

Implementing Citrix Virtual Apps and Desktops in Oracle Cloud Infrastructure

ORACLE WHITE PAPER | AUGUST 2019





Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

The following revisions have been made to this white paper since its initial publication:

Date	Revision
August 30, 2019	Initial publication



Table of Contents

Overview	4
Benefits	5
Architecture	6
Control Environment	6
Deployment Options	8
Internal Structure of Hyper-V Instances	11
Requirements	12
Determine the Number of Required Bare Metal Instances	12
Other Requirements	13
Deploying Citrix Virtual Apps and Desktops on Oracle Cloud Infrastructure	15
Initial Deployment Steps	15
Deploy the Hyper-V Instances	16
Configure DNS and DHCP for the Hyper-V Guests	28
Create Hyper-V Helper Guests	32
Add Hyper-V Hosts to SCVMM	39
Conclusion	54
Appendix A: Deploying Dual Citrix ADCs	55
Additional Requirements for Dual ADC deployment	56
Configuration Procedure	57



Overview

When end users interact with enterprise applications, their experience is important. Users must be able to interact smoothly and efficiently with an application to be productive and achieve the goals of the enterprise. Users also expect that the applications they depend on are consistent in their presentation. Enterprises want to maintain a consistent user experience and provide a secure and protected environment in which their users can complete their tasks. When deploying standard enterprise applications within an on-premises environment, many enterprises use Citrix Virtual Apps and Desktops to both control the user experience and abstract the application interaction away from the user.

When these applications are migrated from on-premises to Oracle Cloud Infrastructure, the same access methodology can be used. Oracle Cloud Infrastructure provides a secure, stable, and high-speed environment in which enterprises can put their most demanding workloads. This now includes the ability to deploy Citrix Virtual Apps and Desktops in Oracle Cloud Infrastructure.

This paper provides the following information:

- How Oracle and Citrix are implementing Citrix Virtual Apps and Desktops on Oracle Cloud Infrastructure
- The various architectural options and how to select the appropriate one for your environment and requirements
- Detailed implementation instructions for the infrastructure required to successfully install Citrix Virtual Apps and Desktops

Note: This paper provides architectures and instructions for the required infrastructure for Citrix Virtual Apps and Desktops. However, it's not a reference for actually performing the configuration. After they are implemented, the infrastructure architectures listed here provide the foundation on which standard Citrix implementation practices can be applied. Because of that, we make no effort to detail the implementation details of the Citrix products beyond what is unique to the Oracle Cloud Infrastructure environment.



Benefits

Moving the Citrix environment from on-premises to the cloud, as a part of an overall migration of application infrastructure, has the following benefits:

- **Reduce perceived latency for application users:** Application latency is an important predictor of end-user experience. Applications with high latency appear to be sluggish and unresponsive, while ones with low latency are perceived as speedy. Particularly in applications that have a traditional “thick client” architecture, latency is often introduced by the network connection between the client tier and the middle or data tier.

A key way to ensure good application performance and responsiveness to user interaction is to have the desktop or application as “close” as possible to the data source. In an on-premises environment, proximity is typically not an issue. Either the end-user desktop is on a local network with relatively high-speed and low-latency access to the data, or the organization has implemented a virtual desktop infrastructure (VDI) solution with Citrix, placing the virtual desktop close to the data source. However, in a cloud environment, the cloud endpoint is typically distant from the end user, and remote access can cause critical data to transit insecure connections. Moving the VDI solution with the data to the cloud restores the connection between desktop and data to high speed and low latency, and provides the security of the Oracle Cloud Infrastructure virtual cloud network (VCN).

- **Deploy known and proven Citrix environments in Oracle Cloud Infrastructure:** Enterprises want to implement known technologies, especially when dealing with end-user productivity. On-premises environments depend on Citrix to provide high-reliability VDI environments. Implementation of Citrix VDI solutions in Oracle Cloud Infrastructure lets enterprises continue to use Citrix in the same way as on-premises, but relocated to the cloud. Citrix has certified the solution in this white paper as “Citrix Ready,” so you can be sure of the reliability of the resulting environment.
- **Maintain current operational models while gaining the elasticity of the cloud:** Organizations have a large investment in operational practices and procedures that they have built over time. By using Citrix VDI solutions in Oracle Cloud Infrastructure, organizations can use the knowledge developed by managing and provisioning desktops and virtual applications, while adding the benefit of expanding capacity to meet need quickly and efficiently.
- **Quickly scale out VDI environment to meet expansion:** One of the disadvantages of running VDI on-premises is the restricted ability to quickly grow to meet increasing demand, or to shift additional applications into the environment. The constraints of space, power, cooling, and connectivity typically limit deployment times to weeks, if not months. Deploying Citrix VDI in Oracle Cloud Infrastructure provides enterprises with the ability to quickly grow environments to meet current demands in a fraction of that time that it can take on-premises.

Architecture

This section describes both the Citrix desktop control environment and the possible deployment architectures.

Control Environment

Before we explore the architectural options, let's identify how the Citrix desktop environment is controlled. Citrix provides two methods of control: through the Citrix Virtual Apps and Desktops Service (CVADS), and local. CVADS provides a cloud-based environment that offloads many of the functions that previously had to be installed on-premises to manage the VDI environment. CVADS vastly simplifies the deployment of Citrix, thus increasing resiliency. However, the traditional method of deploying the Citrix Virtual Apps and Desktops software inside Oracle Cloud Infrastructure, as part of the overall VDI deployment, is also supported.

Figure 1 shows a typical CVADS deployment, in which CVADS control originates outside of Oracle Cloud Infrastructure and links to localized Citrix Cloud Connectors.

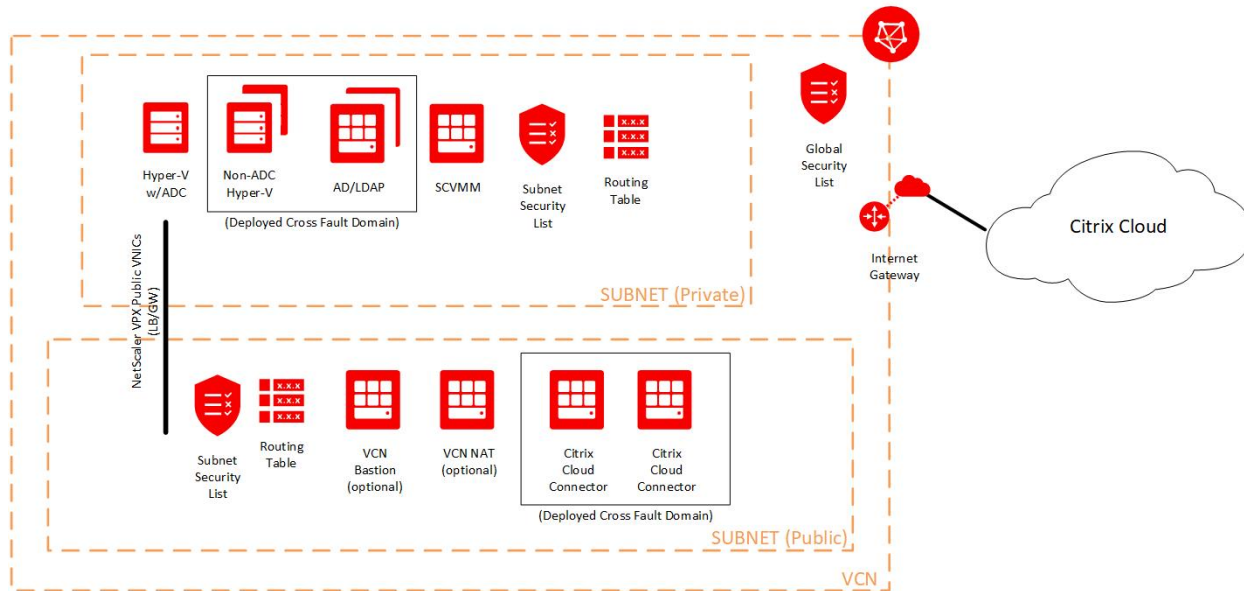


Figure 1: CVADS Deployment

This model lets organizations deploy multiple Citrix environments, all with different configurations, potentially across different physical environments, without replicating localized Citrix configuration and control instances. Having Citrix Virtual Apps and Desktops services in this environment can provide a great deal of flexibility that can't necessarily be replicated to an on-premises environment.

Contrast the CVADS deployment with a typical local control environment, as shown in Figure 2. Although there is no dependency on the outside Citrix Virtual Apps and Desktops services, additional Storefront and Delivery Controller (DDC) instances must be deployed to provide the same functionality. These instances would need to be replicated to each Citrix environment that is deployed within Oracle Cloud Infrastructure, potentially multiple times within the same region.

