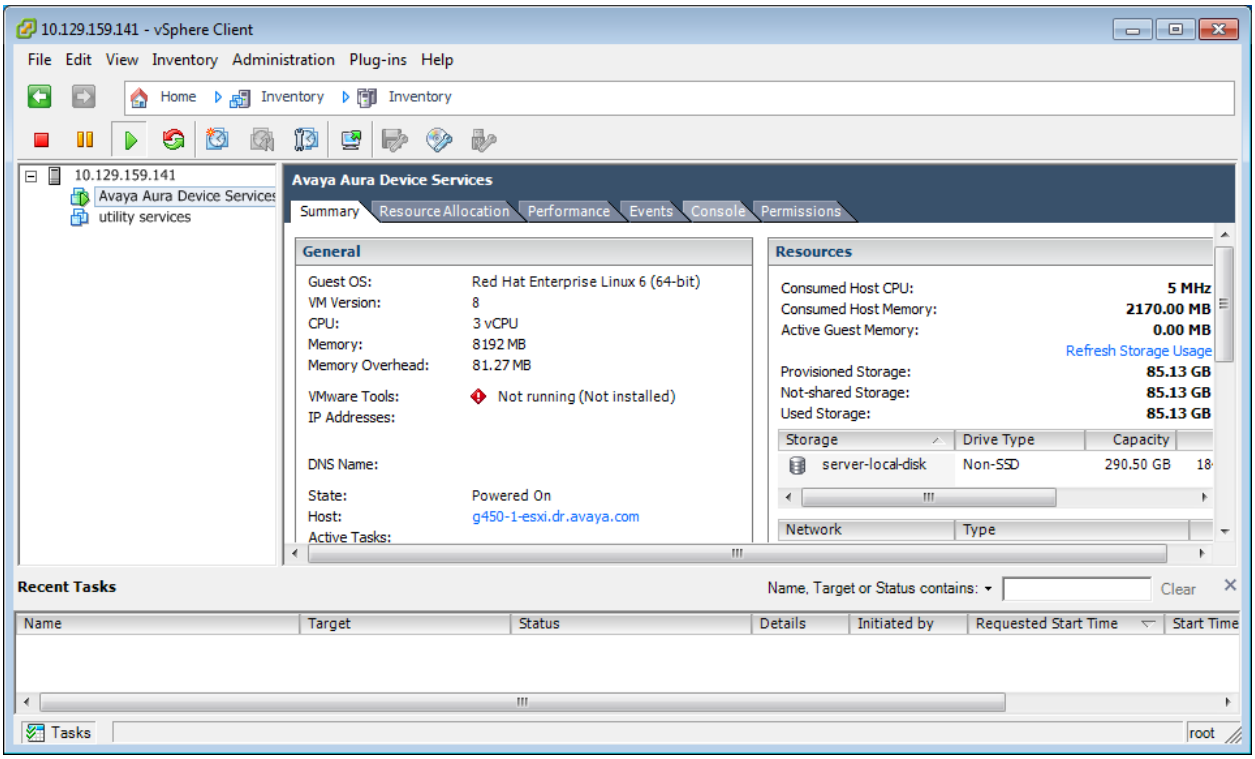
Enter the IP address or Fully Qualified Domain Name (FQDN) of the AVP host you wish to connect to.

Enter the root username and root password to access the system.



