Oracle® SD-WAN Edge

Virtual Appliance Installation Guide

Release 9.1
F38218-06
July 2022

ORACLE

Oracle SD-WAN Edge Virtual Appliance Installation Guide, Release 9.1

F38218-06

Contents

About This Guide

The purpose of this document is to provide an understanding of how to install a Virtual Appliance on a supported hypervisor.

Documentation Set

The following table lists related documentation.

Document Name	Document Description
Oracle SD-WAN Edge Release Notes	Contains information about added features, resolved issues, requirements for use, and known issues in the latest Oracle SD-WAN Edge release.
Oracle SD-WAN OS Release Notes and Upgrade Guide	Contains information about inserting an OS Partition Image or OS Patch on an appliance in order to migrate to a new OS version or apply fixes to an existing version.
Oracle SD-WAN Security Guide	Contains information about security methods within the Oracle SD-WAN solution.
Oracle SD-WAN Edge Features Guide	Contains feature descriptions and procedures for all incremental releases of Oracle SD-WAN Edge. This guide is organized by release version.
Oracle SD-WAN Edge High Availability Guide	Contains information about implementing High Availability, as well as deployments and configuration.
Oracle SD-WAN Edge Virtual Appliance Installation Guide	Contains information about how to install a Virtual Appliance on a supported hypervisor.
Oracle SD-WAN Edge Service Chaining Guide	Contains information about installing a Guest Virtual Machine using the Service Chaining UI.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select `2` for New Service Request.
2. Select `3` for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select `1`.

- For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Click the **Oracle Communications** link.
   Under the **SD-WAN** header, select a product.
4. Select the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Revision History

The following table provides the revision history for this document.

Date	Description
April 2021	• Initial release.
May 2021	• Updates Microsoft Azure and OCI IaaS topics with updated first-time login instructions.
June 2021	• Removes the bullet from the "WAN Deployment with a Virtual Appliance" topic that stated High Availability is not supported. • Updates the table in the "Virtual Machine Performance Specifications" topic for accuracy.
March 2022	• Removes the "OCI IaaS Configuration" topic from the Virtual Talari Appliance Installation chapter and adds the "Install SD-WAN Edge from the Oracle Cloud Marketplace" topic.
July 2022	• Updates the OCI specifications in the "Public Cloud Specifications" table in the "Virtual Machine Performance Specifications" topic.

1

Introduction

Oracle SD-WAN Edge for virtual environments has two download packages. The VT800 package supports up to 32 devices as a Network Controller Node (NCN). The VT800-128 package supports up to 128 devices as a NCN.

Multiple Virtual Appliance VMs can be supported on a single, physical platform, provided each VM is supplied with sufficient dedicated resources.

The following requirements are per Virtual Appliance VM depending on the appliance model and installed license.

Supported Environments

	VMware ESXi	Microsoft Hyper-V	OCI	Microsoft Azure	KVM
Software Version	6.5 or higher	Windows Server 2012 R2 or higher	VM.Standard.2.4 or higher	DS13 v2 or higher, Disk: P10 or higher	qemu-kvm-1.5.3-167.el7 or higher
CPU Requirements	64 Bit, 2.1GHz or better, AES-NI, Intel Xeon Skylake CPUs or better	64 Bit, 2.1 GHz or better, AES-NI, Intel Xeon Skylake CPU's or better	Refer to VM.Standard.2.4 specifications	Refer to DS13 v2 specifications	64 Bit, 2.2 GHz or better, AES-NI, Intel Xeon Skylake, Intel Atom Denverton CPU's or better

> **Note:**
>
> Environments suggested above denote minimum recommended configurations. Any configurations that does not meet these requirements is NOT supported. Please refer to Virtual Machine Performance Specifications and Public Cloud Performance Specifications for details.

Virtual Machine Performance Specifications

The following table lists the performance specifications for supported virtual machines.

Platform	Appliance Model	Max Performance Levels	Dedicated VCPUs	RAM	Minimum Processor Ghz
Hyper-V	VT800	20 Mbps	4	8 GB	2.10 Ghz
Hyper-V	VT800	200 Mbps	10	10 GB	2.10 Ghz
Hyper-V	VT800-128	200 Mbps	10	32 GB	2.10 Ghz

Platform	Appliance Model	Max Performance Levels	Dedicated VCPUs	RAM	Minimum Processor Ghz
ESXi	VT800	20 Mbps	4	4 GB	2.10 Ghz [1]
ESXi	VT800	1 Gbps	8	16 GB	2.10 Ghz [1]
ESXi	VT800-128	1 Gbps	8	32 GB	2.10 Ghz [1]
ESXi	VT800-128	2 Gbps	14	32 GB	2.10 Ghz [1]
KVM	VT800	100 Mbps	4	4 GB	2.20 Ghz [2]
KVM	VT800	400 Mbps	8	8 GB	2.20 Ghz [3]
KVM	VT800	1 Gbps	8	16 GB	2.30 Ghz [4]
KVM	VT800	2.5 Gbps	16	16 GB	2.30 Ghz [5]

Note:

[1] For performance levels up to 1 Gbps with ESXi, Intel Silver 4114 or better is required.

Note:

[2] For performance level for 100 Mbps with KVM, Intel Atom Denverton C3558 or better is required.

Note:

[3] For performance level for 400 Mbps with KVM, Intel Atom Denverton C3758 or better is required.

Note:

[4]
For performance levels above 400 Mbps and up to 1 Gbps with KVM, Intel Silver 4114 or better is required.

Note:

[5] For performance levels above 1 Gbps and up to 2.5 Gbps with KVM, Intel Gold 5218 or better is required/

Table 1-1 Public Cloud Specifications

Platform	Appliance Model	License Level	Dedicated VCPUs	RAM	Minimum Processor Ghz	Instance Type
Azure	VT800	500 Mbps	8	56 GB	2.4 Ghz	DS13 v2
Azure	VT800-128	500 Mbps	8	56 GB	2.4 Ghz	DS13 v2
OCI	VT800	1 Gbps	16	120 GB	2.0 Ghz	VM.Standard2.8
OCI	VT800-128	1 Gbps	16	120 GB	2.0 Ghz	VM.Standard2.8
OCI Note: The information in this row applies to the R9.1.1.1.0 patch and newer.	VT800	3 Gbps	16	112 GB	3.0 Ghz	VM.Optimzed3
OCI Note: The information in this row applies to the R9.1.1.1.0 patch and newer.	VT800-128	3 Gbps	16	112 GB	3.0 Ghz	VM.Optimzed3

Configuration Guidelines and Caveats

- Oracle recommends Directly Attached Storage (DAS) for all Virtual Appliances.
- Storage requirements for a virtual appliance depend on its role and the functions supported. The following list shows minimum disk space requirements:
  - Edge software as a Client without WAN Op – 40 GB
  - Edge software as an NCN without WAN Op – 100 GB
  - Edge software as a Client with WAN Op – 120 GB
  - Edge software as an NCN with WAN Op – 180 GB
- **Note:**

  The preceding space requirements do not include the host OS and hypervisor space requirements.
- ESXi and Hyper-V Virtual instances require at least 1 shared or dedicated management interface.
- KVM based environments require a dedicated management interface.
- Virtual Appliances require at least 1 dedicated, but not more than 7 total, non-management network interfaces.

- Virtual Appliances require CPU's, RAM and disk resource to be dedicated for those instances only.
- Virtual Appliances deployed without dedicated (pinned) resources is not supported.
- Virtual Appliances must be allocated with pinned CPU resources from same NUMA node to achieve the performance levels you want.
- Intel Atom CPU-based virtual instances are not supported as NCN.
- Service chaining Oracle SD-WAN virtual instances with other products is not supported, unless preapproved by Oracle.
- Any configurations with performance levels below 500 Mbps are not supported as NCN.
- All Virtual Deployments must adhere to the configurations and optimizations specified in the *Virtual Appliance Installation Guide*. Oracle does not support configurations that deviate from the installation guide.

Upgrading from VT800 to VT800-128

An existing VT800 instance cannot be converted directly into a VT800-128. To upgrade a site from a VT800 to a VT800-128, deploy a new virtual appliance and cut over when ready, as with hardware appliance upgrades.

WAN Optimization System Specifications

WAN Optimization is supported on VT800s running Edge 7.3 P3 or above and VT800-128s running Edge 7.3 P4 or above at the following levels with the specified resources.

> **Note:**
>
> For Disk size recommendations please refer to the "Configuration Guidelines and Caveats" section in "Virtual Machine Specifications."

Platform	Max Performance Levels	WANOp Capacity	VCPUs	RAM	Max WANOp Sessions	Cloud Instance Type
VMWare ESXi	2 Gbps	200 Mbps	14 (2.10GHz)	16GB (VT800-128: 32GB)	10,000	NA
Microsoft Hyper-V	200 Mbps	100 Mbps	10 (2.10GHz)	10GB	5,000	NA
KVM	1 Gbps	500 Mbps	8 (2.30 GHz)	16 GB	10,000	NA
OCI	1 Gbps	500 Mbps	16 (2 GHz)	60 GB	10,000	VM.Standard.2.8
Microsoft Azure	500 Mbps	100 Mbps	8 (2.4 GHz)	56 GB	16,000	DS13 v2

Support for Virtual Appliances

Before calling or emailing for support, please ensure that your Virtual Appliance deployment matches the above specifications. Configurations outside of this scope cannot be supported.

2

Virtual Appliance Installation

VMware ESXi

Follow these instructions to deploy on VMWare ESXi.

> **Note:**
>
> You must perform the following procedure from a Microsoft Windows environment.

Prerequisites

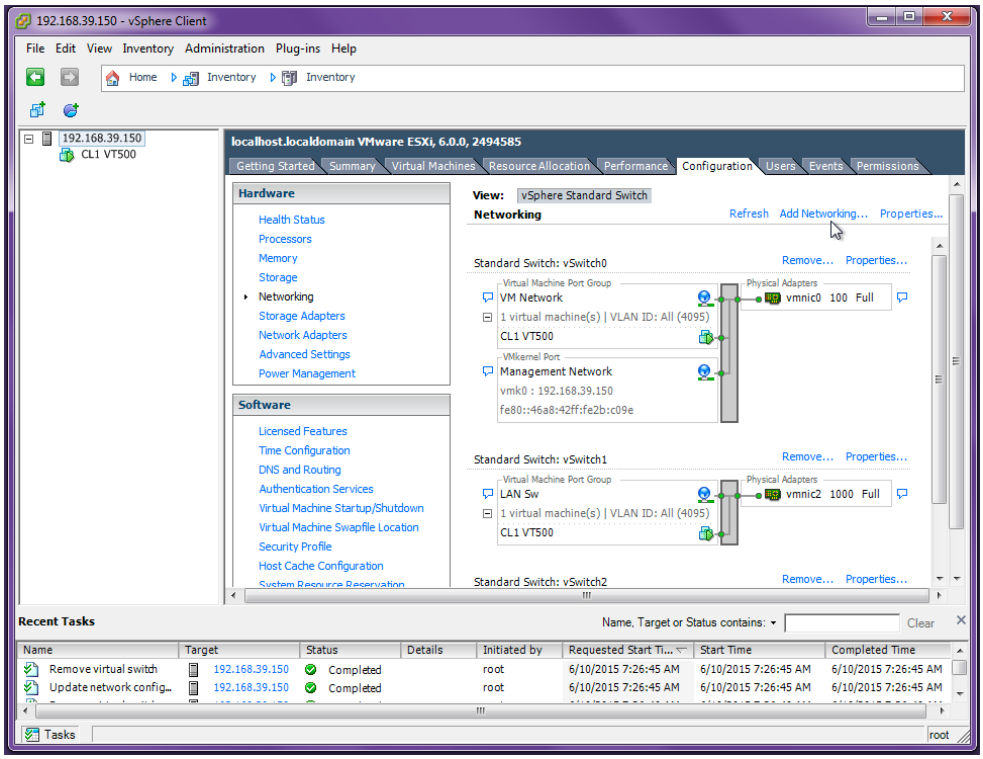
Before deploying on VMWare ESXi, you will need:

- Virtual Image for ESXi
- Full Install for VMWare file for the desired Virtual Appliance
- vSphere client

Prepare to Deploy the Virtual Appliance

1. From the **Inventory** available, click the server's IP address then click the **Configuration** tab.

Figure 2-1 VM Server Configuration Tab

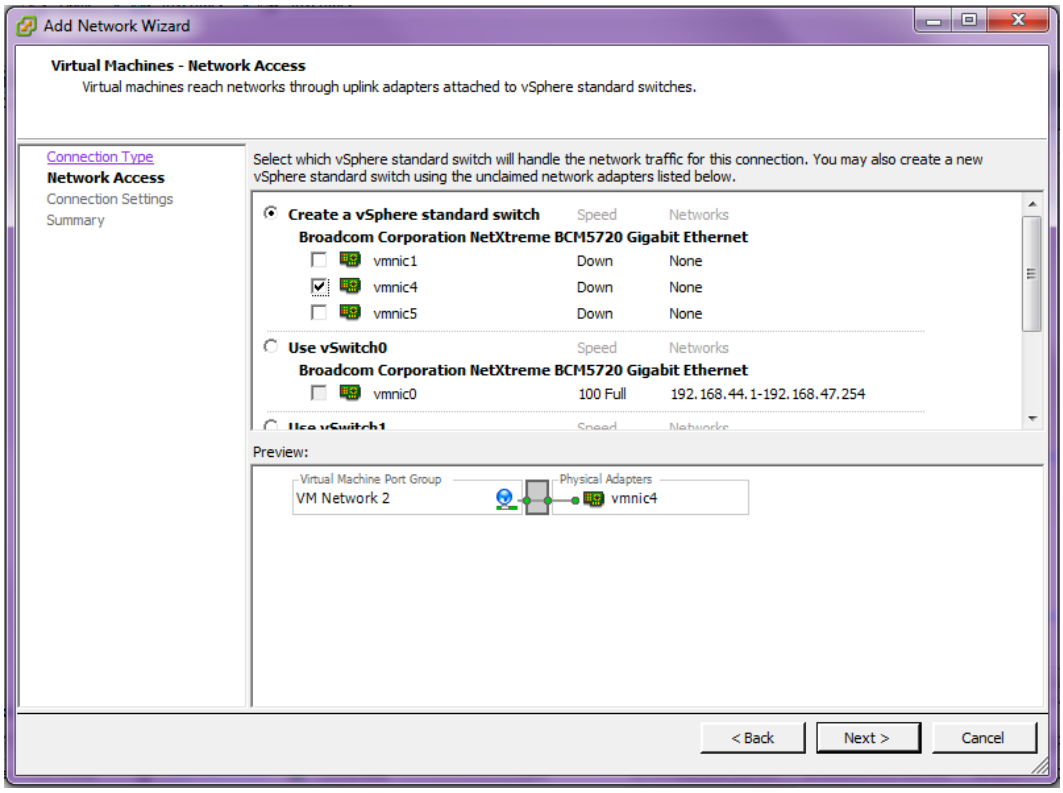


2. Click **Networking** from the left menu then click the **Add Networking…** link.
3. Choose **Virtual Machine** as the **Connection Type** and click **Next**.

> **Note:**
>
> The physical network adapters on the server appliance (vmnic1, vmnic2, etc.) can only be assigned to a single vSphere standard switch. Once a vmnic is assigned to a vSphere standard switch, it will no longer be available when creating a new vSphere standard switch.

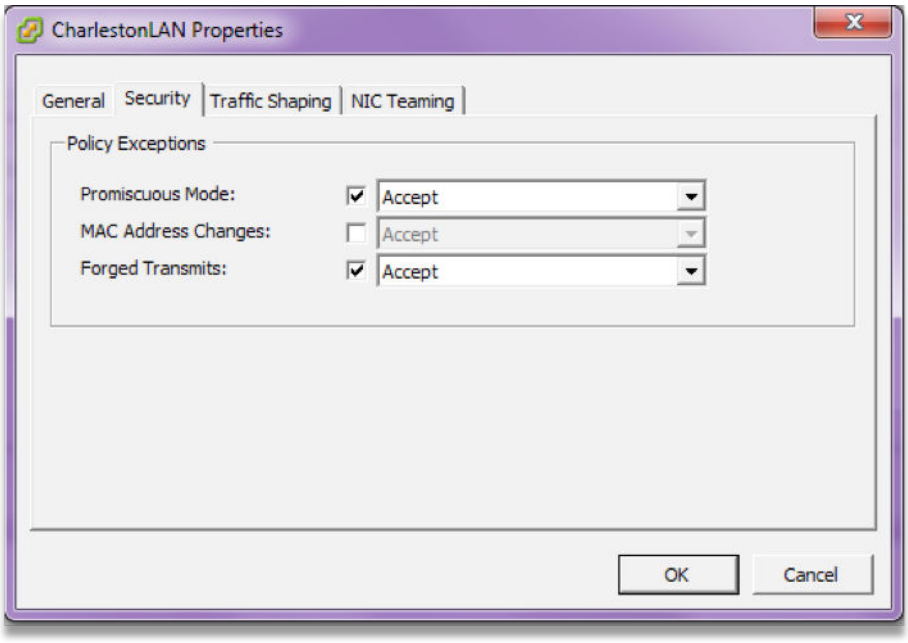
4. Click **Create a vSphere standard switch**, choose one of the available virtual machine NICs, and click **Next**.

Figure 2-2 Create a Switch



5. Give the **Virtual Machine Port Group** for the switch you created in step 4 an appropriate **Network Label**. If VLAN tags will be used on the associated appliance port, set the **VLAN ID** field to **All (4095)**. Click **Next**.
6. Confirm that the information for the new virtual switch is correct then click **Finish**.
7. If this switch will be attached to the appliance management port, skip to step 18. Otherwise, after creating the switch, remain on the Networking panel of the Configuration tab and locate the switch within the panel. You may need to scroll down.
8. Click **Properties...** for the switch. Then, from the **Ports** tab, highlight the **Virtual Machine Port Group** and click **Edit…**
9. On the **Security** tab ensure that **Promiscuous Mode** and **Forged Transmits** are set to **Accept** then click **OK.**

Figure 2-3 Configure Promiscuous Mode



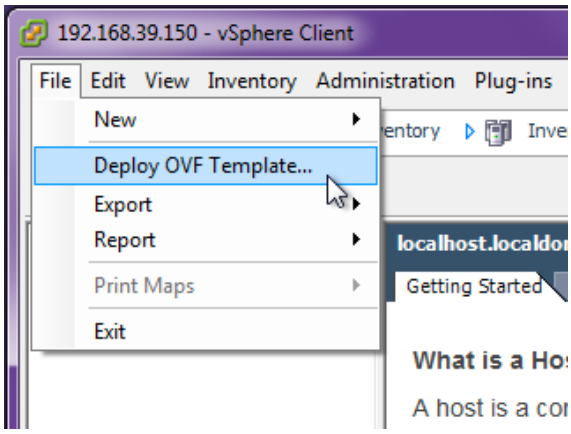
10. Repeat steps 4 through 9 to create a separate virtual switch for each Virtual Appliance port that will be used in your deployment.
11. Repeat steps 4 through 9, and do not choose a virtual machine NIC to create a null virtual switch for Virtual Appliance ports that will not be used in your deployment.

> **Note:**
>
> Virtual Appliances have 7 network ports. All 7 network ports must be assigned to a virtual switch even if you do not intend to use all of them in your deployment. A null virtual switch that is not tied to any physical NIC can be used for this purpose.

Deploy the Virtual Appliance

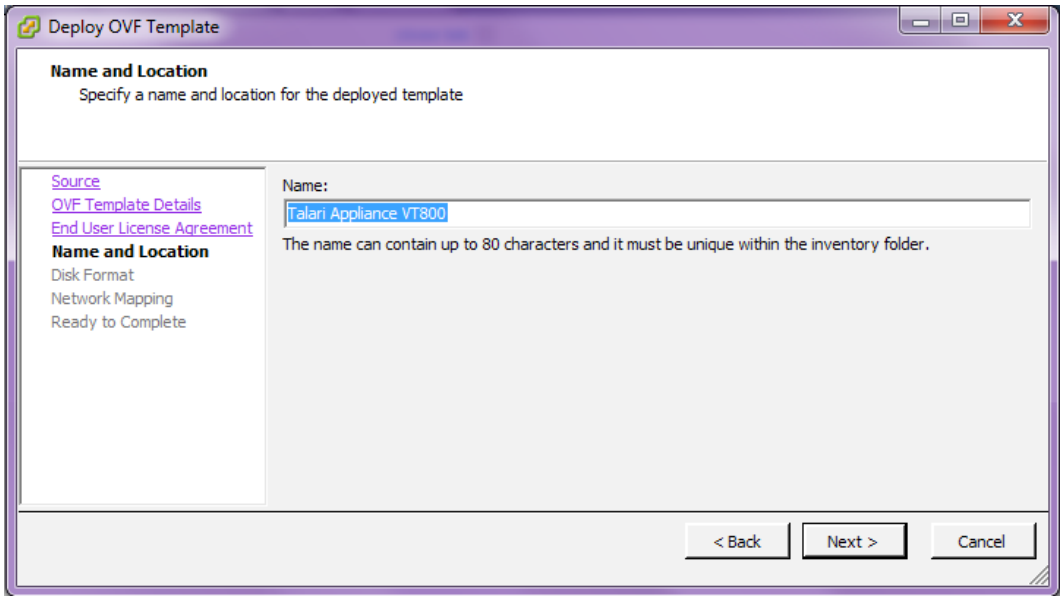
1. Click **File**, **Deploy OVF Template...**

Figure 2-4 Deploy OVF Template



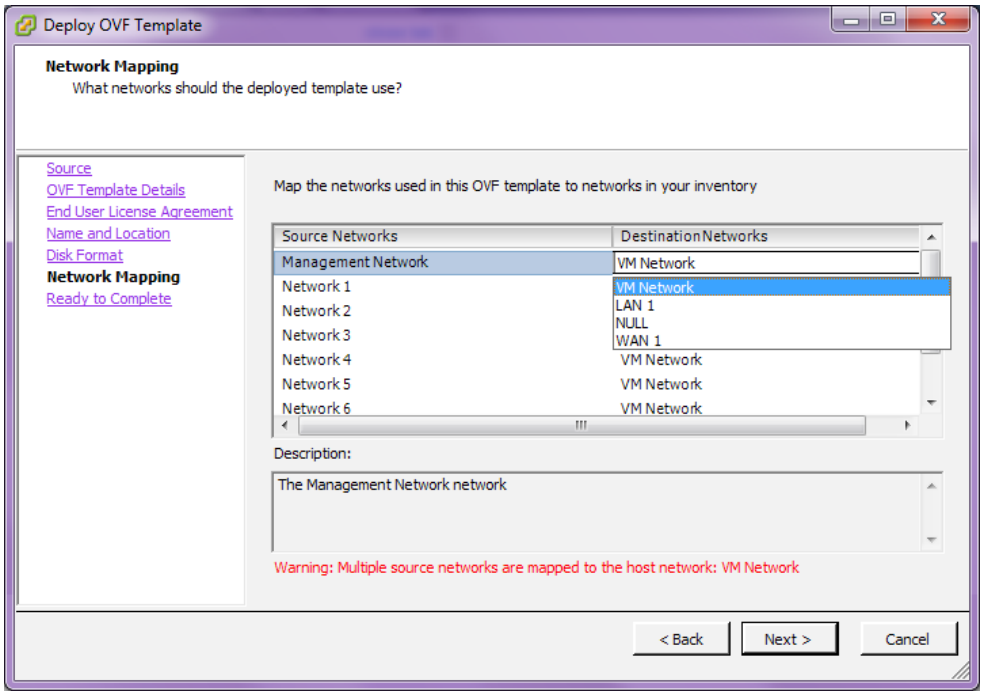
2. **Browse** to the location of the Appliance VM Image (.ova package) that you downloaded. Select the file and click **Open**.
3. Click **Next** and a screen will display information for the VM being imported.
4. Click **Next** and a screen will display the End User License Agreement. After reading, click **Accept** then click **Next**.
5. The **Name and Location** screen displays a default name for the VM. Change the name if desired and click **Next**.

Figure 2-5 Name the VM



6. Accept the default settings on the **Disk Format** screen and click **Next**.
7. On the **Network Mapping** screen, use the drop-down menus under **Destination Networks** to assign the Virtual Appliance ports (**Source Networks**) to the previously configured virtual switch port groups. Any port that will not be used in your deployment must be assigned to the null virtual switch (see step 19 of **Prepare to Deploy the Virtual Appliance)**. Click **Next**.

Figure 2-6 Map Networks from Inventory



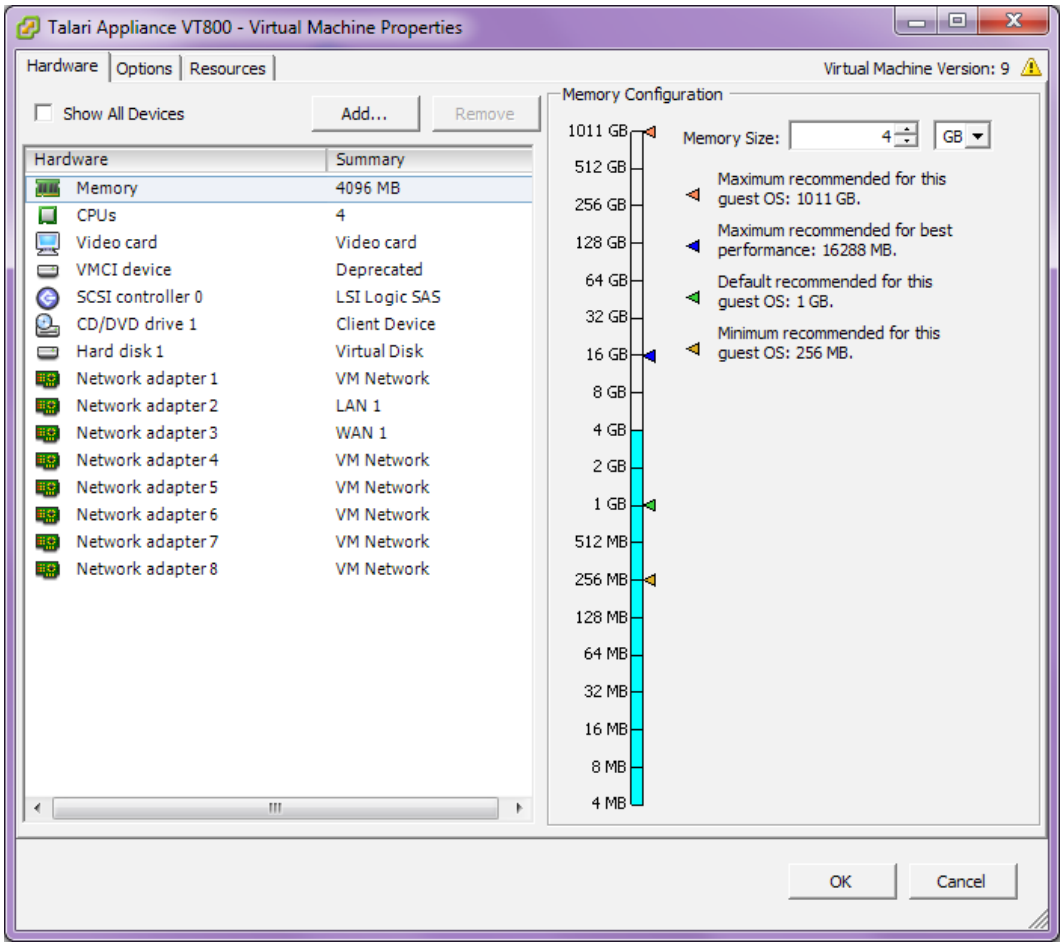
8. Click **Finish** on the **Ready to Complete** screen.

