Oracle® SD-WAN Edge

Virtual Appliance Installation Guide

Release 8.2
F26391-01
March 2020

Oracle SD-WAN Edge Virtual Appliance Installation Guide, Release 8.2

F26391-01

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.

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

This section provides a revision history for this document.

(Required) Enter introductory text here, including the definition and purpose of the concept.

Date	Description
February 2020	• Initial release of this publication, including 8.2M1 features "OCI Iaas Configuration" and "Deploying Edge on KVM"
March 2020	• Adds OCI Marketplace Support section

1

Software and Hardware Requirements

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.

VT800 Supported Hypervisors

	VMware ESXi	Microsoft Hyper-V	Microsoft Azure	KVM
Software Version	6.0 or later	Windows Server 2012 R2	VM: Standard_DS3 +, Disk: P10 +	qemu-kvm-1.5.3-167.el7
CPU Requirements	64-Bit, 3GHz +, AES-NI, Intel CPU only	64-Bit, 3GHz +, AES-NI, Intel CPU only	64-Bit, 3GHz +, AES-NI, Intel CPU only	8 vCPU,
Special Requirements / Recommendations	DAS recommended [1]	DAS SSD recommended [1]	DAS Recommended [1]	DAS recommended [1]

> **Note:**
>
> [1] Directly Attached Storage (DAS) is recommended for all Virtual Appliances.

VT800-128 Supported Hypervisors

	VMware ESXi	Microsoft Hyper-V	Microsoft Azure	KVM
Software Version	6.5.0 or later	Windows Server 2012 R2	VM: Standard_DS3 +, Disk: P10 +	qemu-kvm-1.5.3-167.el7
CPU Requirements	64-Bit, 3GHz +, AES-NI, Intel CPU only	64-Bit, 3GHz +, AES-NI, Intel CPU only	64-Bit, 3GHz +, AES-NI, Intel CPU only	8 vCPU
Special Requirements / Recommendations	DAS recommended [1]	DAS SSD recommended [1]	DAS Recommended [1]	DAS Recommended [1]

> **Note:**
>
> [1] Directly Attached Storage (DAS) is recommended for all Virtual Appliances.

Virtual Machine Specifications

Platform	Appliance Model	License Level	Dedicated VCPUs [1]	RAM	Minimum Processor Ghz	Instance Type
Hyper-V	VT800	20 Mbps	2	8 GB	2.10 Ghz	
	VT800	200 Mbps	10	10 GB	2.10 Ghz	
	VT800-128	200 Mbps	10	32 GB	2.10 Ghz	
Azure	VT800	20 Mbps	4	28 GB	2.4 Ghz	D12 v2
	VT800	500 Mbps	8	56 GB	2.4 Ghz	D13 v2
	VT800-128	500 Mbps	8	56 GB	2.4 Ghz	D13 v2
ESXi	VT800	20 Mbps	2	4 GB	2.10 Ghz	
	VT800	1 Gbps	8	8 GB	2.10 Ghz	
	VT800	2 Gbps	14	16 GB	2.10 Ghz	
	VT800-128	1 Gbps	8	32 GB	2.10 Ghz	
	VT800-128	2 Gbps	14	32 GB	2.10 Ghz	
KVM	VT800	175 Mbps	8	16 GB	2.10 Ghz	
	VT800-128	175 Mbps	8	32 GB	2.10 Ghz	
OCI	VT800	200 Mbps	4	60 GB	2.0 Ghz	VM.Standard2.4
	VT800-128	200 Mbps	4	60 GB	2.0 Ghz	VM.Standard2.4

> **Note:**
>
> [1] For 1 Gbps and 2 Gbps license levels, Intel Xeon E7-8870v4 or better with L3 cache of 50MB or more is required for expected performance.

Additionally, all Virtual Appliances require:

- a minimum of 180 GB dedicated storage.

  > **Note:**
  >
  > Directly Attached Storage (DAS) is recommended for all Virtual Appliances.

- 1 shared or dedicated management interface

> **Note:**
>
> KVM cannot have a shared management interface

- 1 dedicated, but not more than 7 total, non-management network interfaces

Important: Virtual Appliances required dedicated resources. A Virtual Appliance deployed without dedicated (pinned) resources may not function as expected.

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.

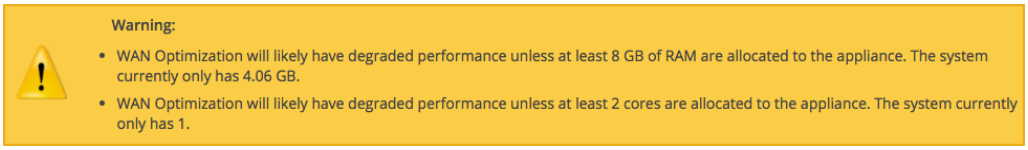
WAN Optimization System Specifications

WAN Optimization is supported on VT800s running Edge 7.1 or above and VT800-128s running Edge 7.3 P4 or above at the following levels with the specified resources:

Platform	License Level	WANOp Capacity	VCPUs	RAM	Max WANOp Sessions	Disk Size	Cloud Instance Type
Hyper-V	20 Mbps	8 Mbps	2	8GB	1,500	160GB	NA
	200 Mbps	100 Mbps	10 (2.10GHz)	10GB	5,000	160GB	NA
Azure	20 Mbps	8 Mbps	4	28GB	10,000	160GB	DS12_v2
	500 Mbps	100 Mbps	8 (2.4GHz)	56GB	16,000	160GB	DS13_v2
ESXi	20 Mbps	8 Mbps	2	8GB	1,500	160GB	NA
	2 Gbps	200 Mbps	14 (2.10GHz)	16GB (VT800-128: 32 GB)	10,000	160GB	NA

> **Note:**
>
> The maximum number of WANOp sessions is scaled based on available memory. If a virtual appliance has insufficient dedicated RAM, the maximum number of WANOp sessions will be lower. Provisioning a virtual appliance below recommended system specifications will not disable WANOp, but will impact WANOp performance. Provisioning a virtual appliance below the defined minimum specifications is not supported.

A warning banner will be displayed in the Web Console if WANOp is enabled on a Virtual Appliance that does not meet the minimum recommended system specifications. An example is shown below, on a VT800 with insufficient RAM and VCPUs:



For information on how to configure WAN Optimization, please see the *WANOp Setup and Configuration Guide*.

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

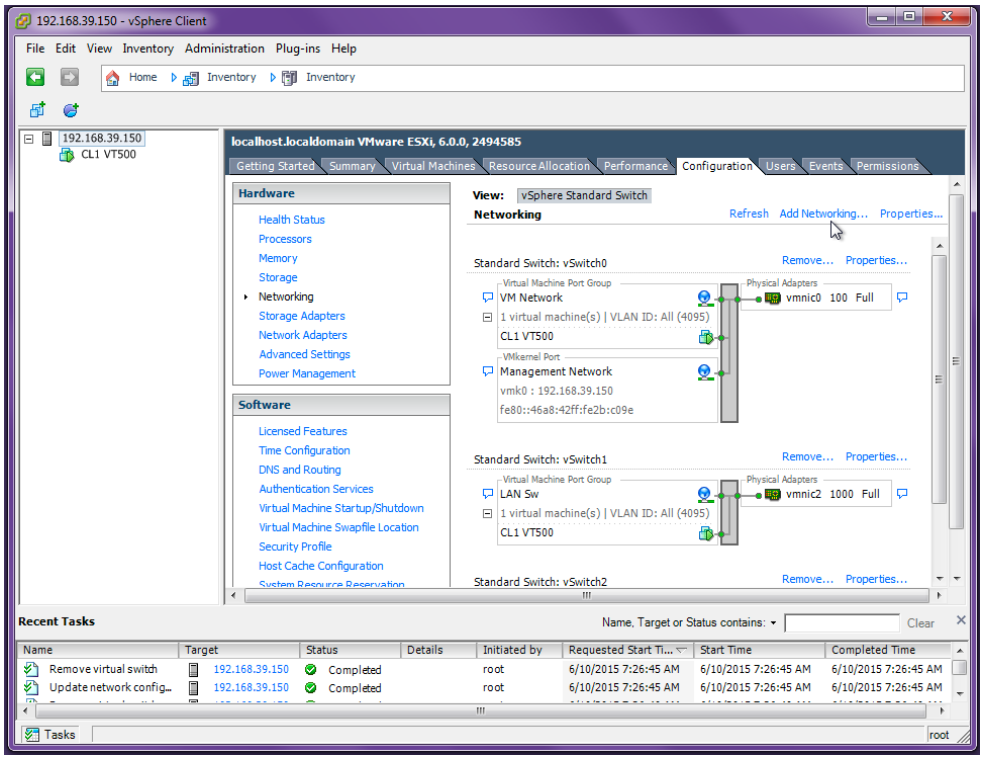
Before deploying on VMWare ESXi, you will need:

- 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

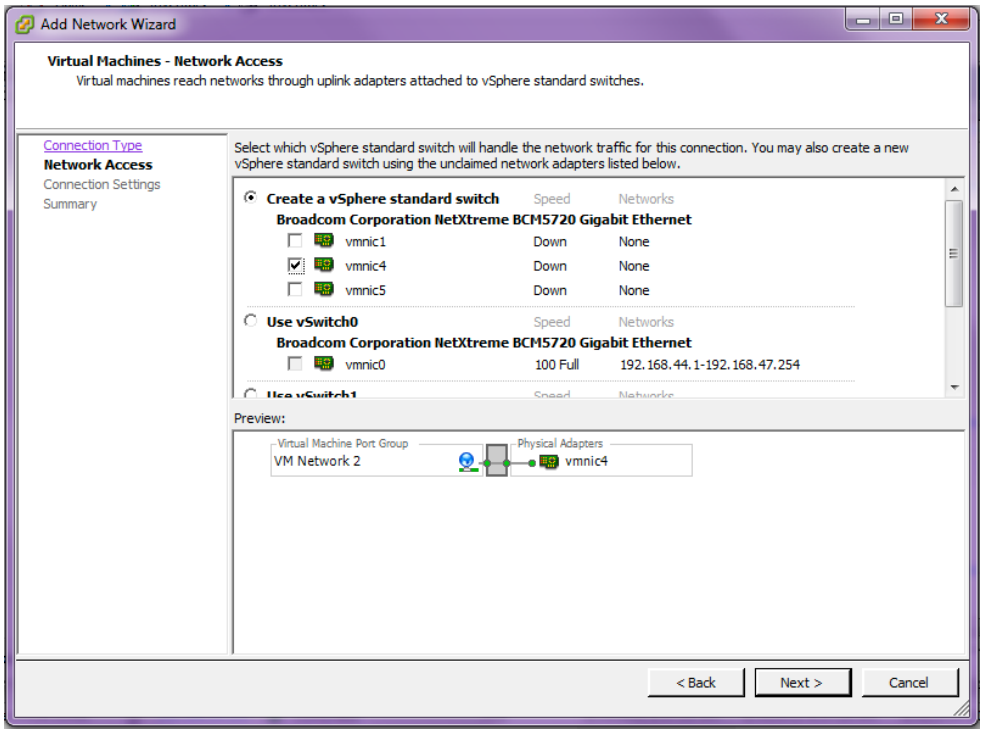


2. Click **Networking** from the left menu then click the **Add Networking…** link.
3. Choose **Virtual Machine** as the **Connection Type** and click **Next**.

> **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.

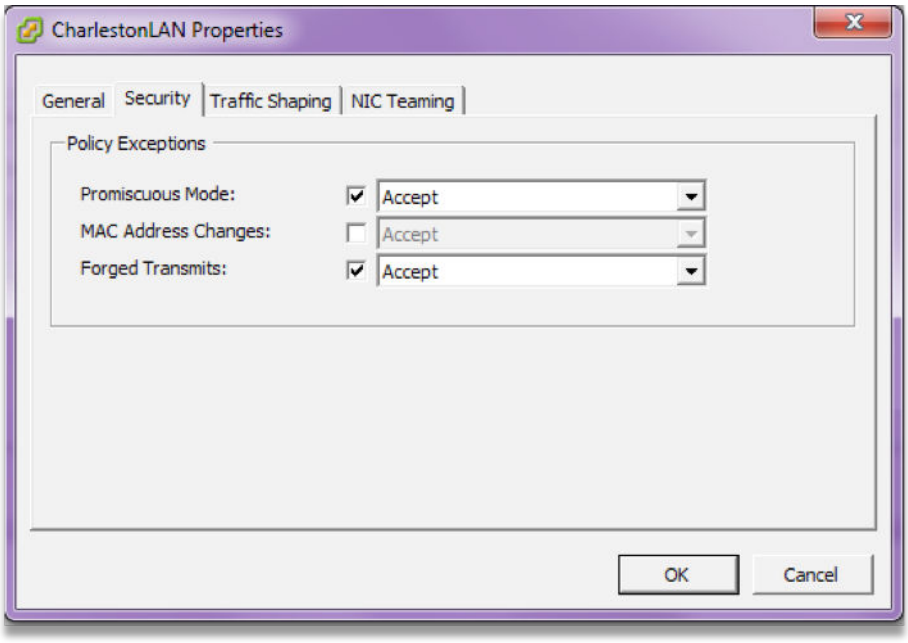
4. Click **Create a vSphere standard switch**, choose one of the available virtual machine NICs, and click **Next**.

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



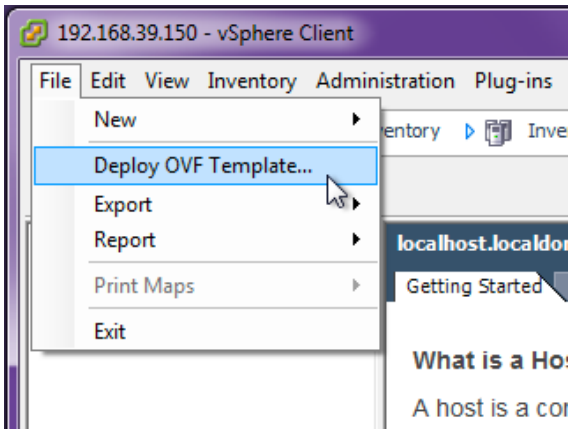
10. Repeat steps 4 through 9 to create a separate virtual switch for each Virtual Appliance port that will be used in your deployment.
11. Repeat steps 4 through 9, and do not choose a virtual machine NIC to create a null virtual switch for Virtual Appliance ports that will not be used in your deployment.

> **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

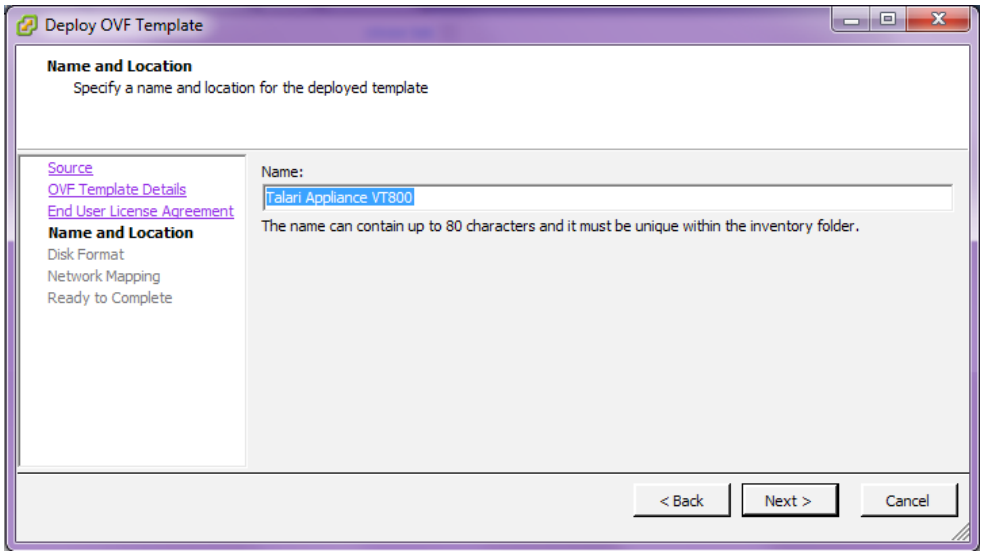
1. Click **File**, **Deploy OVF Template...**