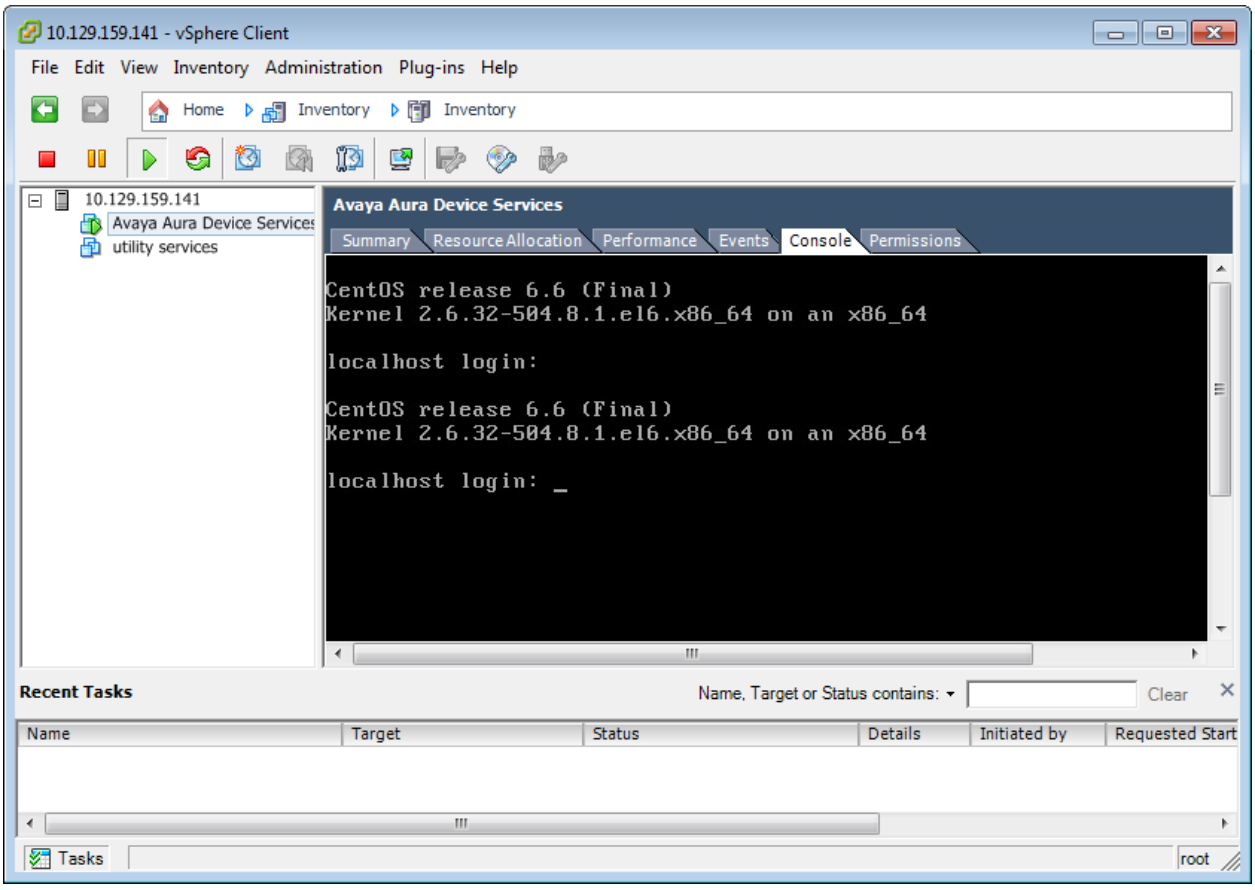
Click login

The main VMware vSphere™ Client window will launch.



Select the VM you wish to console to from the menu on the left of the screen and then click the virtual console tab. Click inside the console window to activate the console.

You may need to press enter or space for the console to activate. You are now connected to the virtual console of the VM.



Troubleshoot the VM as directed by the documentation relating to the VM.

After you have finished on the console press “alt + ctrl” to exit the window and release the mouse pointer.