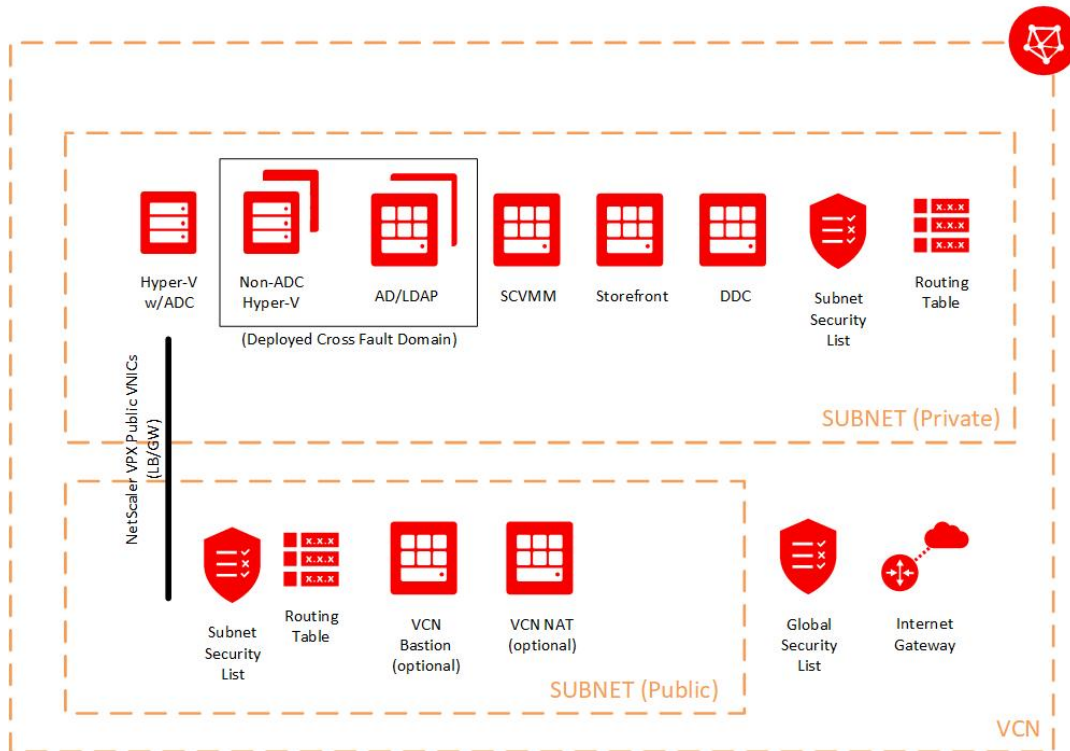


Figure 2: Local Control Deployment

Both approaches have their advantages, based on your approach to cloud. If you want to get out of the software-management business as much as possible, consider using CVADS. Citrix is responsible for managing all of the Citrix software infrastructure, so you can focus on issues that are related to your business. However, if you want to extend your presence to the cloud but still control the timing and application of patches and upgrades, Citrix Virtual Apps and Desktops (minus the services) might be a better choice. Your local Citrix technical representative can help you with your options and to discuss the advantages and options for deploying Citrix using Citrix Virtual Apps and Desktops services.

One option that you don't need to decide before deployment is the provisioning mechanism used to deploy desktops. If you are using an Oracle Cloud Infrastructure Compute bare metal instance, both Citrix Provisioning Services (PVS) and Machine Creation Services (MCS) are fully supported

when you deploy your VDI environment on Oracle Cloud Infrastructure. Deploying Citrix VDI without a provisioning mechanism is also supported but not covered as part of this document.

Deployment Options

After you pick the control mechanism, you need to consider the options for deploying the Citrix infrastructure: Storefront Only, Single Citrix application delivery controller (ADC), or Dual Citrix ADCs.

Storefront Only Deployment

The Storefront Only deployment doesn't use a Citrix ADC; it requires only the deployment of a Citrix Storefront and DDC to act as a desktop provisioning mechanism. Citrix ADC deployments are generally used to provide virtual application or desktop services to end users through the public internet. Organizations that have a private connection to Oracle Cloud Infrastructure and use that connection to provide the virtual application or desktop services can use a Storefront Only deployment to meet their needs. This architecture is shown in Figure 3.

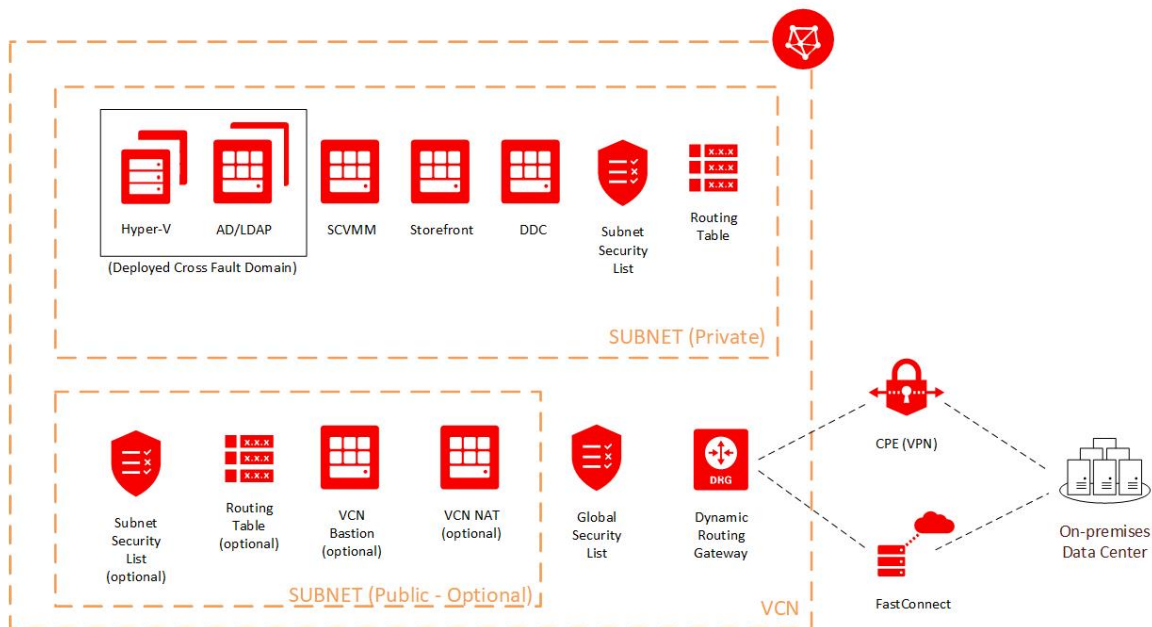


Figure 3: Storefront Only Deployment Architecture

The Storefront Only option uses a standard Hyper-V deployment combined with the required Citrix infrastructure servers. If the desktop count requirement exceeds what a single Hyper-V server can support, more Hyper-V servers are created and then added to both System Center Virtual Machine Manager and the Citrix infrastructure.

The advantages of this architecture are simplicity, scalability, and (potentially) resiliency:

- Because no Citrix ADCs are required, the overall complexity of the environment is reduced. The desktop servers are all the same.
- Scalability is linear. The number of Hyper-V servers is a direct function of the number of desktops required.
- Resiliency can be increased by building multiples of both Hyper-V and the Citrix infrastructure servers (Storefront and DDC servers).

Single Citrix ADC Deployment

The Single Citrix ADC deployment uses a single Citrix ADC virtual instance, embedded in the VDI environment, to provide VDI gateway and load balancing services to the overall deployment. This architecture is shown in Figure 4.

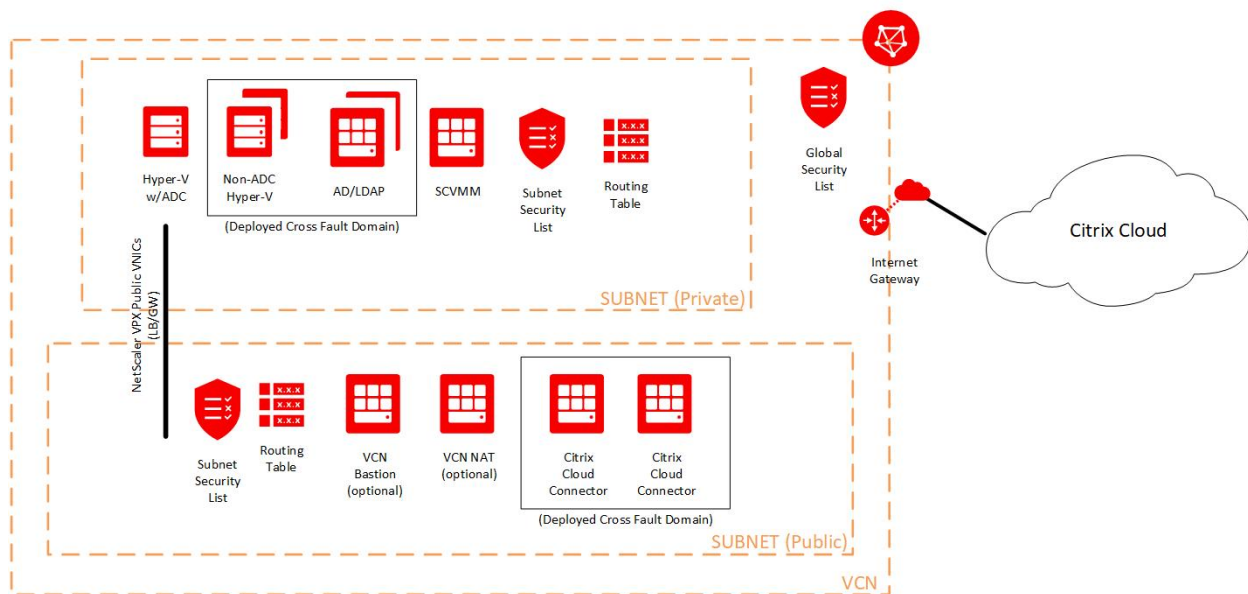


Figure 4: Single Citrix ADC Deployment Architecture

In this environment, the Citrix ADC needed to provide the gateway services is located in the Oracle Cloud Infrastructure bare metal instance labeled **Hyper-V w/ADC**. Any deployment of Citrix VDI services with provisioning requires at least one instance with the Citrix ADC installed within the bare metal server. Later instances, used to scale out the deployment, don't require any more Citrix ADC implementations.