> **Note:**
>
> Decompressing the disk image onto the server could take several minutes.

Configure the Virtual Machine

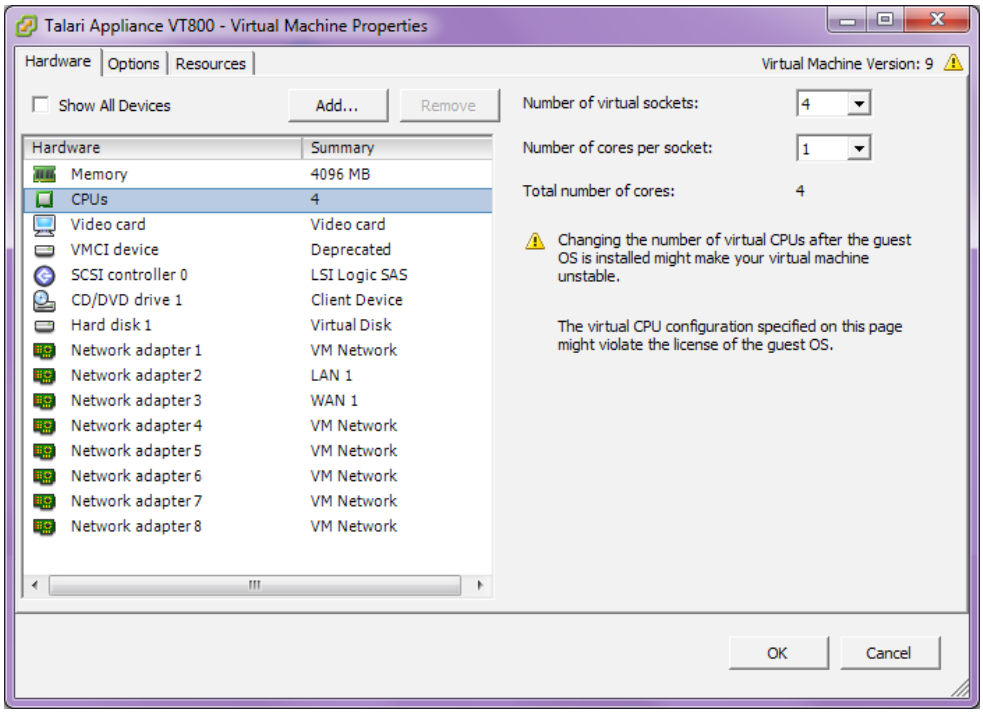
1. If this is the first time you have used the vSphere Client, you may need to click the **Inventory** icon, identify the server, and expand its inventory list.
2. Click the name of your Virtual Appliance's VM in the inventory list.
3. Click the **Summary** tab and click **Edit Settings** underneath the **Commands** section to open the **Virtual Machine Properties** window.
4. Click **Memory** from the **Hardware** tab of the **Virtual Machine Properties** screen and ensure that the required amount of memory is configured for the intended performance level of your Virtual Appliance (see the **Virtual Machine Specifications** section for details).

Figure 2-7 Adjust Memory Size



5. Click **CPUs** from the **Hardware** tab of the **Virtual Machine Properties** screen and ensure that the required number of cores (i.e., Virtual CPUs) is configured for the intended performance level of your Virtual Appliance (see **Virtual Machine Specifications** section for details). You may configure these cores on a single virtual socket or across multiple virtual sockets.

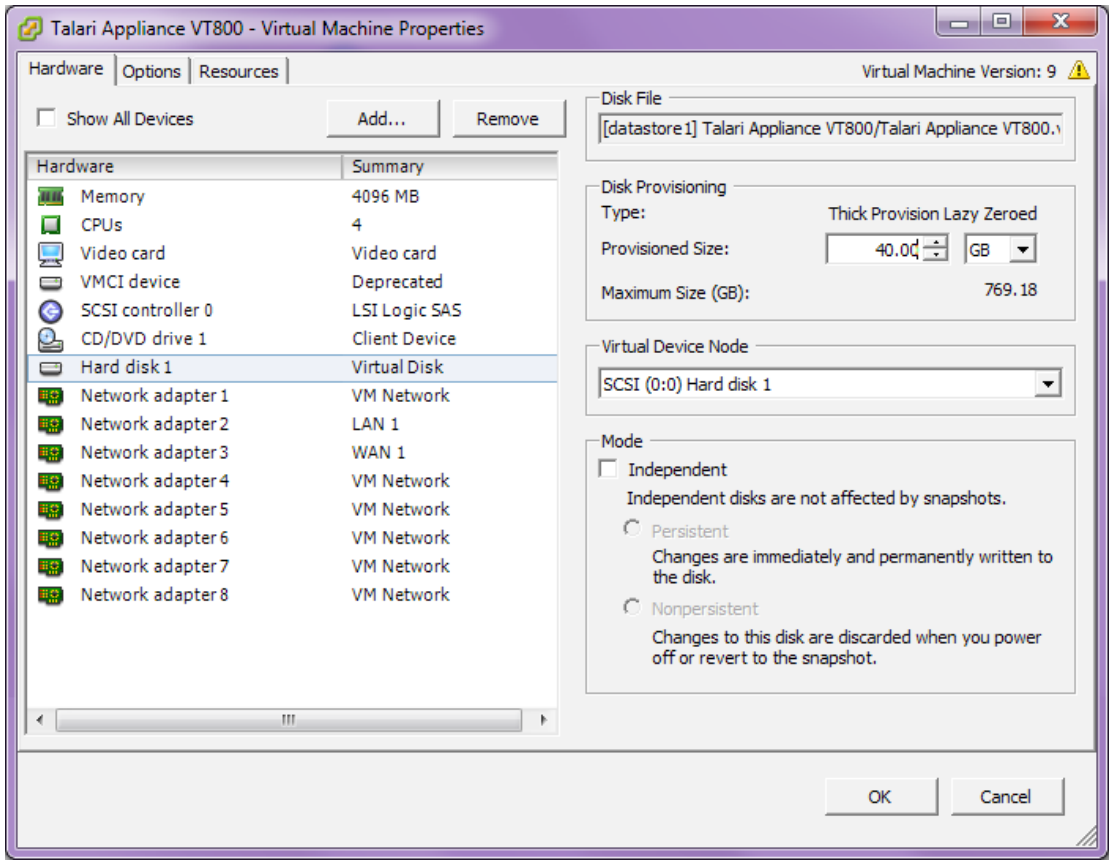
Figure 2-8 Adjust the Number of Sockets and Cores



> **Note:**
>
> The number of virtual sockets should either be 2 or 4, based on the licensed performance from **Virtual Machine Specifications** section. The number of cores per socket must be 1.

6. Click **Hard disk 1** from the **Hardware** tab of the **Virtual Machine Properties** screen and ensure that at least 160GB of storage is configured in the **Provisioned Size** field.

Figure 2-9 Add Hard Disk



Click **OK** to save the changes to the Virtual Appliance and exit the **Virtual Machine Properties** screen.

Start the Virtual Appliance

1. From the inventory list, make sure your new VM is still selected and power it on by clicking the green **Play** icon.
2. Click the **Console** tab in the right hand pane of the vSphere Client screen then click inside the console screen and hit **Enter**.

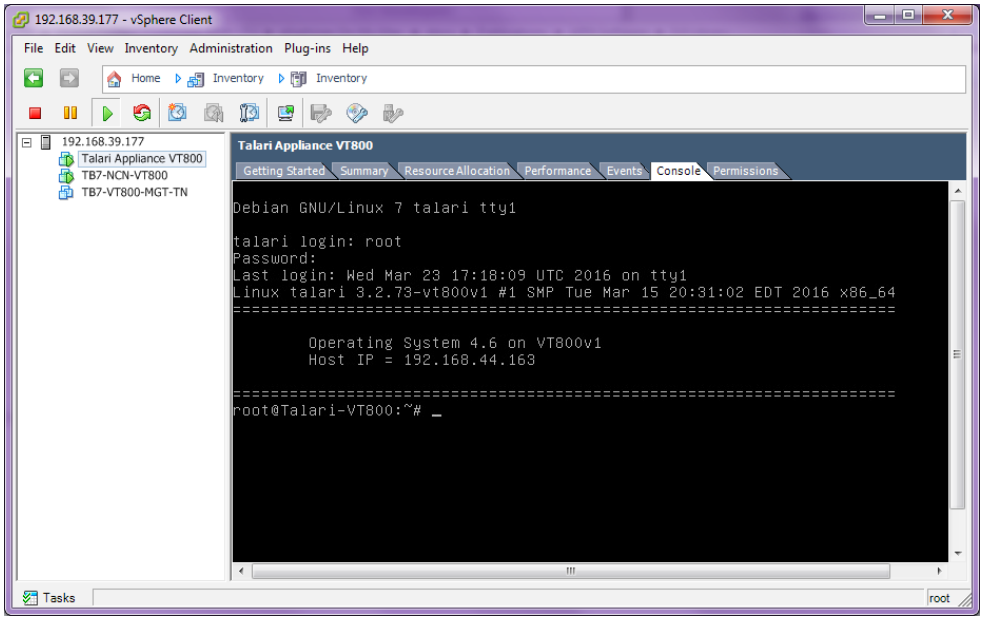
> **Note:**
>
> To exit the console, release the mouse by pressing and holding the **Ctrl** and **Alt** buttons simultaneously.

3. At the **login** prompt enter the following credentials:
   Login: talariuser

   Password: talari
4. The Edge OS level and Host IP are displayed.

> **Note:**
>
> The Virtual Appliance is configured to use DHCP by default. If you want to manually configure the management IP, follow steps 5 through 9; otherwise, take note of the Host IP and skip to **Configure and License the Virtual Appliance**.

Figure 2-10 Virtual Appliance Console Login

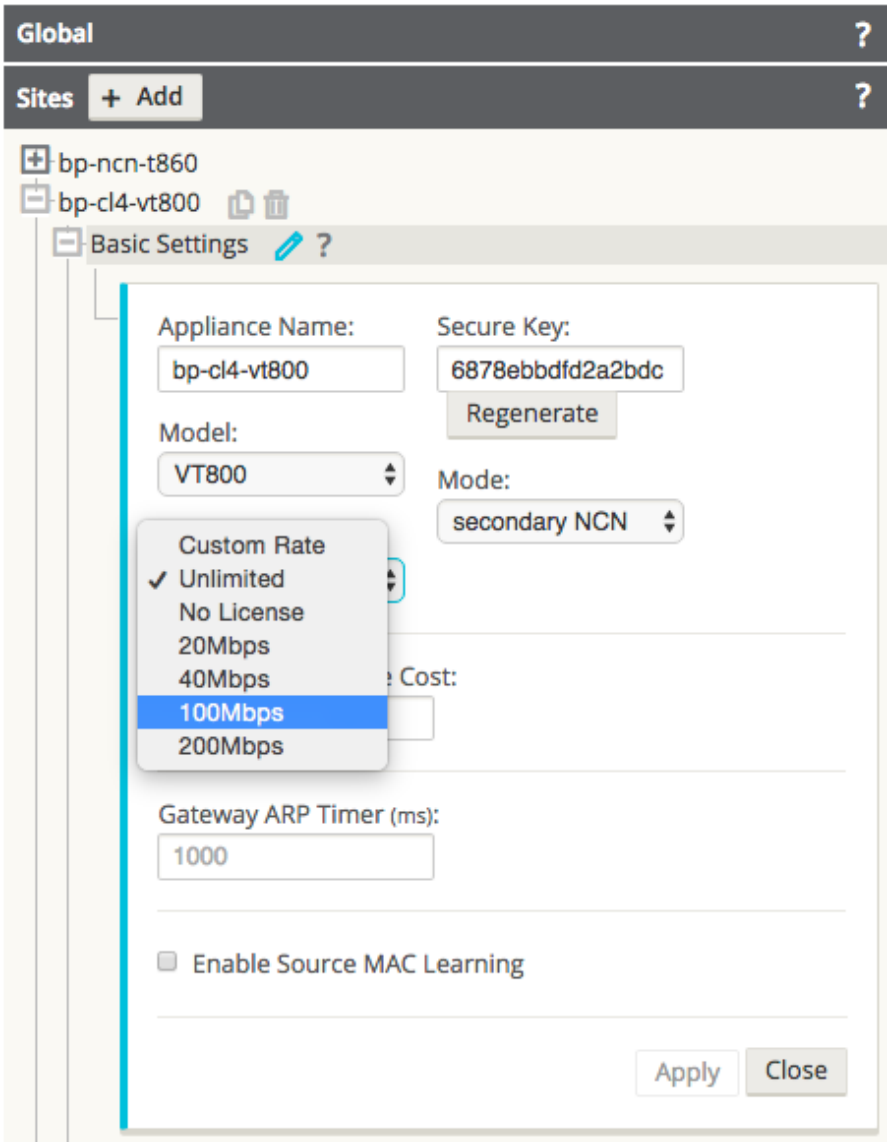


5. Run the **tcon** command to acquire the console.
6. Run the **management_IP** command to enter the set_management_ip prompt.
7. Run **set interface <ip_address> <subnet_mask> <gateway_ip_address>** (e.g., set interface 192.168.44.196 255.255.240.0 192.168.35.2).
8. Run **apply**.
9. Run **main_menu** to exit the set_management_ip prompt.

Configure and License the Virtual Appliance

1. If you intend to deploy your Virtual Appliance as a Network Control Node, skip to step 6. Otherwise, access the **Configuration Editor** available from the web console of your Network Control Node or your Oracle SD-WAN Aware instance.
2. From the **Configuration Editor**, modify your current configuration to include the Virtual Appliance as a new Site or as an update to an existing Site.
3. Under **Sites → [Virtual Appliance Site Name] → Basic Settings**, when you choose a Virtual Appliance model from the **Model** drop-down menu also choose the correct license from the **License** drop-down menu.

Figure 2-11 Choose Correct Virtual Appliance License from the Configuration Editor



4. Stage the modified configuration on your network as you would any other configuration change.
5. Download the staged Appliance Package for the Virtual Appliance to your local workstation.

> **Note:**
>
> At this point, if desired, continue and complete the Change Management process to activate the configuration changes across Edge in preparation for the Virtual Appliance addition.

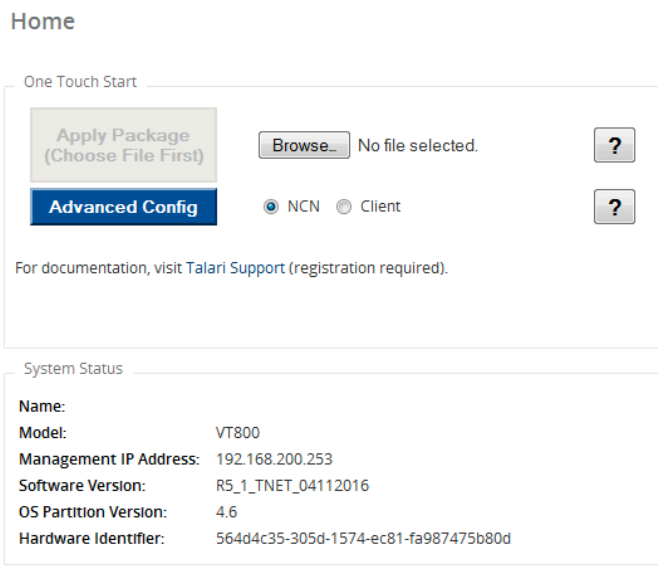
6. Open any supported browser and navigate to the management IP of the Virtual Appliance. At the **Login** prompt enter the following credentials and click **Login**: **Login:** talariuser **Password:** talari

7. Request a license for the Virtual Appliance by submitting the **Hardware Identifier** (found on the **Home** page when you log in) to your Sales Representative. Your Sales Representative will issue a License file based on the performance level you specified.

> **Note:**
>
> If you have a pre-prepared Appliance Package for the Virtual Appliance, continue with step 8. If you do not have a pre-prepared Appliance Package for the Appliance, click **Advanced Config** to manually configure and license your Virtual Appliance.

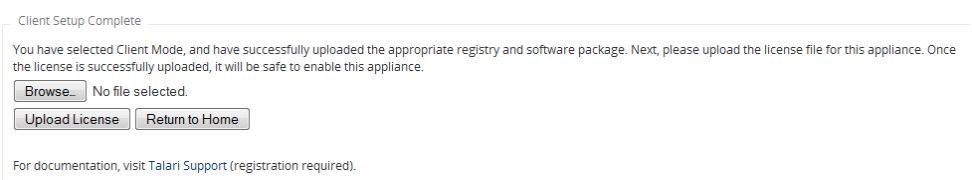
8. Under **One Touch Start**, click **Browse** and select the pre-prepared Appliance Package from your workstation.

Figure 2-12 Oracle SD-WAN Edge Software Home Screen



9. Select **Client** or Network Control Node (**NCN**) and click **Apply Package**.
10. Once the Appliance Package is uploaded the **Client Setup Complete** (or NCN Setup Complete) page will be displayed.

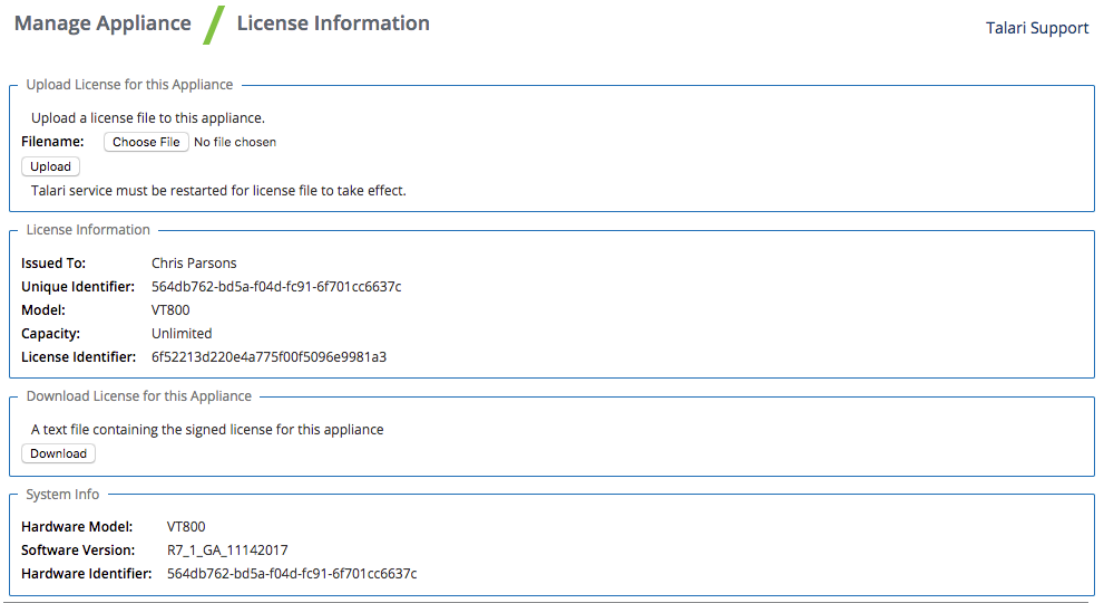
Figure 2-13 Client Setup Complete



> **Note:**
>
> The service starts automatically, but before you can take advantage of the performance level you purchased a license for, you must upload the license to the Virtual Appliance. An unlicensed Virtual Appliance will override the permitted rates of all configured WAN Links so their total does not exceed 10 Mbps full-duplex (i.e., 20 Mbps total).

11. Download the License file issued by your Sales Representative to your workstation. From this page or the **Manage Appliance → License Information** page, click the **Browse** button and choose the License file you downloaded.
12. Click **Upload License.** The page will reload to display your **License Information**.

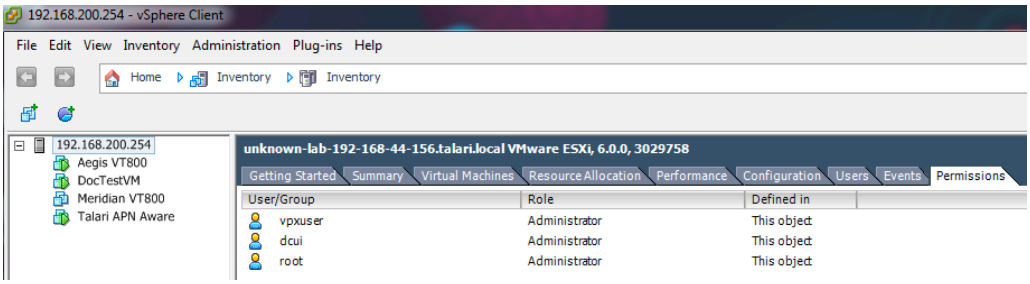
Figure 2-14 Successfully Licensed Virtual Appliance



> **Note:**
>
> In order for the license to take effect, the Service must be restarted.

Troubleshooting VM Permissions

If you encounter permissions issues attempting to run a Virtual Appliance on VMware ESXi, highlight the Virtual Machine from the server's Inventory list and click the **Permissions** tab to verify that the correct users have Administrator access to the Virtual Appliance. If the necessary users are not listed and/or their role is not set properly, you must contact your VMware server's administrator for help.



Microsoft Hyper-V

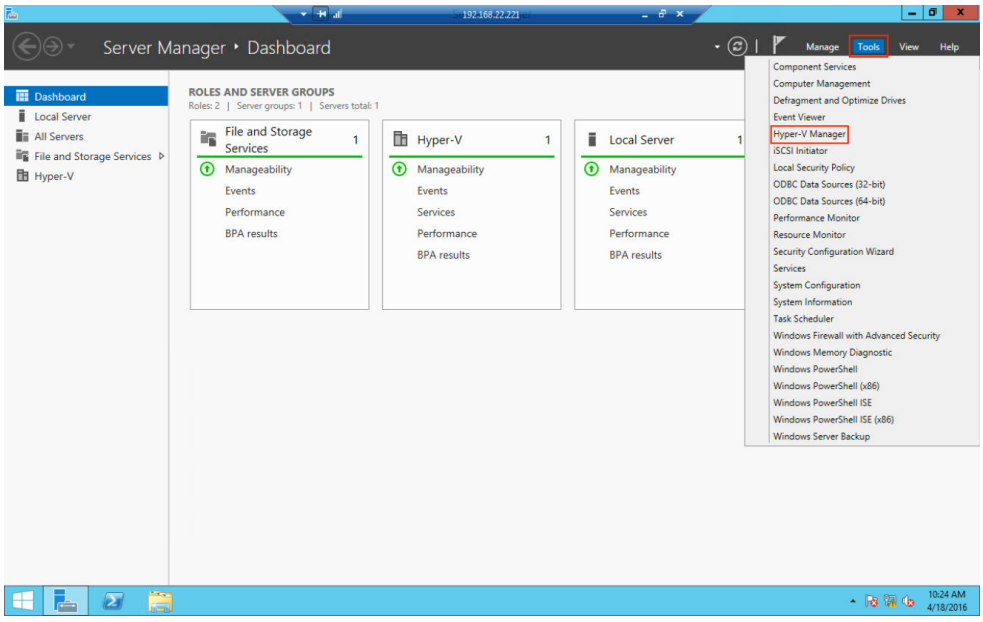
Virtual Appliances deployed on Microsoft Hyper-V are subject to the following configuration limitations:

- Hyper-V does not support layer 2 bridging; therefore, the Passthrough Service is not supported in Virtual Appliances deployed on Hyper-V.
- Hyper-V does not support multiple VLANs to use a single virtual interface, therefore only one VLAN can be supported on an Interface Group.

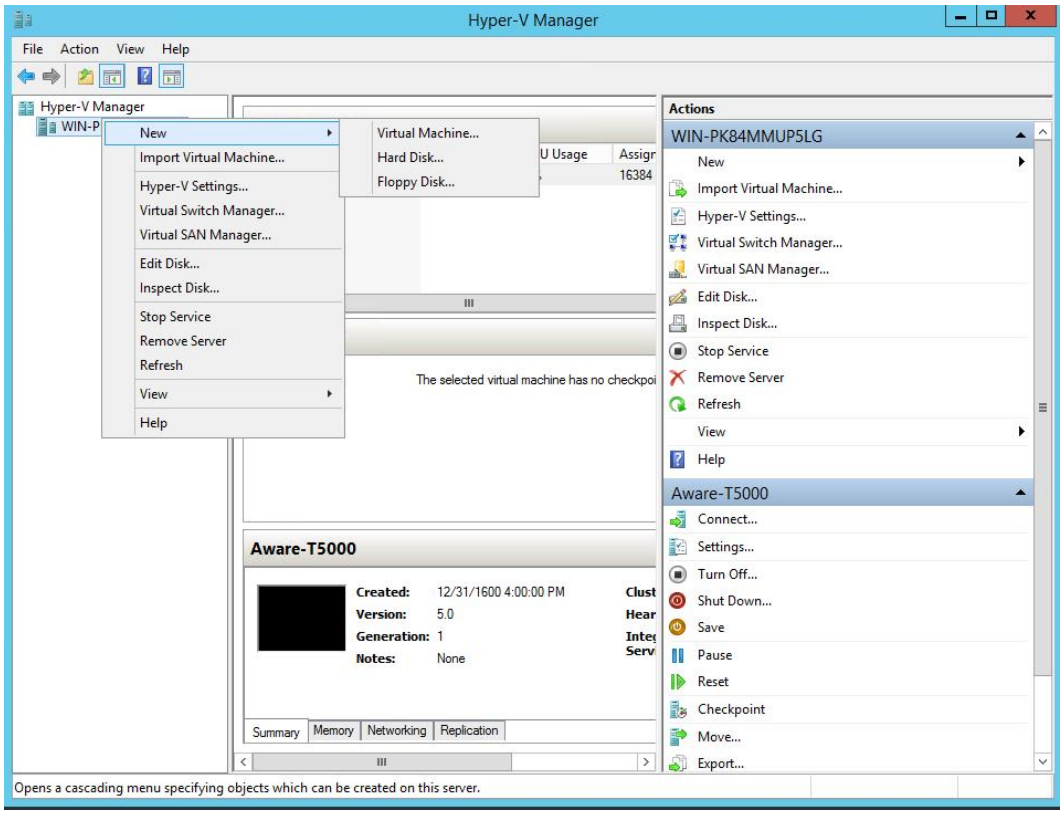
Important: When shutting down Virtual Appliances deployed on Hyper-V, use the “Shut Down” option rather than the “Turn Off” option to ensure graceful shutdown. If the “Turn Off” option is used, the Virtual Appliance may not start up properly.