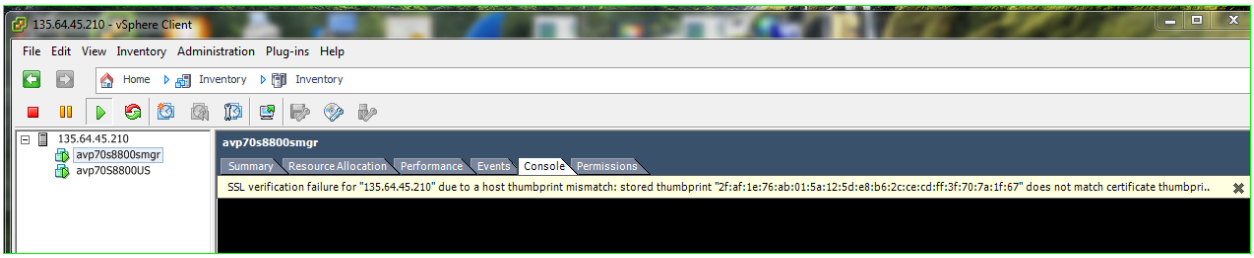
Close VMware vSphere™ Client window.

Additional Troubleshooting tips

If you suspect a system does not have the VMs registered correctly to Utility Services or the Services Port is not working correctly to the VM, use SDM in System Manager to refresh the static route under the host table for the VMs following this process:

- “Refresh VM” on US using SDM UI
- “Update static route” on the VM using SDM UI.

NOTE: if you see a SSL verification failure on the VMware vSphere™ Client console on AVP, this is because SDM has updated the host certificate and the host needs a reboot to pick up the new certificate for the virtual console. A host reboot would be service affecting and applications on the host should be shutdown gracefully prior to the system being rebooted.



Services Port operation:

On AVP server NIC 2 (Eth1) is addressed as 192.168.13.6, and Utility Services will be addressed 192.11.13.6 on the same port.
A laptop addressed as 192.11.13.5 255.255.255.252 with default gateway of 192.11.13.6, can connect to the Utility Services IP address.

The Services Port hypervisor address 192.168.13.6 can also be reached from the Laptop in the 192.11.13.5 address as the hypervisor has routing for that network also. The public address AVP cannot be reached from 192.11.13.5 and the static services port IP address should be used to connect to the hypervisor from the Services port.

Logging into Utility Services IP forwarding can be turned on and the management interfaces of the other applications can be displayed.

These IP addresses can be connected to from the Services Port IP address 192.11.13.5 because the VM has been deployed with a static route pointing the Services Port traffic through Utility Services. (Traffic only passes through Utility Services when IP forwarding is enabled, in normal operation IP forwarding should be de-activated).

If the VMs are not deployed with SDM or SDM client the static route will not be added to the VM or registered with Utility Services and the Services Port will not be able to contact the VM.

If CM is 10.10.10.5 and Utility Services is 10.10.10.2 on the customer network the following is the traffic from the laptop

Traffic path to and from the laptop to Communication Manager:

The laptop network port is configured with the IP settings of 192.11.13.5 255.255.255.252 with a default gateway of 192.11.13.6 (Utility Services).

Traffic destined for Communication Manager (10.10.10.5) will be passed to the default gateway of Utility Services.