This first bare metal instance is deployed with Microsoft Windows 2012 Datacenter or 2016 Datacenter, and configured to run Hyper-V. Desktops are served directly through the gateway on

the embedded Citrix ADC. If the desktop count exceeds the capacity of the first bare metal instance, more instances can be added to support the load, thereby providing a “scale-out” architecture. These other bare metal instances don’t require an additional Citrix ADC, however, and can be simply added to the inventory of the overall Citrix environment for use in provisioning desktops. Access control is provided through a localized Active Directory server, and control of the bare metal instances are provided by System Center Virtual Machine Manager (SCVMM).

This deployment architecture has the advantage of cost. Only the number of bare metal instances required to provide the necessary desktop coverage must be deployed to cover the number of desktops and virtual applications. Also, only a single Citrix ADC license must be sourced from Citrix, and a limited number of additional instances must be provided from Oracle to support the environment as a whole.

However, this cost advantage is balanced by a possible loss of resiliency. Because only a single Citrix ADC is embedded in a bare metal instance, if the instance fails, access to the desktops is lost. Although this kind of failure is rare in Oracle Cloud Infrastructure, it does represent risk.

Dual Citrix ADC Deployment

The Dual Citrix ADC deployment model is the deployment of multiple Citrix ADC devices within instances inside Oracle Cloud Infrastructure that allow for desktops to be spread between two different environments yet integrated into a single VDI deployment. This architecture is shown in Figure 5.

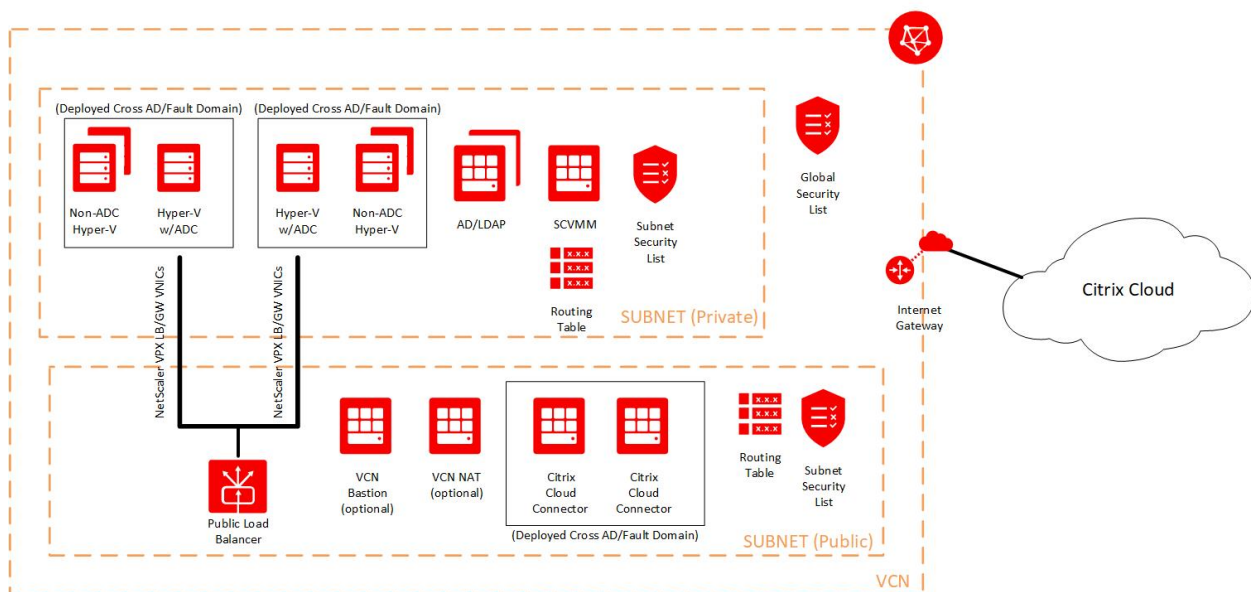



Figure 5: Dual Citrix ADC Deployment Architecture



This architecture places two of the bare metal instances, each with their own copy of the virtual Citrix ADC embedded, behind an Oracle Cloud Infrastructure load balancer. This type of deployment provides protection in the unlikely event of a bare metal instance failure, and provides a mechanism to further scale out the overall environment to other fault domains.

This architecture uses the Oracle Cloud Infrastructure Load Balancer service to provide a balance endpoint to the Citrix ADC gateway. This gateway is referenced by the Citrix management infrastructure (whether that is a local Storefront and DDC or Citrix Virtual Apps and Desktops Service), and desktops are served by the load balancer to consumers. The bare metal instances are deployed as with the single Citrix ADC model: Windows 2012 Datacenter or 2016 Datacenter with Hyper-V, and separate Active Directory and SCVMM servers. Scale-out is still part of this architecture, with individual additional bare metal instances “associated” with Hyper-V instances.

However, this ability to achieve both fault protection and additional scale-out comes at a cost: more required Oracle Cloud Infrastructure resources, an increased number and cost of Citrix ADC licenses, and a complexity of deployment that might actually reduce resiliency. This complexity results from two different factors—the need to designate which Citrix ADC uses which of the expansion Hyper-V bare metal instances, and the use of the load balancer to distribute load between different Citrix ADCs.

Internal Structure of Hyper-V Instances

Regardless of the deployment option, the internal structure of the Hyper-V bare metal instance is the same. The Hyper-V server is structured to provide direct access to Citrix Virtual Apps and Desktops and to allow for expansion, which maintains either the Storefront or the Citrix ADC as the primary endpoint for users who are consuming the virtual apps and desktops. The only difference between Hyper-V servers deployed using the Storefront option versus those using the Citrix ADC options is that the additional Citrix ADC Hyper-V guest and associated VNICs are not provisioned.

Figure 6 shows the deployment of the Hyper-V instance that contains the Citrix ADC.