Deploy the Virtual Appliance in Hyper-V

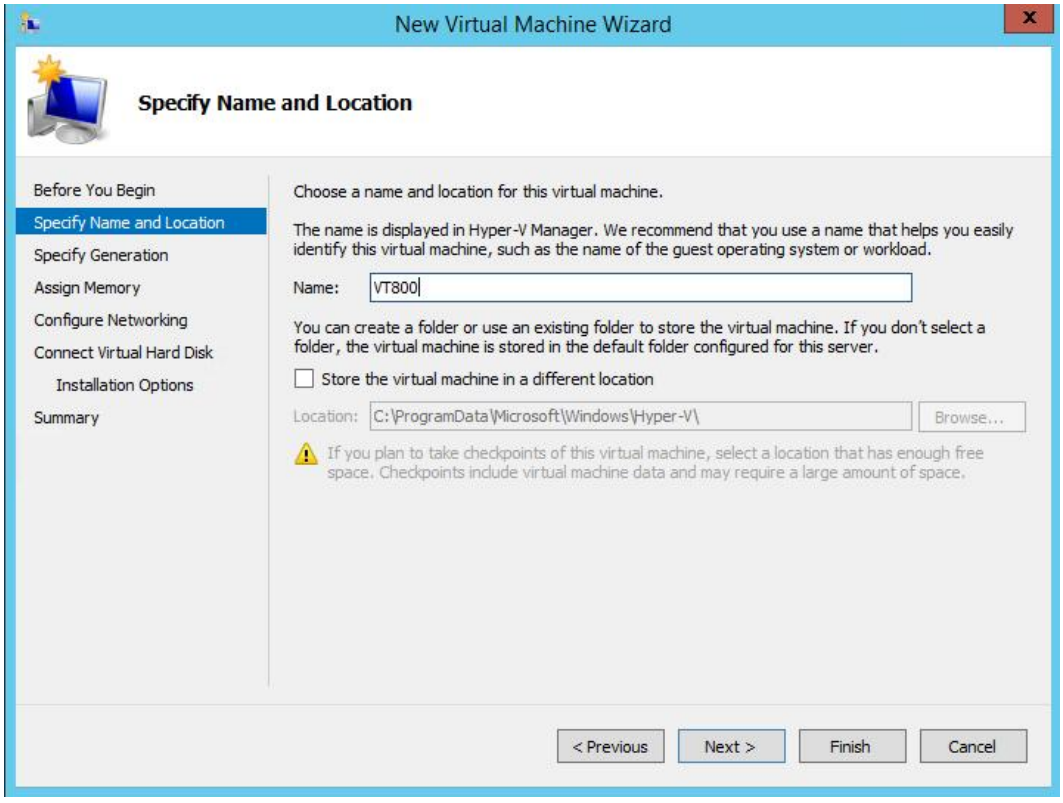
1. Open **Server Manager**, select the **Tools** pull-down menu, and click **Hyper-V Manager**. This will open the Hyper-V Manager window.



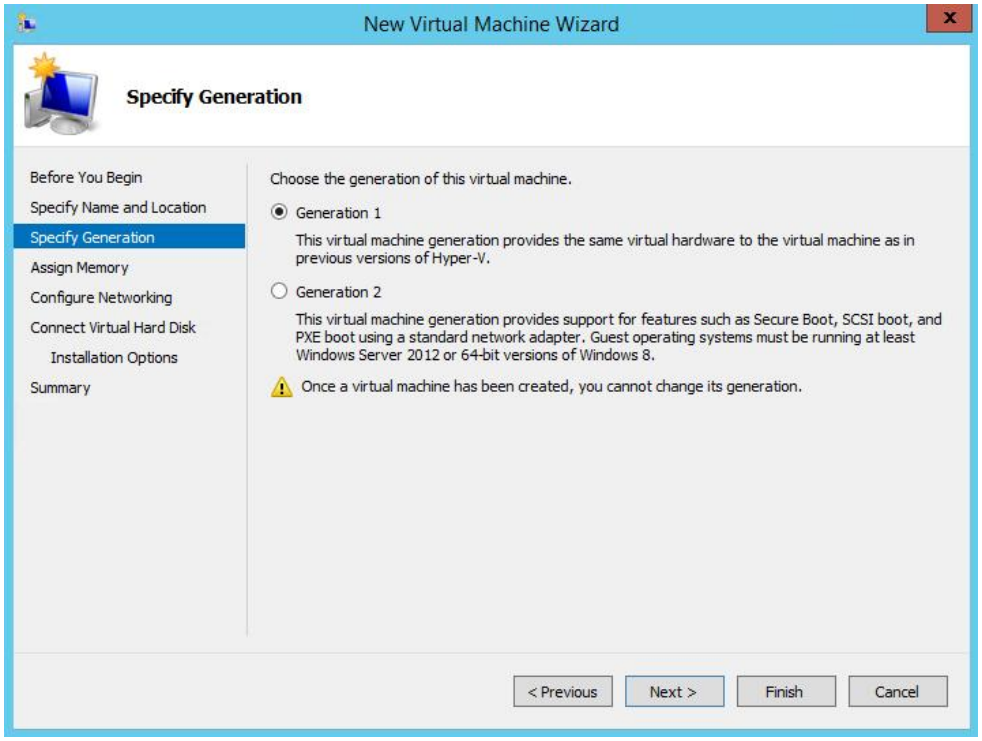
2. In the Hyper-V Manager window, make sure your server is selected from the dropdown list in the left. Select **New**, and then **Virtual Machine**. This will open the New Virtual Machine Wizard.



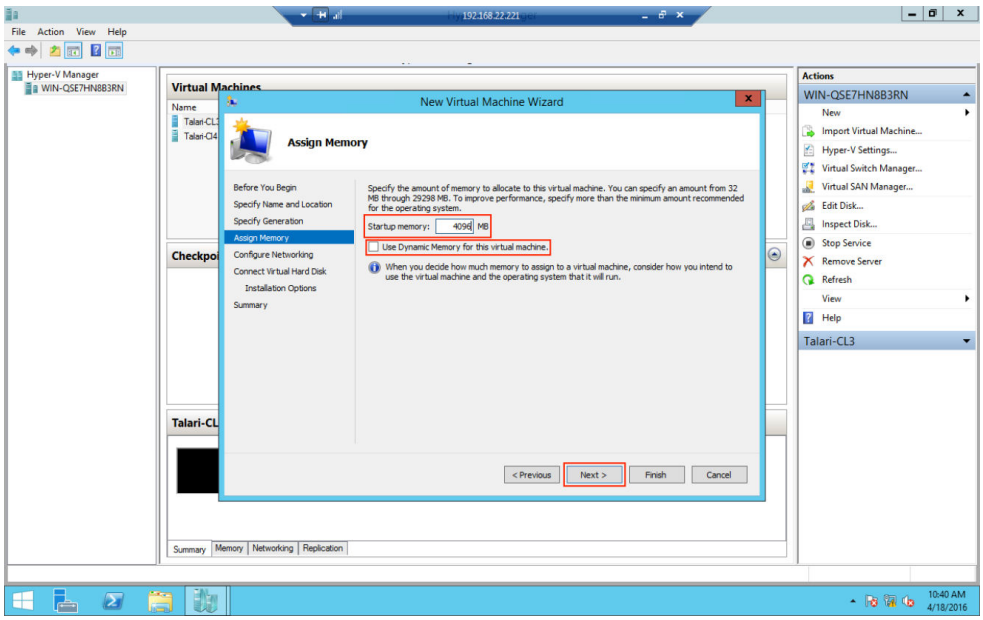
3. Review the **Before You Begin** tab, then click next.
4. On the **Specify Name and Location** tab, type an appropriate name for your virtual machine into the name box. Click **Next**.



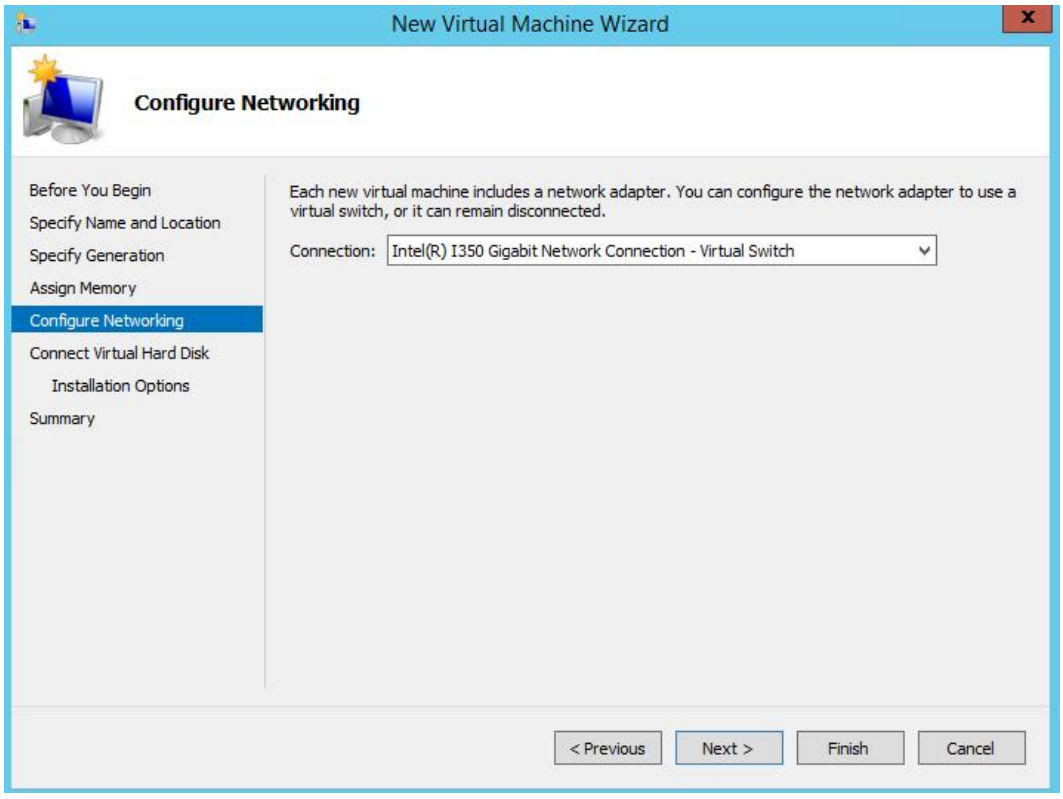
5. On the **Specify Generation** tab, ensure that **Generation 1** is selected and click **Next**.



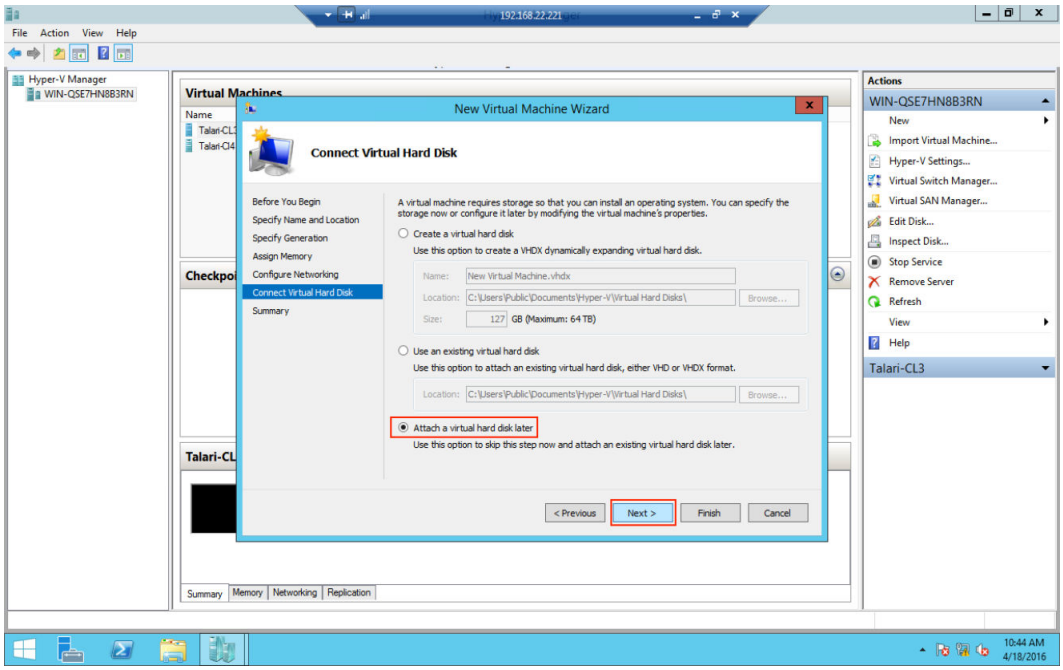
6. On the **Assign Memory** tab, chose the appropriate amount of memory necessary for the Virtual Appliance being deployed and input that value into the Startup memory box. Confirm “Use Dynamic Memory for the virtual machine” is not selected, then click **Next**.



7. On the **Configure Networking** tab, select a Virtual Switch to connect to the default network adapter. This network adapter will be used as the management interface for the Virtual Appliance. If you have not yet configured any Virtual Switches, you may leave the network adapter disconnected for the moment. Click **Next**.

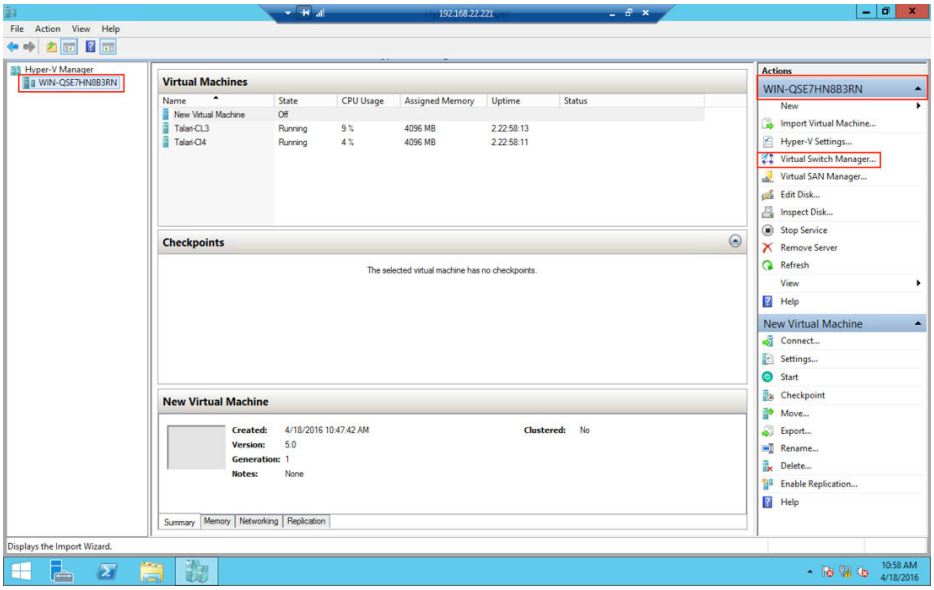


8. On the **Connect Virtual Hard Disk** tab, select the "Attach a virtual hard disk later" option and click **Next**.



9. On the **Summary** page, review the information for accuracy then click **Finish**.
10. The next step is to use the Virtual Switch Manager to configure Virtual Switches for the network interface ports. If this has already been done for other virtual machines on the server, skip to the next step.

a. On the Hyper-V Manager window, select the server and from the dropdown then select **Virtual Switch Manager.**

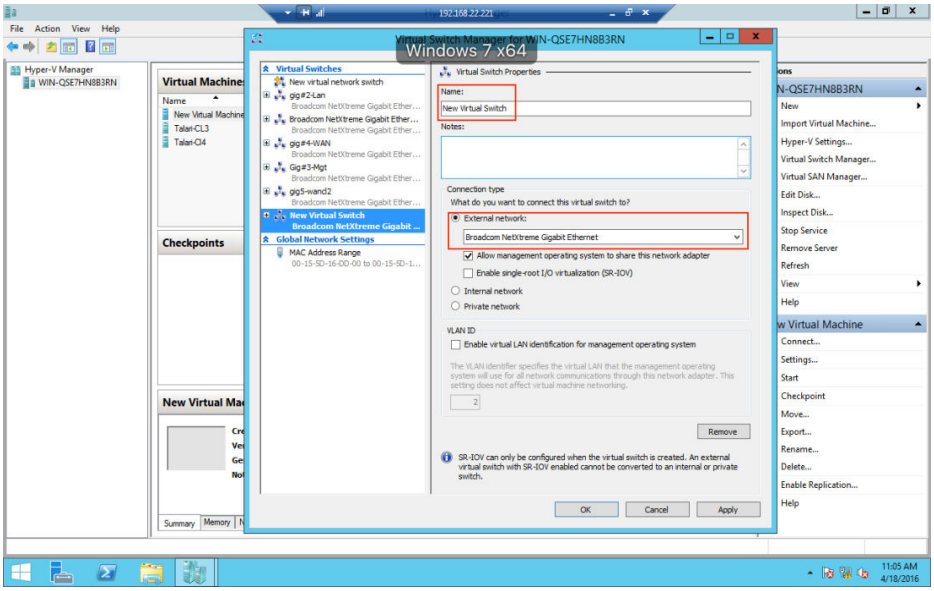


a. Select **New Virtual Switch**, make sure **External Network** (for connection to external Ethernet ports) is selected under type, and click **Create Virtual Switch**.

b. In the **Name** box, choose an appropriate name for the Virtual Switch (i.e. MGT, WAN, or LAN).

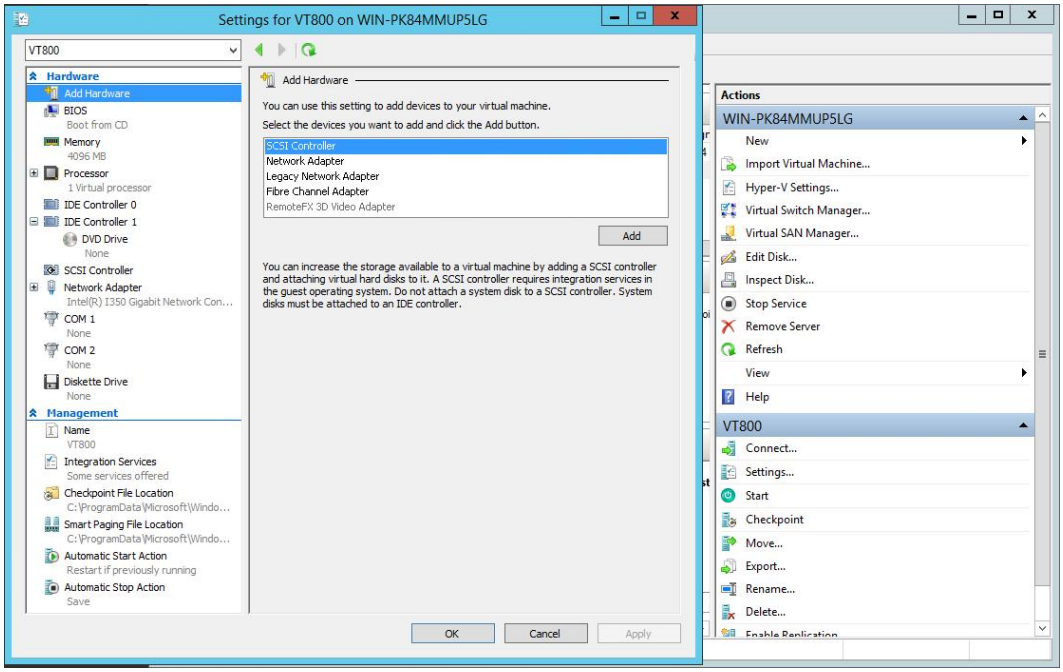
c. Under **Connection Type**, choose the physical NIC this Virtual Switch will represent. Disable the "Allow management operating system to share this network adapter" option, unless this is the management NIC and you would like it to be shared among VMs.

d. Under **VLAN ID**, allow tagging and choose the VLAN if required, click **Apply.**

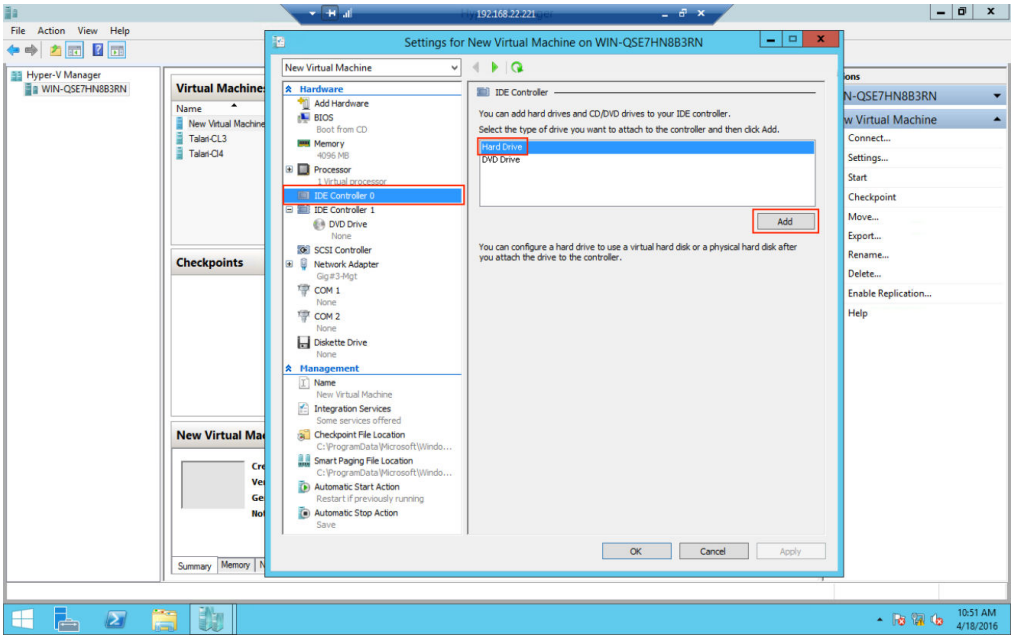


e. Repeat these steps for each NIC that will be used on the virtual appliance. Then, click **OK**. In a typical deployment the virtual appliance will require a minimum of three NICs – Management, LAN, and WAN.

11. Back on the Hyper-V Manager window, select the new virtual machine and click **Settings.**



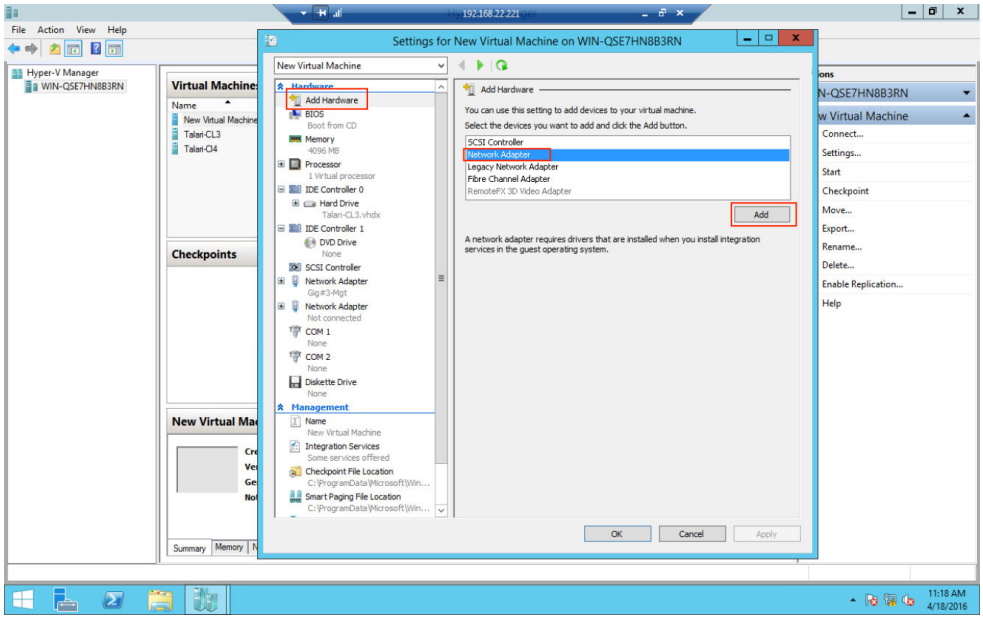
a. In the settings window for your virtual machine select the **IDE Controller 0** from the Hardware dropdown menu. Ensure that Hard Drive is selected and click **Add.**



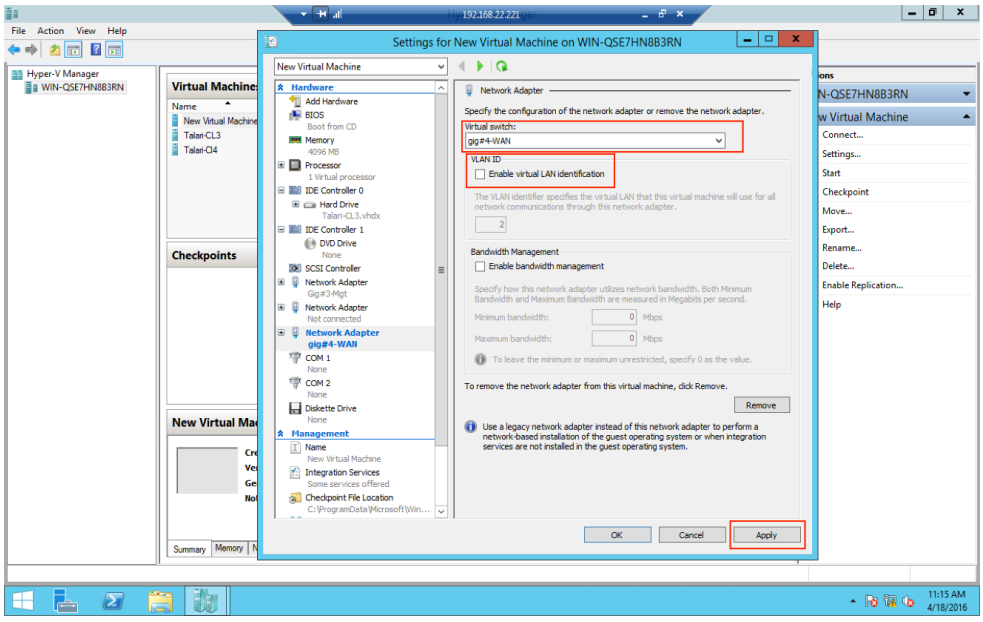
12. Under **Media,** choose **Virtual Hard Disk** and browse to where the .vhd for the Virtual Appliance is stored on the server. Click **Apply** then **OK**.

13. Go back to your virtual machine **Settings** window. You will notice that one network adapter has already been created during the VM deployment. This network adapter provides management connectivity for the Virtual Appliance. If it is not connected to the Virtual Switch designated for management traffic, select that Virtual Switch from the dropdown and click **Apply**.

14. You will need to create network adapters for the remaining data ports that will be used on your Virtual Appliance. Select **Add Hardware** from the Hardware dropdown menu, then choose **Network Adapter** and click **Add**.