Figure 2-4 Deploy OVF Template



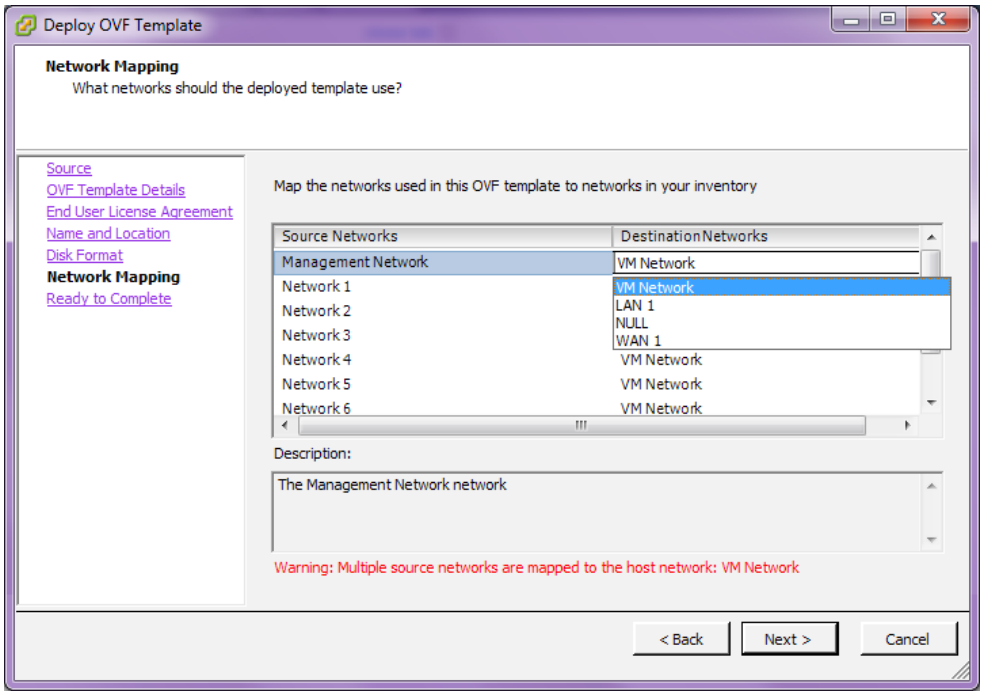
2. **Browse** to the location of the Appliance VM Image (.ova package) that you downloaded. Select the file and click **Open**.
3. Click **Next** and a screen will display information for the VM being imported.
4. Click **Next** and a screen will display the End User License Agreement. After reading, 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



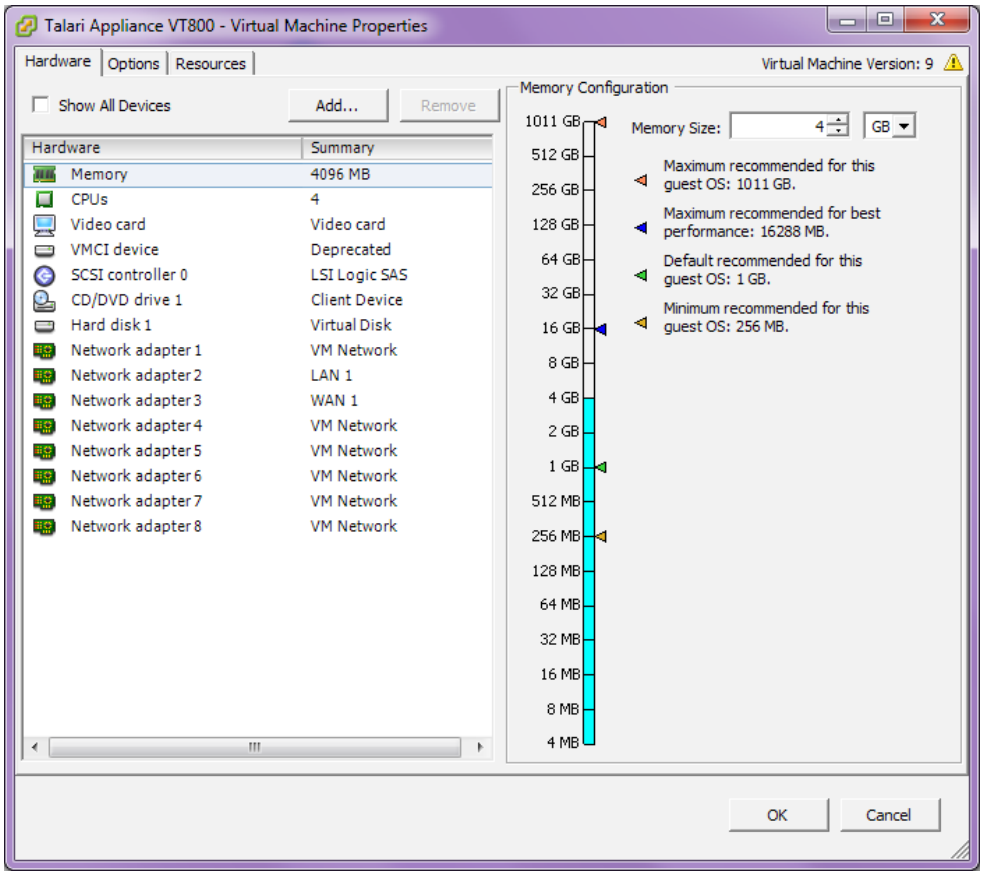
8. Click **Finish** on the **Ready to Complete** screen.

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

Configure the Virtual Machine

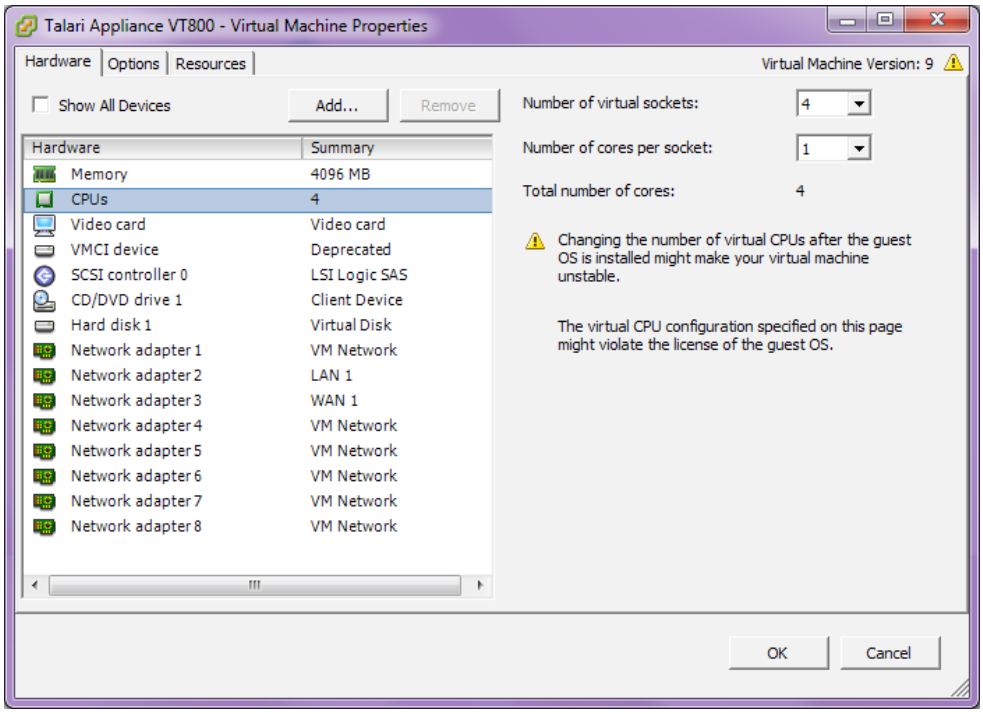
1. If this is the first time you have used the vSphere Client, you may need to click the **Inventory** icon, identify the server, and expand its inventory list.
2. Click the name of your Virtual Appliance's VM in the inventory list.
3. Click the **Summary** tab and click **Edit Settings** underneath 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.

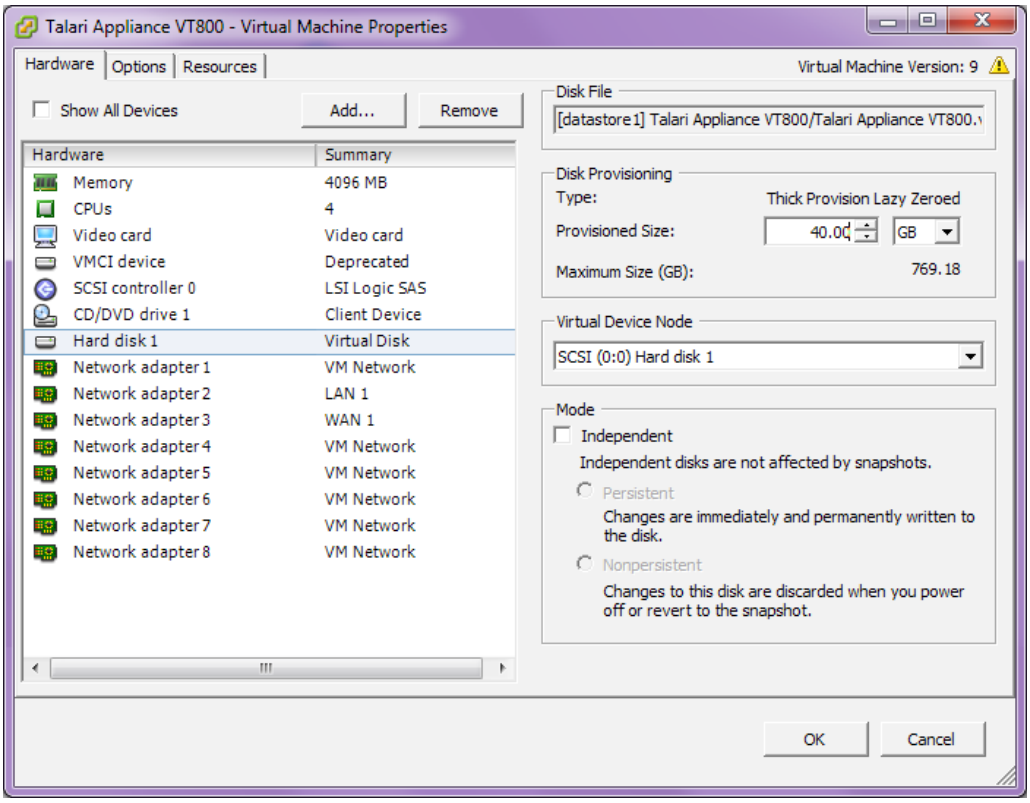
Figure 2-8 Adjust the Number of Sockets and Cores



> **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**.

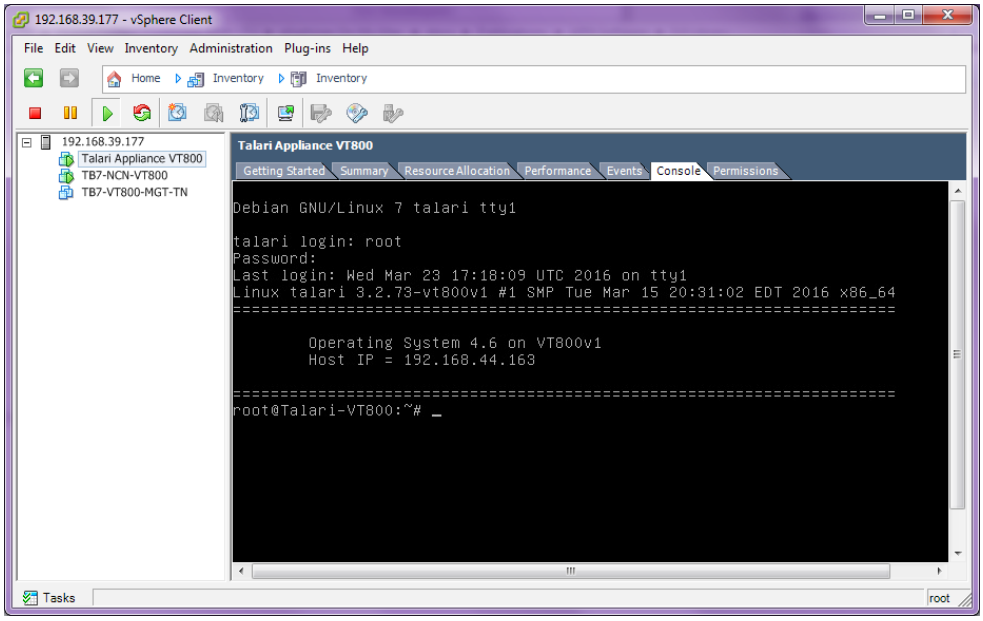
> **Note:**
>
> To exit the console, release the mouse by pressing and holding the **Ctrl** and **Alt** buttons simultaneously.

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

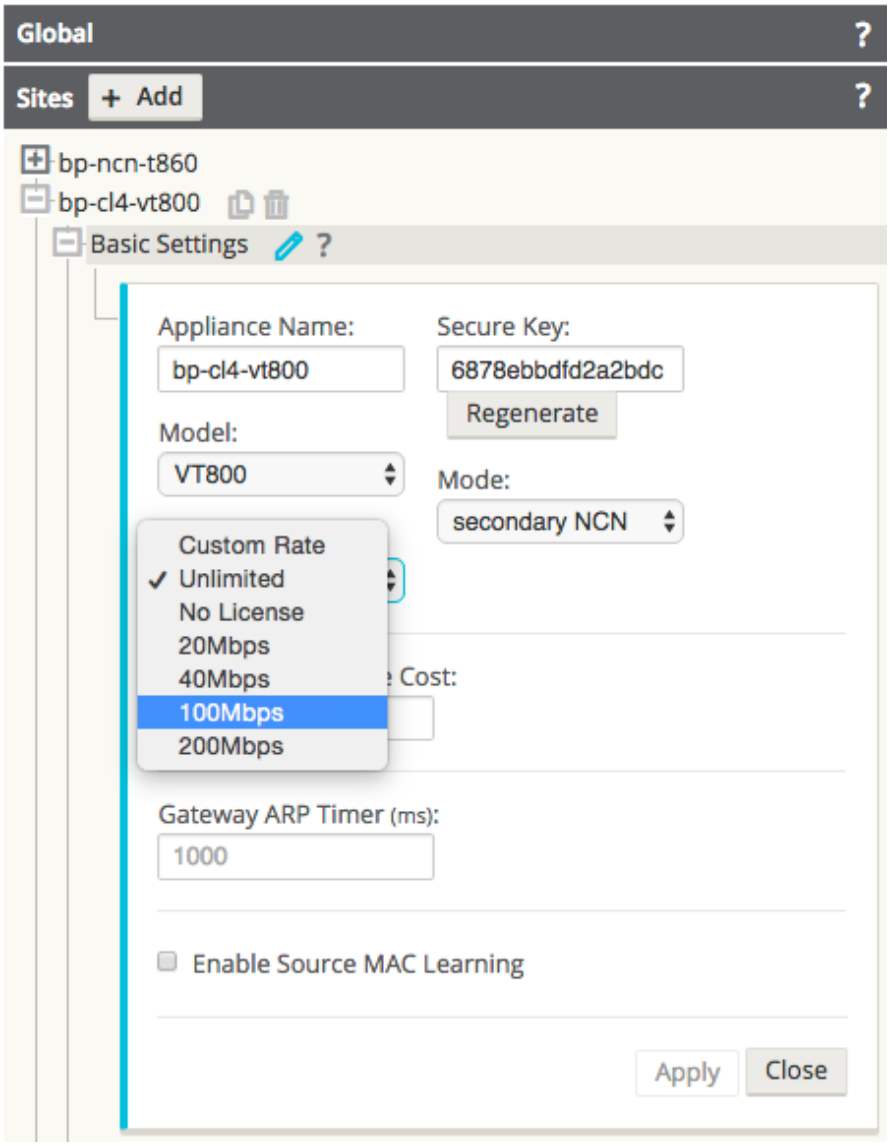


5. Run the **tcon** command to acquire the console.
6. Run the **management_IP** command to enter the set_management_ip prompt.
7. Run **set interface <ip_address> <subnet_mask> <gateway_ip_address>** (e.g., set interface 192.168.44.196 255.255.240.0 192.168.35.2).
8. Run **apply**.
9. Run **main_menu**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

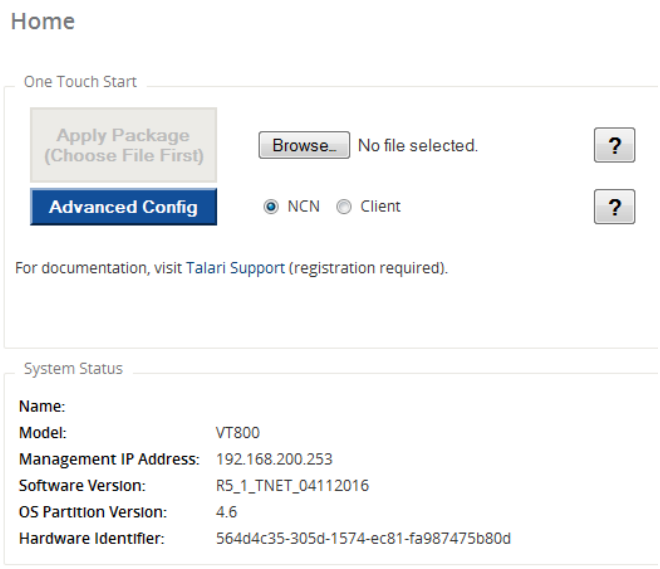
6. Open any supported browser and navigate to the management IP of the Virtual Appliance. At the **Login** prompt enter the following credentials and click **Login**: **Login:** talariuser **Password:** talari

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.

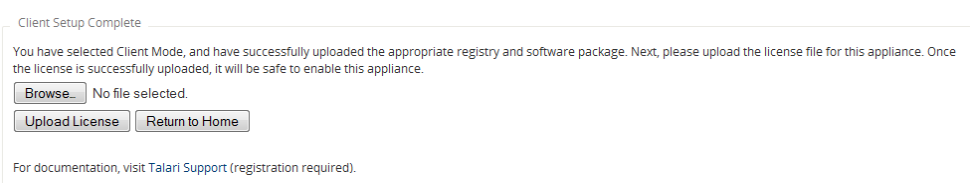
8. Under **One Touch Start**, click **Browse** and select the pre-prepared Appliance Package from your workstation.