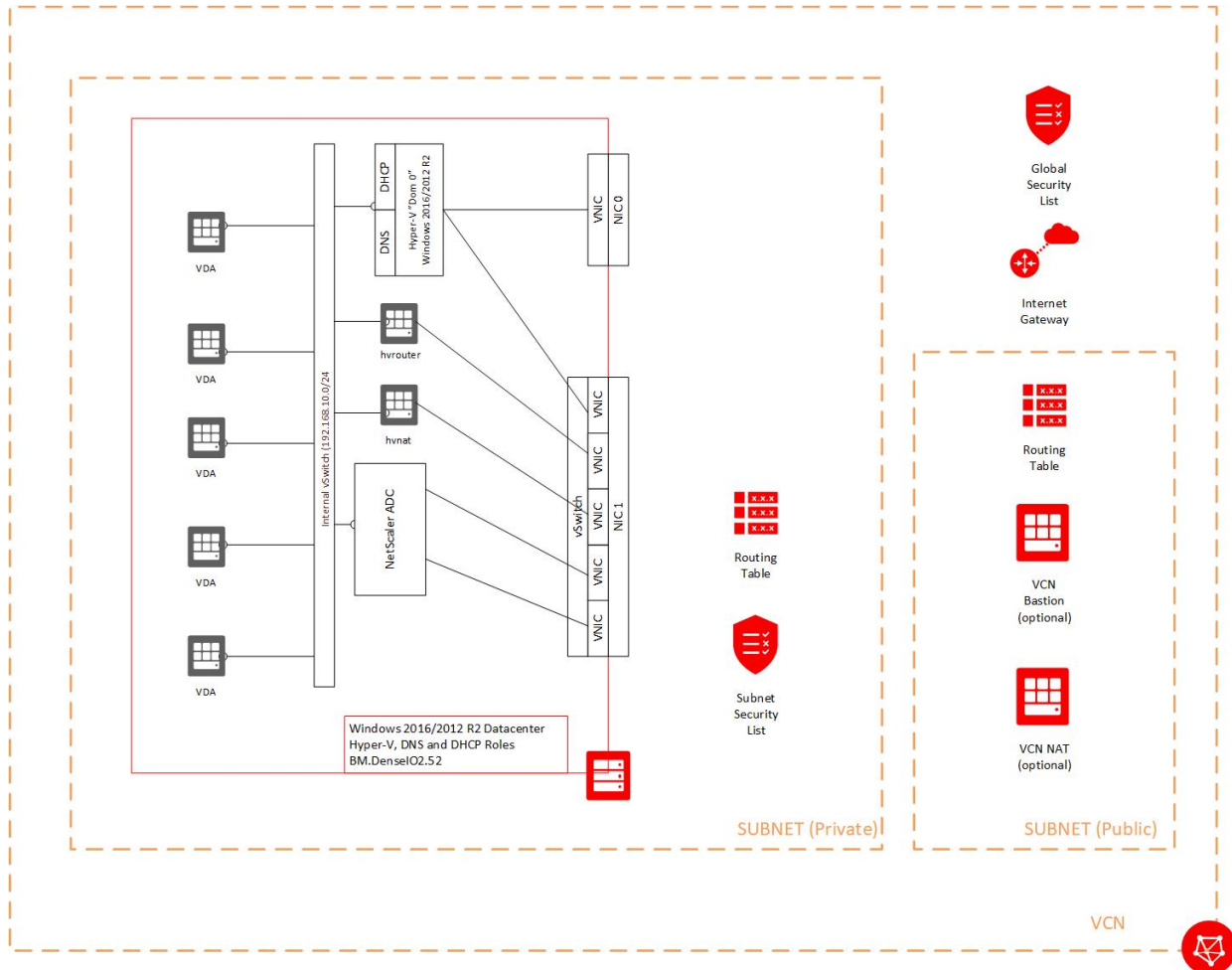


Figure 6: Structure of the Hyper-V Instance with the Citrix ADC

Requirements

This section lists the components that are required to deploy a base implementation of Citrix VDI within Oracle Cloud Infrastructure.

Determine the Number of Required Bare Metal Instances

Oracle and Citrix have extensively researched these deployments, including using the Login VSI benchmark, to determine the optimal number of guests that can be run within a single bare metal instance. Based on this research, you should use the following calculations to determine the number of bare metal instances to use during the initial deployment.

1. Determine the amount of RAM required by all desktop and virtual application deployments:

```
number of desktops * amount of RAM per desktop in GB
```

2. Determine the number of CPUs to be deployed:

```
number of desktops * number of CPUs per desktop
```

3. Select the larger value of the following two calculations, rounded to the next highest value. That value is the number of bare metal instances that you need.

```
<sum of RAM required> / 752 GB per bare metal instance
```

```
<sum of CPUs required> / 182 CPUs per bare metal instance
```


Note: The 182 CPUs number assumes a 1:1.75 oversubscription ratio between the actual number of cores present in a bare metal instance (104) and the oversubscribed number (182).

Other Requirements

The following requirements are based on the selection of either a single or dual Citrix ADC deployment model, and the selection of either using Citrix Virtual Apps and Desktops Service (CVADS) or local control for the provisioning control plane.

Common Requirements

- A minimum of one BM.DenseIO2.52 instance running Windows 2016 Datacenter Edition. The actual number of instances is based on the preceding calculation.
- Single virtual cloud network (VCN) with two subnets.
 - For implementations that use CVADS, create one public and one private subnet. Ensure that the public subnet can use the public internet.
 - For implementations that use local control, subnets can be public, private, or a mix, depending on the organization's requirements.
- One Citrix ADC license for the required throughput.
- Citrix Virtual Apps and Desktops licenses for the environment
- A Microsoft license for System Center Virtual Machine Manager (SCVMM) and an associated SQL Server license
- [Citrix ADC image for Hyper-V](#).
- If deploying without the use of CVADS, [software for local control of the Citrix Virtual Apps and Desktops deployment](#).
- SSL certificate for the Citrix ADCs and optional load balancer.

- 
- An established Active Directory (AD) domain. This domain can be new or part of an existing AD forest.
 - The AD server must be a Backup Domain Controller, at a minimum.
 - Windows DNS must be running for the environment to support the AD implementation
 - One VM.Standard2.8 instance running Windows 2016 Standard Edition. This instance is used for the Active Directory, SCVMM, and SQL Server deployments.
 - An IP range, not part of the VCN IP range, that you want to use for the internal Hyper-V network. Identify the first three addresses of the IP range for use by Hyper-V:
 - Hyper-V NAT helper instance (hvnat)
 - Hyper-V Traffic Forwarder helper instance (hvrouter)
 - Citrix ADC internal address (required only for Hyper-V instances with an ADC)
 - DNS/DHCP

For example, if you used 10.50.0.0/24 as your VCN IP range, you could select 192.168.10.0/24 as your internal network address. You could not, however, select 10.50.0.128/25 as your internal address space because it overlaps with the VCN addresses.

If you are deploying the dual Citrix ADC model, the IP addresses required here *cannot* overlap, and they *cannot* overlap with other addresses within the VCN.

CVADS Requirement

- Two VM.Standard2.4 instances running Windows 2016 Standard Edition. These instances are used for the dual, redundant Citrix Cloud Connectors.

Local Control Requirements

- One VM.Standard2.2 instance running Windows 2016 Standard Edition. This instance is for the Citrix Storefront software.
- One VM.Standard2.8 instance running Windows 2016 Standard Edition. This instance is for the Citrix DDC software.

Deploying Citrix Virtual Apps and Desktops on Oracle Cloud Infrastructure

The process described here is based on the general method of deploying Hyper-V within Oracle Cloud Infrastructure. Given that, we recommend that you download the [Deploying Hyper-V on Oracle Cloud Infrastructure](#) white paper before attempting deployment.

This Citrix paper uses the “indirect” method described in the Hyper-V paper. The deployment steps listed here duplicate the steps in the main Hyper-V paper only to meet the needs of implementing Citrix. However, the Hyper-V paper is a good reference for the deployment of Hyper-V in general.

Some of the steps in this section are used *only* for the Hyper-V instances that will contain a Citrix ADC. All other steps cover both ADC and non-ADC deployments. If you are deploying a non-ADC instance, follow this procedure *excluding* any ADC-specific steps.

In addition, this paper doesn't cover the installation, configuration, and operation of Citrix Virtual Apps and Desktops beyond what is unique to the installation in Oracle Cloud Infrastructure. After the initial deployment is complete, all further steps follow the standard Citrix methodology. Consult your Citrix documentation and technical resources for more information.

Initial Deployment Steps

The following steps are common for the deployment of the single and dual Citrix ADC models. Perform these steps before deploying the selected architecture.

1. If not already done, provision the VCN and required subnets.

For detailed information regarding Oracle Cloud Infrastructure networking concepts, processes, and procedures, see the [Networking documentation](#).

2. Provision the VM.Standard2.8 instance and attach it to the private subnet. Configure the instance as a Domain Controller, and install SQL Server and SCVMM according to Microsoft provided instructions. See the following Microsoft documents for background information:

- [Install SQL Server](#)
- [Install VMM](#)

3. If you are using Citrix Virtual Apps and Desktops Service (CVADS), deploy the two VM.Standard2.2 Cloud Connector instances, attaching them to the public subnet. Join them to the Active Directory domain and install the Cloud Connector software on each instance, from the Citrix Cloud website. Also install the SCVMM console software on each Cloud Controller instance. For more information, see [Citrix Cloud Connector](#).

4. If you are using local control, deploy the VM.Standard2.2 and VM.Standard2.8 instances. Install Citrix Storefront on the VM.Standard2.2 instance and install DDC software on the VM.Standard2.8 instance. Consult your Citrix documentation for requirements for connectivity to SCVMM and Hyper-V resources.
5. Select the IP range, as described in the “Common Requirements” section.
6. [Download the Citrix ADC software](#) (formerly Citrix NetScaler) for Hyper-V from the Citrix website.

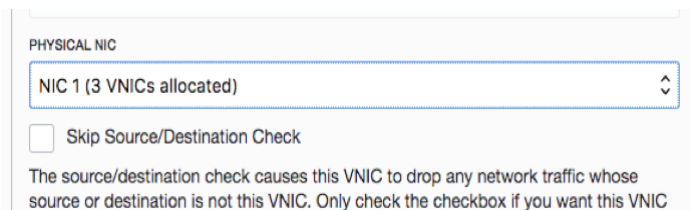
Deploy the Hyper-V Instances

This task has several parts:

- Set Up Networking
- Configure the NVMe Drives as a Single Volume
- Configure Networking on the Bare Metal Instance
- Install the Microsoft KM-TEST Loopback Adapter
- Configure Power Settings
- Configure Roles
- Reconfigure the External VNIC

Set Up Networking

1. If you haven't done so already, provision a BM.DenseIO2.52 bare metal instance.
2. Provision a VNIC for the secondary NIC (NIC 1) on the bare metal instance, preferably in a different subnet than that used for the bare metal instance. For instructions on how to deploy secondary VNICs, see the [Virtual Network Interface Cards \(VNICs\) topic](#) in the Oracle Cloud Infrastructure Networking service documentation.