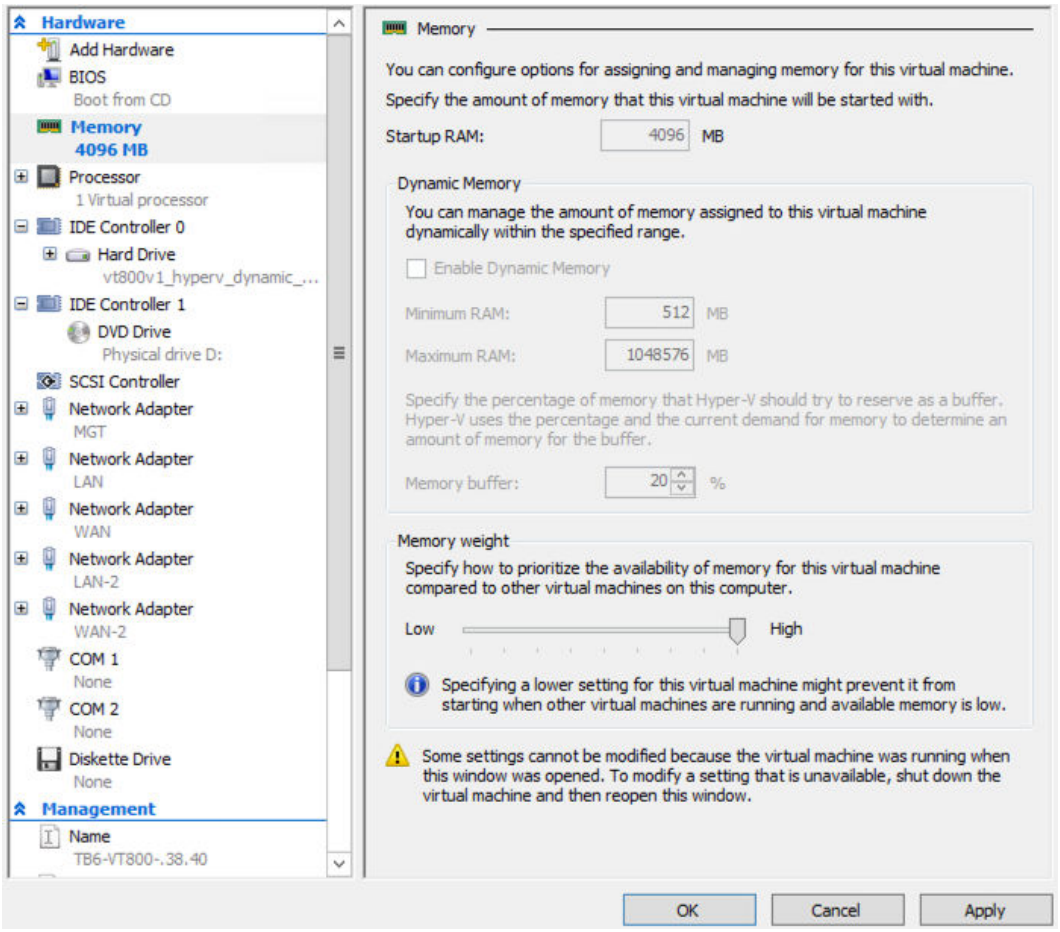


15. Choose the appropriate previously configured Virtual Switch for the desired physical port from the dropdown menu. If VLAN tagging will be used on this port, select the **Enable virtual LAN identification** button. Click **Apply** and repeat for each virtual machine port. Click **OK** when all network adapters have been created.

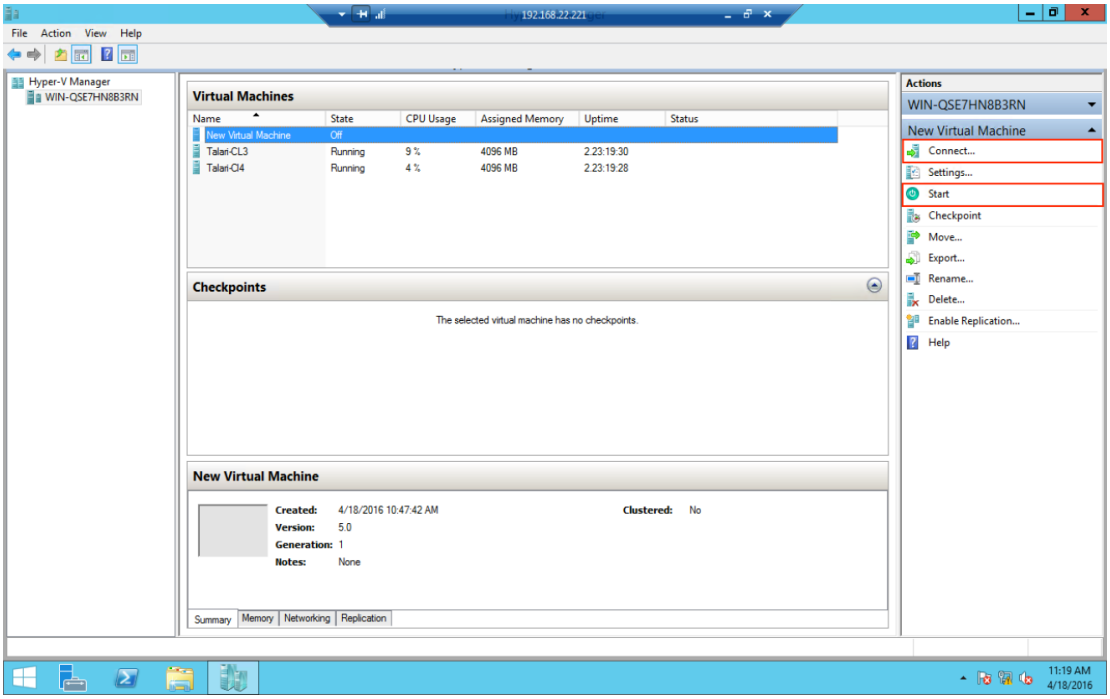


16. Finally, the Memory Weight for the Virtual Appliance must be set to High. Select **Memory** from the Hardware dropdown menu. Ensure that the slider for **Memory**

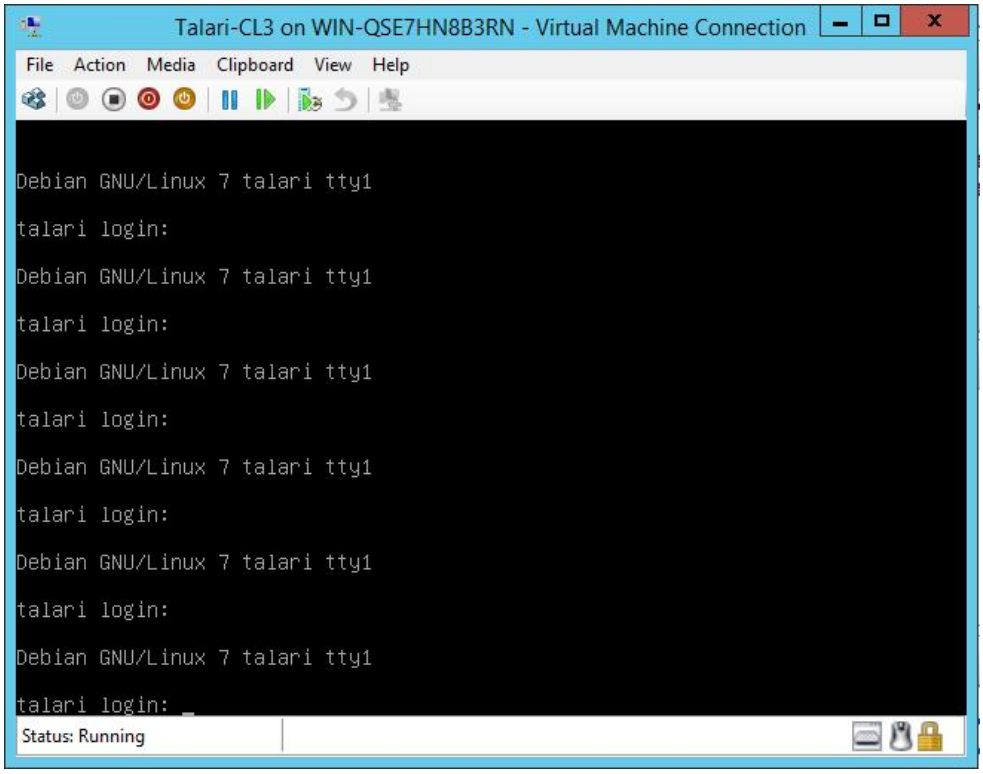
Weight is set to **High**, then click **Apply.**



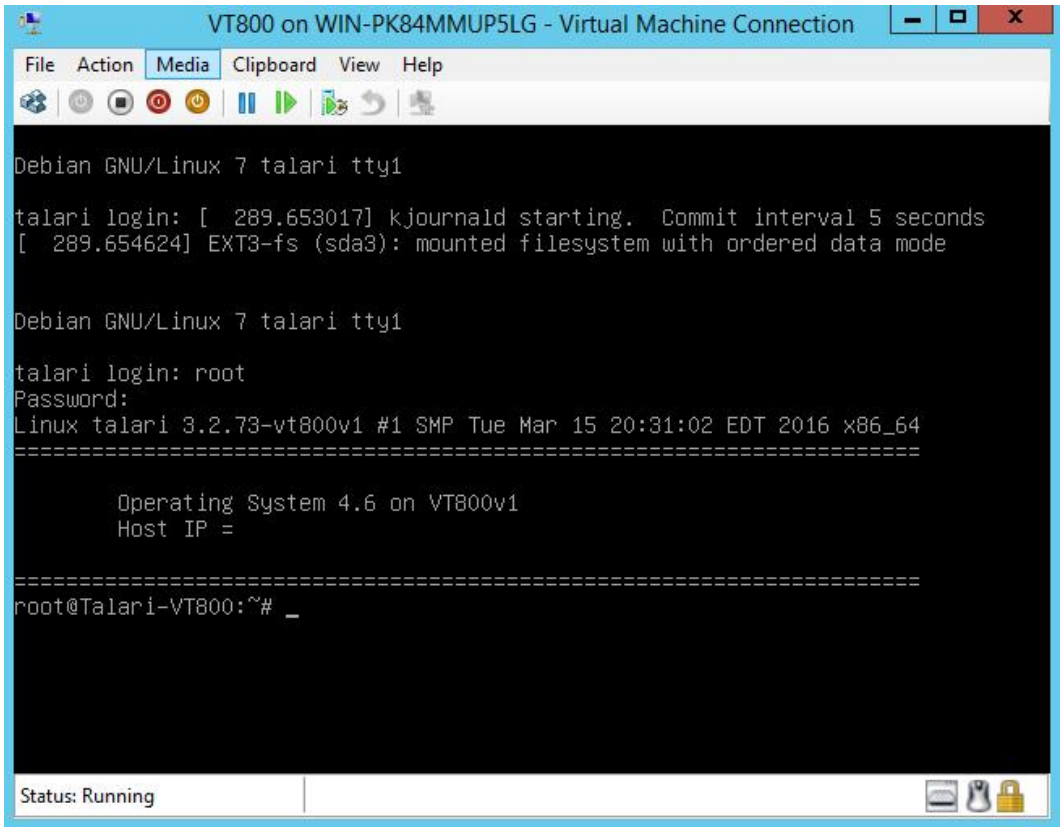
17. At this point the Virtual Appliance is ready for boot. Click **Start** from the VM's dropdown menu, then **Connect** to console into the device.



1. Verify that the Virtual Appliance boots properly by hitting return to get the login prompt.



2. Log into the Virtual Appliance using the default credentials (talariuser/talari) and determine the management IP address as displayed at login as Host IP. If DHCP is not configured for this Ethernet segment, there will not be an IP address displayed at login (see below) so the user will have to manually configure the management IP address on the Appliance.



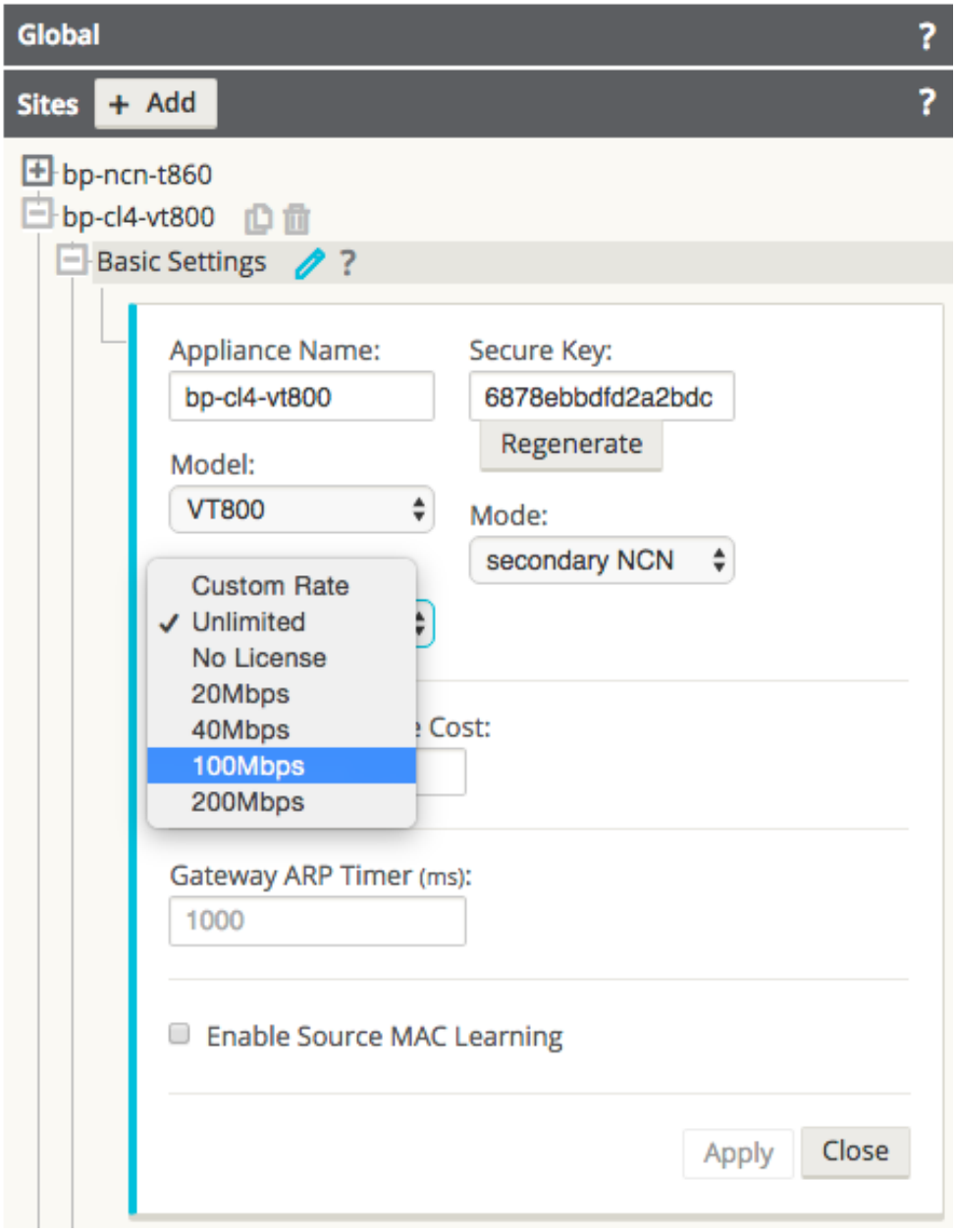
To manually configure a management IP address on the Virtual Appliance:

- Run the **tcon** command to acquire the console.
- Run the **management_IP** command.
- At the set_management_ip> prompt type **set interface** followed by the **IP**, **subnet mask**, and **gateway** (e.g., **set interface 172.16.28.31 255.255.255.0 172.16.0.6**).
- Hit Enter.
- Type **apply** and hit Enter.
- Run **main_menu** to exit.

Once access to the management IP has been confirmed, you may configure and license the Virtual Appliance.

Configure and License the Virtual Appliance

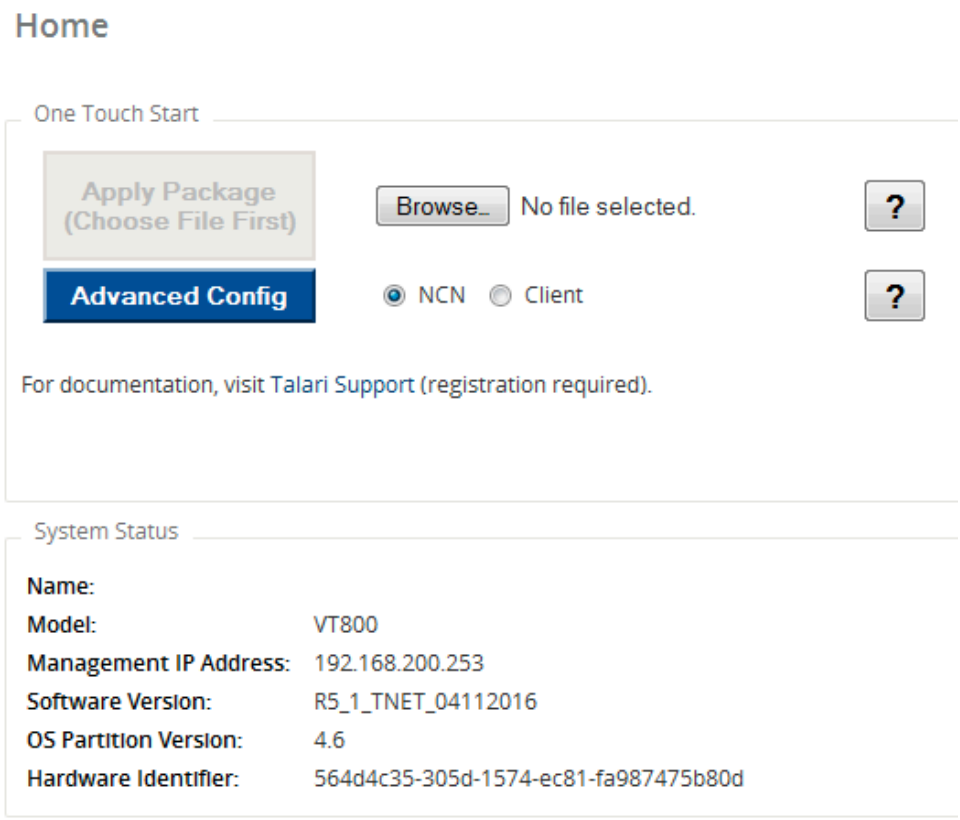
1. If you intend to deploy your Virtual Appliance as a Network Control Node, skip to step 6. Otherwise, access the **Talari Configuration Editor** available from the web console of your Network Control Node or your Oracle SD-WAN Aware instance.
2. From the **Talari Configuration Editor**, modify your current Configuration to include the Virtual Appliance as a new Site or as an update to an existing Site.
3. Under **Sites** → **[Virtual Appliance Site Name]** → **Basic Settings**, when you choose a Virtual Appliance model from the **Model** drop-down menu, you will also be given the option to choose the correct license from the **License** drop-down menu.



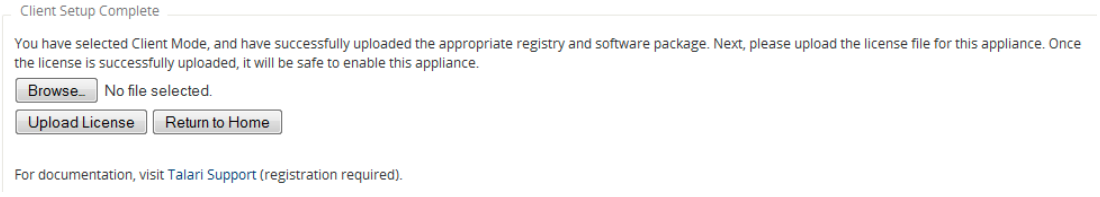
4. Stage the modified Configuration on your network as you would any other configuration change.
5. Download the staged Appliance Package for the Virtual Appliance to your local workstation.
6. Open any supported browser and navigate to the management IP of the Virtual Appliance. At the **Login** prompt enter the following credentials and click **Login**: **Login:** talariuser **Password:** talari
7. Request a license for the Virtual Appliance by submitting the **Hardware Identifier** (found on the **Home** page when you log in) to your Sales Representative. Your Sales Representative will issue a License file based on the performance level you specified.

> **Note:**
>
> If you have a pre-prepared Appliance Package for the Virtual Appliance, continue with step 8. If you do not have a pre-prepared Appliance Package for the Virtual Appliance, click **Advanced Config** to manually configure and license your Virtual Appliance.

1. Under **One Touch Start**, click **Browse** and select the pre-prepared Appliance Package from your workstation.

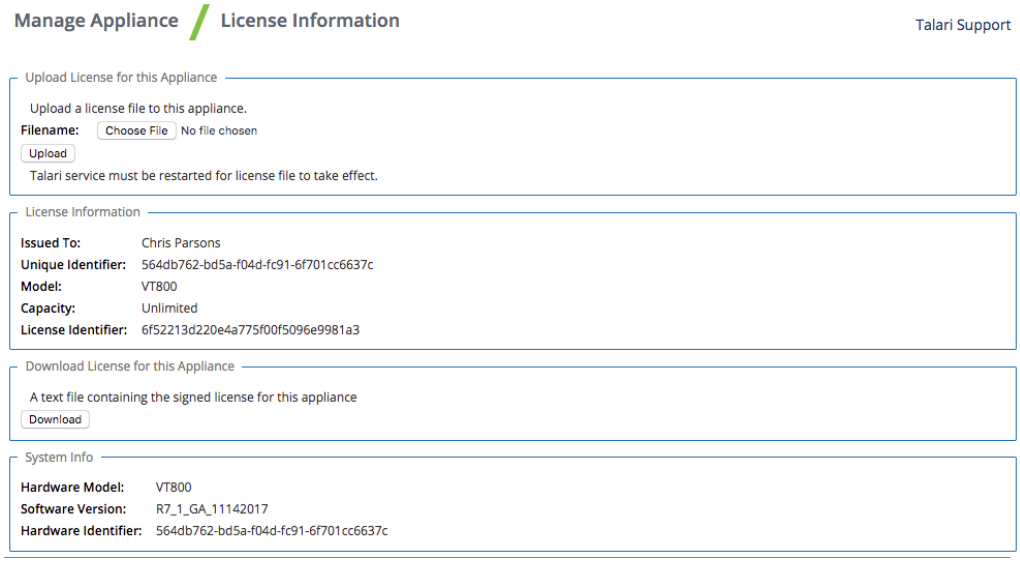


2. Select **Client** or Network Control Node (**NCN**) and click **Apply Package**.
3. Once the Appliance Package is uploaded the **Client Setup Complete** (or NCN Setup Complete) page will load.



> **Note:**
>
> The Service starts automatically, but before you can take advantage of the performance level you purchased a license for, you must upload the license to the Virtual Appliance. An unlicensed Virtual Appliance will override the permitted rates of all configured WAN Links so their total does not exceed 10 Mbps full-duplex (i.e., 20 Mbps total).

1. Download the License file issued by your Sales Representative to your workstation. From this page or the **Manage Appliance → License Information** page, click the **Browse** button and choose the License file you downloaded.
2. Click **Upload License.** The page will reload to display your **License Information**.



> **Note:**
>
> In order for the license to take effect, the Service must be restarted.

> **Important:**
>
> When shutting down Virtual Appliances deployed on Hyper-V, use the “Shut Down” option rather than the “Turn Off” option to ensure graceful shutdown. If the “Turn Off” option is used, the Virtual Appliance may not start up properly.

Microsoft Azure

Virtual Appliances deployed on Microsoft Azure are subject to the following configuration limitations:

- Azure does not support layer 2 bridging; therefore, the Passthrough Service is not supported in Virtual Appliances deployed on Azure.
- Azure supports one subnet per virtual interface, therefore only one VLAN can be supported on an Interface Group.

> **Note:**
>
> This document describes a basic setup of a Virtual Appliance in the Microsoft Azure cloud, at a single Azure location, within a single VNET. For assistance with deploying more complex Azure configurations, please contact support.