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.

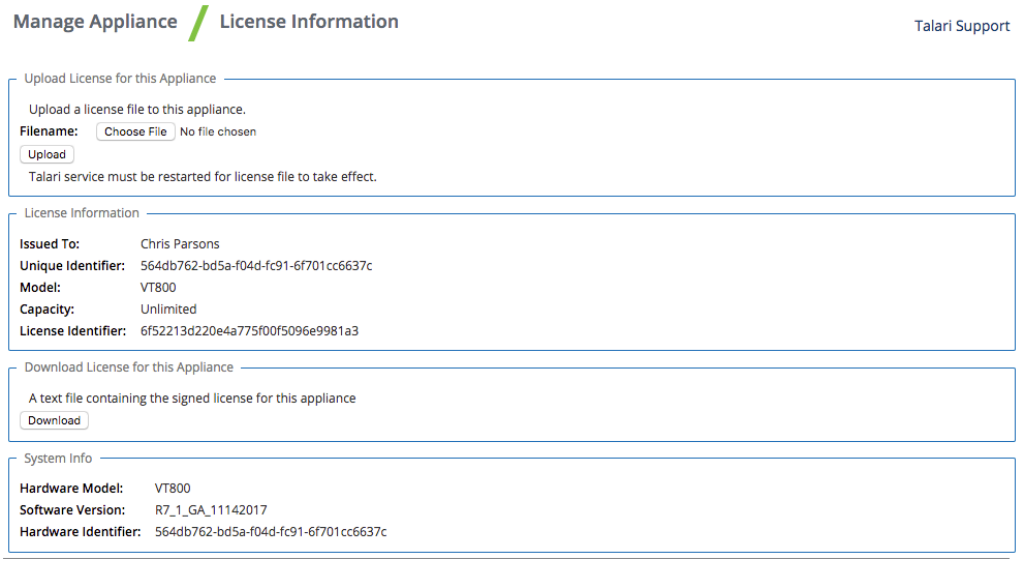
Figure 2-13 Client Setup Complete



> **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**.

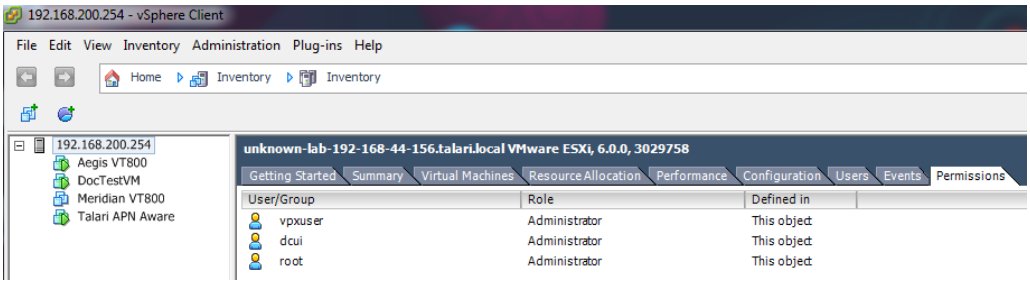
Figure 2-14 Successfully Licensed Virtual Appliance



> **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

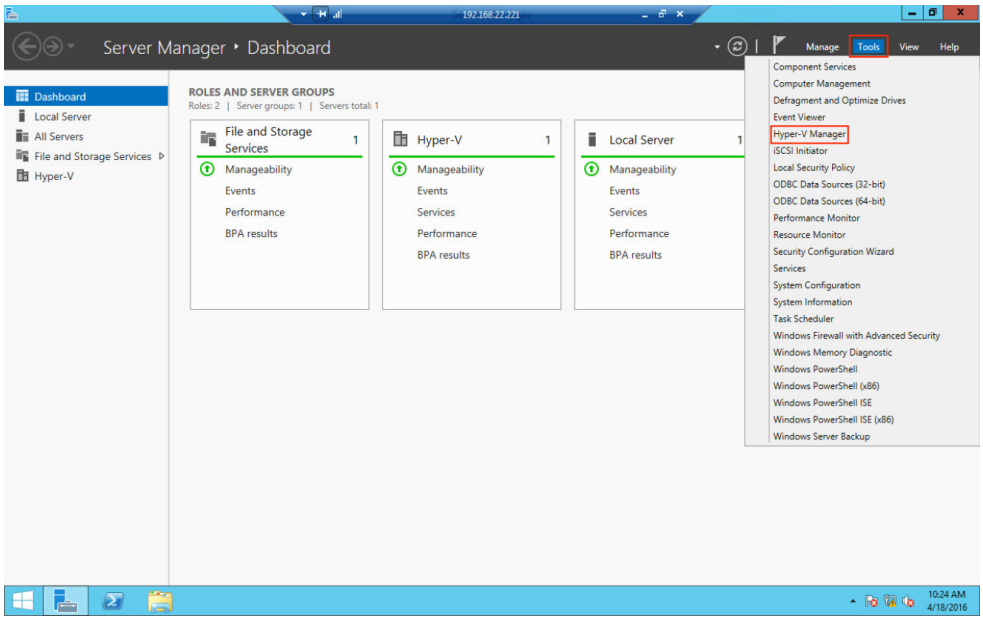
Virtual Appliances deployed on Microsoft Hyper-V are subject to the following configuration limitations:

- 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.

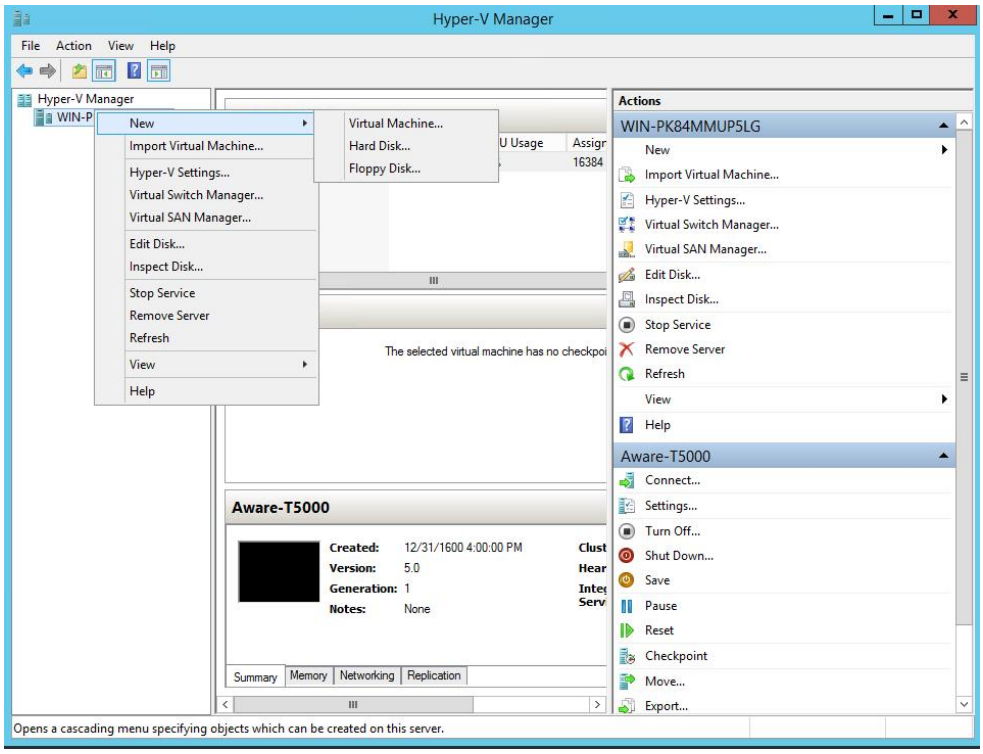
Important: When shutting down Virtual Appliances deployed on Hyper-V, use the “Shut Down” option rather than the “Turn Off” option to ensure graceful shutdown. If the “Turn Off” option is used, the Virtual Appliance may not start up properly.

Deploy the Virtual Appliance in Hyper-V

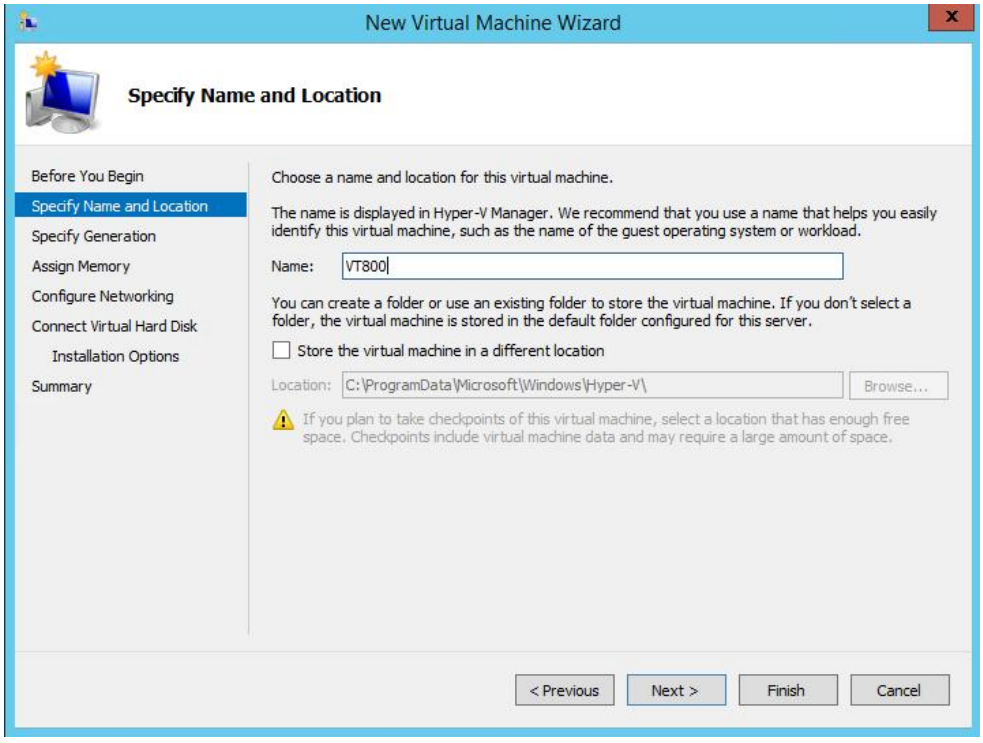
1. Open **Server Manager**, select the **Tools** pull-down menu, and click **Hyper-V Manager**. This will open the Hyper-V Manager window.



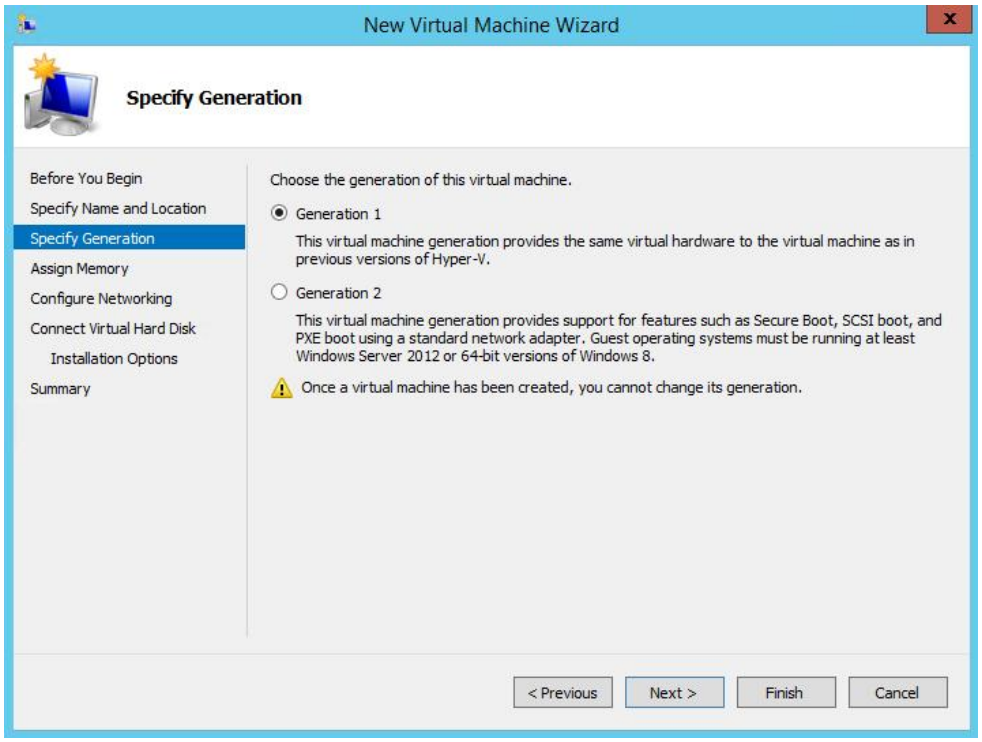
2. In the Hyper-V Manager window, make sure your server is selected from the dropdown list in the left. Select **New**, and then **Virtual Machine**. This will open the New Virtual Machine Wizard.



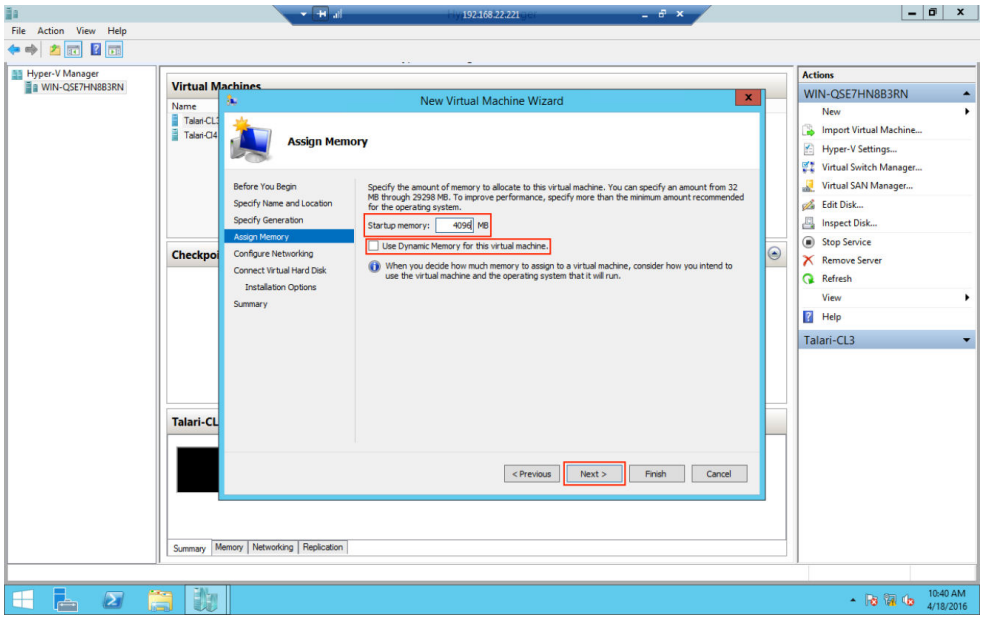
3. Review the **Before You Begin** tab, then click next.
4. On the **Specify Name and Location** tab, type an appropriate name for your virtual machine into the name box. Click **Next**.



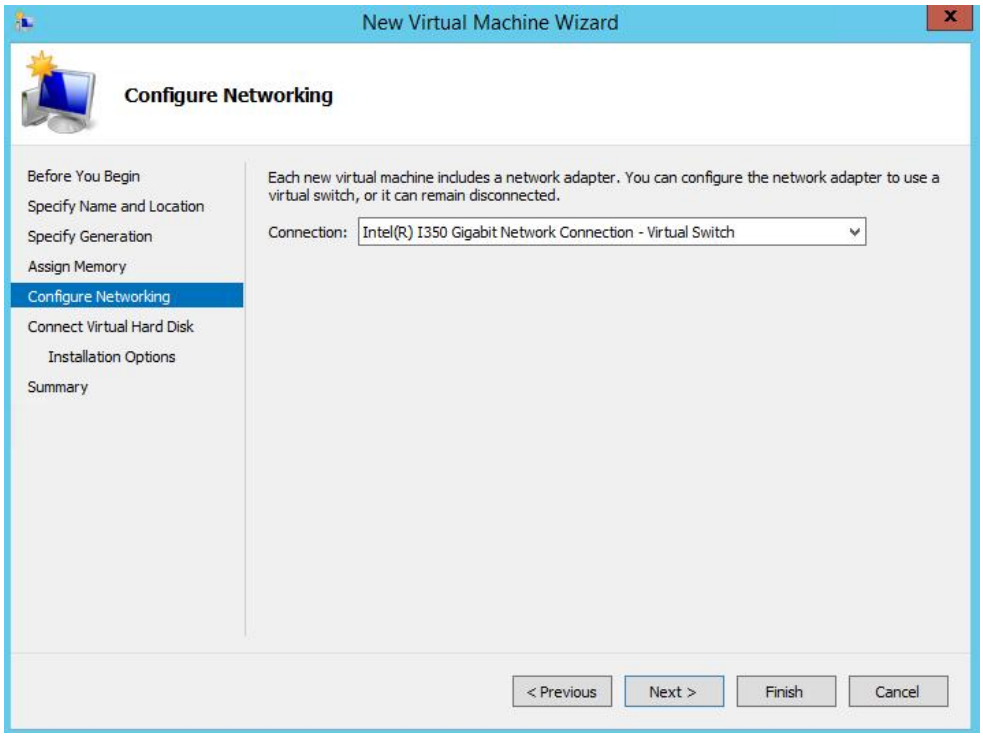
5. On the **Specify Generation** tab, ensure that **Generation 1** is selected and click **Next**.