PHYSICAL NIC

NIC 1 (3 VNICs allocated)

Skip Source/Destination Check

The source/destination check causes this VNIC to drop any network traffic whose source or destination is not this VNIC. Only check the checkbox if you want this VNIC

Do *not* select the **Skip Source/Destination Check** option. This VNIC can be on either a public or private subnet. If this VNIC is on a private subnet, we recommend that you

configure a NAT gateway (see the “Prerequisites” section in the [Deploying Hyper-V on Oracle Cloud Infrastructure](#) white paper).

3. Create secondary VNICs for the secondary NICs. Use one of the following options:
 - If this Hyper-V instance will host a Citrix ADC, create four VNICs. These VNICs will have the following functions:
 - ADC gateway
 - ADC NSIP/SNIP
 - NAT Hyper-V helper instance (hvnat)
 - Traffic forwarder helper instance (hvrouter)
 - If this instance will *not* host a Citrix ADC, create only two VNICs for the following functions:
 - NAT Hyper-V helper instance (hvnat)
 - Traffic forwarder helper instance (hvrouter)

NAME (Optional)
hvnat

VIRTUAL CLOUD NETWORK
c4-vcn1

SUBNET
c4-vcn1-ad3-sn3

PHYSICAL NIC
NIC 1 (3 VNICs allocated)

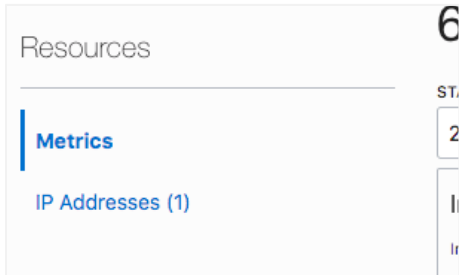
Skip Source/Destination Check
The source/destination check causes this VNIC to drop any network traffic whose

Be sure to *select* the **Skip Source/Destination Check** option for all VNICs created in this step. Record the MAC and private IP addresses, and the VLAN ID of these secondary VNIC.

Note: If you are using the Citrix Virtual Apps and Desktop Service (Citrix Cloud), or are presenting the desktop services via the public internet, the gateway VNIC should be on a public subnet. In the case of using Citrix Cloud, this should be the same public subnet as the Citrix Cloud Connectors. If you are deploying without the Citrix Cloud (that is, using a local Storefront and DDC), the gateway VNIC can be on any subnet that is part of the VCN.

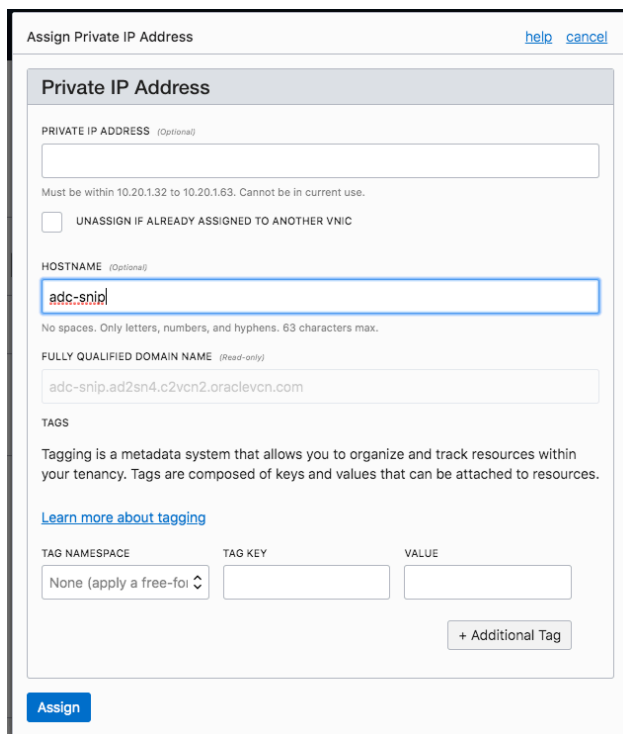
4. Add a secondary IP address to the VNIC designated at the NSIP interface.
 - A. In the Console, select the appropriate VNIC.

- B. Under **Resources**, click **IP Addresses**.



- C. Click **Assign Private IP Address**.

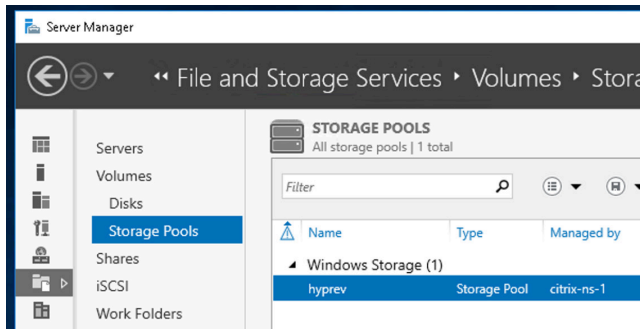
- D. In the dialog box, optionally assign a specific IP address and hostname, or allow the system to generate one or both. Then click **Assign**.



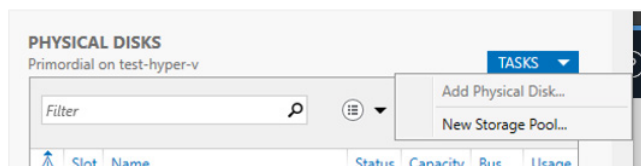
Configure the NVMe Drives as a Single Volume

1. Log in to the bare metal instance using RDP.
2. Open the Server Manager.

3. In the navigation menu, select **File and Storage Services**.
4. Select the **Storage Pools** page.



5. In the **Physical Disks** area, open the **Tasks** menu and select **New Storage Pool**.

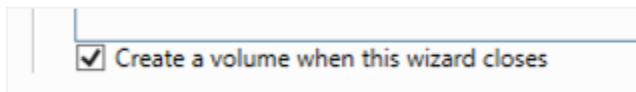


6. Follow the wizard to create the storage pool. On the **Physical Disks** page, select All drives, and change their allocation to **Manual**. Then, click **Next**.

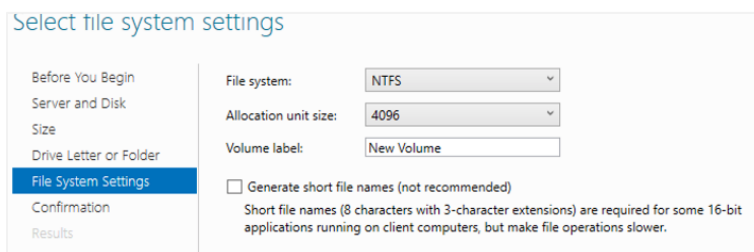
	Allocation	Chassis
DD	Automatic	PCI Slot 900
DD	Automatic	PCI Slot 801
DD	Hot Spare	PCI Slot 306
DD	Manual	PCI Slot 306
DD	Automatic	PCI Slot 302

7. On the next page, click **Create**.
8. When the **Results** page appears, select the **Create a virtual disk when this wizard closes** check box.
9. Select your newly created storage pool, and click **Ok**.
10. In the New Virtual Disk wizard, specify a name for the virtual disk, and then click **Next**.
11. Select all physical disks, and then click **Next**.
12. On the **Storage Layout** page, select **Parity**, and then click **Next**.

13. Select either single or dual parity, depending on your tolerance for risk. A discussion of these options is beyond the scope of this document; however, dual parity provides an extra layer of data protection at the cost of space and some performance.
14. Change the interleave size to **16 KB**. Leave the number of columns to **Auto**.
15. On the **Provisioning** page, keep **Fixed** provisioning set, and then click **Next**.
16. On the **Size** page, select the **Maximum size** option, and then click **Next**.
17. Click **Create**.
18. When the **Results** page is displayed, ensure that the **Create a volume when this wizard closes** check box is selected, and then click **Close**.



19. In the New Volume wizard, ensure that the new virtual disk is selected, and then click **Next**.
20. On the **Size** page, keep the indicated size, and then click **Next**.
21. Assign a drive letter or indicate a mount point folder, depending on preference. Record the location of the volume for future use. Click **Next**.
22. On the **File System Settings** page, change the **Allocation unit size** to **4096** and enter a name for the volume.