Prerequisites for Microsoft Azure

- Administrative access to your Azure Portal
- Active Azure Subscription & Azure Location
- Active Registration to the following Resource Providers:
  - Microsoft.Network
  - Microsoft.Compute
  - Microsoft.Storage
- Sufficient amount of compute resources available in the Resource Group that you are deploying in (ex. Number of vCPUs available)
- Azure Express Route (if required)

Prerequisites

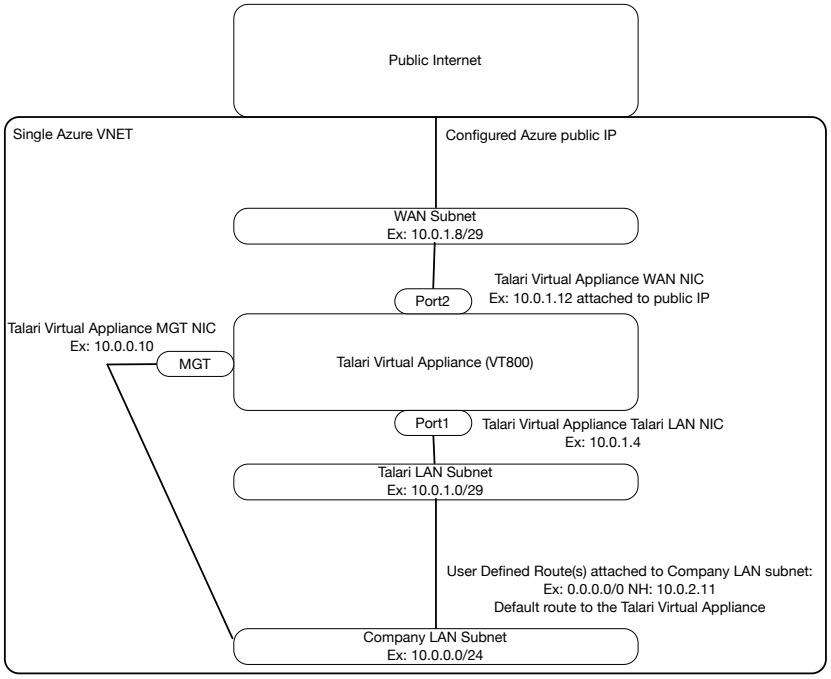
- A valid license
  - In order to acquire a license, you will first need to spin-up the new appliance so that you can obtain the UUID of the appliance.
  - Once a UUID has been obtained from the appliance, please contact your Account Team who will assist you with procuring a valid license that will need to be applied to the Virtual Appliance before service can be enabled.
- An Appliance Package for the specific site being deployed (available from your NCN's Change Management Page once the configuration containing the new site has been staged

Supported Topologies

There are 3 basic topologies supported for Microsoft Azure:

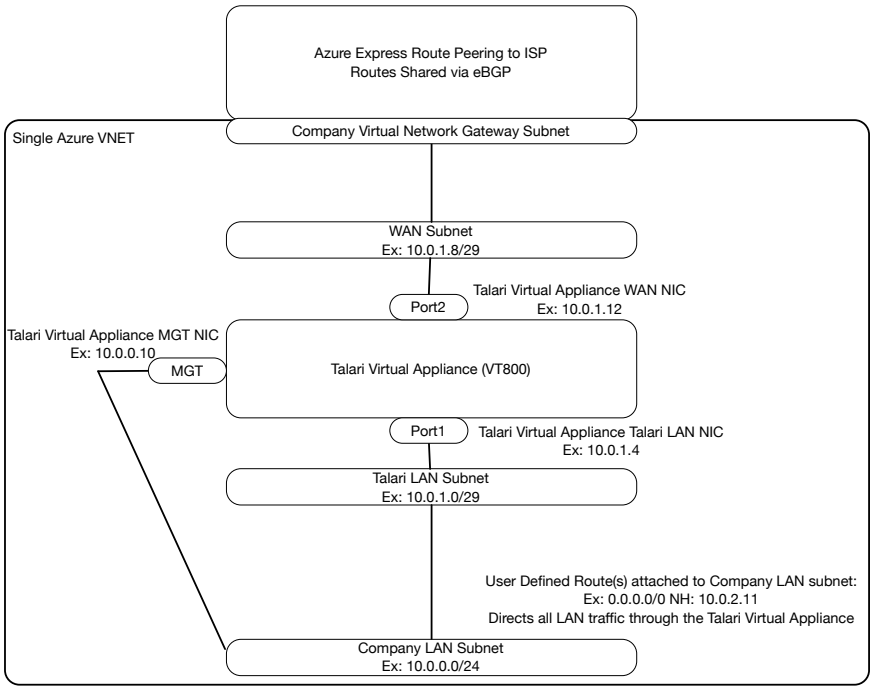
1. Single WAN Link Using Azure Public IP Address

Figure 2-15 Sample Topology for Single WAN Link using Azure Public IP Address



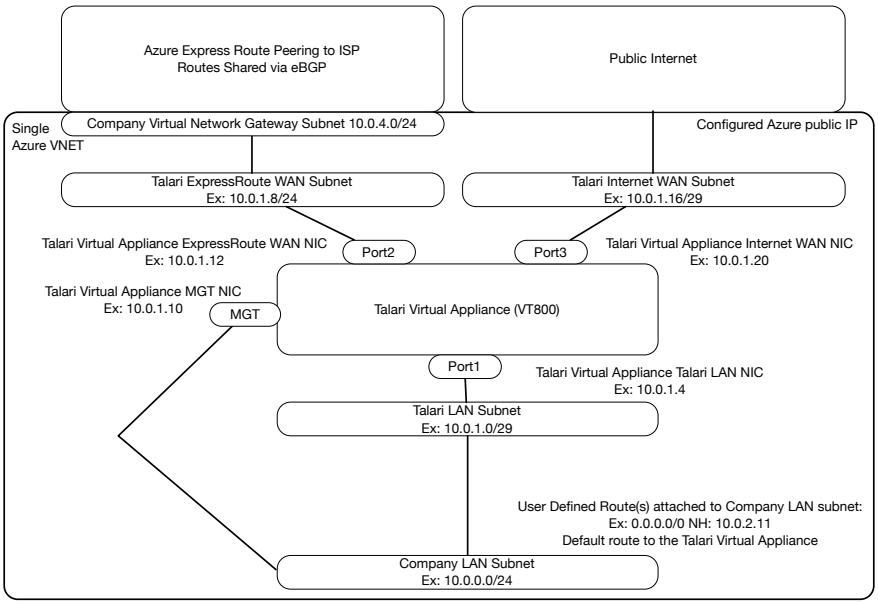
2. Single WAN Link Using Azure Express Route

Figure 2-16 Sample Topology for Single WAN Link using Azure Express Route



3. Dual WAN Link using Azure Public IP address and Azure Express Route

Figure 2-17 Sample Topology for Dual WAN Links with Azure Public IP and Azure Express Route



Deployment Notes

1. Standard deployment of the Virtual Appliance with a single public WAN Link requires two Public IP Addresses:
   a. One for permanent use by the WAN VIP.
   b. One for permanent or temporary use by the MGT IP:
      i. Permanent Public IP – if you wish to have the MGT accessible via Public IP permanently.
      ii. Temporary Public IP – if you wish to temporarily access the Virtual Appliance and then remove the Public IP access once Conduit MGT access has been established.
2. The Azure Virtual Appliance requires dedicated LAN and WAN subnets for Talari use only.
3. Other subnets that exist in your Azure environment can be connected to the LAN subnet via User Defined Routes.
4. If Internet service is required at the Virtual Appliance site, the Configuration must utilize a Dynamic Outbound PAT to the Public IP Address of the Virtual Appliance's WAN VIP.
5. IP forwarding must be enabled on all Azure NICs connected to the Virtual Appliance, with the exception of the MGT NIC.
6. All required NICs must be attached to the Virtual Appliance prior to enabling the service on the virtual appliance.
7. If requirements dictate more complex topologies, please consult with Talari to ensure supportability.

VM Size Requirements

Choose a VM size most appropriate for your deployment scenario and performance requirements. Deploying a virtual machine that does not meet the requirements is not

supported. Additionally, this may result in instability and/or suboptimal performance of the Virtual Appliance.

Addressing Guidelines and Planning

Before creating or appropriating Microsoft Azure resources, determine how many IP subnets will be required by reviewing the supported topologies discussed above along with your configuration needs. For standard deployment, define a minimum of:

1. A unique Address Space for the Virtual Network (VNET).
2. At least one Company LAN subnet for company assets contained within that VNET.
3. A unique, LAN subnet contained within that VNET.
4. A WAN subnet contained within the VNET for each WAN Link.
5. LAN & WAN VIPs for the Virtual Appliance, contained within their respective subnets.
6. Optional (for MGT): you may choose to leave your MGT address accessible via Public IP, place it into your already-existing Company LAN Subnet, or create an entirely new MGT Subnet for the Interface. In this example, we will assume that the MGT Interface and MGT IPs will live on the Company LAN Subnet as discussed in the topology overview.

Single WAN Link Example

- VNET Address Space: 10.0.0.0/23
- Existing Company LAN Subnet: 10.0.0.0/24
- LAN Subnet: 10.0.1.0/24
  - LAN Virtual IP (VIP): 10.0.1.11/24
- WAN Subnet: 10.0.2.0/24
  - WAN Virtual IP (VIP): 10.0.2.11/24
- MGT Virtual IP (VIP): 10.0.0.4

> **Note:**
>
> Subnet size prefixes as small as /29 may to be used. Smaller subnets are not permitted by Azure due to the requirements of their reserved IP addresses. The first three addresses in each subnet are reserved by Azure for their internal services and cannot be assigned to the Virtual Appliance.

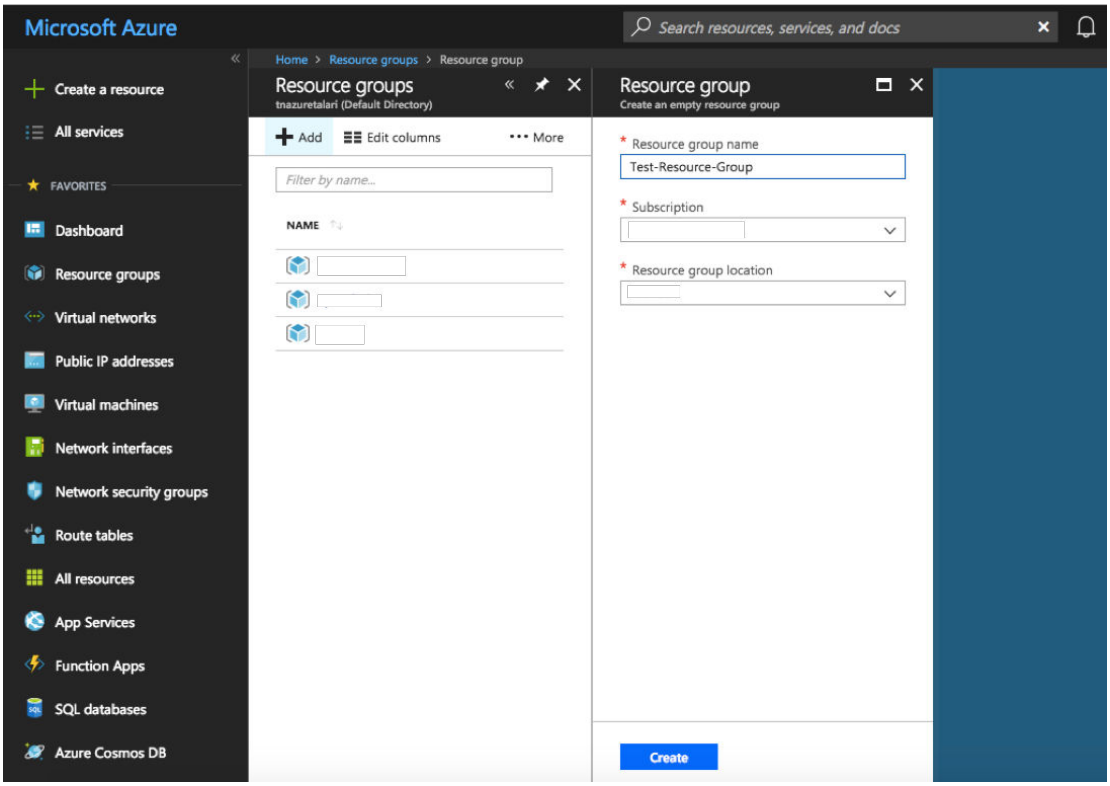
Create Network Resources

Prior to deploying a Virtual Appliance, you should ensure that you have all the Microsoft Azure resources required by your topology and configuration. If you have already gathered the required resources, please skip ahead to the section below. If you do not have already-existing Microsoft Azure resources that can be used for the Virtual Appliance, the following steps will walk through the process of creating each of the following: Resource Groups, VNET, Subnets, Route Tables, Network Security Groups, Public IPs, and Virtual NICs.

Resource Group

If you are not using an existing Azure Resource Group, you will need to create a new resource group in your chosen region. To create a new resource group, select “Resource Groups” from “All Services” in the Azure Portal Menu, and click “Add.” Enter a name for the Resource Group, select the Subscription and Location, then click “Create.”

Figure 2-18 Create Resource Group



Virtual Network (VNET)

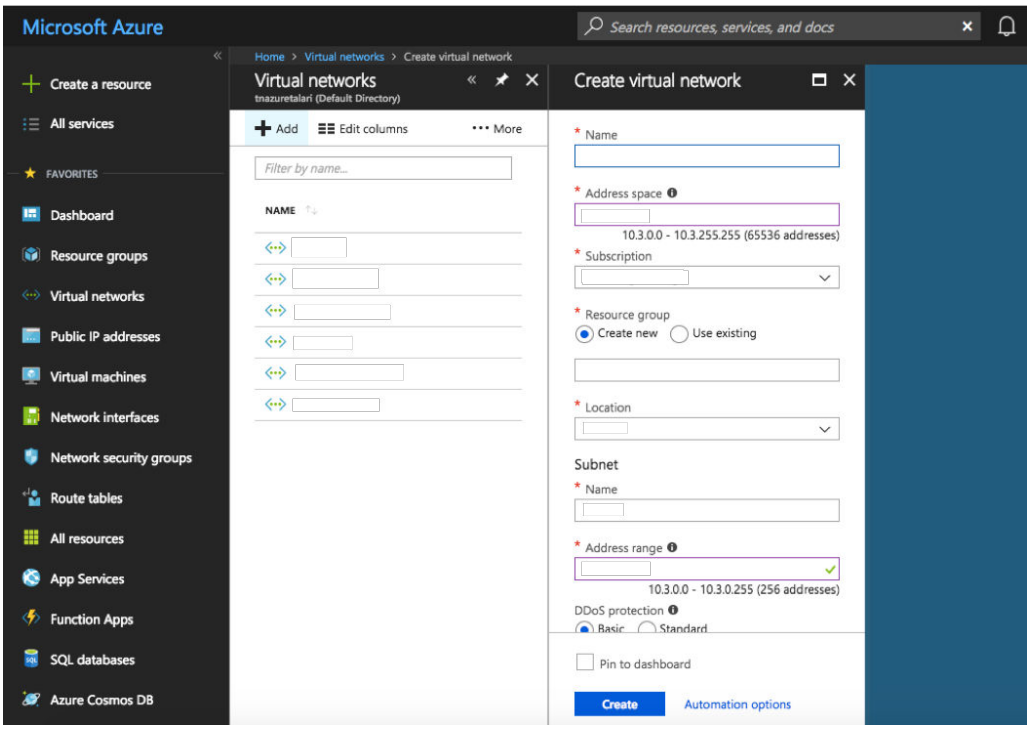
If you do not have an already-existing VNET with free Address Space, you will need to create a new VNET or alter an existing VNET to include the Address Space you defined in the “Addressing Guidelines & Planning” section.

To create a new VNET:

1. Select “Virtual Network” from “All Services” in the Azure Portal Menu.
2. Select “Add” to create a new VNET.
3. Enter a Name for the VNET.
4. Type the Address Space defined in the “Addressing Guidelines & Planning” section.
5. Select the Resource Group and Location defined in the “What You Need Before Starting” section.
6. Give the Subnet (one that will be created for the VNET) a Name and type the Address Range defined above in the “Addressing Guidelines & Planning” section above.

7. Select “Basic” for DDoS protection and click “Create.”

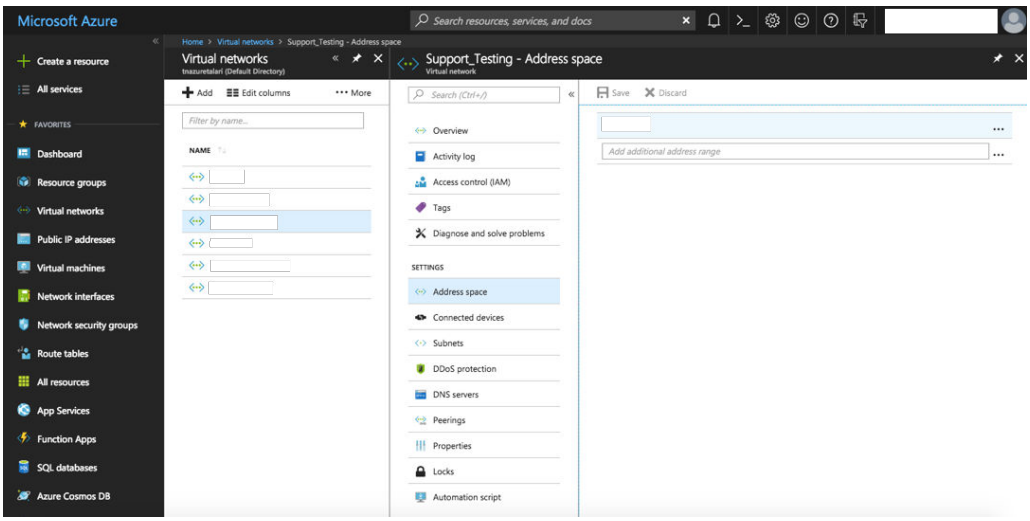
Figure 2-19 Create VNET



To modify an existing VNET:

1. Select “Virtual Network” from “All Services” in the Azure Portal Menu.
2. Select an existing VNET and select “Address Space” and “Subnets” to alter an existing VNET.

Figure 2-20 Modify VNET



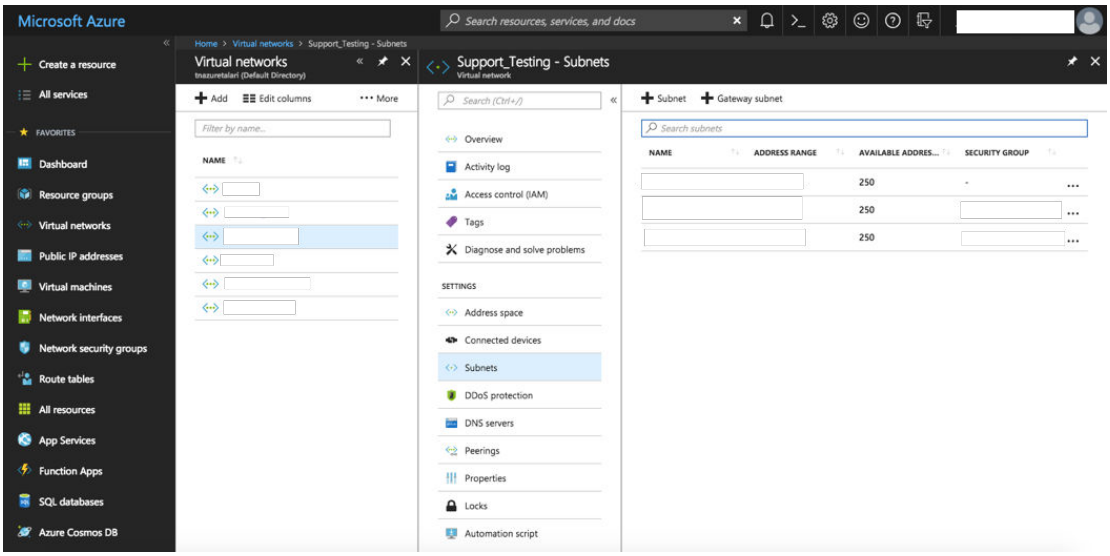
Subnets

Create the Subnets defined in the “Addressing Guidelines & Planning” section above.

To create a new Subnet:

1. Select “Virtual Network” from “All Services” in the Azure Portal Menu.
2. Select the desired VNET.
3. Select “Subnets”.
4. Click the “+ Subnet” button to create a new subnet within the Address Space of the VNET.
5. Repeat for each required Subnet.

Figure 2-21 Create Subnet



Route Tables

Route Tables will need to be created for each Subnet created above. The following routes are required for each Subnet's Route Table:

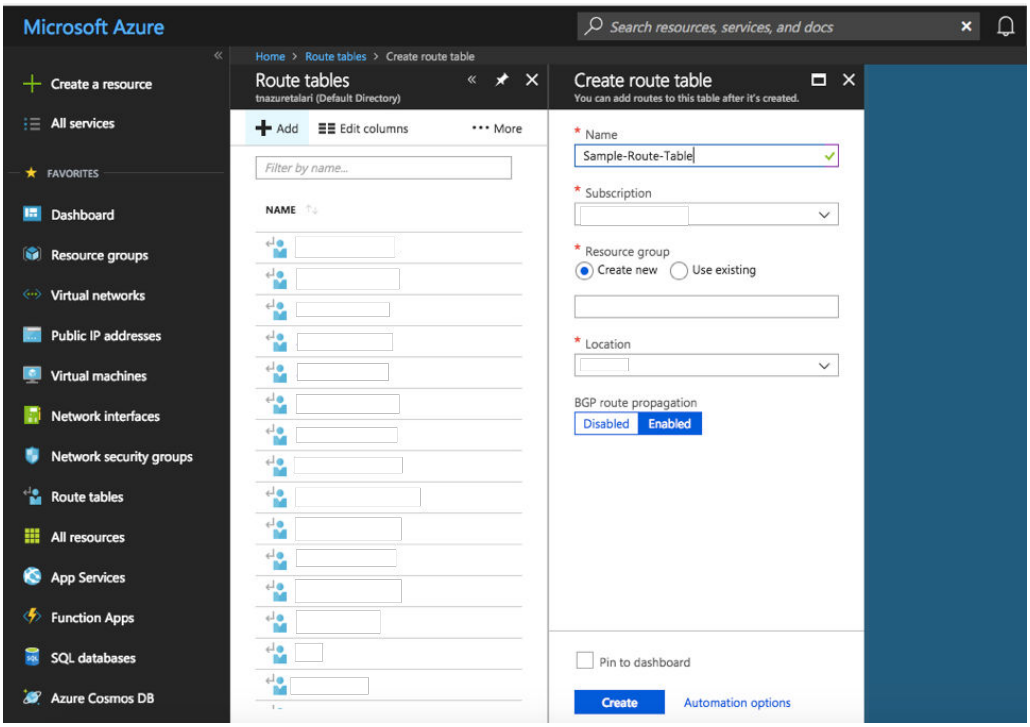
- MGT – 0.0.0.0/0 Internet
- LAN – next hop set as Company LAN Subnet
- WAN – 0.0.0.0/0 Internet

To create a new Route Table:

1. Select “Route Tables” from “All Services” in the Azure Portal Menu.
2. Click “+ Add.”
3. Enter a Name for the Route Table.
4. Select the Subscription and Location chosen in the “Prerequisites” section above.
5. Enable BGP route propagation if desired.

6. Click “Create.”
7. Repeat for each required Route Table.

Figure 2-22 Create Route Table

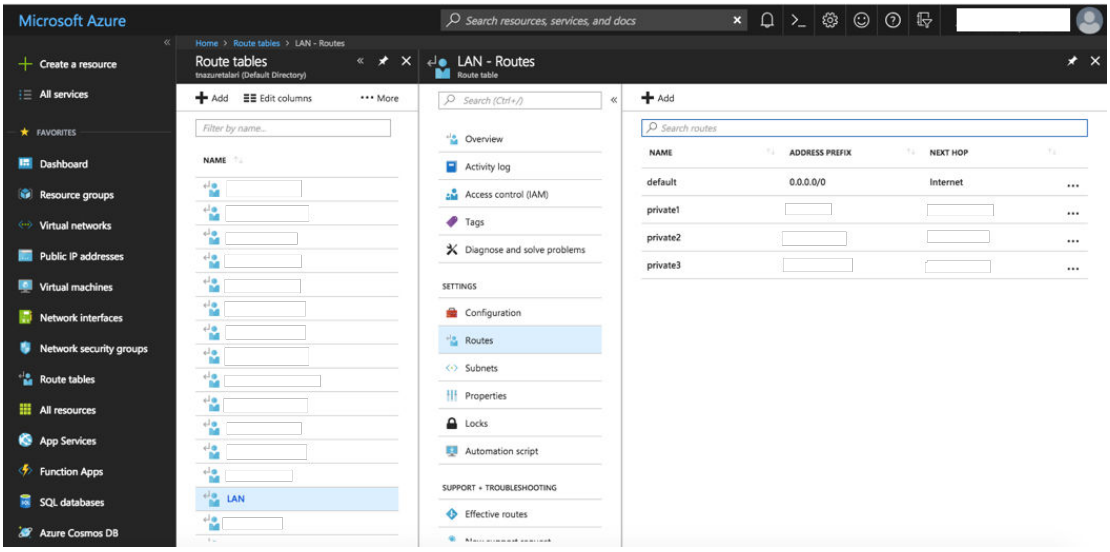


Once created, the new Route Table will have to be modified to include all required routes, with a minimum of the above-discussed routes included in each Subnet's Route Table.

To modify an existing Route Table:

1. Select “Route Tables” from “All Services” in the Azure Portal Menu.
2. Select the desired Route Table.
3. Select “Routes.”
4. Click “+ Add” to add a new route.

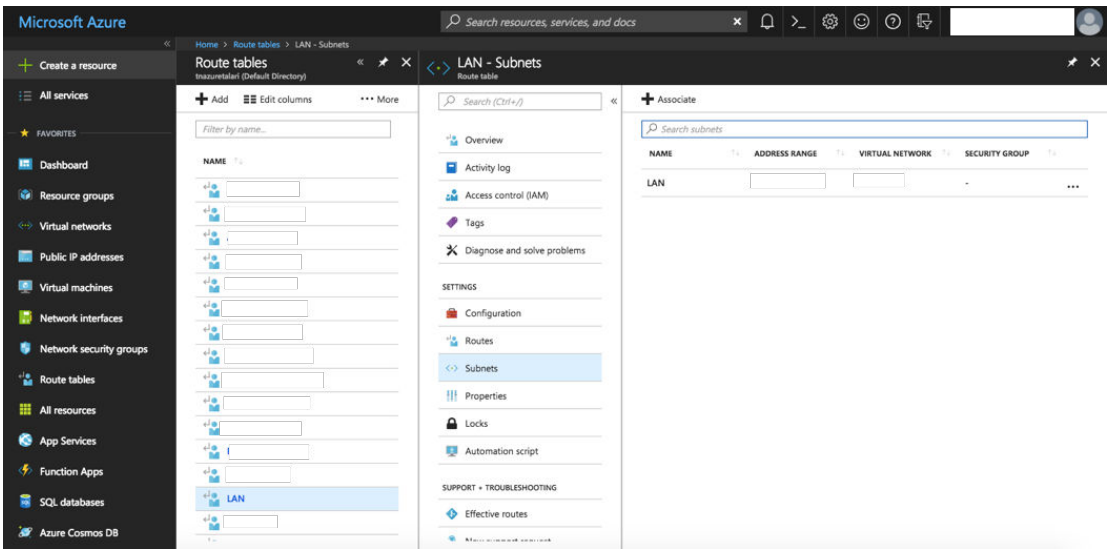
Figure 2-23 Modify Route Table



Once all required routes are added to the newly-created Route Tables, each Route Table will need to be associated with the appropriate Subnet. To associate a Subnet with a Route Table:

1. Select “Route Tables” from “All Services” in the Azure Portal Menu.
2. Select the Route Table you wish to associate with a Subnet.
3. Select “Subnets.”
4. Click “+ Associate.”
5. Select the VNET & Subnet you wish to associate the Route Table with.

Figure 2-24 Associate Route Table with Subnet



> **Note:**
>
> You may also need to add routes to your already-existing Company LAN Subnet(s) so they can route traffic to the newly-created Subnets.

Network Security Groups (NSGs)

You will need to create two Network Security Groups (NSGs): one for the MGT Interface (to be created in a later step) and one for the WAN Interface (to be created in a later step).