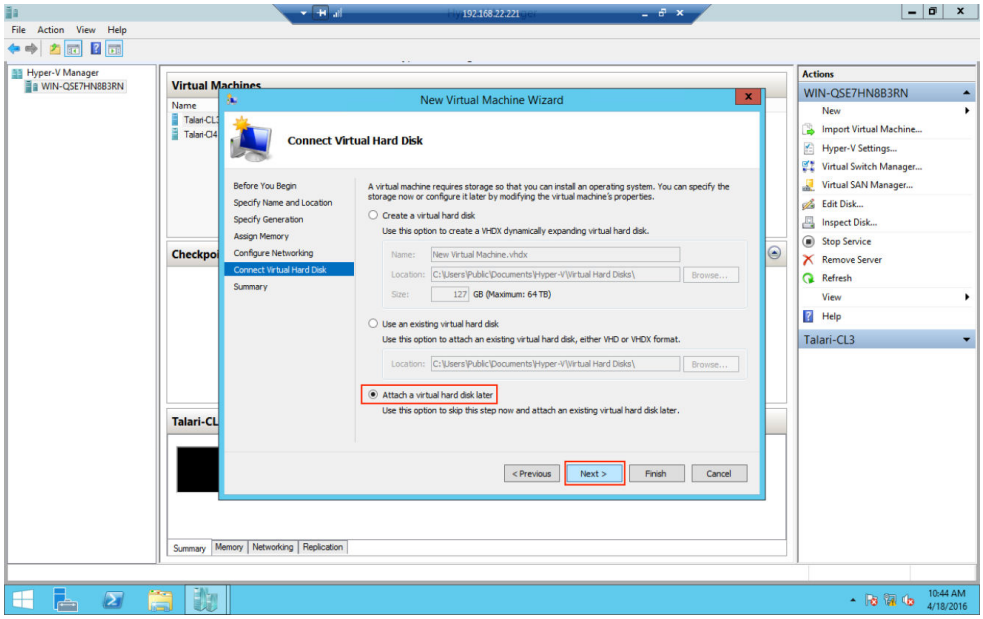
6. On the **Assign Memory** tab, chose the appropriate amount of memory necessary for the Virtual Appliance being deployed and input that value into the Startup memory box. Confirm “Use Dynamic Memory for the virtual machine” is not selected, then click **Next**.



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**.



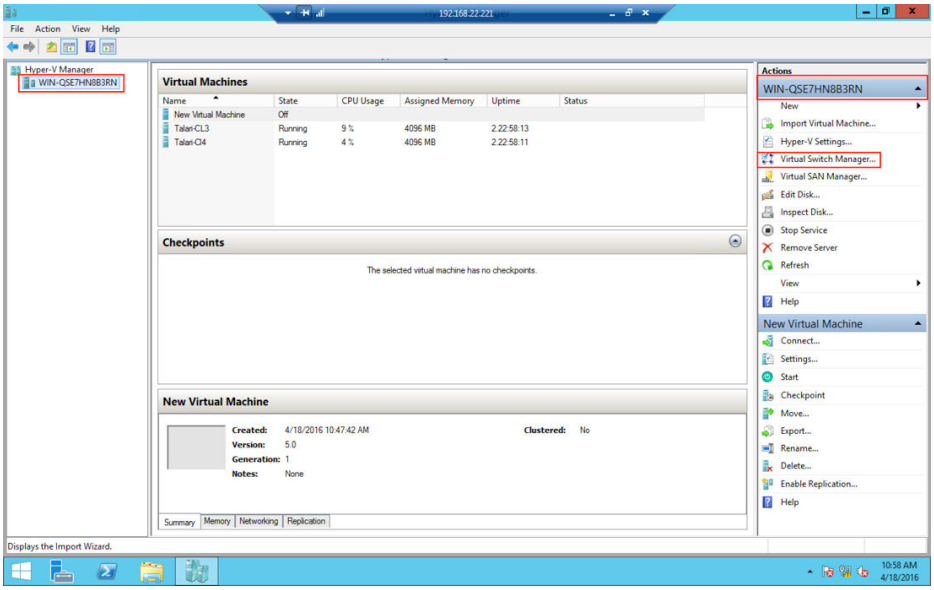
8. On the **Connect Virtual Hard Disk** tab, select the "Attach a virtual hard disk later" option and click **Next**.



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.**

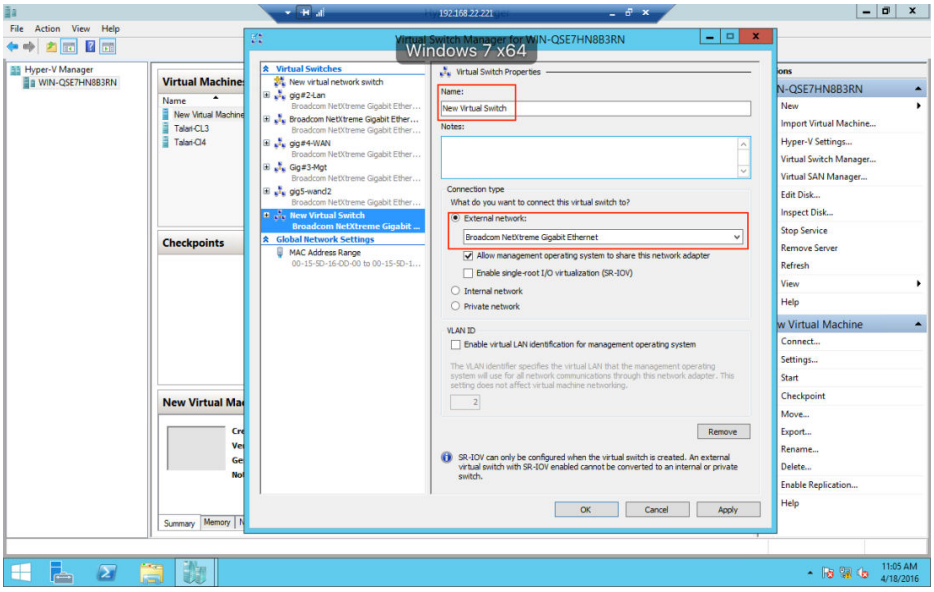


a. Select **New Virtual Switch**, make sure **External Network** (for connection to external Ethernet ports) is selected under type, and click **Create Virtual Switch**.

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

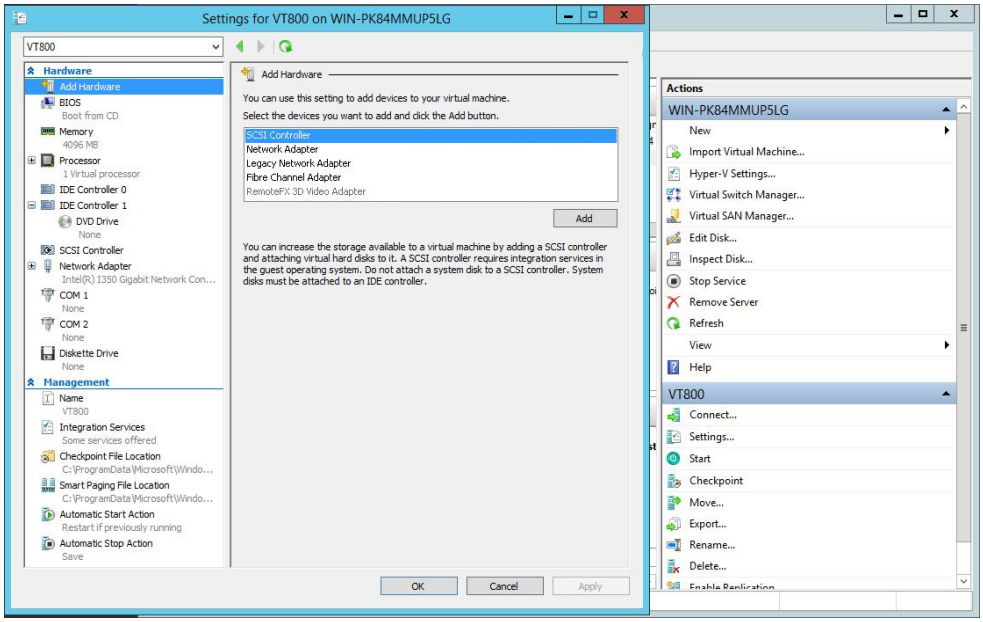
c. Under **Connection Type**, choose the physical NIC this Virtual Switch will represent. Disable the "Allow management operating system to share this network adapter" option, unless this is the management NIC and you would like it to be shared among VMs.

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

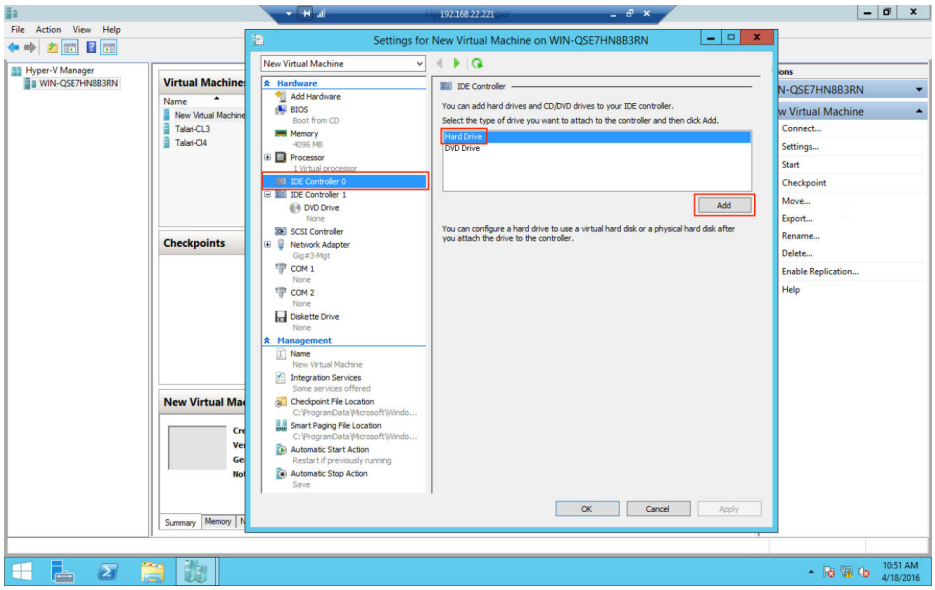


e. Repeat these steps for each NIC that will be used on the virtual appliance. Then, click **OK**. In a typical deployment the virtual appliance will require a minimum of three NICs – Management, LAN, and WAN.

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



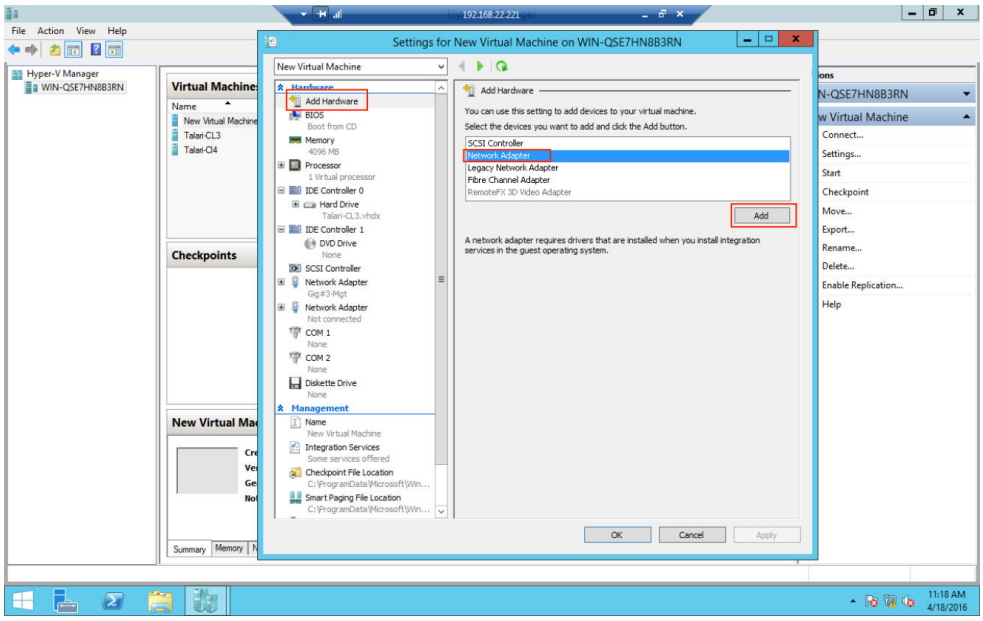
a. In the settings window for your virtual machine select the **IDE Controller 0** from the Hardware dropdown menu. Ensure that Hard Drive is selected and click **Add.**



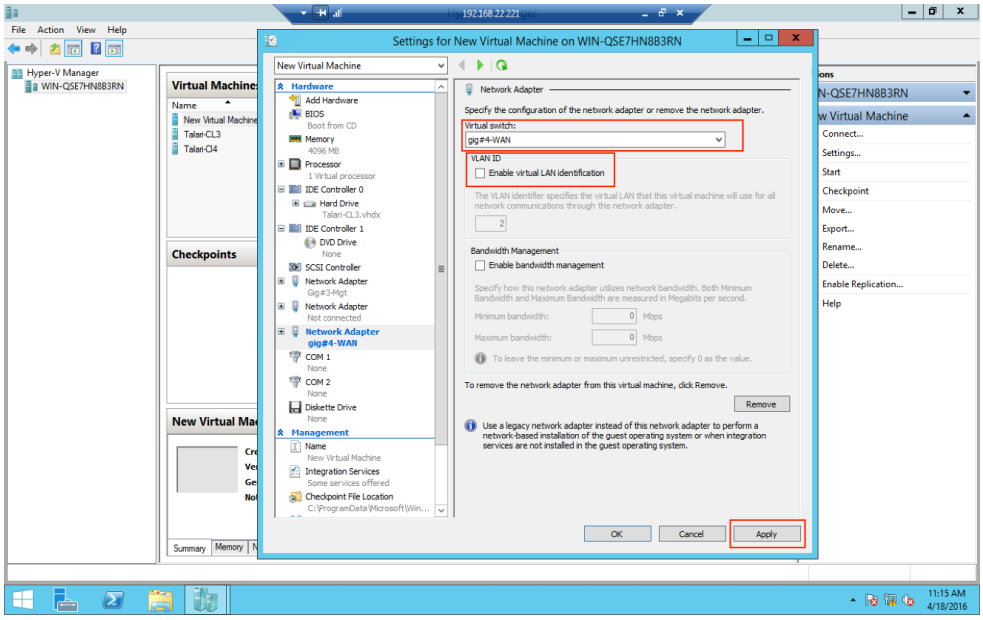
12. Under **Media,** choose **Virtual Hard Disk** and browse to where the .vhd for the Virtual Appliance is stored on the server. Click **Apply** then **OK**.

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**.