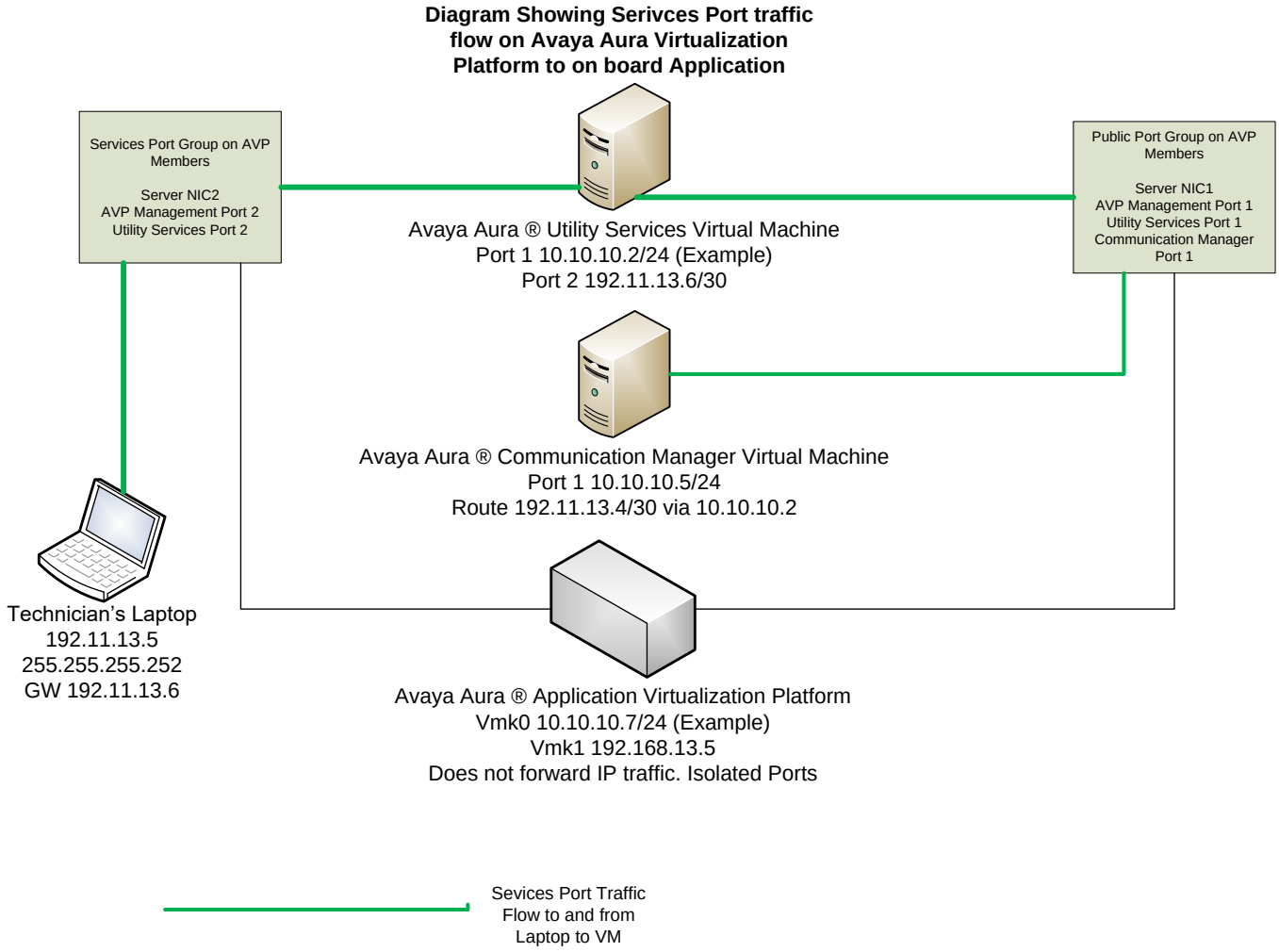
Utility Services will have an interface on the public network of 10.10.10.2 and (when IP forwarding is on) send the packet to 10.10.10.5 (Communication Manager).

When Communication Manager goes to reply to the packet from the laptop it will look in its routing table for 192.11.13.4 network to communication to the 192.11.13.5 address of the laptop.

CM will have a static route pointing 192.11.13.4/30 network traffic to Utility Services (10.10.10.2).

Utility Services will take the packet and forward it from its 192.11.13.6 address to the laptop and the network connection is complete.

If the VM does not have the static route added at deployment the return packet for 192.11.13.5 will go out into the customer network and never reach the laptop. Network connection will not be established.



Workaround or alternative remediation

N/A

Remarks

Issue 2: Added bullet for VM to auto power on/off when AVP server boots/shuts down when deploying with SDM onto AVP.
Issue 3: Added VMware Embedded Host references and updated to include AVP 7.0.x – 8.0.x

Patch Notes

N/A

Backup before applying the patch	
N/A	
Download	
N/A	
Patch install instructions	Service-interrupting?
N/A	No
Verification	
N/A	
Failure	
N/A	
Patch uninstall instructions	
N/A	

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks
N/A
Avaya Security Vulnerability Classification
N/A
Mitigation
N/A

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686