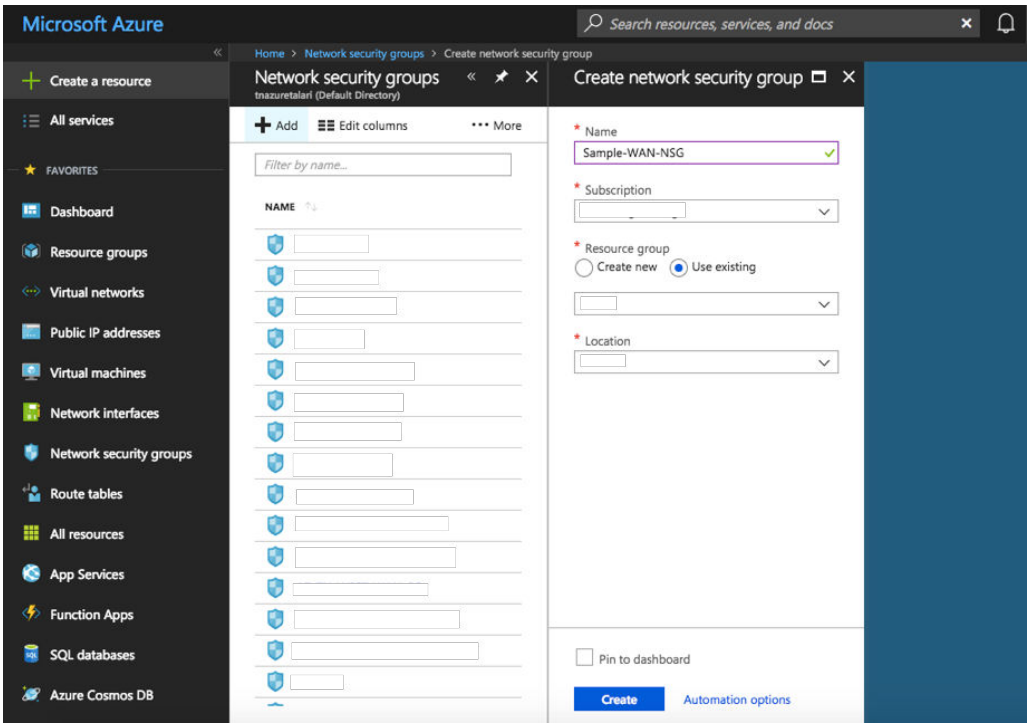
The following rules must to be added for both inbound and outbound traffic for the MGT & WAN NSGs:

- NSG-MGT - Permit TCP 443 | Permit TCP 22 (for browser & SSH access)
- NSG-WAN - Permit UDP 2156-2157 (TRP access)

To create a new Network Security Group:

1. Select “Network Security Groups” from “All Services” in the Azure Portal Menu.
2. Click “+ Add.”
3. Give the Network Security Group a Name.
4. Select the Subscription, Resource Group, and Location previously selected.
5. Click “Create.”

Figure 2-25 Create new Network Security Group



Once the new NSGs are created, the Inbound and Outbound Security Rules discussed above must to be added to each respective NSG.

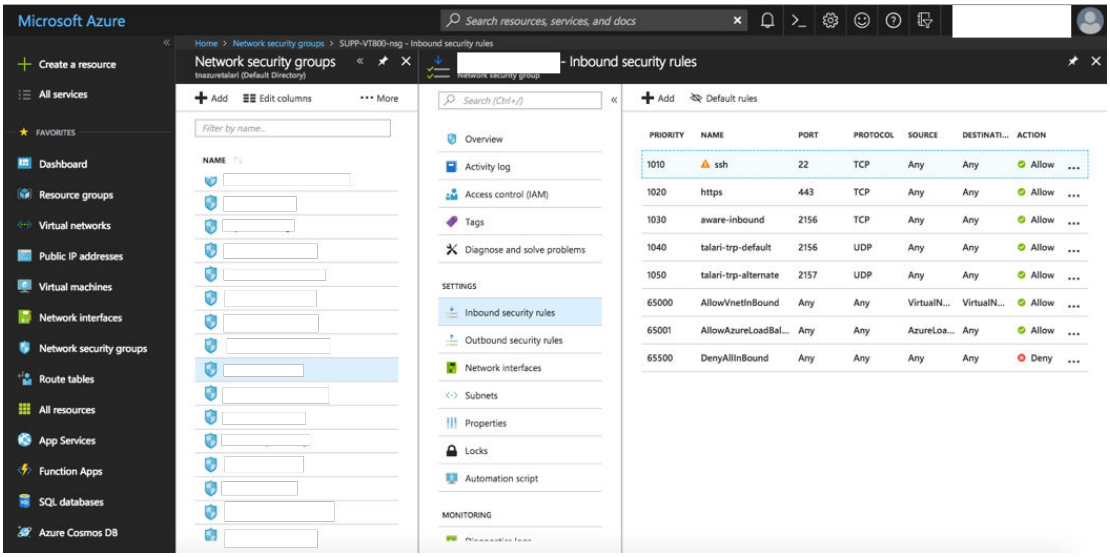
To modify an existing NSG and/or a new Inbound/Outbound Security Rule to an existing NSG:

1. Select “Network Security Groups” from “All Services” in the Azure Portal Menu.
2. Select the desired NSG.
3. Select “[Inbound | Outbound] security rules.”
4. Add rules as required.

Example Security Rule Configuration: An Inbound Rule allowing TRP Traffic (Talari UDP 2156 traffic) requires the following parameters:

- Source: any
- Source Port Ranges: *
- Destination: any
- Destination Port Ranges: 2156
- Protocol: UDP
- Action: Allow

Figure 2-26 Create Inbound/Outbound Security Rule on NSG



Public IP Addresses

At a minimum, the Virtual Appliance requires 1 Public IP Address:

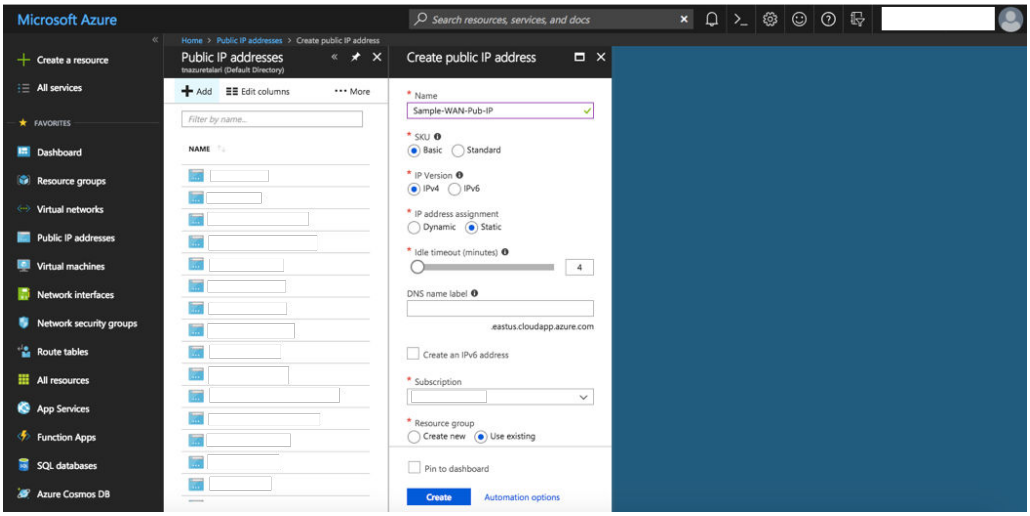
- WAN Pub IP – Public IP Address to be associated with the WAN Interface.
- MGT Pub IP – Public IP Address to be associated with the MGT Interface (optional once deployment is complete).

> **Note:**
>
> The MGT Interface may be permanently associated with a Public IP if public MGT access is desired. Should MGT access be set-up through the Conduit, however, the temporary Pub IP created for the MGT Interface here can be de-allocated once an Appliance Package has been applied to the Virtual Appliance and MGT access has been verified through the Conduit.

To Create a new Public IP Address:

1. Select “Public IP Addresses” from “All Services” in the Azure Portal Menu.
2. Click “+ Add.”
3. Enter a name for the Public IP Address.
4. Select “Basic” for “SKU” and “IPv4” for IP Version.
5. Static IP addresses are recommended to guarantee use of same Public IP by the Virtual Appliance WAN Links.
6. Select the Resource Group and Location defined in the “What You Need Before Starting” section.
7. Click “Create.”

Figure 2-27 Create Public IP Address



Virtual Network Interfaces (NICs)

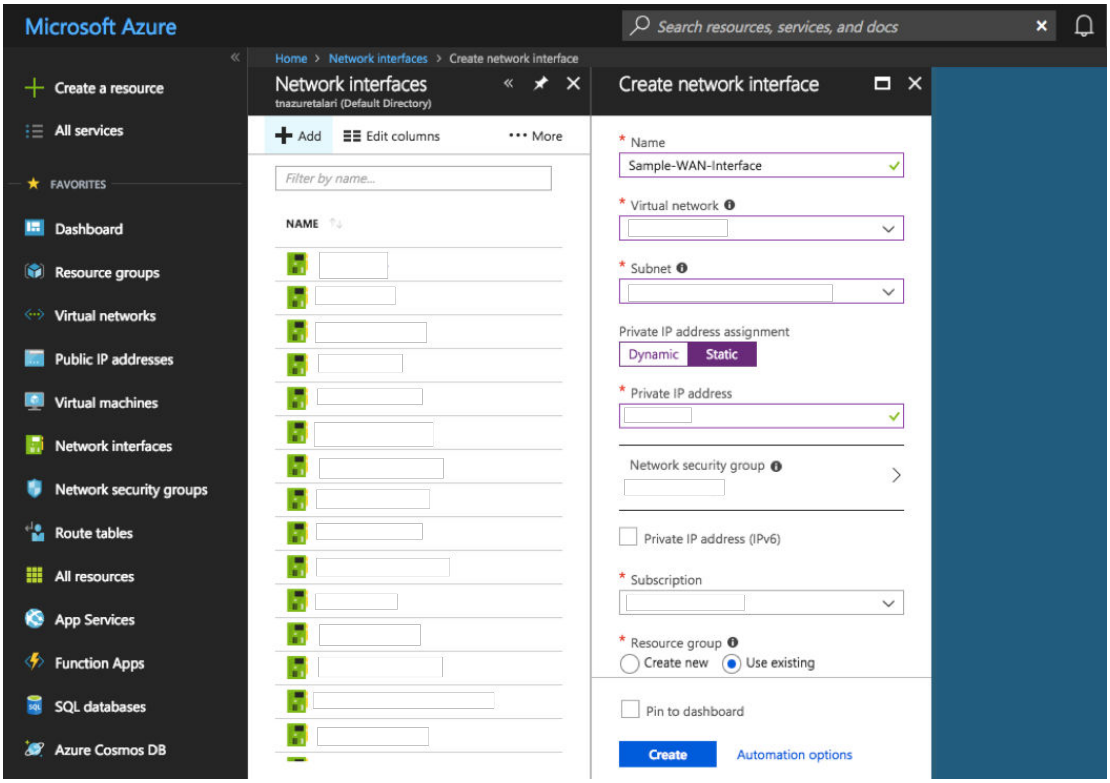
The Virtual Appliance requires 3 Virtual NICs at a minimum: one for MGT, one for LAN, and one for WAN. If additional WAN Links are used in the deployment, additional Interfaces will have to be created. Please contact Talari for assistance with advanced topology configuration & deployment.

To create a new Network Interface:

1. Select “Network Interfaces” from “All Services” in the Azure Portal Menu.

2. Click “+ Add.”
3. Enter a name for the new Interface.
4. Select the VNET & Subnet to be associated with that Interface.
5. Choose “Static” IP Address Assignment and give your Interface an IP defined in the “Addressing Guidelines & Planning” section.
6. Select the Subscription, Resource Group, and Location defined in the “What You Need Before Starting” section.
7. Click “Create.”

Figure 2-28 Create a Network Interface



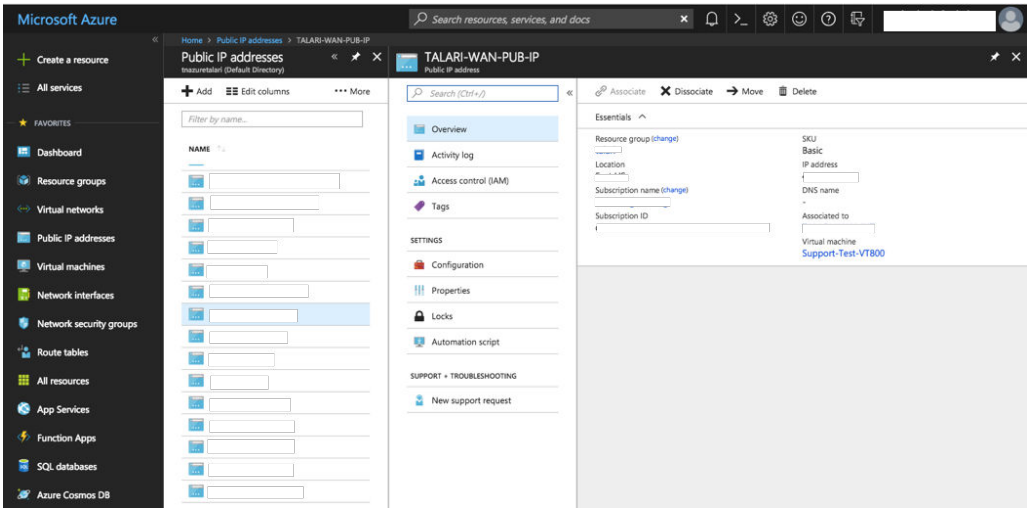
Virtual NIC Configuration

The WAN and MGT Interfaces created above will have to be associated with a previously-created or already-existing Public IP Address and NSG. All Interfaces will also have to be configured for IP Forwarding.

To Associate a Public IP Address with a Virtual NIC:

1. Select “Public IP Addresses” from “All Services” in the Azure Portal Menu.
2. Select a previously-created Public IP Address.
3. Click “Associate.”

Figure 2-29 Associate Public IP to Network Interface



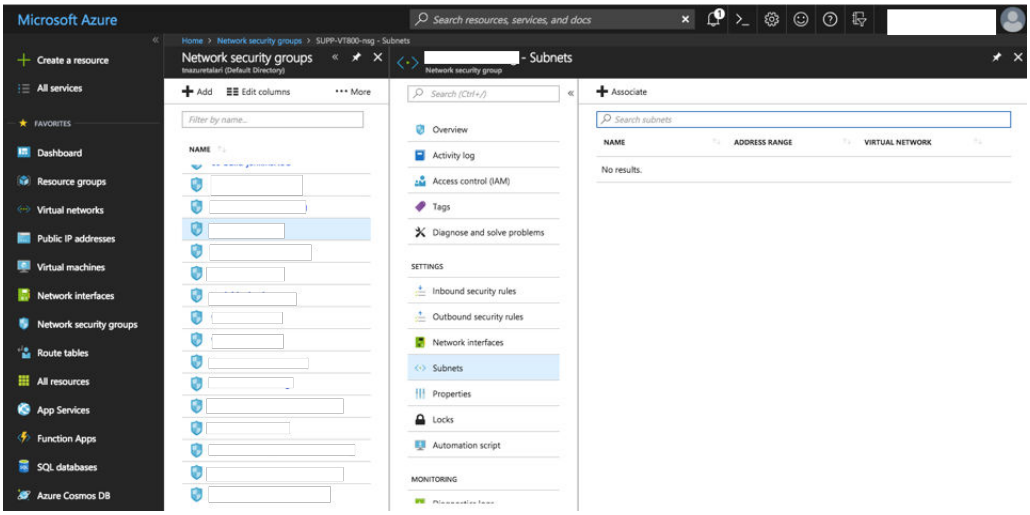
In the “Associate Public IP Address” sub-menu:

1. Select “Network Interface” as the Resource Type.
2. Select the appropriate Network Interface from the “Network Interface” selection menu.

To Associate a Network Security Group with a Virtual NIC:

1. Select “Network Security Groups” from “All Services” in the Azure Portal Menu.
2. Select to a previously-created NSG.
3. Select “Subnets.”
4. Click “Associate.”

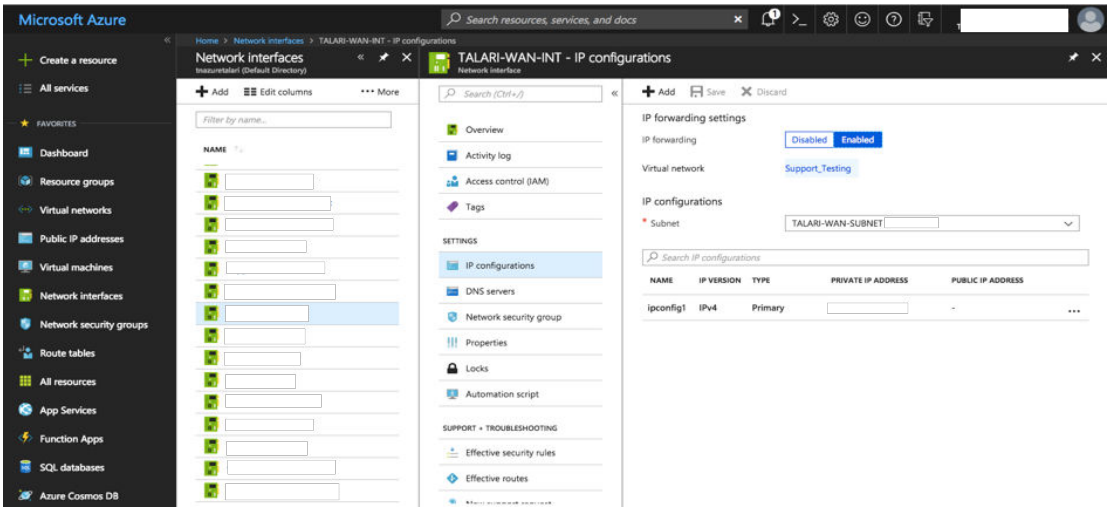
Figure 2-30 Associate Network Security Group with Virtual NIC



To enable IP Forwarding on a Virtual NIC:

1. Select “Network Interfaces” from “All Services” in the Azure Portal Menu.
2. Select to a previously-created Virtual NIC.
3. Select “IP Configurations.”
4. “Enable” IP Forwarding and click “Save.”

Figure 2-31 Enable IP Forwarding on Virtual NIC



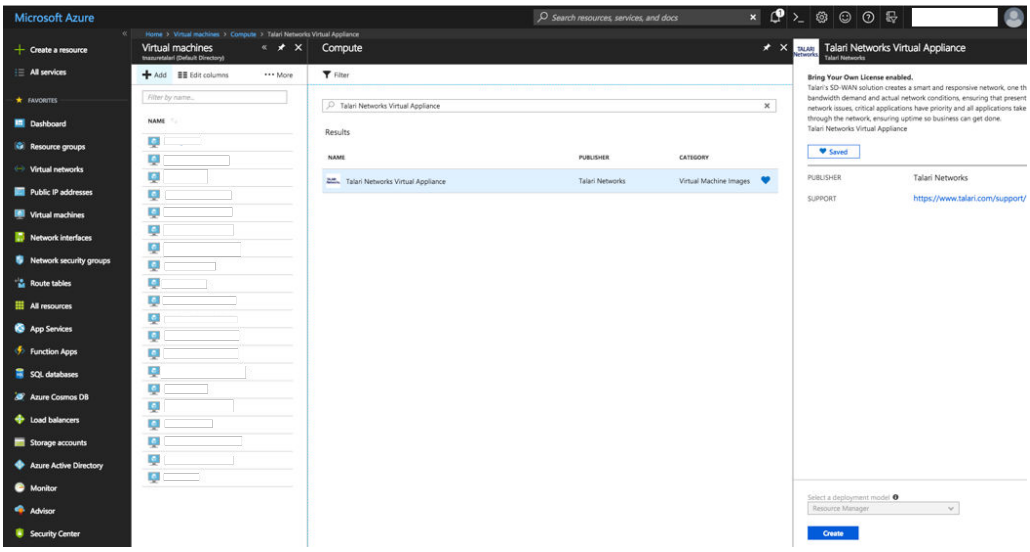
Deploy The Virtual Appliance

Once all Azure Resources have been created, configured, and gathered, the Virtual Appliance is may be created.

To create a new Virtual Appliance:

1. Navigate to “Virtual Machines” from “All Services” in the Azure Portal Menu
2. Click “+ Add.”
3. Search for “Talari” in the Azure Marketplace.
4. Select the “Talari Networks Virtual Appliance” image.
5. Click “Create”.

Figure 2-32 Select Marketplace Image



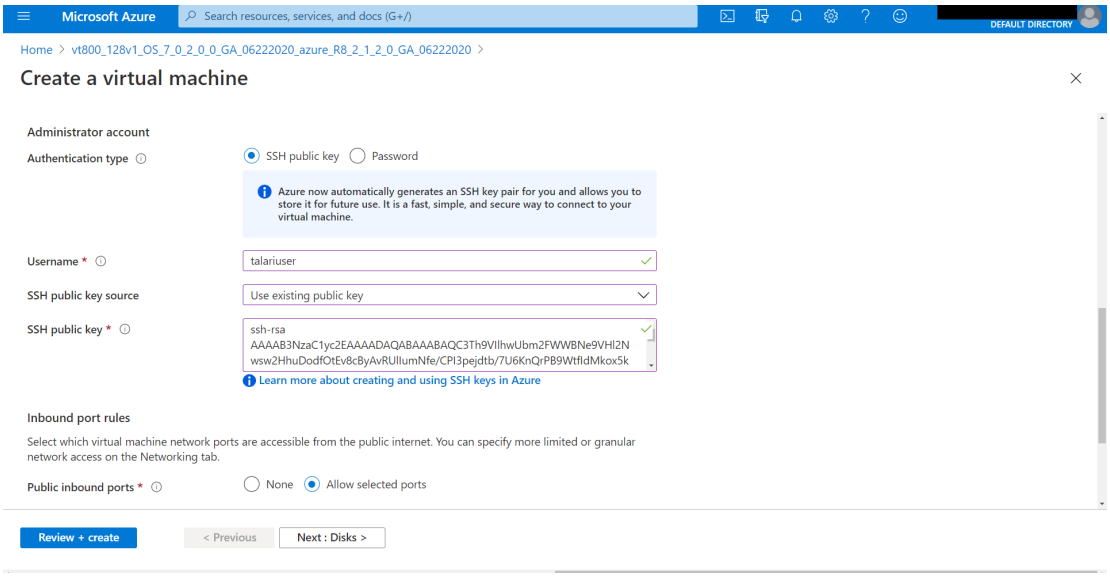
Once “Create” is clicked the page will redirect to a settings configuration sub-menu. In order to complete the Virtual Appliance creation process, the user must:

1. Configure basic settings.
2. Choose virtual machine size.
3. Configure optional features.
4. Confirm all appliance setting configurations.

Step 1: Configure Basic Settings

1. Enter a unique name for the Virtual Appliance.
2. Select “SSD” as the VM disk type.
3. Select Authentication type SSH public key
4. Enter “talariuser” for the Username.
5. Select and configure the SSH public key source (example below is for existing public key)
6. Select the Subscription, Resource Group, and Location defined in the “What You Need Before Starting” section.
7. Click “OK.”

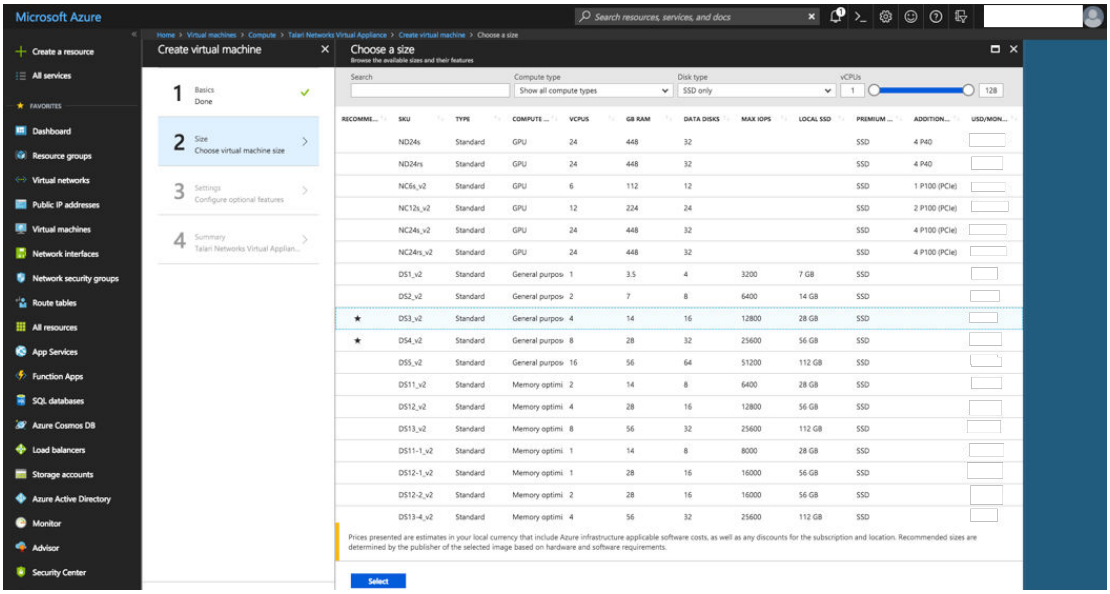
Figure 2-33 Create Virtual Machine: Configure Basic Settings



Step 2: Choose Virtual Machine Size

1. Select a desired VM size based your needs and the minimum supported requirements discussed in the “Prepare Your Azure Environment” section above.
2. Click “Select.”

Figure 2-34 Create Virtual Machine: Select a VM Size

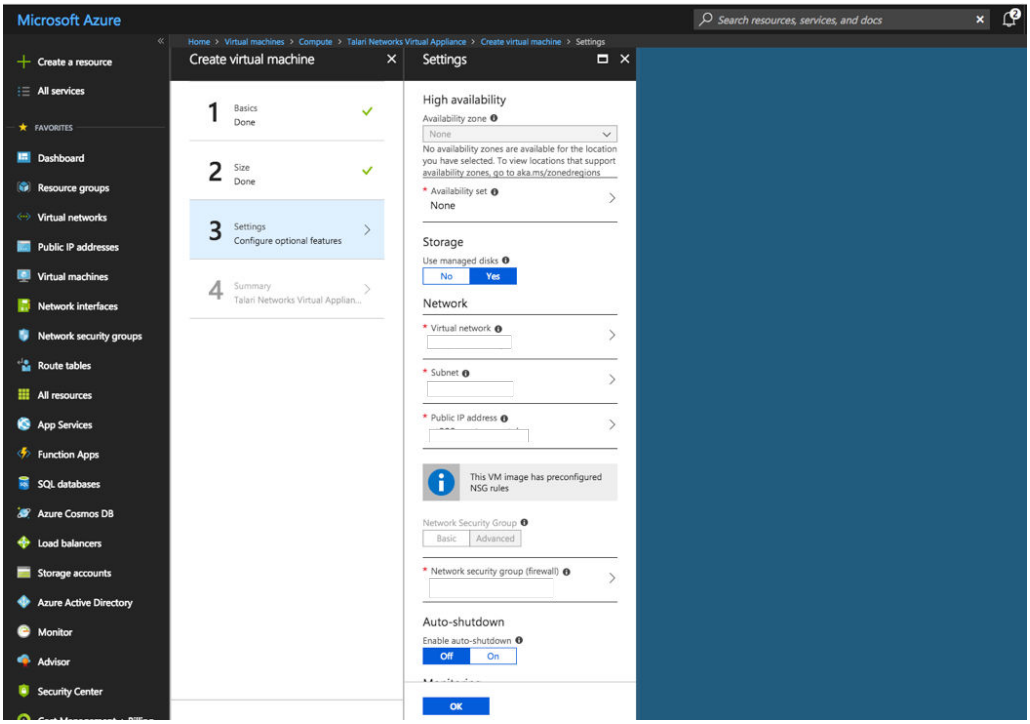


Step 3: Configure Optional Features

1. Leave “High Availability” at “None.”

2. Select “Yes” for “Use managed disks.”
3. Select the previously-created/designated VNET.
4. Select the previously-created MGT Subnet.
5. Select the previously-created MGT Public IP Address.
6. Select the previously-created MGT NSG.
7. Select “Off” for the “Auto-shutdown” menu.
8. Enable “Monitoring.”
9. Select the auto-populated Diagnostic storage account.
10. Select “No” for the “Managed service identity” option.
11. Click “OK.”