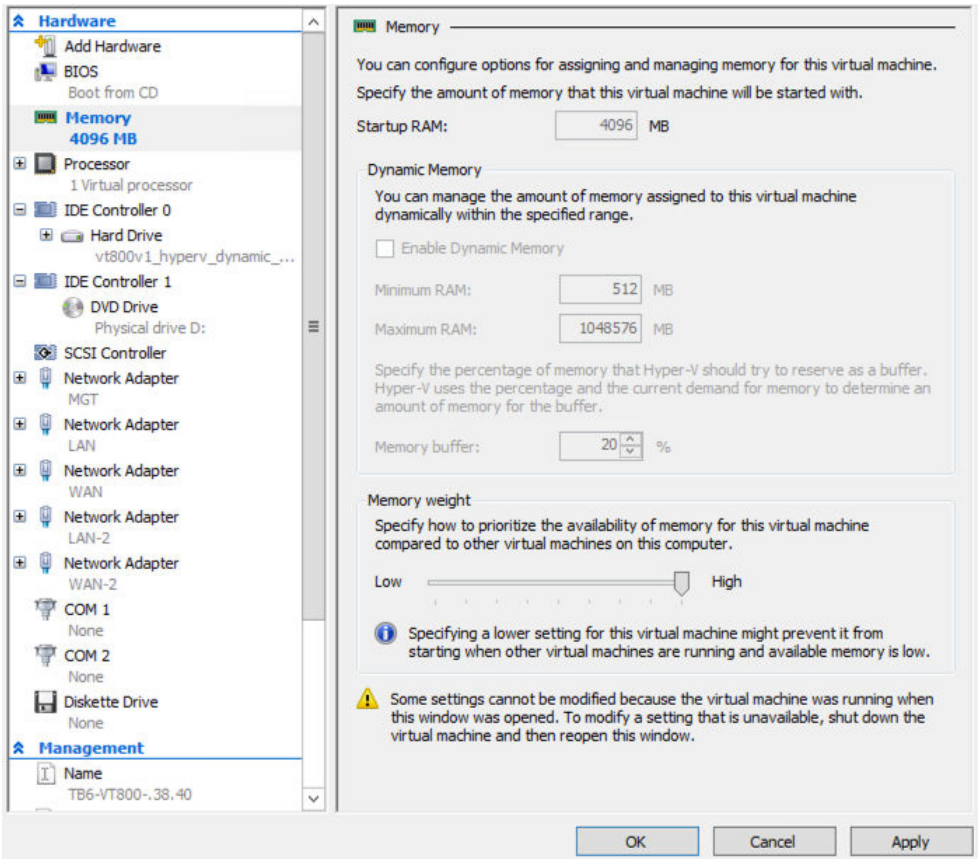


15. Choose the appropriate previously configured Virtual Switch for the desired physical port from the dropdown menu. If VLAN tagging will be used on this port, select the **Enable virtual LAN identification** button. Click **Apply** and repeat for each virtual machine port. Click **OK** when all network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

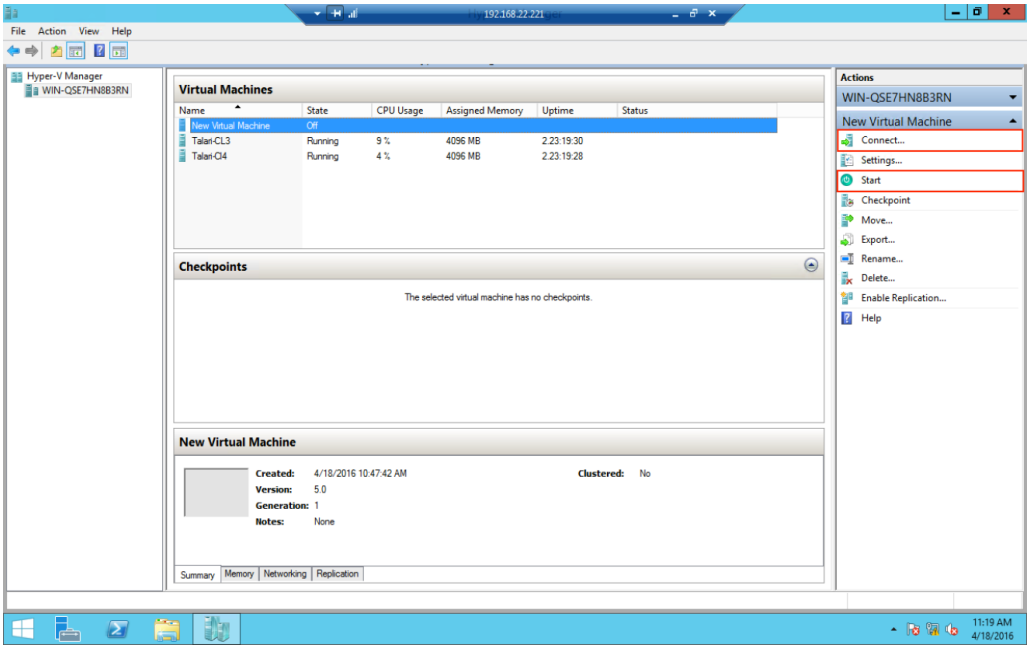


16. Finally, the Memory Weight for the Virtual Appliance must be set to High. Select **Memory** from the Hardware dropdown menu. Ensure that the slider for **Memory**

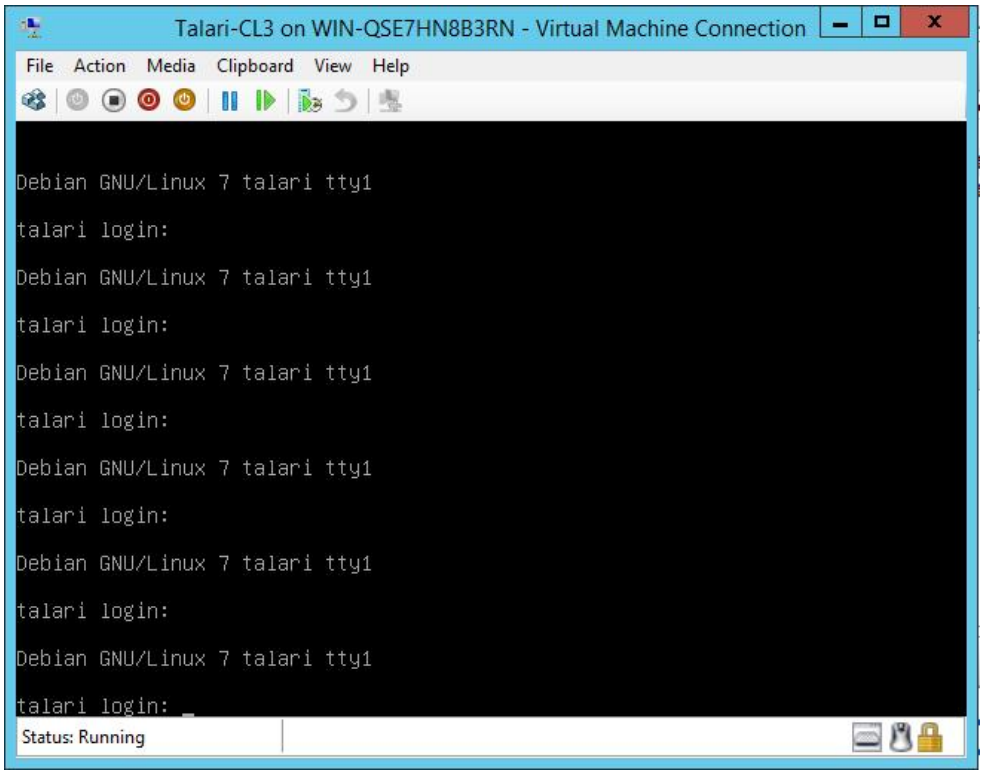
Weight is set to **High**, then click **Apply.**



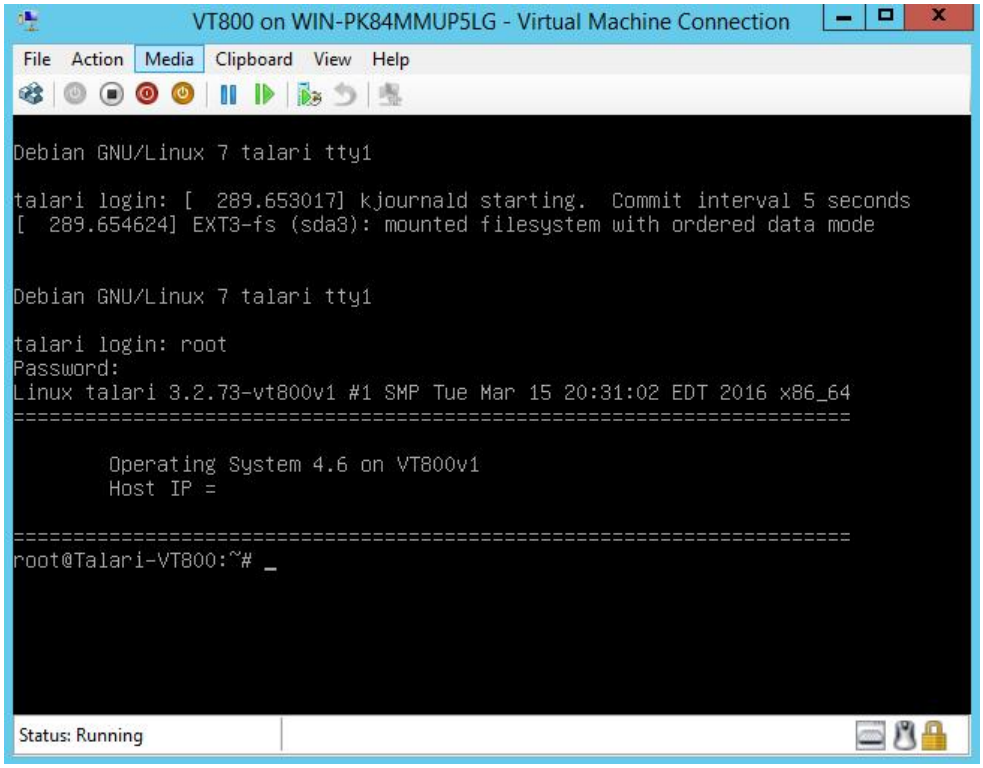
17. At this point the Virtual Appliance is ready for boot. Click **Start** from the VM's dropdown menu, then **Connect** to console into the device.



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.



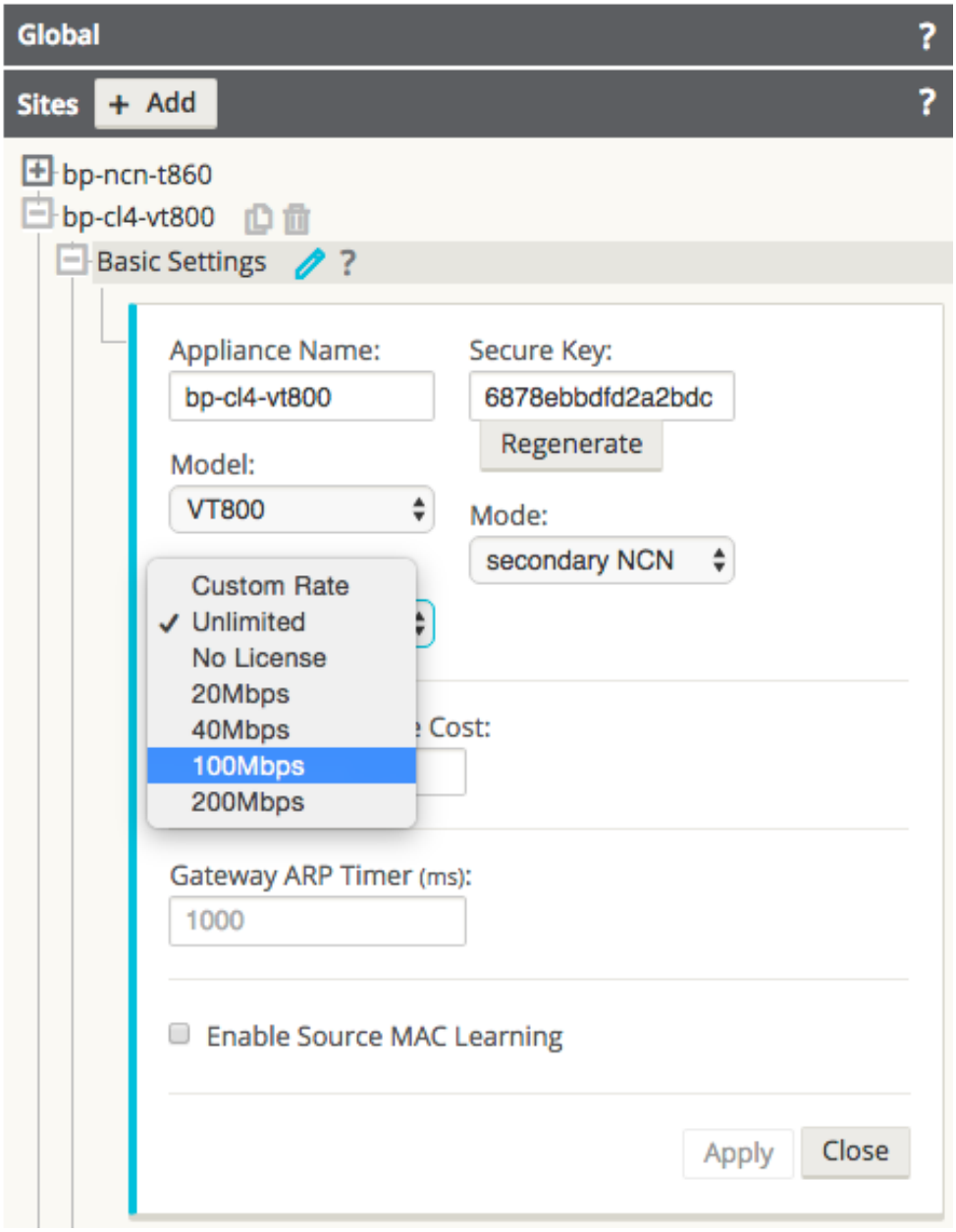
To manually configure a management IP address on the Virtual Appliance:

- 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

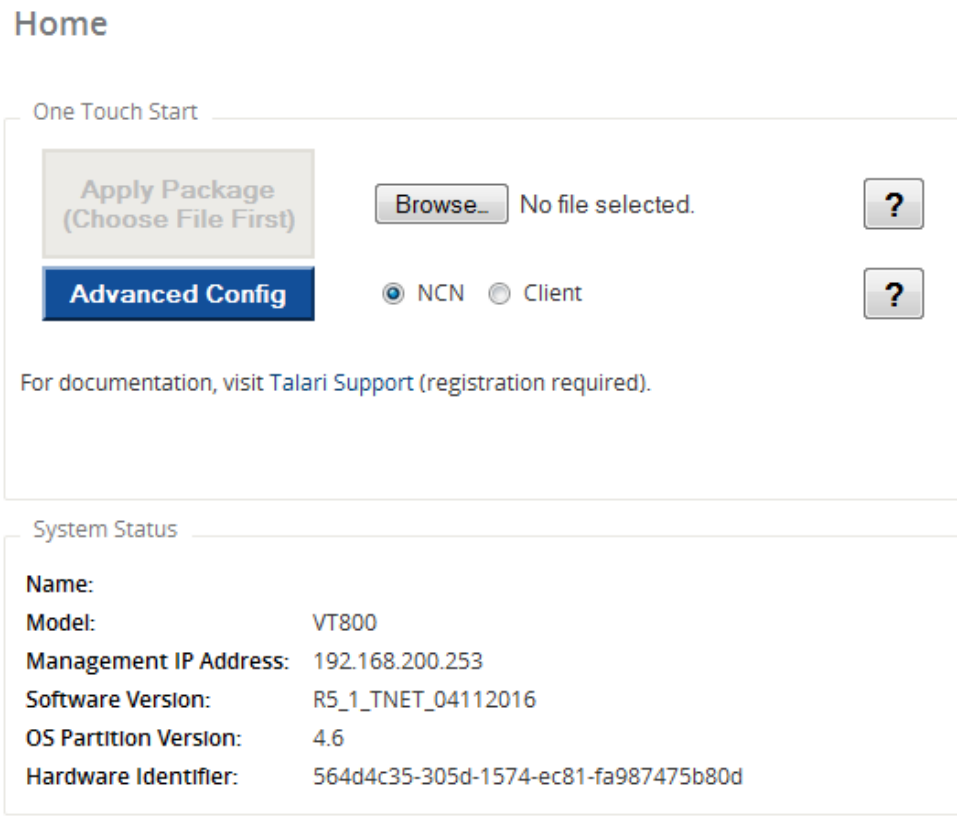
1. If you intend to deploy your Virtual Appliance as a Network Control Node, skip to step 6. Otherwise, access the **Talari Configuration Editor** available from the web console of your Network Control Node or your Oracle SD-WAN Aware instance.
2. From the **Talari Configuration Editor**, modify your 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.



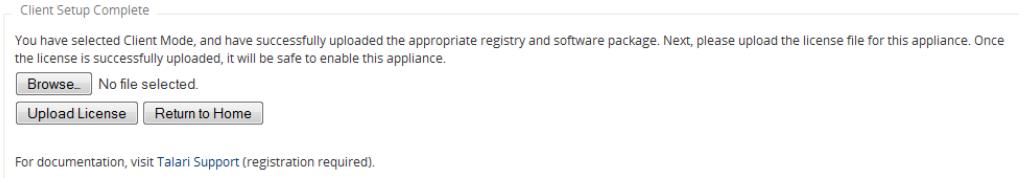
4. Stage the modified Configuration on your network as you would any other configuration change.
5. Download the staged Appliance Package for the Virtual Appliance to your local workstation.
6. Open any supported browser and navigate to the management IP of the Virtual Appliance. At the **Login** prompt 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.