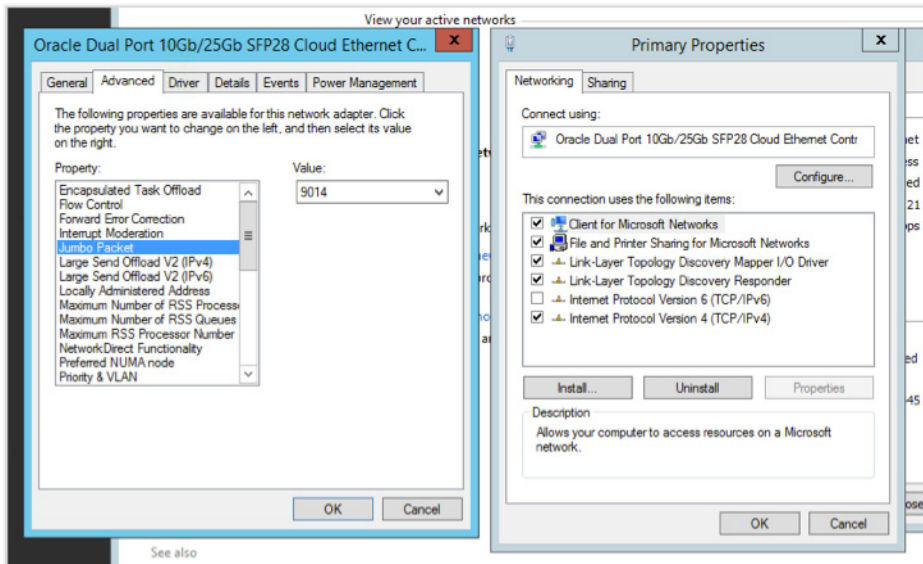


23. On the **Confirmation** page, click **Create**.

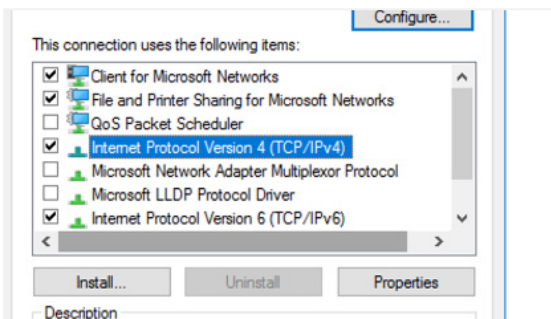
Configure Networking on the Bare Metal Instance

1. Log in to the provisioned Windows bare metal instance.
2. In Windows Firewall, enable ICMP for the bare metal instance. The firewall rule for ICMP is labeled **File and Printer Sharing (Echo Request - ICMPv4-In)**.

3. Open the Network and Shared Center, and click **Change adapter settings**.
4. If the secondary NIC is disabled, enable the NIC.
5. Verify that the MTU for each NIC is set to 9014.
 - A. Access the properties of the network adapter.
 - B. Click **Configure**.
 - C. On the **Advanced** tab, ensure that the value of **Jumbo Packet** is **9014**.



6. On the NIC 0 adapter only, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



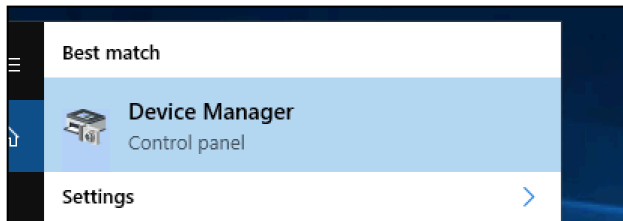
7. Change **Obtain DNS server address automatically** to **Use the following DNS server addresses**. Use the following IP addresses in this order:
 - A. Windows AD DNS server address
 - B. Oracle Cloud Infrastructure local address (169.254.169.254)

Note: We recommend renaming the adapters to something recognizable. This document uses “Base” for NIC0 and “External” for NIC1.

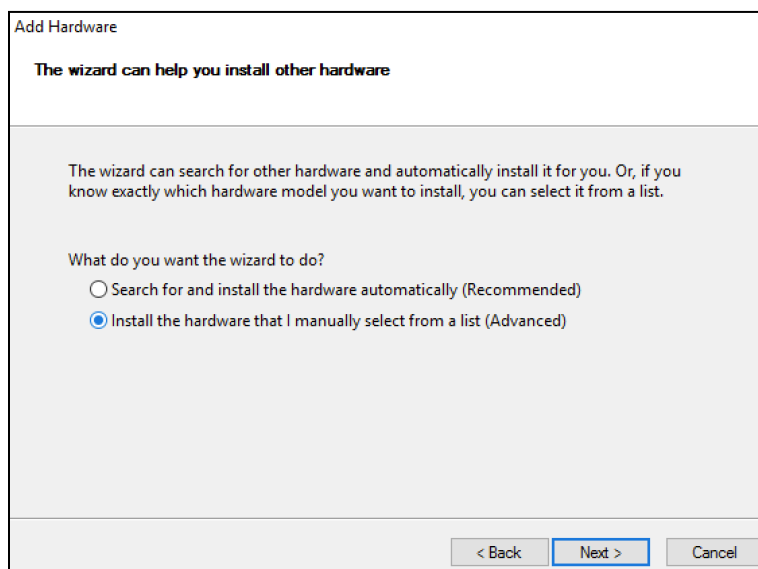
Install the Microsoft KM-TEST Loopback Adapter

The Microsoft KM-TEST Loopback Adapter is a localized loopback network adapter that is used for guest connectivity.

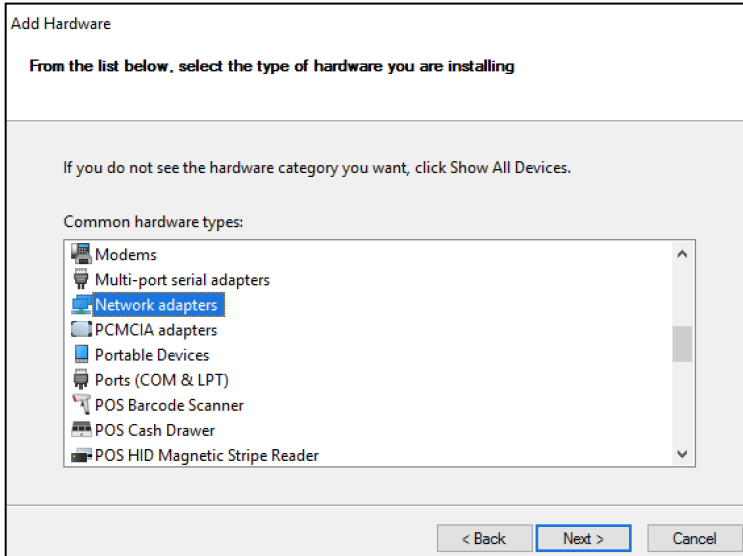
1. Open Device Manager.



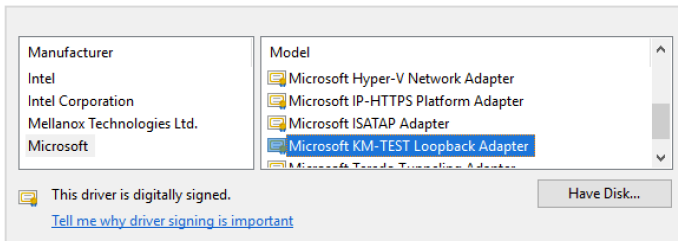
2. Right-click the server (top of the device tree) and select **Add legacy hardware**.
3. In the wizard, select the **Advanced** option.



- In the list of options, select **Network adapters**.

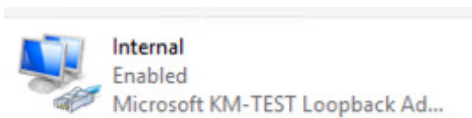


- In the box on the left, select **Microsoft**, and in the box on the right, select **Microsoft KM-TEST Loopback Adapter**.



- Finish the installation wizard.
- Open the Network and Sharing Center, and click **Change adapter settings**.

A new adapter similar to the following one should appear.

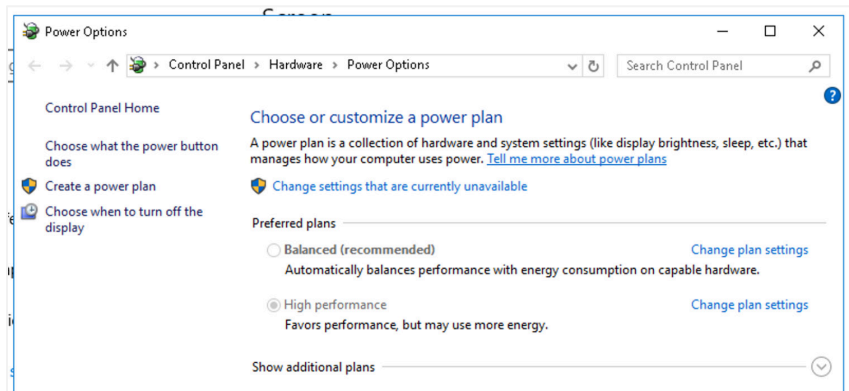


Note: We recommend relabeling this adapter. This paper uses “Internal” to identify this adapter.

8. Configure the loopback adapter with the IP address that you intend to assign for the DNS/DHCP interface in Hyper-V. Don't assign a default gateway or DNS address now. In the process of performing this configuration, you might get a warning that the DNS server list is empty. You can safely ignore it.

Configure Power Settings

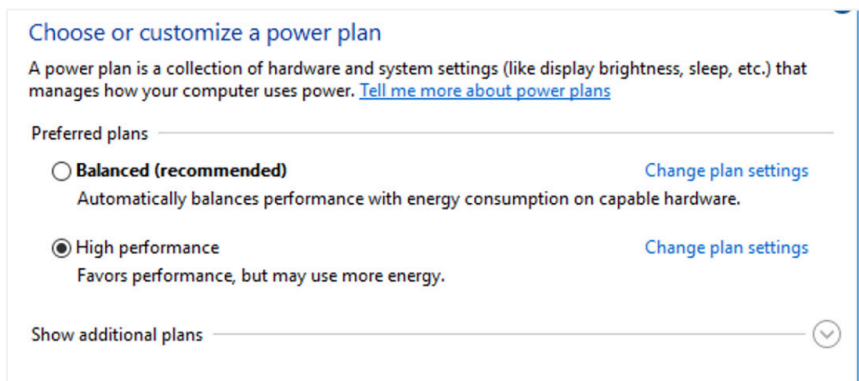
1. Open the Control Panel and navigate to **Hardware > Power Options**.