Figure 2-35 Create Virtual Machine: Configure Optional Features



Step 4: Summary and Deployment

1. Review the summary information and Terms of Use.
2. When satisfied and ready to accept the Terms of Use, click “Create” to build the Virtual Appliance. Wait until the deployment has completed (this can be verified in the notification window).

> **Note:**
>
> Full appliance deployment will take up to 10 minutes.

Step 5: Add Additional Network Interfaces

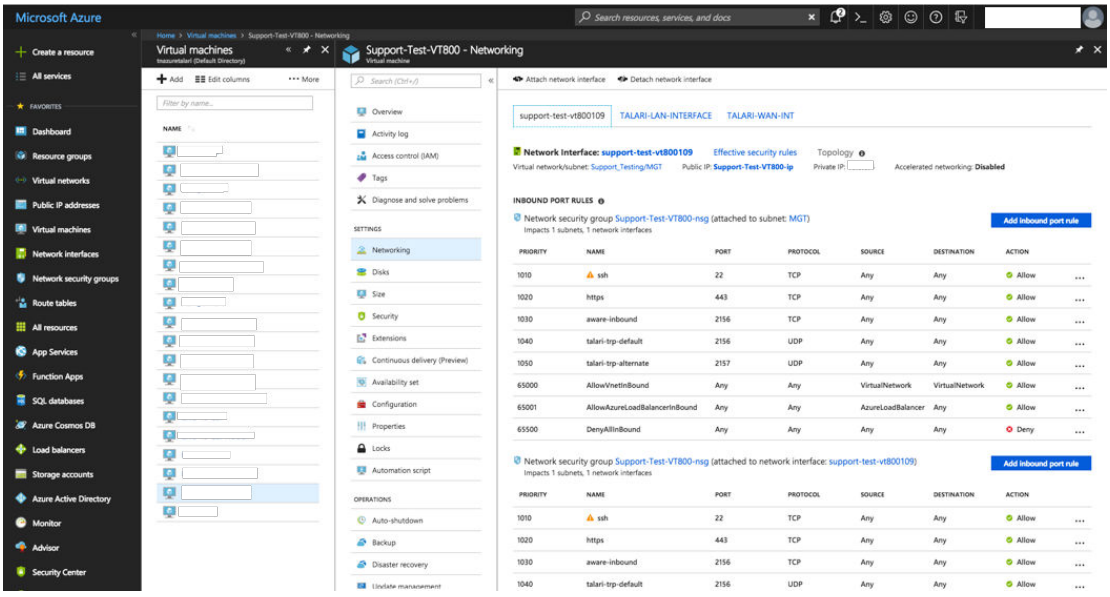
Once deployed, navigate to the newly-created Virtual Appliance and stop it. You will need to add the additional LAN/WAN Interfaces.

To add a Virtual NIC to a Virtual Machine:

1. Navigate to “Virtual Machines” from “All Services” in the Azure Portal Menu .
2. Select the newly-created Virtual Appliance.
3. Select “Networking” from the VM Menu.
4. Click “Attach network interface.”

> **Note:**
>
> The Interfaces must be attached in the following order: MGT | LAN | WAN. Failure to do so will incorrectly associate the interfaces, resulting in non-operability.

Figure 2-36 Attach Network Interface to VM



Verify all Public IPs, NSGs, Subnets, and NICs are configured, attached, and associated per the instructions above prior to turning the appliance back on.

Final Verification and Network Integration

1. Start the Virtual Appliance.
2. Using the above ssh key pair, login to talariuser on the appliance through the Public IP MGT interface

> **Note:**
>
> Even after deployment is successful, it may take some time (up to 10 additional minutes) before the management port will respond on the MGT IP as the software activates. Unless you have custom security rules in place to allow ICMP, you will NOT be able to ping the MGT IP even when it is accessible.

3. Change the talariuser password (sudo passwd talariuser)
4. Open a web browser and navigate to the Public IP. This should give you access to the standard Web GUI. Use talariuser for the user and the password created in the previous step.
5. Install the initial configuration package for the Virtual Appliance site gathered in the “What You Need Before Starting” section. Follow the prompts on the screen to install the package and enable the service.
6. Verify that the Virtual Appliance is connecting to Edge properly and that all paths are functioning as expected. This can be verified either on the Virtual Appliance side or the NCN.
7. Confirm connectivity from the new Virtual Appliance to the APN. At this point, the GUI should be accessible by the previously-defined private management IP. Once confirmed, the Public IP associated with the Management Interface may be dissociated and removed so the Web UI is no longer accessible via the Public IP if desired.

The Virtual Appliance in Azure should now be fully functional and integrated.

KVM Hypervisor

Follow these instructions to deploy Oracle SD-WAN Edge Virtual Appliance on Kernel-based Virtual Machine (KVM).

- Install virtual manager on the KVM
- Configure LAN and WAN Bridges
- Use CPU affinity to pin the VM vCPU to physical CPUs

1. Login to the KVM server and create a new virtual machine.
2. Open Virtual Manager (**Application**, **System Tools**, **Virtual Machine Manager**).
3. From the **File** menu, click on **New Virtual Machine**.
4. Select Import existing disk image as the installation type.
5. Click on **Forward**.
6. Enter the storage path where **qcow2 image for vt800 or vt800_128** is available.
7. Enter **16GB** for the RAM configuration (32GB for vt800_128) and **8** for the CPU configuration.
8. Click on **Forward**.
9. Enter a name for the virtual machine. Alphanumeric characters, underscores (_), periods (.), and hyphens (-) are allowed.

10. Click on the checkbox before **Customize configuration before install**.
11. Click on **Finish**.
12. Click on the **Add Hardware** button and select **Storage** from the menu on the left.
13. Enter **180GB** as the storage disk size.
14. Click on **Finish**.
15. Select **Interface (Management)**, which begins with **NIC:**.

> **Note:**
>
> Use Host devices like eno1: macvtap" for the management interfaces, and host devices like ens1f0:macvtap for APN-facing interfaces

16. Make the network source value **Host device <no.>:macvtap**.
17. Make the source mode **Bridge**.
18. Make the device model **Virtio**.
19. Click on **Apply**.
20. Click on **Add Hardware**.
21. Click on **Network** from the menu on the left.
22. Create a virtual interface using one of the following methods:
    a. mactvap: Select **host device <no.>:macvtap** as the network source.
    b. Linux bridge: Follow the instructions in Create Linux/Networking Bridge and then select **Bridge lanbr<no.>: Host Device ens<no.>** as the network source.
23. Select **Bridge** as the Source Mode.
24. Select **Virtio** as the Device Model.
25. Click on **Finish**.
26. Click on **Begin Installation**.
27. Enter your credentials.
28. Enter the following commands to set the Management IP

```
$tcon
$management_ip
$set interface <ip_address> <subnet_mask> <gateway>
apply
```

29. Power off the instance, then power it back on.
30. Login to SD-WAN Edge.

Create Linux/Networking Bridge

Follow these instructions to create a networking bridge.

1. Log in to the KVM server.

2. Create a file called `ifcfg-lanbrN` and replace N with the interface number under `/etc/sysconfig/network-scripts/ .`
3. Open the file in an editor and enter the following

```
[localadmin@localhost network-scripts]$ cat ifcfg-lanbr201
DEVICE=lanbr201
TYPE=Bridge
BOOTPROTO=none
ONBOOT=yes
DELAY=0
[localadmin@localhost network-scripts]$
```

4. To add the virtual interface to the LAN bridge, ensure `ONBOOT=yes` and `BRIDGE=`the name of the LAN bridge in the `ifcfg-ens2f0` file, where `ifcfg-ens2f0` is the virtual interface.

```
[localadmin@localhost network-scripts]$ cat ifcfg-ens2f0
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens2f0
UUID=bf4196e3-b003-41ff-8b02-29ed79ea3552
DEVICE=ens2f0
ONBOOT=yes
BRIDGE=lanbr201
[localadmin@localhost network-scripts]$
```

5. Create a WAN bridge by logging into the KVM server.
6. Create a file called `ifcfg-wanbrN` and replace N with the interface number under `/etc/sysconfig/network-scripts`.
7. Open the file in an editor and enter the following.

```
[localadmin@localhost network-scripts]$ cat ifcfg-wanbr201
DEVICE=wanbr201
TYPE=Bridge
BOOTPROTO=none
ONBOOT=yes
DELAY=0
[localadmin@localhost network-scripts]$
```

8. To add the virtual interface to the WAN bridge, ensure `ONBOOT=yes` and `BRIDGE=`the name of the WAN bridge in the `ifcfg-ens2f1` file, where `ifcfg-ens2f1` is the virtual interface.

```
[localadmin@localhost network-scripts]$ cat ifcfg-ens2f1
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens2f1
UUID=f45577ab-f733-4c53-a791-fe44662cc5b4
DEVICE=ens2f1
ONBOOT=yes
BRIDGE=wanbr201
[localadmin@localhost network-scripts]$
```

9. Restart the network by entering the following.

```
$sudo systemctl restart network
```

10. Verify the interfaces are connected to the bridges by entering the following.

```
$sudo brctl show
```

The interfaces should look like the following

```
[localadmin@localhost network-scripts]$ brctl show
bridge name     bridge id               STP enabled     interfaces
lanbr201        8000.3cfdfe6272a8       no              ens2f0
                                                        vnet0
lanbr202        8000.3cfdfe6272aa       no              ens2f2
                                                        vnet1
lanbr203        8000.3cfdfe6272b8       no              ens3f0
                                                        vnet2

wanbr201        8000.3cfdfe6272a9       no              ens2f1
                                                        vnet3
wanbr202        8000.3cfdfe6272ab       no              ens2f3
                                                        vnet4
wanbr203        8000.3cfdfe6272b9       no              ens3f1
                                                        vnet5
                                                        vnet6
[localadmin@localhost network-scripts]$
```

Automatically Starting Guests After Reboot

Follow these steps to make guests start automatically during the reboot phase.

1. Set a guest to start automatically by entering the following command

```
[localadmin@localhost network-scripts]$ sudo virsh autostart
vt800_128
[sudo] password for localadmin:
Domain vt800_128 marked as autostarted
[localadmin@localhost network-scripts]$
```

2. Stop a guest from starting automatically by entering the following command

```
[localadmin@localhost network-scripts]$ sudo virsh autostart --
disable vt800_128
Domain vt800_128 unmarked as autostarted

[localadmin@localhost network-scripts]$
```

Extending the Guest VM hard disk

The default disk size of the created instance is 175.8G. Follow these instructions to extend the guest VM.

1. Shut down a running guest machine's virtual disk by entering its name or ID.

```
[localadmin@localhost network-scripts]$ sudo virsh list
[sudo] password for localadmin:
 Id    Name                           State
----------------------------------------------------
 1     EngPerf3-CL1-TN                running
 2     EngPerf3-NCN-TN                running
 9     vt800_128                      running

[localadmin@localhost network-scripts]$


[localadmin@localhost network-scripts]$ sudo virsh shutdown
<instance-name>
Domain vt800_128 is being shutdown

[localadmin@localhost network-scripts]$


[localadmin@localhost network-scripts]$ sudo virsh list
 Id    Name                           State
----------------------------------------------------
 2     EngPerf3-CL1-TN                running
 3     EngPerf3-NCN-TN                running

[localadmin@localhost network-scripts]$
```

2. Locate the guest image disk path.

```
[localadmin@localhost ~]$ sudo virsh domblklist vt800_128
Target     Source
------------------------------------------------
hda        /home/localadmin/Downloads/
vt800_128v1_OS_7_0_0_0_0_GA_09132019_kvm_R8_2_0_1_0_GA_10172019.qcow2

[localadmin@localhost ~]$
```

3. Extend the disk size to the desired capacity by entering the following command.

```
[localadmin@localhost ~]$ sudo qemu-img resize /home/localadmin/Downloads/
vt800_128v1_OS_7_0_0_0_0_GA_09132019_kvm_R8_2_0_1_0_GA_10172019.qcow2 +10G
```

> **Note:**
>
> quemu-img cannot resize an image that contains snapshots. You must first remove all VM snapshots:
>
> ```
> [localadmin@localhost ~]$ sudo virsh snapshot-list vt800_128
> Name        Creation Time               State
> ------------------------------------------------
>  snapshot1   2019-04-16 08:54:24 +0300   shutoff
>
>
> [localadmin@localhost ~]$ sudo virsh snapshot-delete --domain
> vt800_128 --snapshotname snapshot1
> Domain snapshot snapshot1 deleted
> ```

4. Extend the disk by using **+** before disk capacity

```
[localadmin@localhost ~]$ sudo qemu-img resize /home/localadmin/Downloads/
vt800_128v1_OS_7_0_0_0_0_GA_09132019_kvm_R8_2_0_1_0_GA_10172019.qcow2 +10G
Image resized.
[localadmin@localhost ~]$
```

5. Power up the guest machine

```
[localadmin@localhost ~]$ sudo virsh start vt800_128
Domain vt800_128 started

[localadmin@localhost ~]$
```

6. Verify the disk layout

```
talariuser@DUT-KVM-VT800:~# sudo lsblk
NAME    MAJ:MIN       RM       SIZE       RO       TYPE      MOUNTPOINT
sda       8:0            0     185.8G    0         disk
├─sda4    8:4            0         1K       0         part
```

```
├─sda2   8:2            0        10G       0         part    /
├─sda5   8:5            0         1G       0         part
[SWAP]
├─sda3   8:3            0        10G       0         part
├─sda1   8:1            0       200M       0         part       /
grub
└─sda6   8:6            0     154.6G    0         part       /home
talariuser@DUT-KVM-VT800:~#
```

KVM Tuning

For better performance, turn off TSO/GSO in KVM by following these steps:

1. Log in to the KVM host.
2. Check to see if each of the data interface offloads are on or off.

   ```
   sudo ethtool -k <interface> | grep offload
   ```

   where the <interface> is the data interface.

   ```
   [root@localhost ~]# sudo ethtool -k eno1 | grep offload
    tcp-segmentation-offload: on
    udp-fragmentation-offload: off
    generic-segmentation-offload: on
    generic-receive-offload: on
    large-receive-offload: off
    rx-vlan-offload: on
    tx-vlan-offload: on
    l2-fwd-offload: off
    hw-tc-offload: off
    esp-hw-offload: on
    esp-tx-csum-hw-offload: on
    rx-udp_tunnel-port-offload: on
   ```

3. If offload is on, turn it off by entering the following command

   ```
   [root@localhost ~]# ethtool -K eno1 rx off tx off tso off ufo off
   gso off gro off lro off
    Cannot change udp-fragmentation-offload
    [root@localhost ~]# sudo ethtool -k eno1 | grep offload tcp-
   segmentation-offload: off
    udp-fragmentation-offload: off
    generic-segmentation-offload: off
    generic-receive-offload: off
    large-receive-offload: off
    rx-vlan-offload: on
    tx-vlan-offload: on
    l2-fwd-offload: off
    hw-tc-offload: off
    esp-hw-offload: on
    esp-tx-csum-hw-offload: on
    rx-udp_tunnel-port-offload: on
    [root@localhost ~]#
   ```

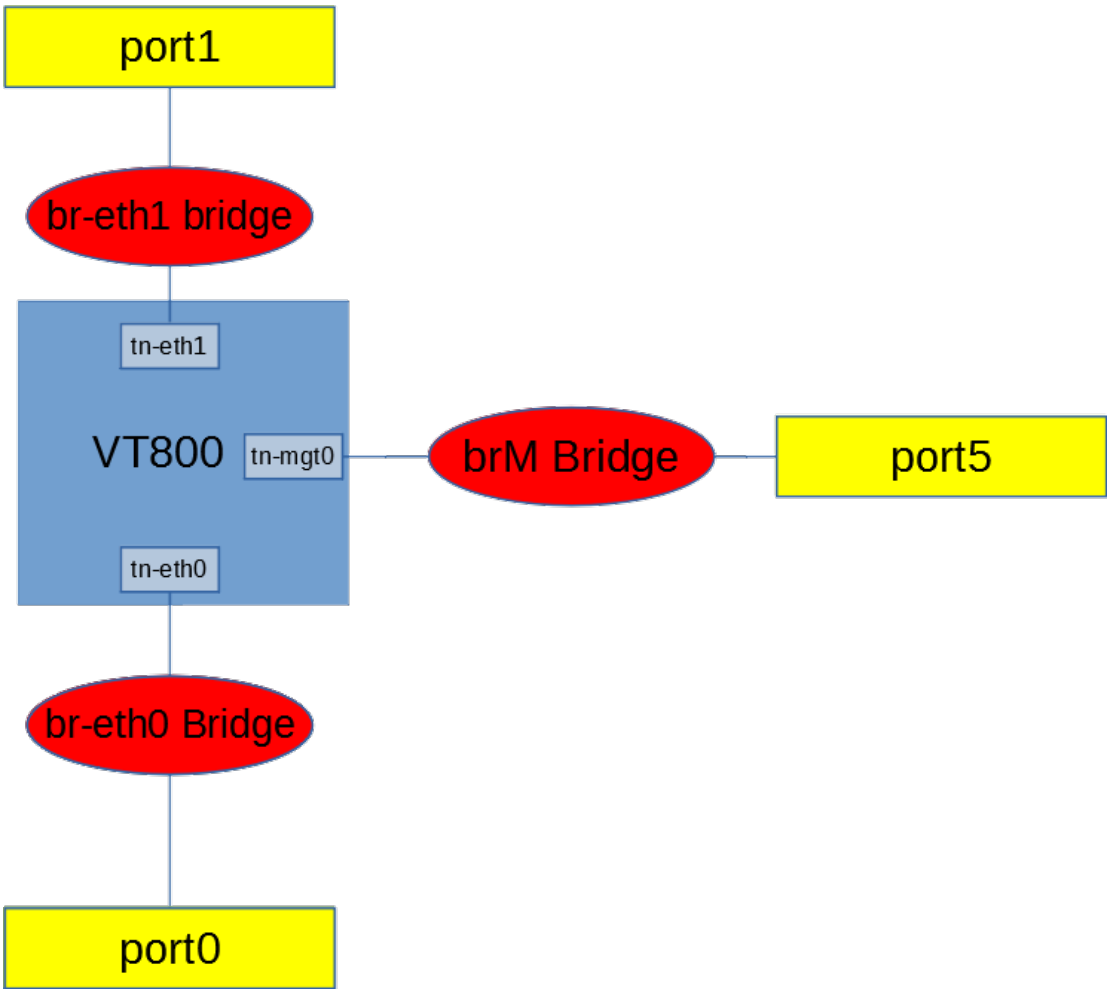
Optimizing KVM for VT800

For higher level hypervisors such as ESXi, much of the details and optimization of the hypervisor are handled for you, as the operating system is optimized to be a hypervisor. As KVM is just a piece of the broader Linux kernel, and other non-KVM entities are present, the tuning of the OS to optimize KVM is left to the administrator. For some deployments of KVM their performance may not be mission critical, so no tuning may be required. These recommendations assume the VT800 is mission critical and may be the only application running on the hardware/system.

These strategies apply to VT800 and VT800_128 and are not limited to 9.1 and may be used at prior releases.

The deployment assumes the VT800 network interfaces use the virtio device model and connect to the device ports via bridges.

The VT800 supports up to 12 data ports. This example demonstrates two data ports and one management port.



The optimizations below assume the VT800 is already running and able to pass traffic.

Interface optimizations

For each used physical data port on the system (port0 and port1, above), set txqueuelen to 10000 and the mtu to 2004. Assuming port0 and port1 port names are eth0 and eth1.

```
sudo ifconfig eth0 txqueuelen 10000 mtu 2004
sudo ifconfig eth1 txqueuelen 10000 mtu 2004
```

Do the same with all the vnet interfaces on the system.

```
sudo ifconfig vnet0 txqueuelen 10000 mtu 2004
sudo ifconfig vnet1 txqueuelen 10000 mtu 2004
sudo ifconfig vnet2 txqueuelen 10000 mtu 2004
```

Do the same with all the data bridges.

```
sudo ifconfig br-eth0 txqueuelen 10000 mtu 2004
sudo ifconfig bt-eth1 txqueuelen 10000 mtu 2004
```

These settings will need to be reset after each guest start or restart.

CPU threading optimization

Inside the VT800 (or any appliance), threads are carefully pinned to the available CPUs. But by default, these CPUs float around on the hypervisor. The VT800 CPUs must be pinned to the physical CPUs. This can be as simple as a one-to-one mapping.

virsh vcpupin <domain> <guest cpu#> <host cpu#>

For example with guest (VT800) name of ol7.9:

```
sudo virsh vcpupin ol7.9 0 0
sudo virsh vcpupin ol7.9 1 1
sudo virsh vcpupin ol7.9 2 2
sudo virsh vcpupin ol7.9 3 3
```

These mapping will need to be reset after each guest start or restart.

Interrupts

On lower end processors and implementations with < 10 CPUs, the interrupts caused by the packet rates are usually not sufficient to impact the overall performance of the vt800. However, as the rates increases, the load on the cores assigned to handling interrupts will affect performance. As packets are processed on the host and the guest, twice the normal number of interrupts occur. If possible, CPUs in the guest (VT800) should be reserved for interrupts and host interrupts should be directed to CPUs that are not used by the guest. The CPU pinnings withing the VT800 reserve CPUs for interrupts, and irqbalance can be used to direct the interrupts there. Irqbalance should be used on the host to direct interrupts to unused CPUs (if available).

halt_poll_ns

CPUs with variable clock rates (Xeon) will delay the CPU from halting even when it is idle. This reduces the latency of a CPU. On these processors setting the value to 600000 has shown to increases overall packet performance.

```
sudo sh -c "echo 600000 > /sys/module/kvm/parameters/halt_poll_ns"
```

On CPUs with static clock rates (Atom), setting the value to 0 has shown to increases overall packet performance.

```
sudo sh -c "echo 0 > /sys/module/kvm/parameters/halt_poll_ns"
```

This setting will revert to default on a host reboot and will need to be reset.

Performance governor

On CPUs with variable clock rates (Xeon), this setting also reduces the latency of a CPU. it disallows a CPU's clock from dropping too low, effectively keeping it "warm". As frequency governors do not exist on an Atom processor, this command has no effect there.

```
sudo cpupower frequency-set --governor performance
```

This setting will revert to default on a host reboot and will need to be reset.

Disk Image and Deployment Size

SD-WAN Edge images are 40 GB by default. This is sufficient for client deployments that do not require WANOp functionality. If you require WANop feature or if you are installing an NCN system, you will need to increase the local file system size. Increases in size will be applied to the /home partition.The following table states disk size requirements for different installation types.

Table 2-1 Installation Types and Disk Space Requirements

Deployment	Required Disk Space	Manually add at least this much to /home
SD-WAN Edge Client	40 GB	0
SD-WAN Edge Client with WANOp	120 GB	80 GB
SD-WAN Edge as NCN	100 GB	60 GB
SD-WAN Edge as NCN with WANOp	180 GB	140 GB

When initially starting the SD-WAN virtual machines, the following volumes will be created:

Table 2-2 SD-WAN Edge Default Disk Layout

Image	Size
Primary OS	6GB

Table 2-2 (Cont.) SD-WAN Edge Default Disk Layout

Image	Size
Secondary OS	6GB
Swap	1GB
/home	26GB

When your deployment requires more space than the default image provides, increase the image size from the hypervisor after starting up the virtual appliance.

The following topics explain how to increase size on different hypervisors.

Increasing Image Size for KVM

See Extending the Guest VM hard disk for more details.

1. Shut down the VM if you have not resized before deployment.
2. Enter the following command

   ```
   qemu-img resize vt…..qcow2 +80G
   ```

3. Start the VM.

Increasing Image Size for ESXi

1. Edit the VM.
2. Change disk size to 120GB.
3. Stop and start the VM.

Increasing Image Size for HyperV

1. Shut down the VM.
2. Navigate to **Actions**, **Edit Disk**.
3. On the Locate Disk page, find the disk image for the desired VM and click on **Next**.
4. On the Choose Action page, select **Expand**, and then click **Next**.
5. Change 40 to 120 and click **Finish**.
6. Start the VM.

Increasing Image Size for OCI

1. Navigate to your desired instance.
2. Under Resources, click on **Boot Volume**.
3. Click on the boot volume link.
4. Click on **Edit**.
5. Add 80 to the **Volume Size** field.

6. Save your changes.
7. Stop the instance, then restart.

Increasing Image Size for Azure

1. Shut down the instance.
2. Go to **Settings**, **Disk**.
3. Select the OS Disk.
4. Click on **Size + Performance**.
5. Select a disk size greater than the desired disk size.
6. Click on **Resize**.
7. Start the instance.

Increasing Image Size for AWS

When launching the instance, on the Add Storage step, the Root Volume size can be increased. You can modify its size attribute.

To increase the size of an existing instance:

1. Stop the instance.
2. From the instance page, click on the Storage tab.
3. Click the Volume ID.
4. From the Actions dropdown, select **Modify Volume**.
5. Change the size field, then click **Modify**.
6. Click **Yes, I am sure**.
7. Start the instance.

Install SD-WAN Edge from the Oracle Cloud Marketplace

You can install the SD-WAN Edge virtual appliance directly from the Oracle Cloud Marketplace, which simplifies the process and lets you run your application sooner. You must have an Oracle Cloud Infrastructure (OCI) account to use the marketplace. Search for "Oracle SD-WAN Edge Virtual Appliance" on the Marketplace web site.

When you sign in to the SD-WAN Edge virtual appliance for the first time, you must use the default user name and set your password.

1. Connect to the Management IP address of the instance with SSH protocol, using the default username `talariuser` and key authentication. For example,

   ```
   ssh -i $keypath talariuser@$instanceIP
   ```

2. Set the user login password by way of `sudo passwd talariuser`.
3. Access SD-WAN Edge by entering the management IP address in your browser, and log in as talariuser with the password you set in the previous step.

For more information, see:

Where to Find Your Tenancy's OCID

Oracle Cloud Marketplace Documentation

Launching a Linux Instance

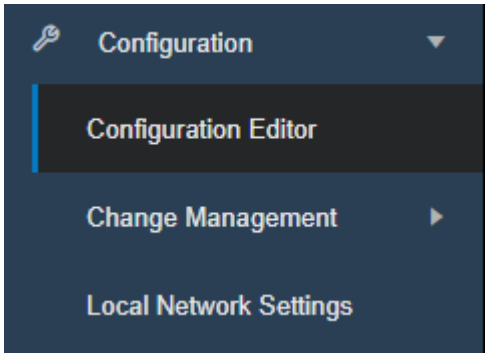
Connecting to Your Instance

Out of Band ZTP

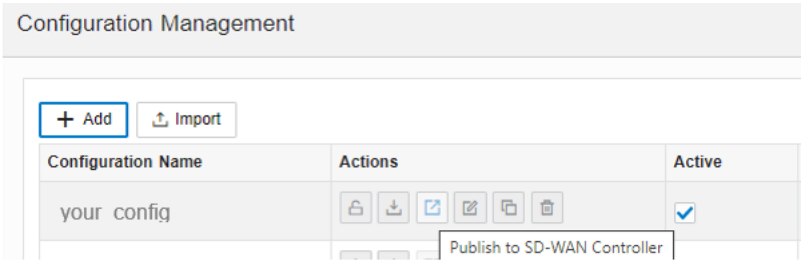
Out of Band ZTP is supported on VT800s and VT800-128s running Oracle SD-WAN Edge 9.1 or above only.