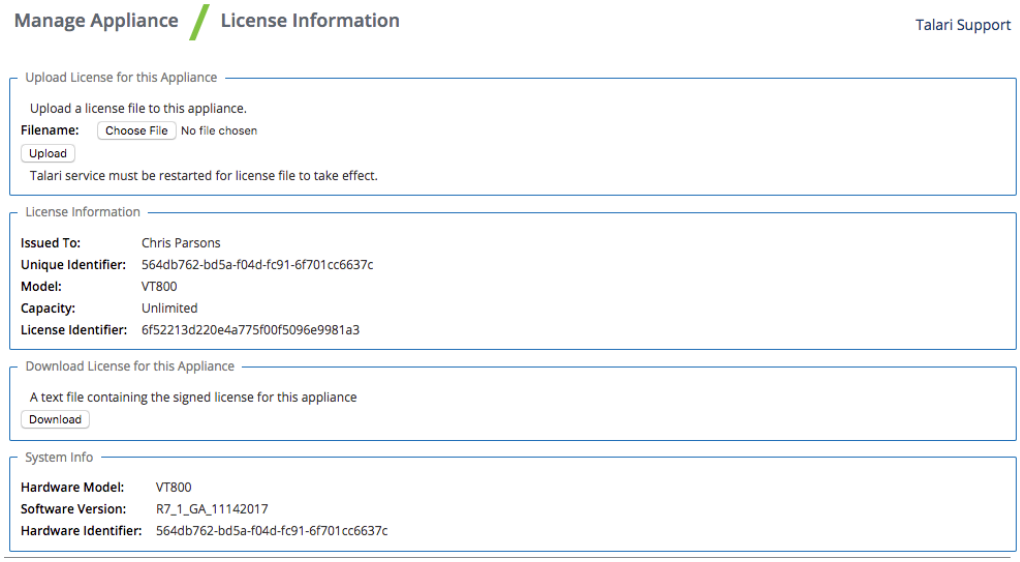


2. Select **Client** or Network Control Node (**NCN**) and click **Apply Package**.
3. Once the Appliance Package is uploaded the **Client Setup Complete** (or NCN Setup Complete) page will load.



> **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

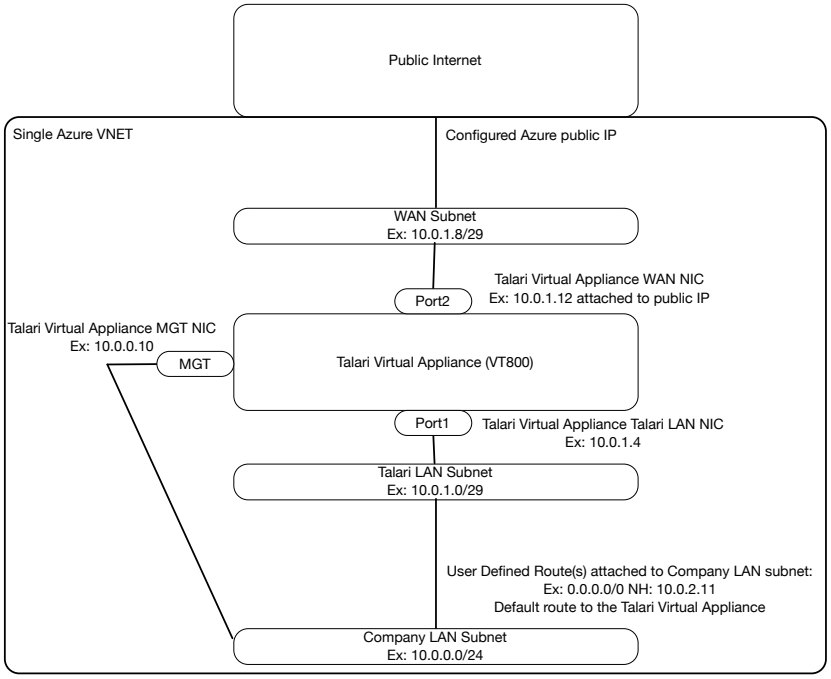
- A valid license
  - In order to acquire a license, you will first need to spin-up the new appliance so that you can obtain the UUID of the appliance.
  - Once a UUID has been obtained from the appliance, please contact your Account Team who will assist you with procuring a valid license that will need 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:

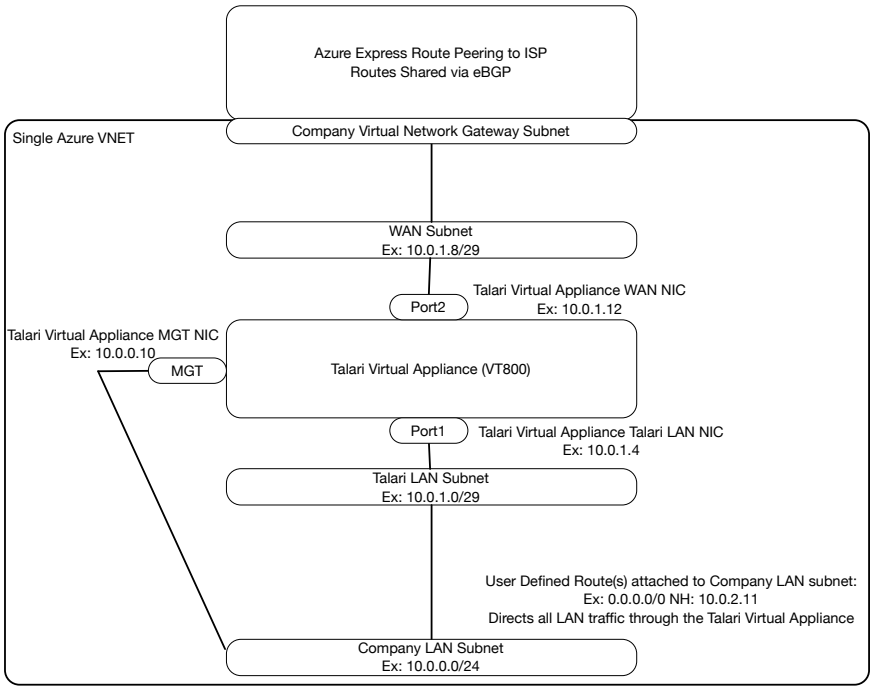
1. Single WAN Link Using Azure Public IP Address

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



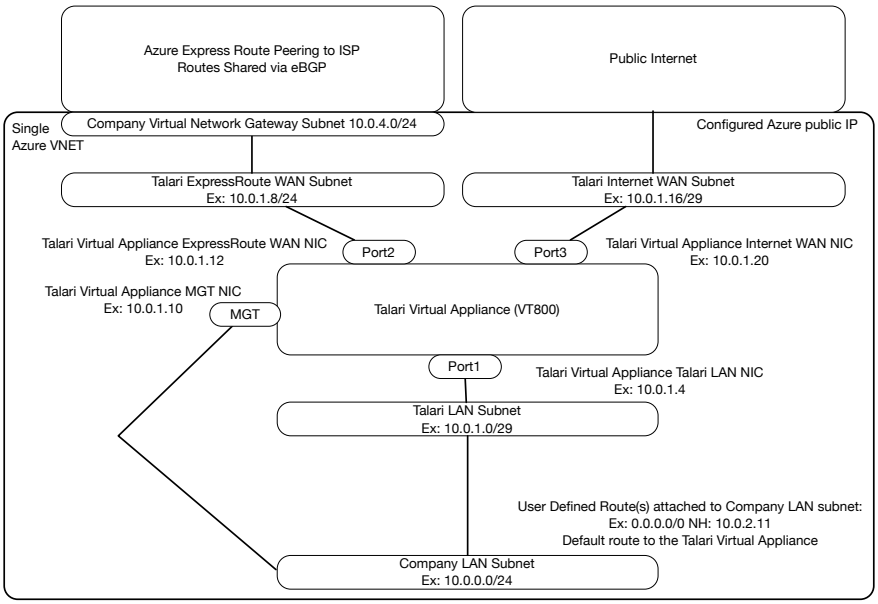
2. Single WAN Link Using Azure Express Route

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

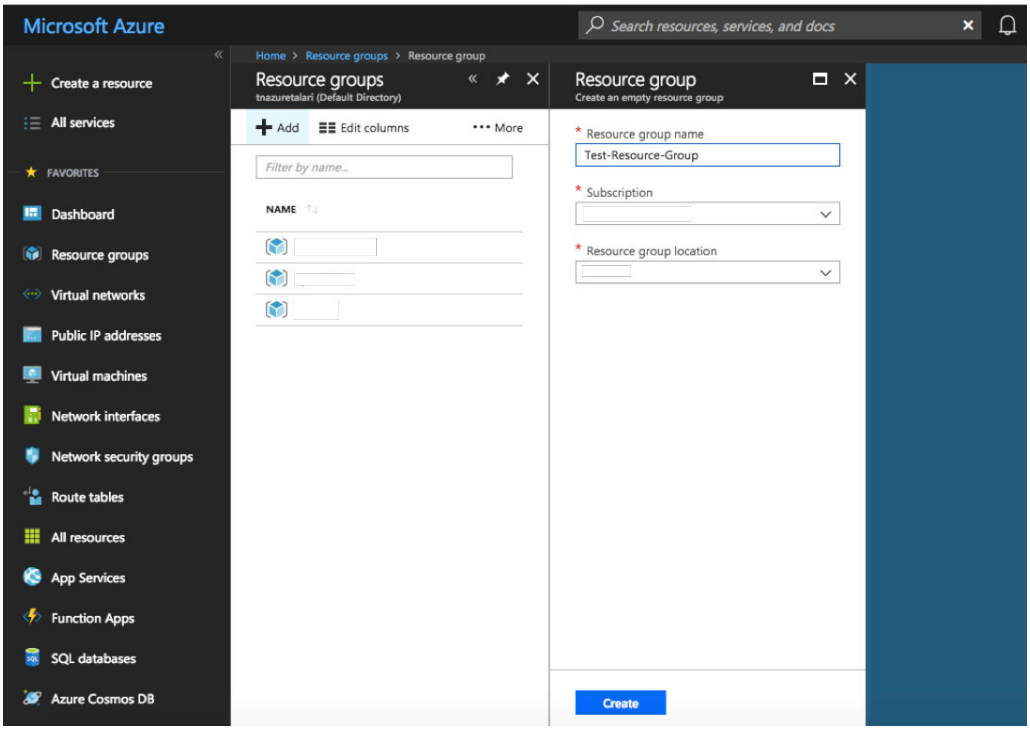
Prior to deploying a Virtual Appliance, you should ensure that you have all the Microsoft Azure resources required by your topology and configuration. If you have already gathered the required resources, please skip ahead to the section below. If

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)

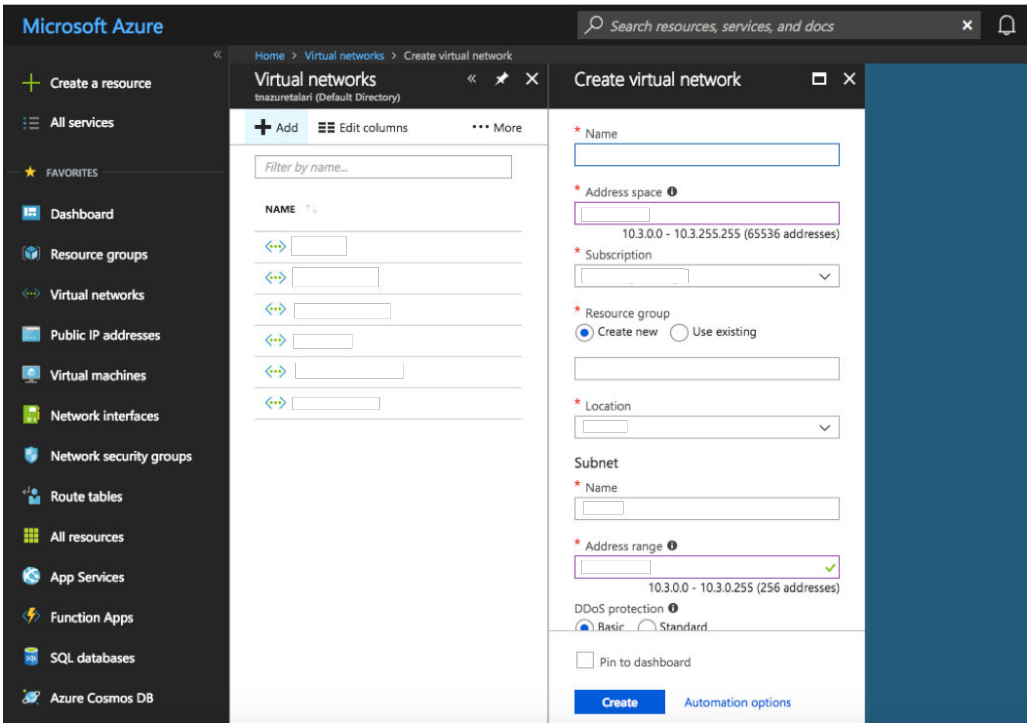
If you do not have an already-existing VNET with free Address Space, you will need to create a new VNET or alter an existing VNET to include the Address Space you defined in the “Addressing Guidelines & Planning” section.

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.”

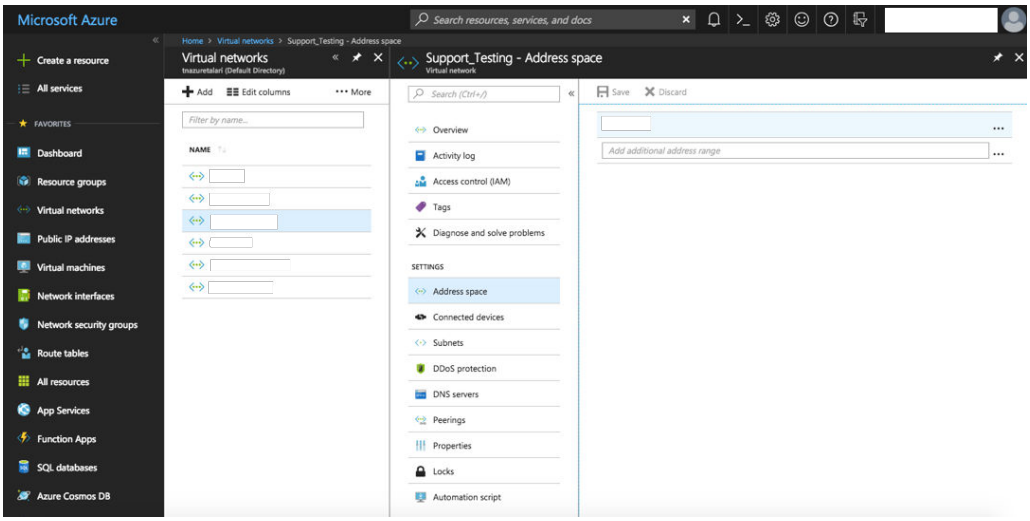
Figure 2-19 Create VNET



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



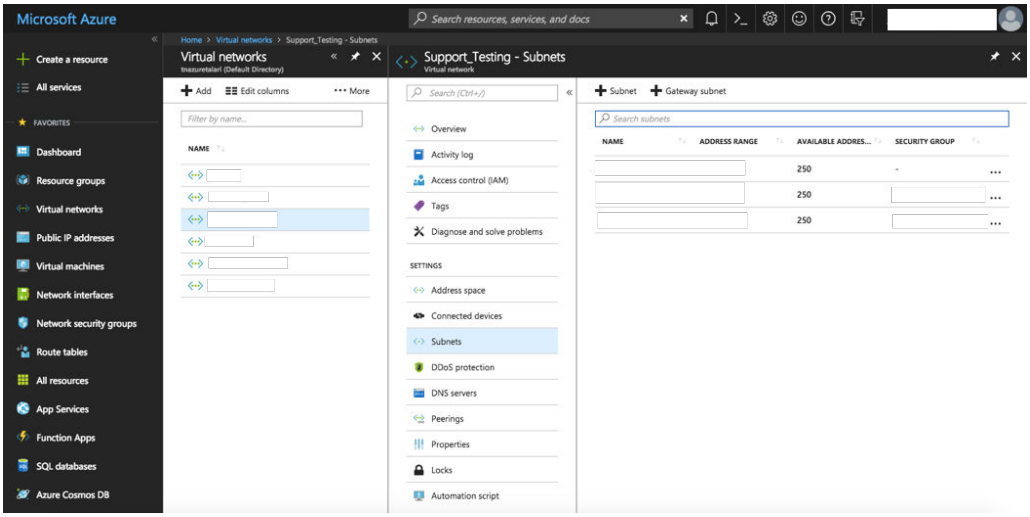
Subnets

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

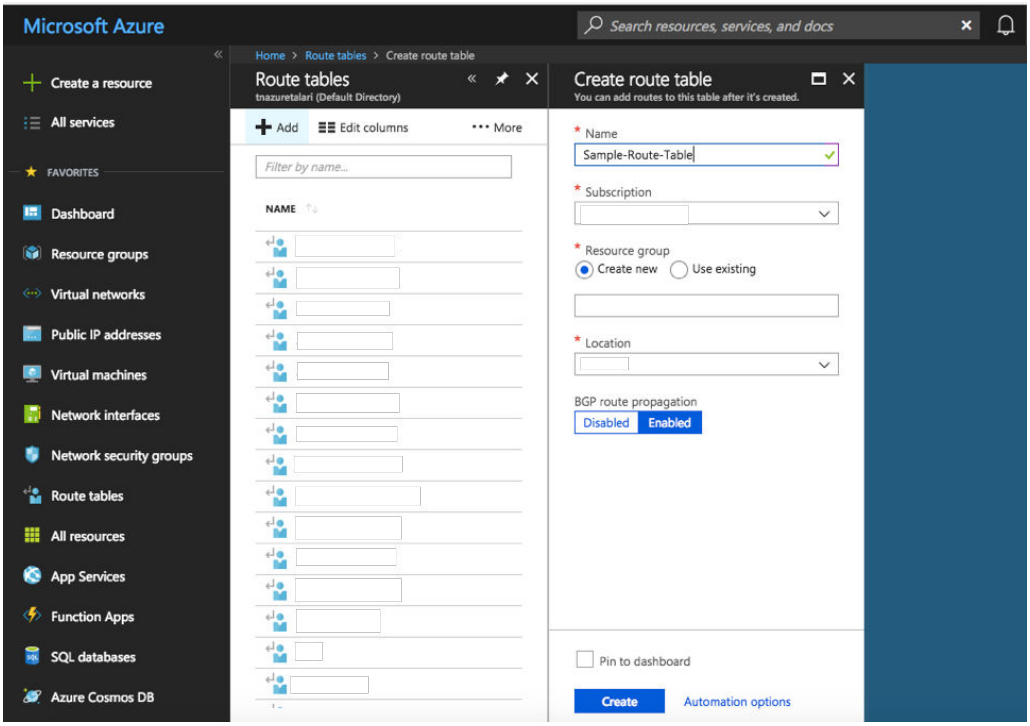
Route Tables will need to be created for each Subnet created above. The following routes are required for each Subnet's Route Table:

- 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

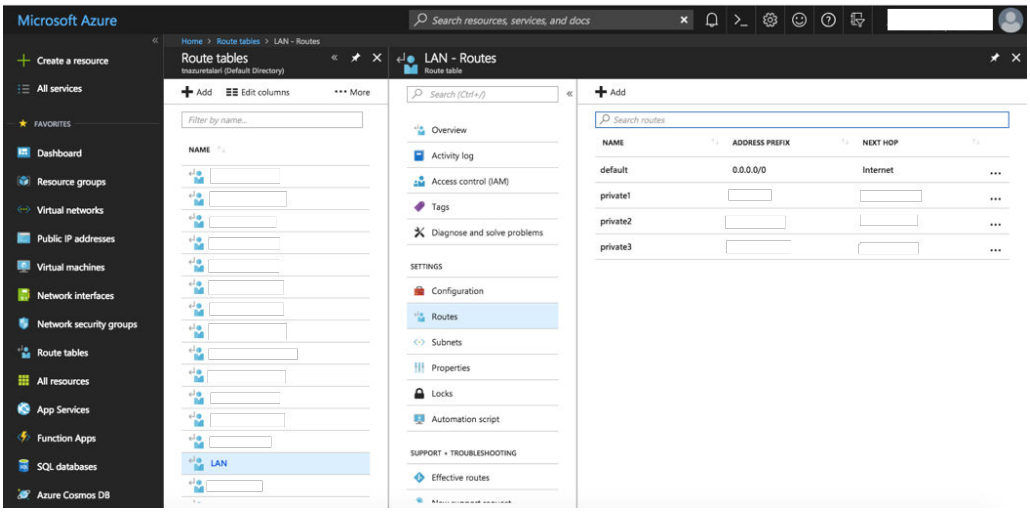


Once created, the new Route Table will have to be modified to include all required routes, with a minimum of the above-discussed routes included in each Subnet's Route Table.

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.

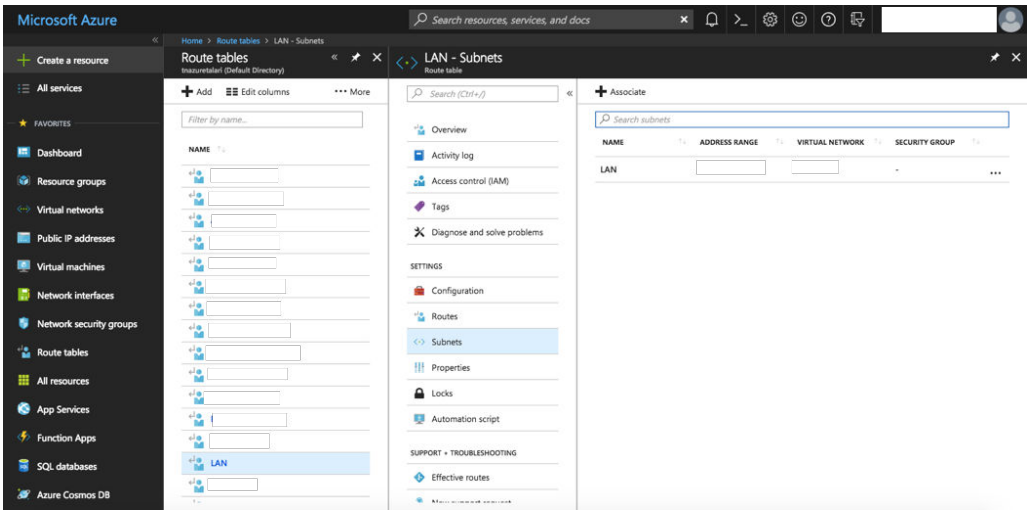
Figure 2-23 Modify Route Table



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).

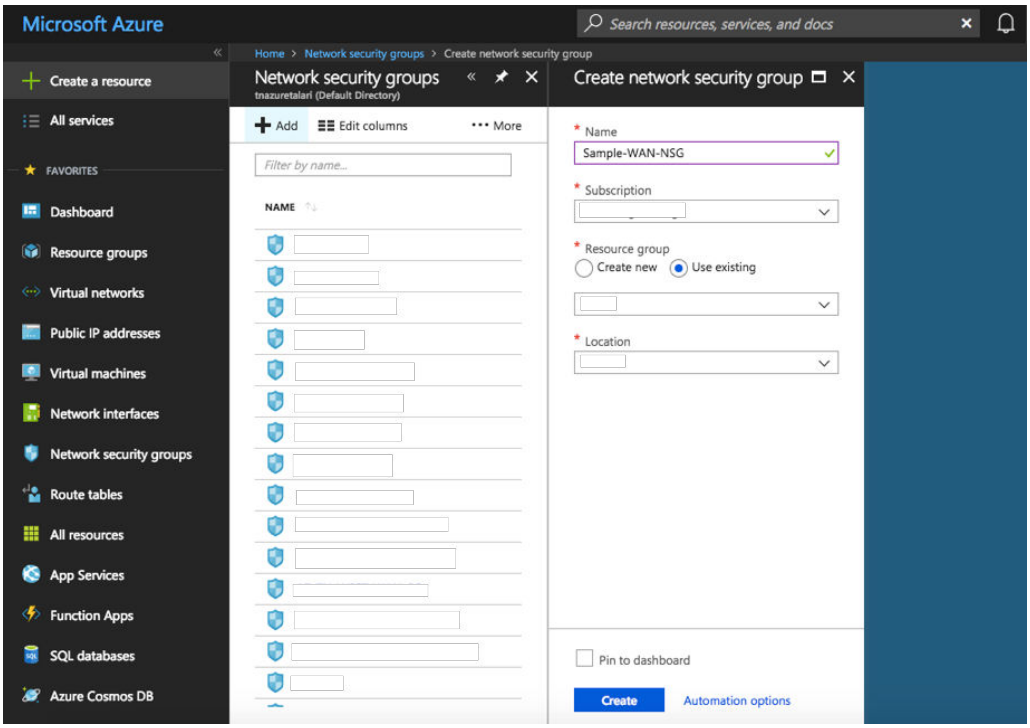
The following rules must to be added for both inbound and outbound traffic for the MGT & WAN NSGs:

- 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.

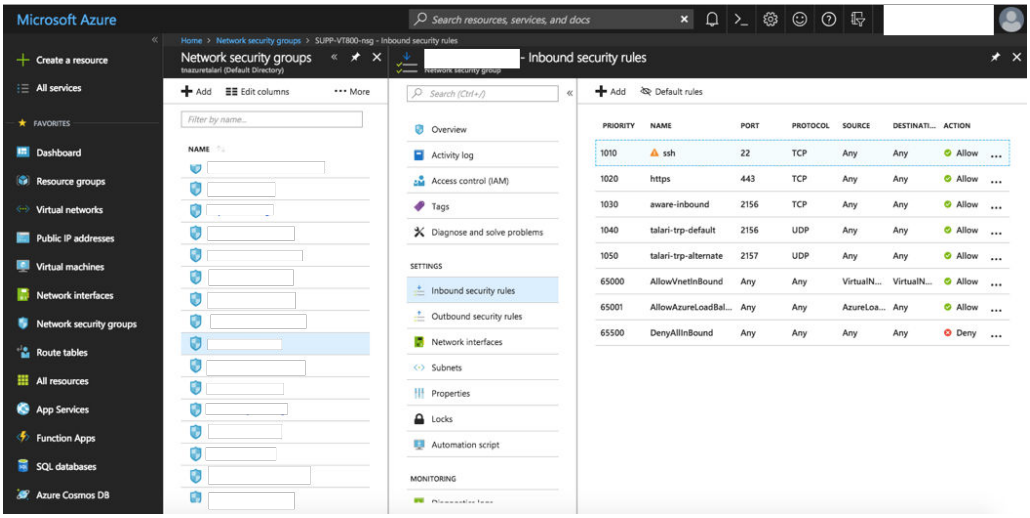
To modify an existing NSG and/or a new Inbound/Outbound Security Rule to an existing NSG:

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:

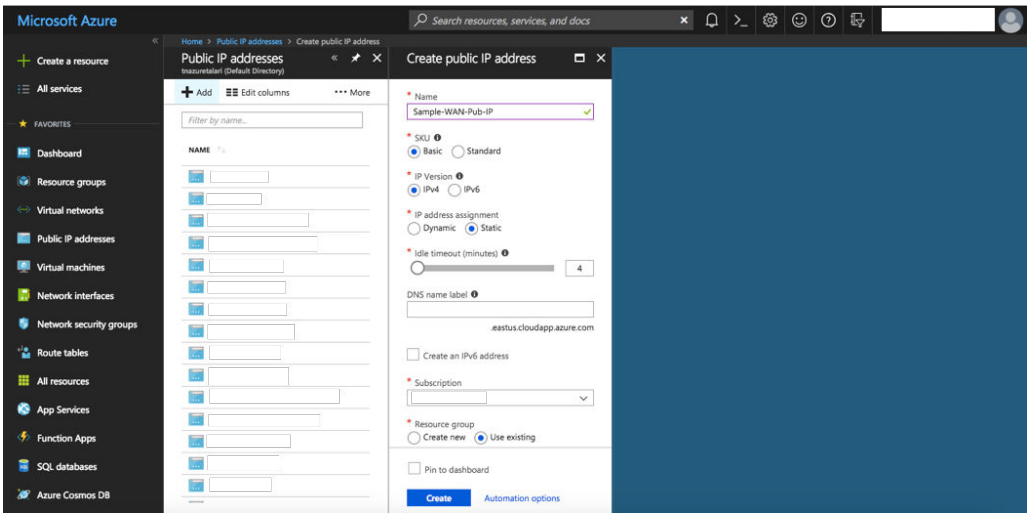
- WAN Pub IP – Public IP Address to be associated with the WAN Interface.
- MGT Pub IP – Public IP Address to be associated with the MGT Interface (optional once deployment is complete).

> **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



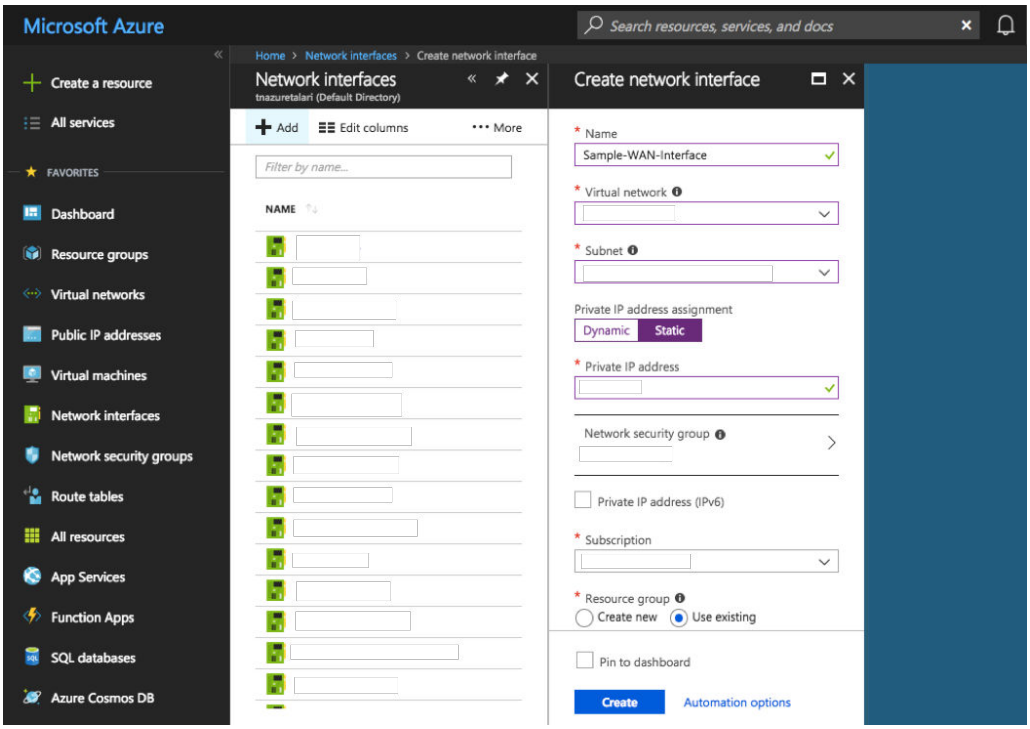
Virtual Network Interfaces (NICs)

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



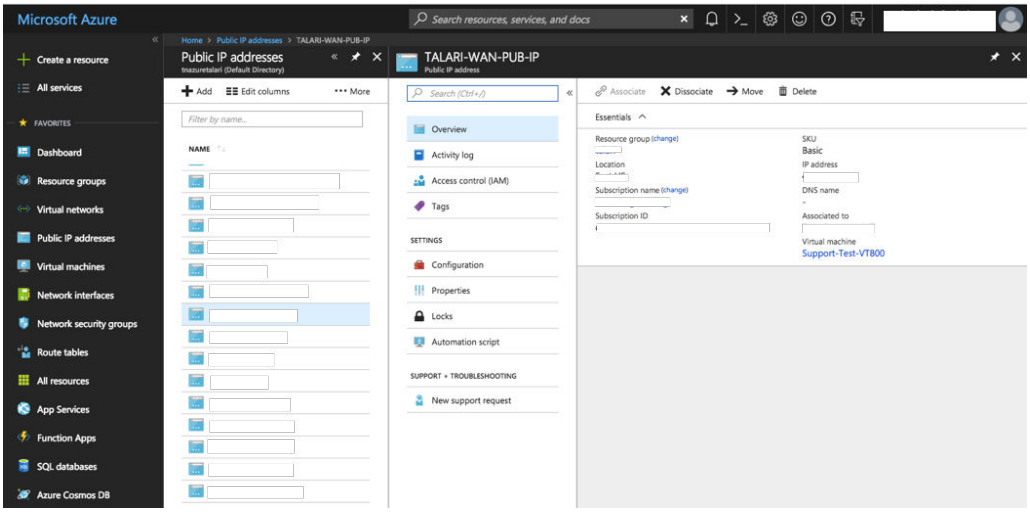
Virtual NIC Configuration

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



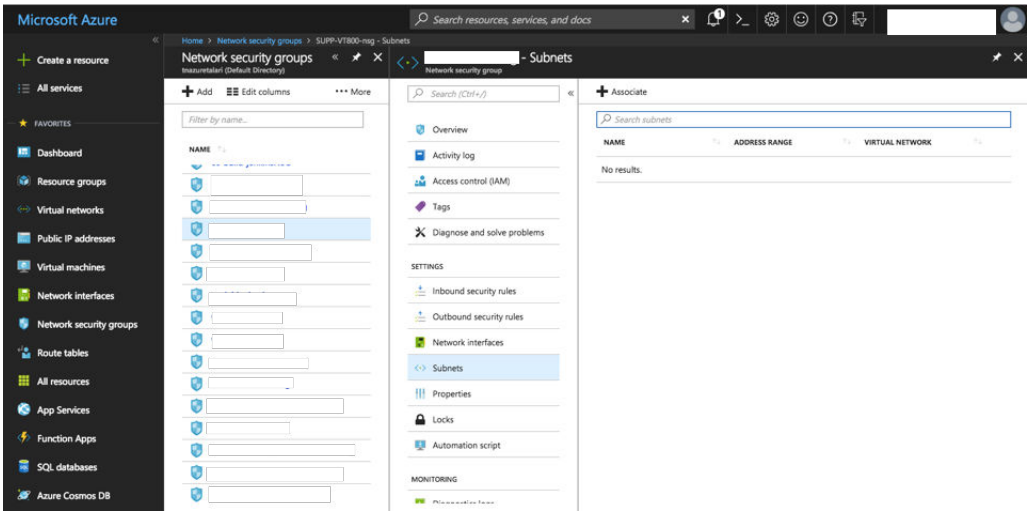
In the “Associate Public IP Address” sub-menu:

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.”