2. Click **Change settings that are currently unavailable**.

Unavailable options are now available.

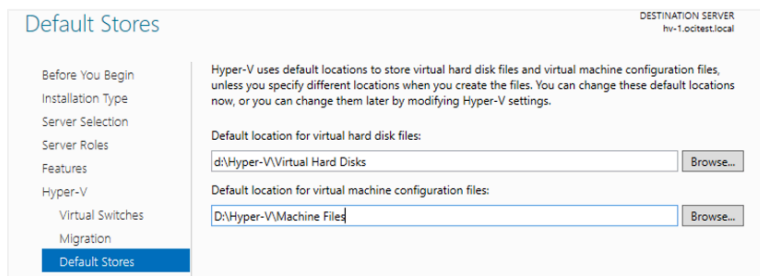
3. Select **High Performance**, if it's not already selected.



4. Close the window.

Configure Roles

1. If the instance is not already joined to the Windows Active Directory domain, join the instance to the domain. Reboot the instance as needed to complete the procedure.
2. Install the following Windows roles and features:
 - DHCP
 - DNS
3. After the roles are installed, click the **Complete DHCP configuration** link in the installation progress status box. Follow the guidance provided by the wizard to authorize DHCP in AD DS. Then, click **Close**.
4. Install the Hyper-V role on the instance. During the role configuration process, follow these steps:
 - A. In the **Virtual Switches** section, select the External and Internal adapters.
 - B. Leave the **Virtual Machine Migration** section as is, and then click **Next**.
 - C. Change the default location for both the virtual hard disk files and the virtual machine configuration files to point to the volume created earlier in this paper. In this example, the **D:** drive was created as the volume. Then, click **Next**.

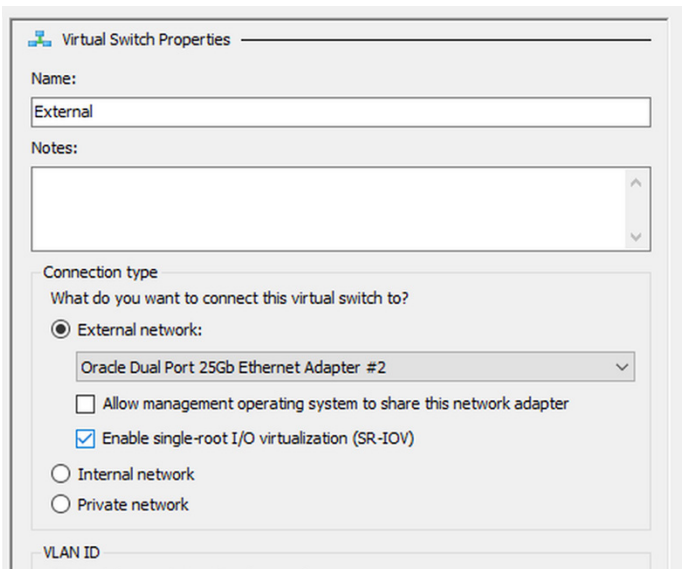


Note: We strongly recommend storing the virtual hard disks and machine files in separate directories.

- D. Click **Install**. Reboot the instance when indicated.

Reconfigure the External VNIC

1. Open the Virtual Switch Manager.
2. Select the switch labeled **Oracle Dual Port 25G Ethernet Adapter #2** and remove this vSwitch.
3. Create a new external vSwitch as follows:
 - A. Name the vSwitch **External**.
 - B. Select **External network**, and then select **Oracle Dual Port 25G Ethernet Adapter #2** from the menu.
 - C. Clear the **Allow management operating system to share this network adapter** check box.
 - D. Select the **Enable single-root IOV virtualization (SR-IOV)** check box.



The screenshot shows the 'Virtual Switch Properties' dialog box. The 'Name' field is set to 'External'. The 'Notes' field is empty. Under 'Connection type', the 'External network' radio button is selected. The dropdown menu for the external network is set to 'Oracle Dual Port 25Gb Ethernet Adapter #2'. The 'Allow management operating system to share this network adapter' checkbox is unchecked, and the 'Enable single-root I/O virtualization (SR-IOV)' checkbox is checked. The 'Internal network' and 'Private network' radio buttons are unselected. The 'VLAN ID' field is partially visible at the bottom.

4. Select the vSwitch named **Microsoft KM-TEST Loopback Adapter**. Rename this vSwitch to **Internal**. Ensure that the **External network** and the **Allow management operating system to share this network adapter** options are selected.

Virtual Switch Properties

Name:
Internal

Notes:

Connection type
What do you want to connect this virtual switch to?

External network:
Microsoft KM-TEST Loopback Adapter
 Allow management operating system to share this network adapter
 Enable single-root I/O virtualization (SR-IOV)

Internal network
 Private network

VLAN ID
 Enable virtual LAN identification for management operating system
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2

Remove

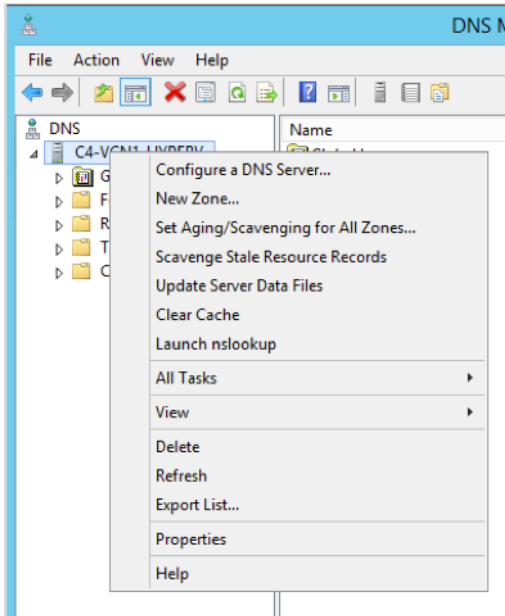
i SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

OK Cancel Apply

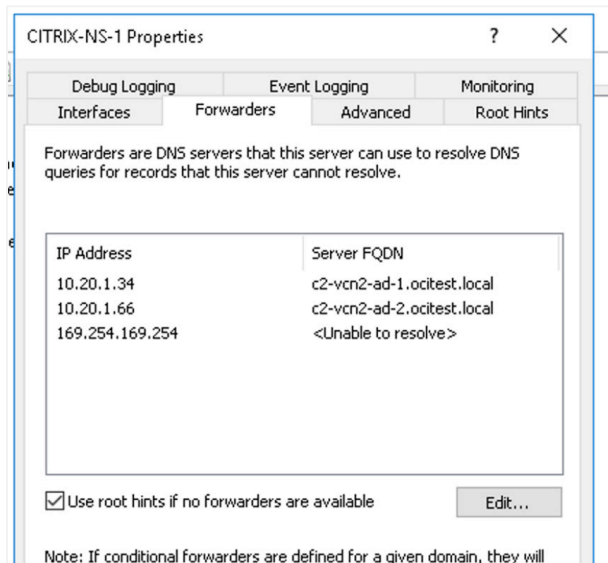
5. In the Network and Sharing Center, right-click the **vEthernet (Internal)** and select **Properties**.
6. Select the option for **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
7. Enter in the IP address and netmask selected for the DHCP/DNS portion of the internal Hyper-V network. In the process of performing this configuration, you might get a warning that the DNS server list is empty. You can safely ignore it.

Configure DNS and DHCP for the Hyper-V Guests

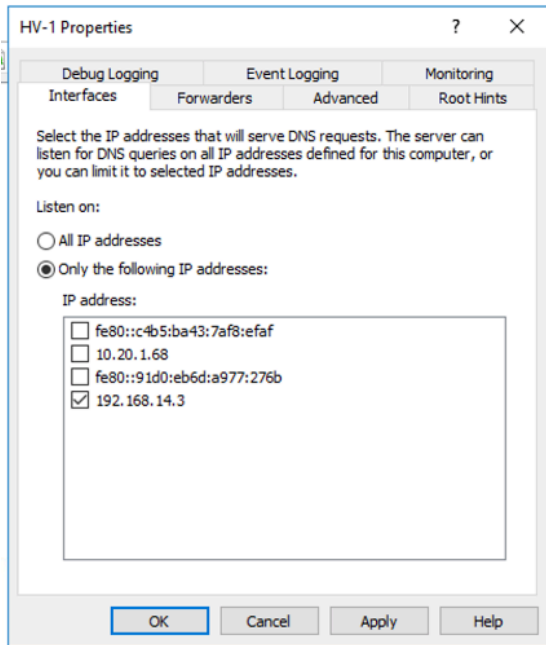
1. Open the DNS management application, right-click the server, and select **Properties**.