Create and Download Software Package

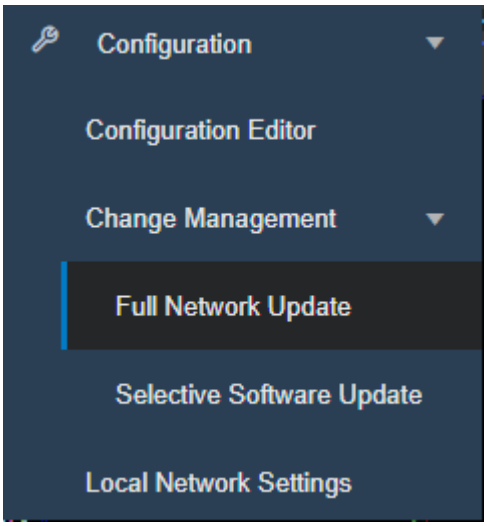
1. Log into the NCN Controller appliance
2. Add the new appliance by navigating to **Configuration** > **Configuration Editor**



3. From the Configuration Editor, export the new configuration to the **Inbox** of the NCN Controller appliance by selecting the **Publish to SD-WAN Controller** action.

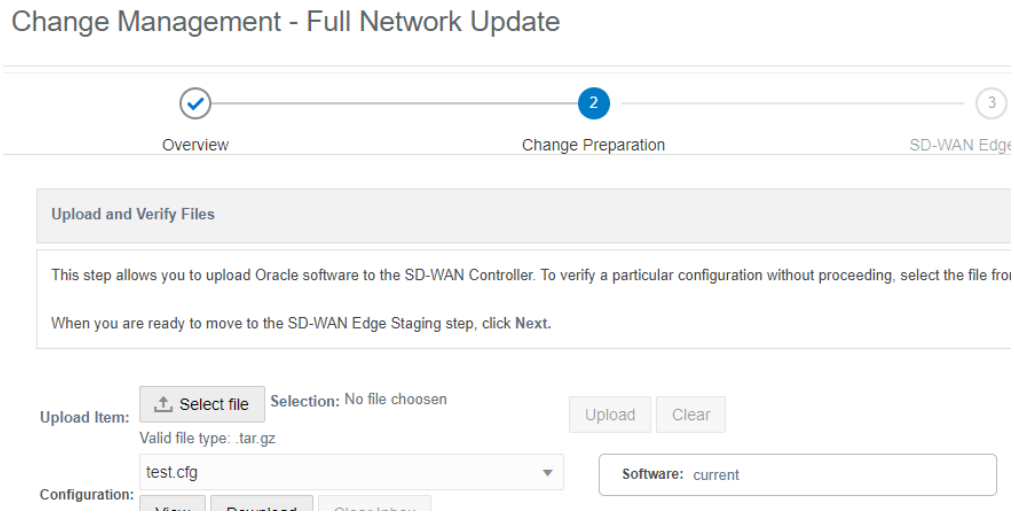


4. Create the software package for the new appliance by applying the new configuration to your system using the following **Full Network Update** steps:
   a. Go to **Configuration** > **Change Management** > **Full Network Update**

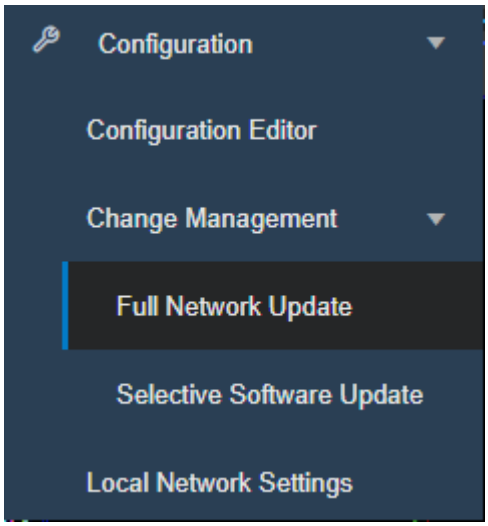


b. The configuration file appears in the **Configuration** pull-down selector.

c. The software should remain current. Continue to **Staging** and **Activation** steps to fully apply the configuration.

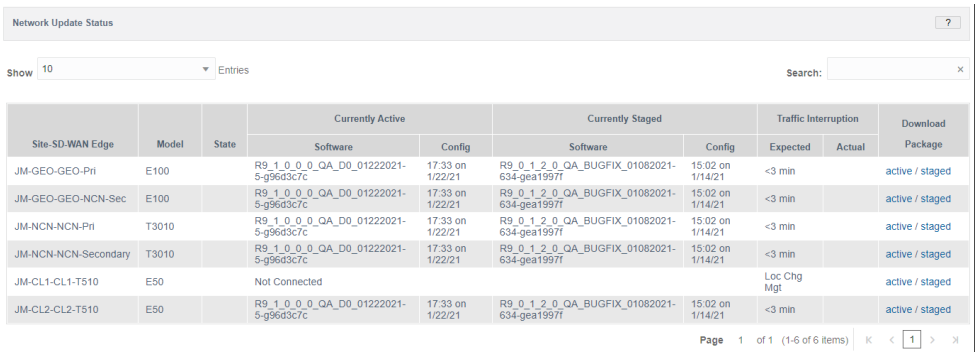


5. After the new configuration is installed and fully activated on the NCN, go back to **Configuration** > **Change Management** > **Full Network Update**.



The new appliance should show up in the **Network Update Status** table at the bottom.

6. In the **Download Package** column there are links to download the Active and Staged software packages needed to configure the appliance. Select the **Active** link.



Site-SD-WAN Edge	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
JM-GEO-GEO-Pri	E100		R9_1_0_0_0_QA_D0_01222021-5-g96d3c7c	17:33 on 1/22/21	R9_0_1_2_0_QA_BUGFIX_01082021-634-gea1997f	15:02 on 1/14/21	<3 min		active / staged
JM-GEO-GEO-NCN-Sec	E100		R9_1_0_0_0_QA_D0_01222021-5-g96d3c7c	17:33 on 1/22/21	R9_0_1_2_0_QA_BUGFIX_01082021-634-gea1997f	15:02 on 1/14/21	<3 min		active / staged
JM-NCN-NCN-Pri	T3010		R9_1_0_0_0_QA_D0_01222021-5-g96d3c7c	17:33 on 1/22/21	R9_0_1_2_0_QA_BUGFIX_01082021-634-gea1997f	15:02 on 1/14/21	<3 min		active / staged
JM-NCN-NCN-Secondary	T3010		R9_1_0_0_0_QA_D0_01222021-5-g96d3c7c	17:33 on 1/22/21	R9_0_1_2_0_QA_BUGFIX_01082021-634-gea1997f	15:02 on 1/14/21	<3 min		active / staged
JM-CL1-CL1-T510	E50		Not Connected				Loc Chg Mgt		active / staged
JM-CL2-CL2-T510	E50		R9_1_0_0_0_QA_D0_01222021-5-g96d3c7c	17:33 on 1/22/21	R9_0_1_2_0_QA_BUGFIX_01082021-634-gea1997f	15:02 on 1/14/21	<3 min		active / staged

Page 1 of 1 (1-6 of 6 items)

7. The software package for the client appliance is downloaded to the computer's **Download** folder/location. (ex. Package name: `<ApplianceName>-A-R9_1_0_0_0_GA_<date>.zip`)
8. Copy the downloaded active package to the FAT32 formatted USB drive with the label of **ZTP**.
9. Ensure that this is the only software package on the USB drive. If not, remove other software packages.

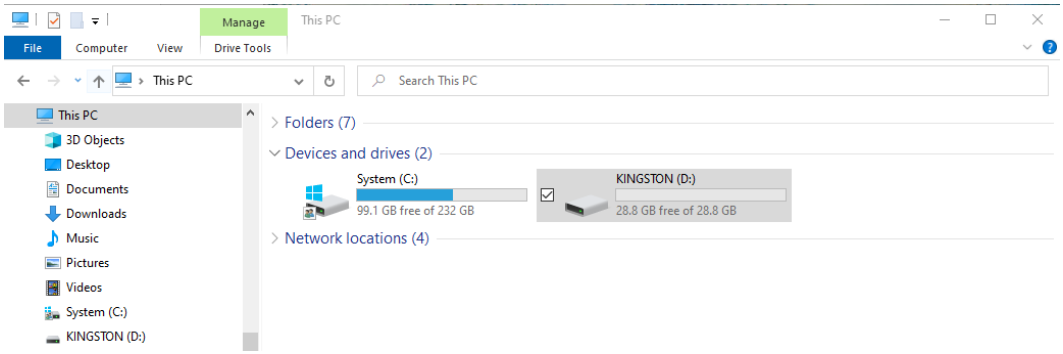
Formatting the USB Drive

Oracle recommends use of a new USB drive to ensure there are no partitions on the device. The SD-WAN appliance expects a single partition with the specified label.

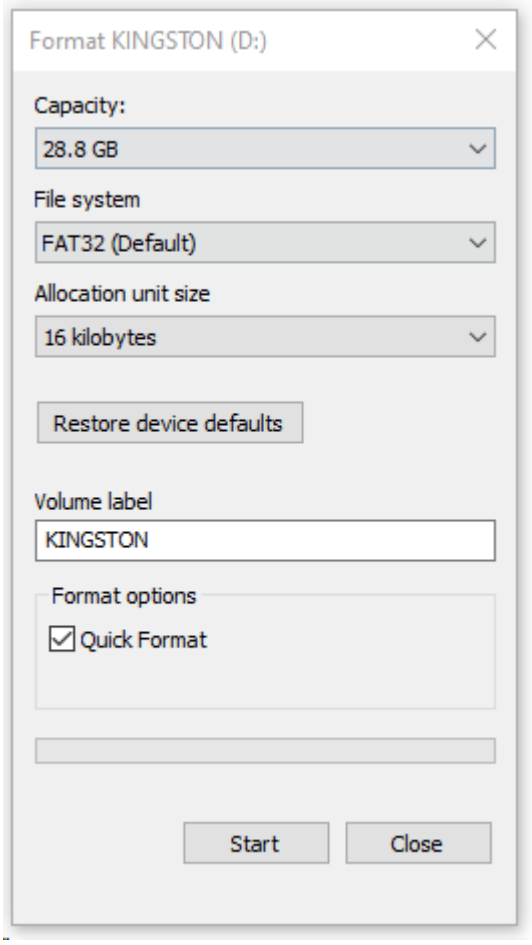
For Windows

1. Insert the USB drive into your computer
2. If asked, do not encrypt your USB drive

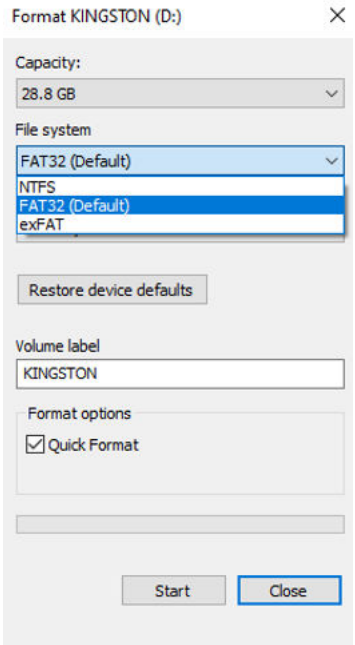
3. Open your Windows or File Explorer to locate the USB drive
4. Ensure the USB drive is at least 100 MB.
5. Select **This PC** to show the USB drive under the **Devices and drives** section



6. Right click on the USB drive and select **Format…** to display the format menu

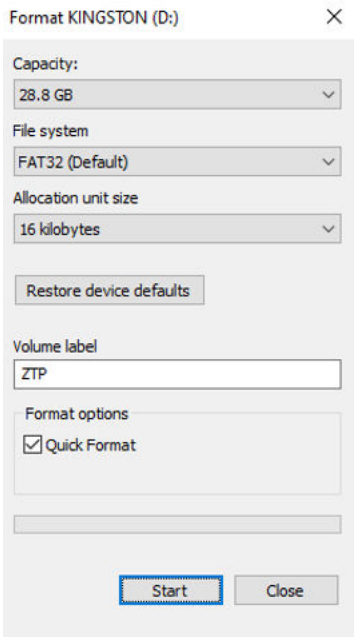


7. In the Format dialog box, do the following:
   a. Select **FAT32** in the **File system** field if not already selected. It is often the default option.

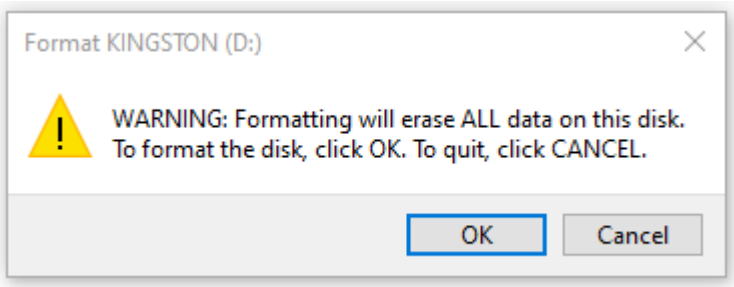


b. Type **ZTP** in the **Volume label** field

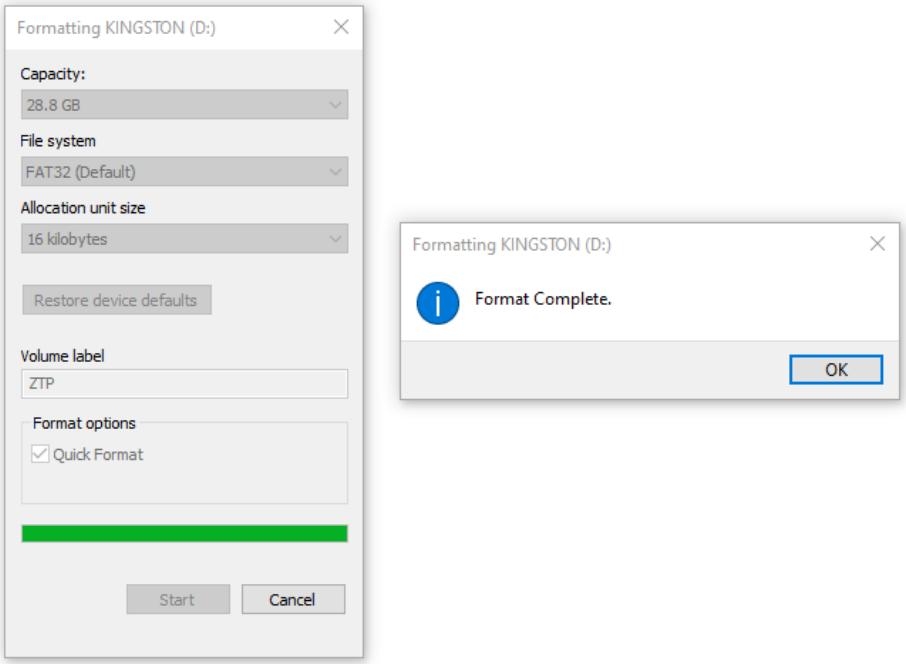
c. Select **Start** button to confirm show the confirmation box



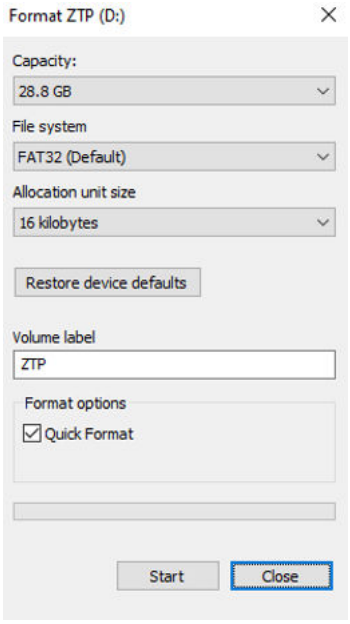
d. Select **OK** to confirm and being formatting



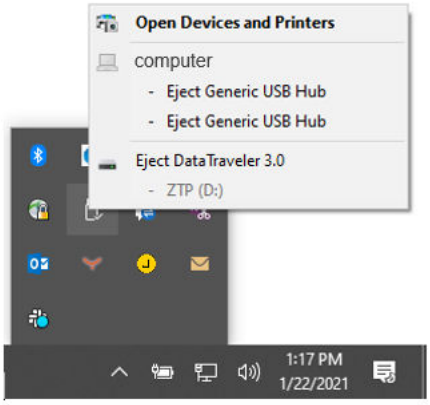
8. After formatting completes, click **OK**.



9. Confirm the Format dialog box by doing the following:
   a. The **Volume label** field and dialog box name shows **ZTP**.
   b. The **File system** type is **FAT32**
   c. After above is confirmed, select the **Close** button at the bottom.



10. Locate the downloaded software package (.zip file) on your computer. (ex. Package name: `<ApplianceName>-A-R9_1_0_0_0_GA_<date>.zip`)
11. Copy the file over to the **ZTP** USB drive. You should have a single software package on the drive in the top directory. Do not create any folders for the file.
12. Eject the **ZTP** USB drive.



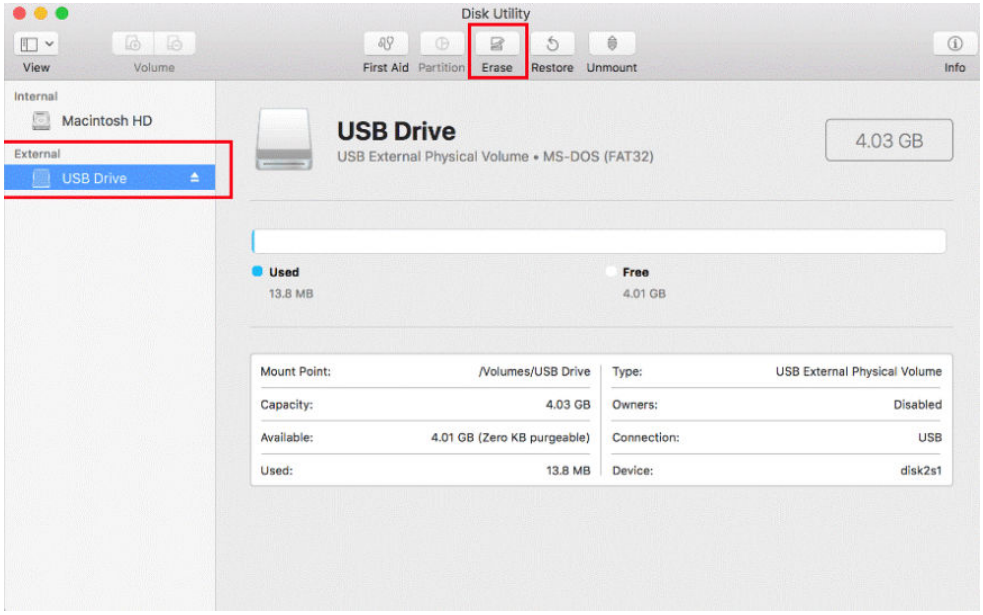
13. Continue to the instructions to Configure SD-WAN using out-of-band ZTP.

For Linux

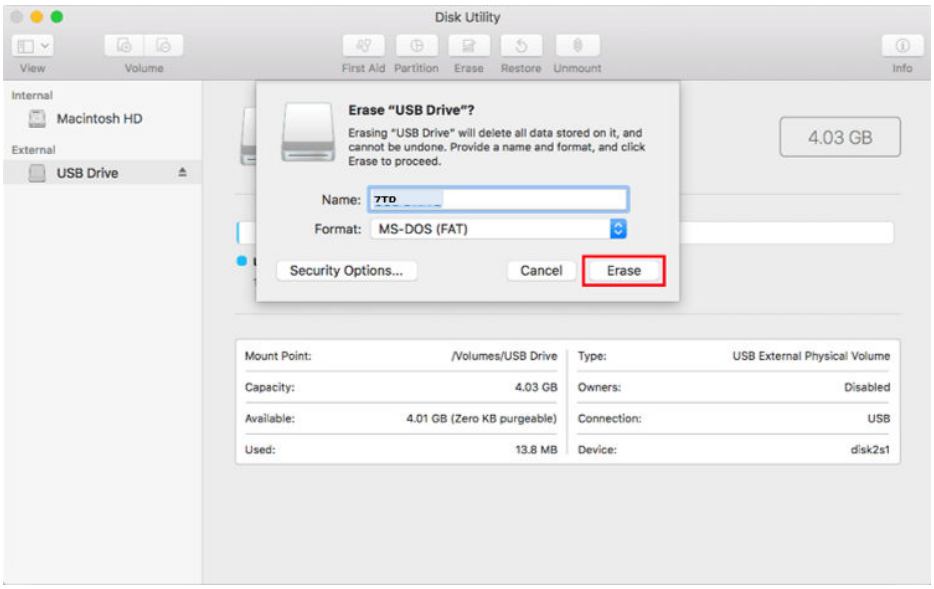
1. Insert the USB drive into the computer
2. Ensure the USB drive is at least 100 MB.
3. Check the device name. These instructions assume it is `/dev/sdb`.
4. Clear the USB using command `sgdisk -Z /dev/sdb`
5. Create a single partition using command `sgdisk /dev/sdb -n 1::0 -t 1:ef00`
6. Format the partition as FAT32 format using command `mkfs.vfat -F32 /dev/sdb1`
7. Format the USB drive for NTFS, naming the volume **ZTP**
8. Copy the downloaded software package (.zip file) onto the USB drive. It should be the ONLY software package on the USB drive. (ex. Package name: `<ApplianceName>-A-R9_1_0_0_0_GA_<date>.zip`)
9. Eject the ZTP USB drive.
10. Continue to the instructions to Configure SD-WAN using out-of-band ZTP

For Mac

1. Insert the USB drive into the Mac
2. Launch Disk Utility, located in **Applications** > **Utilities**
3. Locate the USB drive name on the left hand side of Disk Utility window and select it



4. Ensure the USB drive is at least 100 MB.
5. In the Disk Utility window for your USB drive, do the following:
   a. Select **FAT** if it is not already the default option in the Format field
   b. Type **ZTP** in the Name field
   c. Select **Erase** to begin formatting



6. Once Erasing is complete, select the **Done** button in the Erasing and creating dialog box
7. Locate the downloaded software package (.zip file) on your computer. (ex. Package name: `<ApplianceName>-A-R9_1_0_0_0_GA_<date>.zip`)
8. Copy the file over to the ZTP USB drive. You should have a single software package on the drive in the top directory. Do not create any folders for the file
9. Eject the ZTP USB drive.

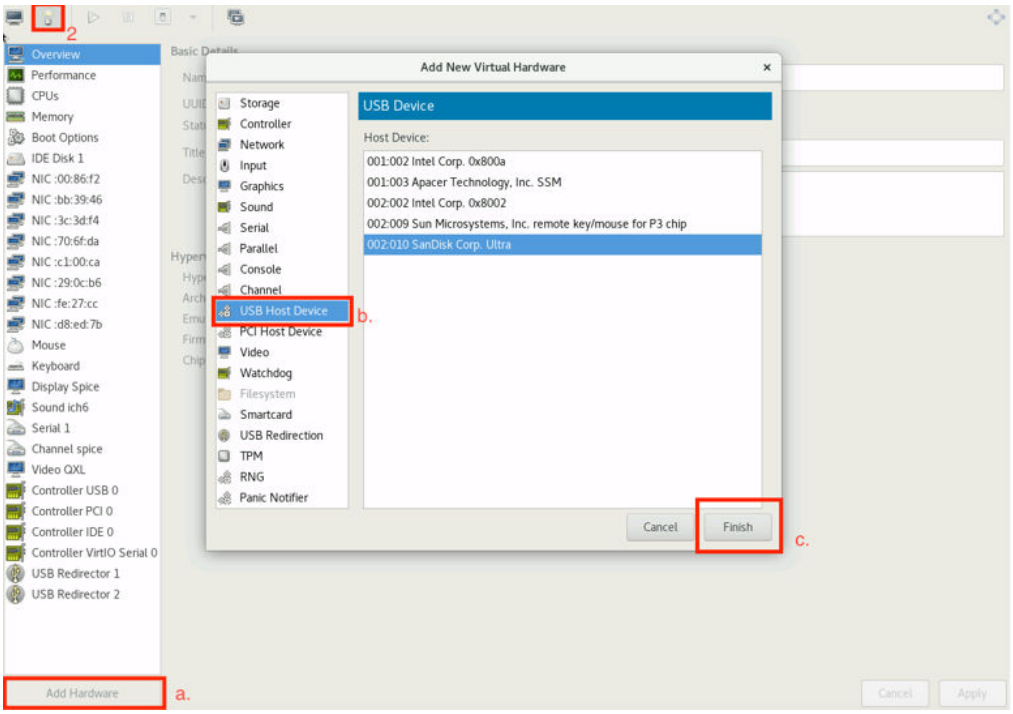
10. Continue to the instructions to Configure SD-WAN using out-of-band ZTP

Create Mapped Drive on Hypervisor

1. Format the USB drive as FAT32 with the label of ZTP as detailed in the Format your USB drive instructions for your computer type.
2. Ensure the VM is powered off
3. Assign Host USB device to a guest VM using instructions for your host.

Assign Host USB Device on KVM

1. Insert USB into a port on the hypervisor
2. Open the virt-manager application and select the desired VM
3. Open the VM settings by selecting the bulb Icon in the top left
   a. Select the **Add Hardware** option at the bottom left
   b. Select **USB Host Device**
   c. Select the desired device and click **Finish**



4. Click **Apply** and power on the VM

Assign Host USB Device on ESXi

1. Insert the USB into a port on the hypervisor.
2. From the Webui, select the **Virtual Machines** tab on the left and select the desired VM.
3. Open the VM settings by selecting **Edit** at the top.
4. In the **Virtual Hardware** menu, select **Add other device** and do the following:

a. Select **USB device**.

b. At the bottom of the settings page, confirm that the correct USB device is connected to the VM.

c. Select **Save**.

Configure SD-WAN Using Out-of-Band ZTP

1. If not powered, plug in your appliance without a USB drive.
2. After it starts, insert the formatted USB drive with single software package for this appliance into the USB port of your SD-WAN appliance/hypervisor.
3. After installation, remove the USB drive from your SD-WAN appliance/hypervisor.

3

WAN Deployment with a Virtual Appliance

Please note that the Virtual Appliance differs from physical Appliances in that it does not support the following:

- Fail-to-Wire for Interface Groups
- Configuration of Ethernet Interface auto-negotiation, speed, or duplex settings through the Appliance Web Console
- Appliance Reports for Temperature