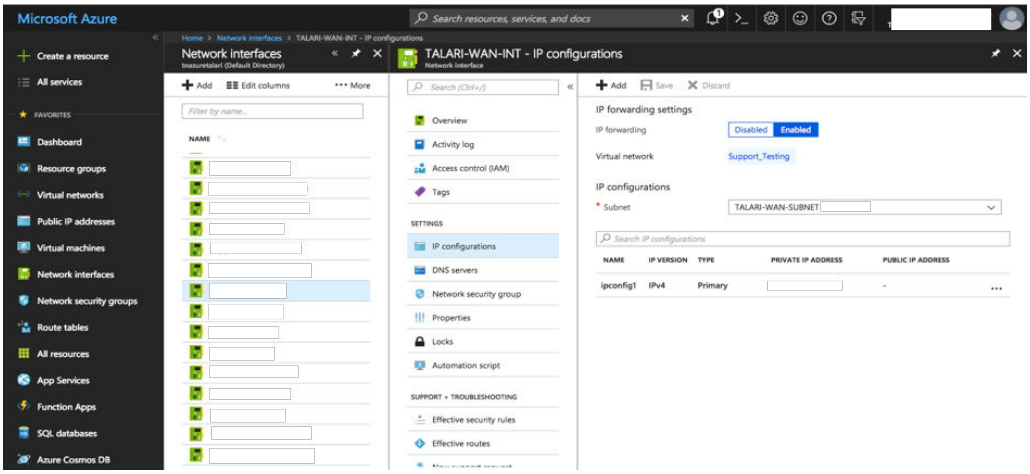
Figure 2-30 Associate Network Security Group with Virtual NIC



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



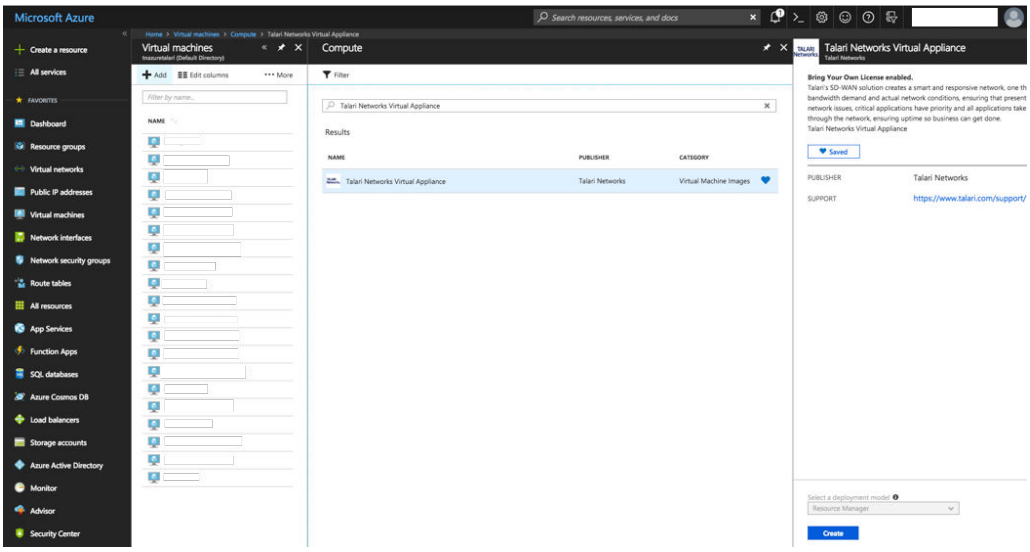
Deploy The Virtual Appliance

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



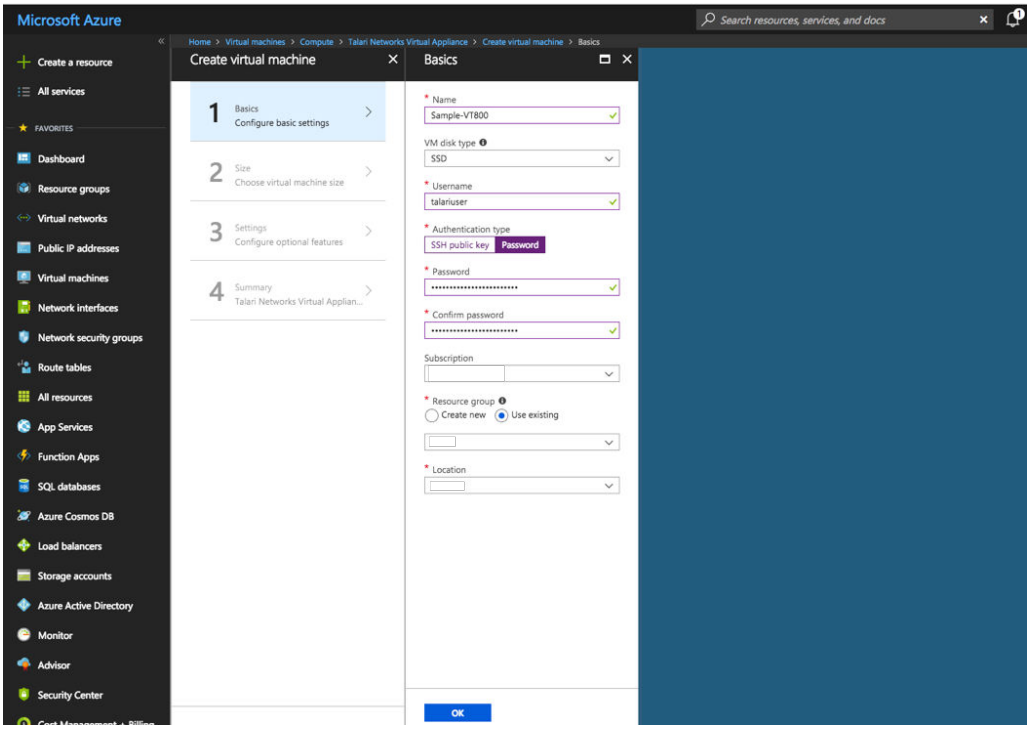
Once “Create” is clicked the page will redirect to a settings configuration sub-menu. In order to complete the Virtual Appliance creation process, the user must:

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. Enter “talariuser” for the Username.
4. Set the Authentication type to “Password.”
5. Create a secure password for the “talariuser” account.
6. Select the Subscription, Resource Group, and Location defined in the “What You Need Before Starting” section.
7. Click “OK.”

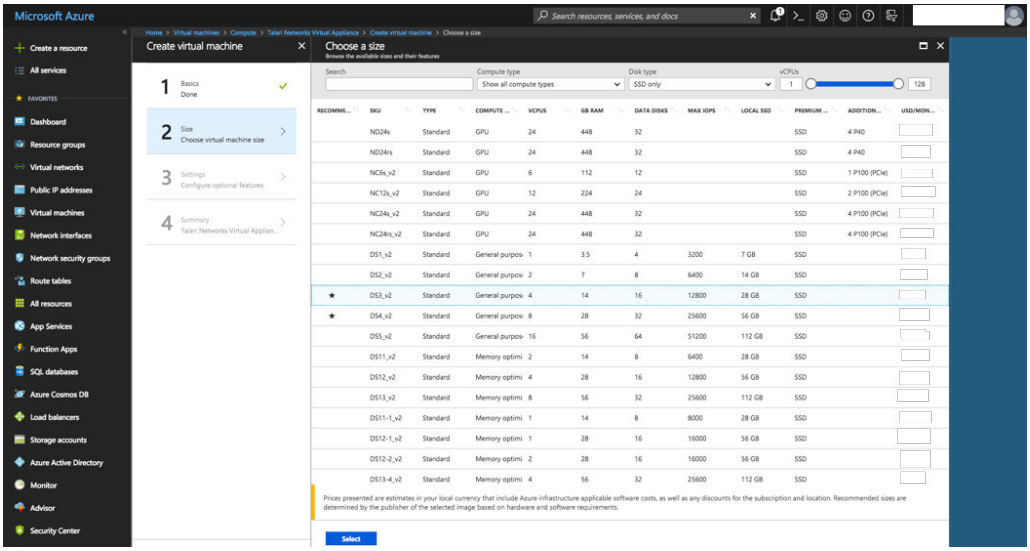
Figure 2-33 Create Virtual Machine: Configure Basic Settings



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.”

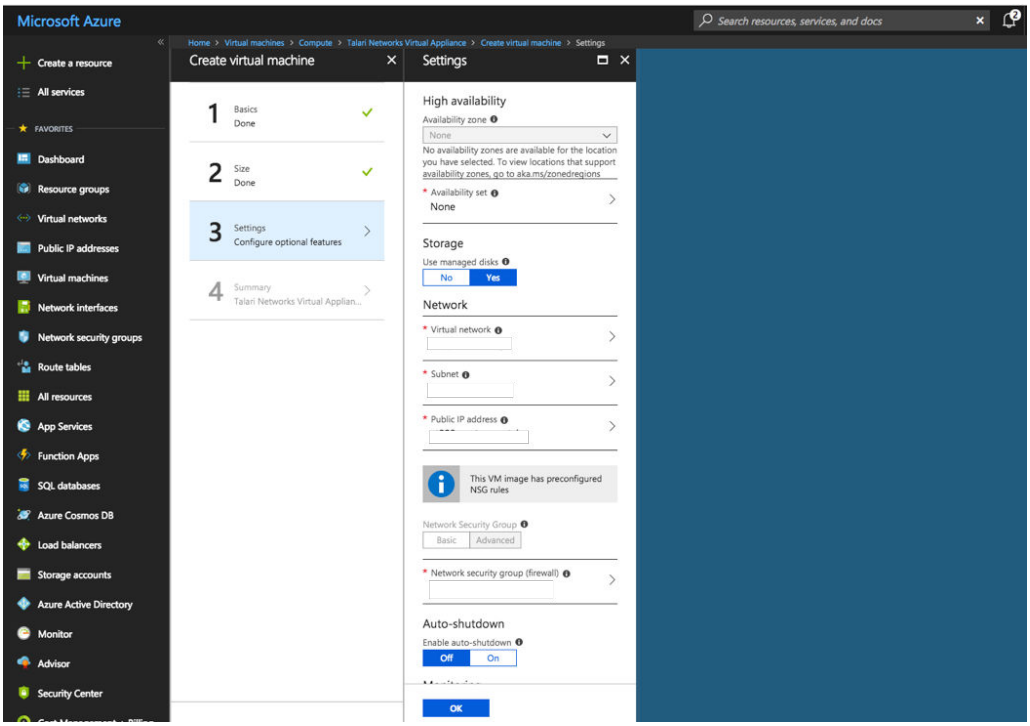
Figure 2-34 Create Virtual Machine: Select a VM Size



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

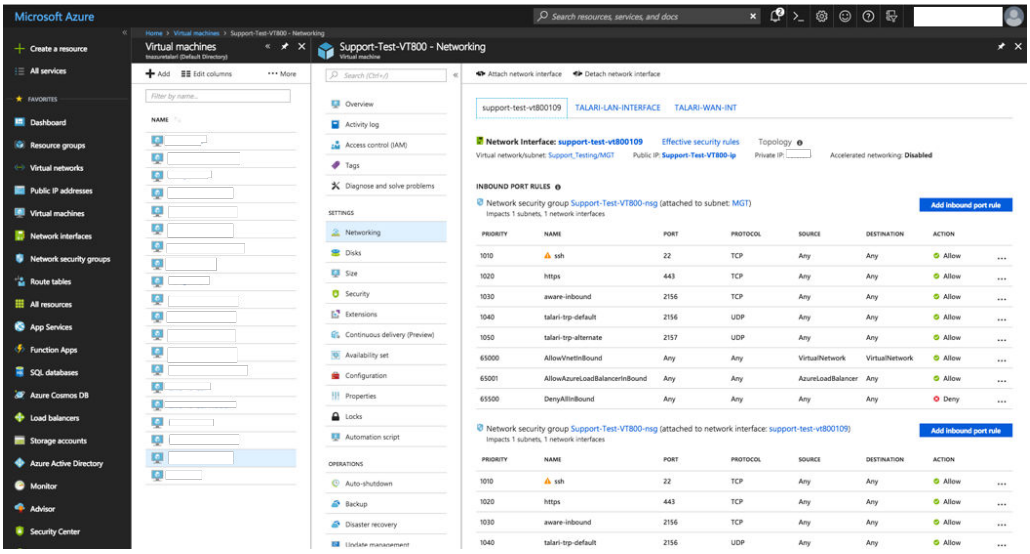
Once deployed, navigate to the newly-created Virtual Appliance and stop it. You will need to add the additional LAN/WAN Interfaces.

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. Navigate to the Public IP associated with the 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. 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 during the VM creation process.
4. 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.
5. Once the package has been installed, note your appliance UUID and reach out to the Account Team for assistance with procuring a Virtual Appliance License.

> **Note:**
>
> Do not enable service on the Virtual Appliance before a license has been applied.

6. Once a valid license has been obtained:
   a. Navigate to **Manage Appliance > License Information** on the Virtual Appliance.
   b. Upload the license obtained through the Account Team.
7. 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.
8. 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 ~]#
```

OCI IaaS Configuration

Follow these instructions to deploy Oracle SD-WAN Edge Virtual Appliance on Oracle's Cloud Infrastructure (OCI) as a Virtual Machine(VM) to provide connectivity to IaaS (Infrastructure as a Service) resources.

1. Log in to Oracle Cloud and select the region where you want to deploy.
2. Enter your credentials, then enter your cloud tenant ID.
3. From the navigation bar, in **Networking**, **Virtual Cloud Networks**, create a new virtual network with the following configuration:
   - Security list: It is recommended to use stateless lists for WAN/LAN interfaces. The LAN security list can be configured as needed. The WAN security list will need to have UDP port 2156 open, at minimum, as this is the default WAN service port. Management ports, however, can be stateful, and should be used as follows
     - SSH—TCP port 22
     - NTP—UDP port 123
     - HTTPS—TCP port 443
   - Subnet configuration: Subnets must be created for management access, LAN access, and WAN access.
   - Internet gateway: Create a default internet gateway.
   - Route table: Use the default.
   - DHCP options: Use the default.
4. From the VCN Compartment dialog, open the drop-down menu and click on **Object Storage**.
5. If there is no bucket available, create one by clicking on the **Create Bucket** button.
6. Select your bucket and click on the **Upload Object** button.
7. Locate your image and upload it to the bucket.

> **Note:**
>
> The image must be in qcow2 format.

8. On the **Overflow** menu, click on **Create a pre-authenticated request**.
9. Click on the **Permit Read On The Object** to enable read permissions.
10. Click on the **Create Pre-Authenticated Request** button.
11. On the **Pre-Authenticated Request Details** menu, click on the copy link under the **Pre-authenticated request URL** field. You will use this URL to access your image.
12. Go to **Compute**, **Custom Images**.
13. On the **Import Image** dialog, select the compartment from the **Create in Compartment** option.
14. Type a name in the **Name** field.
15. On the **Operating System** drop-down, select **Linux**.
16. Paste the pre-authenticated request URL into the **Object Storage URL** field.
17. From the **Image Type** radio buttons, select **QCOW2**.
18. From the **Launch Mode** radio buttons, select **Paravirtualized Mode**.
19. Go to **Compute**, **Instances** from the menu.
20. Click on the **Create Instance** button.
21. Select the uploaded custom image from the **Create Compute Instance** dialog.
22. Enter a name and an availability domain.
23. Select **Virtual Machine** as the instance type.
24. Select the **VM.Standard2.4** shape.
25. In the **Configure Networking** section, select the VCN compartment, VCN, subnet compartment, and subnet for the management interface.
26. Click on the **Show Advanced Options** link, then select **Hardware-assisted SR-IOV networking** on the **Networking** tab.
27. Leave the **Boot Volume** parameters at its default.
28. Optional: Add an SSH key for logging into the appliance with SSH in the **Add SSH Key** section.
29. Click on the **Create** button.
30. Go to **Compute**, **Instances** and open the instance.
31. Click on the **Stop** button. Interfaces cannot be added to an instance while it is running.
32. In the Attached VNICs section, click on the **Create VNIC** button.
33. Name the VNICs and select the subnets you created.
34. Repeat the last two steps for the number of LAN/WAN interfaces you are adding, in the order you want them to be in.
35. Click on the **Start** button.

You can now access the Oracle SD-WAN Edge instance through its management interface.

Oracle Cloud Marketplace Support

SD-WAN Edge virtual appliance is available for installation directly from the Oracle Cloud Marketplace. Installing SD-WAN Edge from the cloud marketplace simplifies the process and lets you run your application sooner.

An OCI account is required to use the marketplace. Search for "Oracle SD-WAN Edge Virtual Appliance" on the Marketplace web site.

Initial sign-in to SD-WAN Edge on OCI

When you sign in to SD-WAN Edge virtual appliance for the first time, a default username and password are provisioned. These are:

- Username: talariuser
- Password: talari-[first 8 characters of OCID string]

For example, A Virtual Appliance with a VM OCID of ocid1.instance.oc1.phx.**anyhqljs**q5fbg5acabkpupy4ew2rickxhkcnuqmqtxdrshbyi25umjngtnh2 would be accessible via the user "talariuser" and password "talari-anyhqljs".

See Where to find your tenancy's OCID for more information.

Refer to the following resources for more information.

- Oracle Cloud Marketplace Documentation
- Oracle Cloud Infrastructure Documentation

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:

- High Availability (HA) appliance pairing
- 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