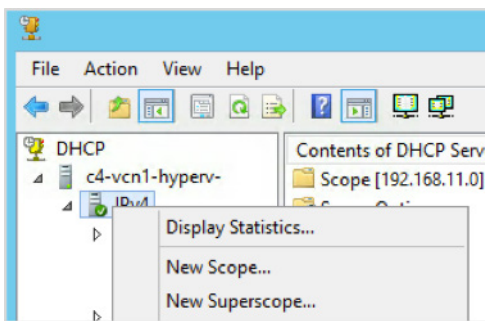
2. On the **Forwarders** tab, click **Edit** and create an entry for 169.254.169.254 and for the IP address of the Windows AD DNS server. The FQDN for the 169.254 address won't resolve, which is a normal condition. Ensure that the IP address for the Windows AD DNS server is listed first.



3. On the **Interfaces** tab, select **Only the following IP addresses**, and then clear the check boxes for all interfaces *except* the IP address associated with the internal Hyper-V network.

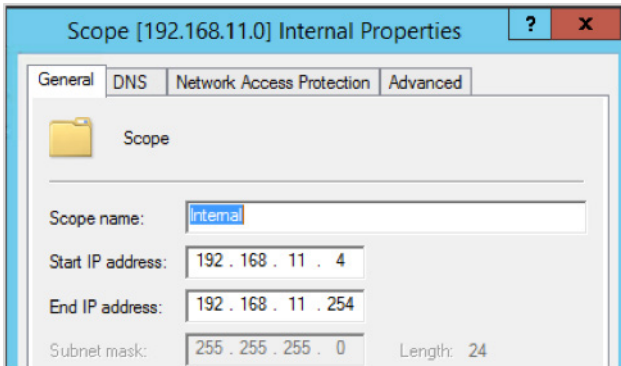


4. Save the configuration and restart DNS.
5. Open the DHCP management application.
6. Expand the server, right-click **IPv4**, and select **New Scope**.

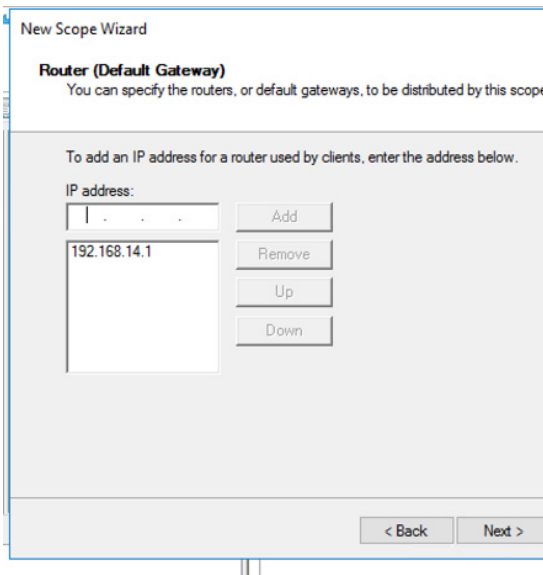


7. Create the scope by using the IP address range selected for the Hyper-V internal network.
 - A. Enter a descriptive name for the scope.
 - B. Start with the address that immediately follows the ones identified in the prerequisites that you are using for this Citrix server. For Hyper-V instances with an ADC, this

address is typically the fifth address from the beginning of the subnet. For non-ADC Hyper-V instances, it is typically the fourth address.

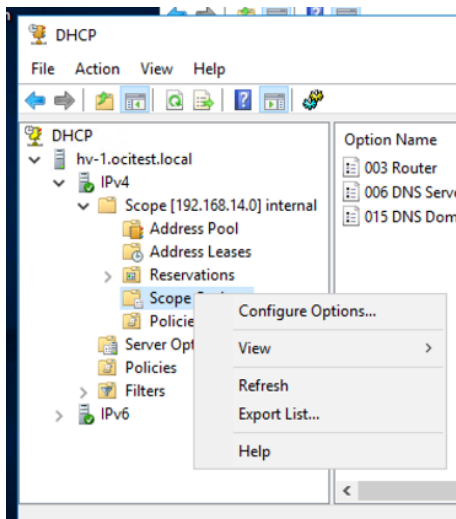


- C. Keep the default values on the **Exclusions and Delay** page and the **Lease Duration** page.
- D. Select to configure the DHCP options.
- E. On the **Router (Default Gateway)** page, specify the address identified for the NAT Hyper-V helper instance (hvnat).



- F. Keep the default values on the **Domain Name and DNS Servers** page and the **WINS Servers** page.
- G. Activate the scope.

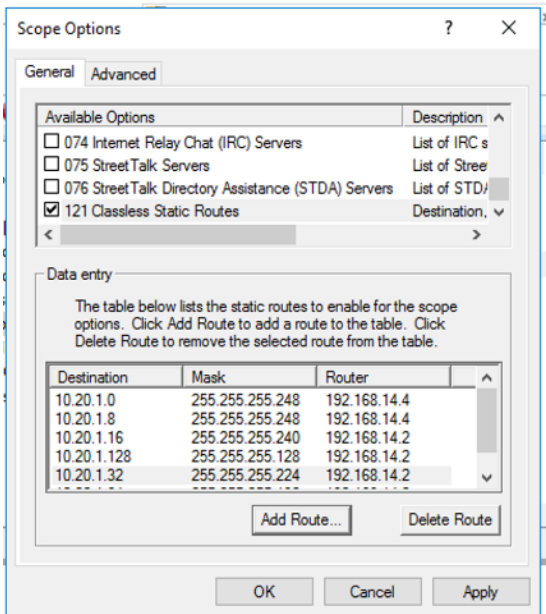
- Expand the scope in the left navigation pane and verify that the Router, DNS Server, and DNS Domain values are set as you configured them. Then, right-click the **Scope Options** folder and select **Configure Options**.



- Scroll down to **121 Classless Static Routes** and select the check box.

The entries in the route table depend on whether this Hyper-V server contains a Citrix ADC:

- For Hyper-V hosts that contain an ADC, the route table should have an entry that directs traffic to the Oracle Cloud Infrastructure subnet with the ADC Gateway VNIC, via the internal address (SNIP) of the Citrix ADC. For instance, if the Hyper-V internal network is 192.168.10.0/24 with the ADC internal interface using 192.168.10.4 as its IP address, the ADC Gateway VNIC is on the 10.20.10.0/24 subnet. You would need to establish an explicit route to 10.20.10.0/24 via 192.168.10.4.
- Hyper-V hosts that contain an ADC should have an entry per VCN subnet (other than the one used for the ADC Gateway) that routes traffic through the address assigned to the Traffic Forwarding helper guest (hvrouter).
- Hyper-V hosts that don't have an ADC should have a single entry that routes traffic to the entire VCN via the Traffic Forwarding helper guest (hvrouter).



Create Hyper-V Helper Guests

This section describes the process to create the helper guests required for Hyper-V to work within Oracle Cloud Infrastructure. These guests can be either Windows 2012 R2 or Windows 2016, depending on your requirements.

Windows Automatic Virtual Machine Activation

The Windows guests listed in the following table can participate in the Automatic Virtual Machine Activation (AVMA) process, which lets guests be installed in the Windows 2016 Datacenter Hyper-V role and still be licensed. Linux and other operating systems don't require Windows licenses to run. Windows Desktop licenses aren't covered in this configuration.

Operating System Version	AVMA Key
Windows Server 2012 R2 Essentials	K2XGM-NMBT3-2R6Q8-WF2FK-P36R2
Windows Server 2012 R2 Standard	DBGBW-NPF86-BJVTX-K3WKJ-MTB6V
Windows Server 2012 R2 Datacenter	Y4TGP-NPTV9-HTC2H-7MGQ3-DV4TW
Windows Server 2016 Essentials	B4YNW-62DX9-W8V6M-82649-MHBKQ
Windows Server 2016 Standard	C3RCX-M6NRP-6CXC9-TW2F2-4RHYD

These keys are publicly available and valid for all installations of these operating systems under Hyper-V.

Activate guests by performing the following steps on each guest:

1. Launch an administrative command prompt.
2. Type the following command:

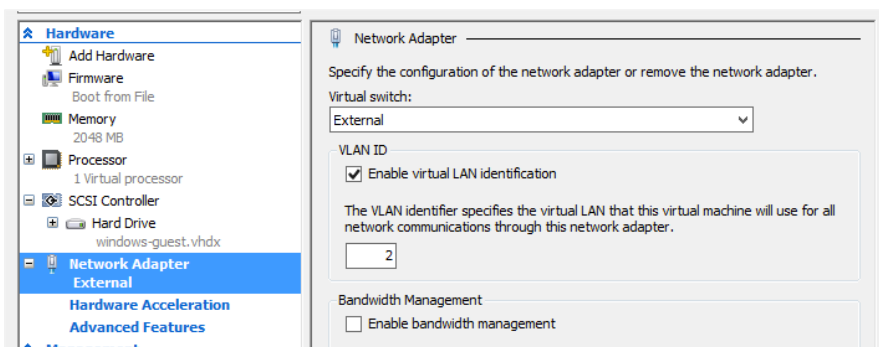
```
slmgr /ipk <AVMA_key>
```

3. Close the command prompt.

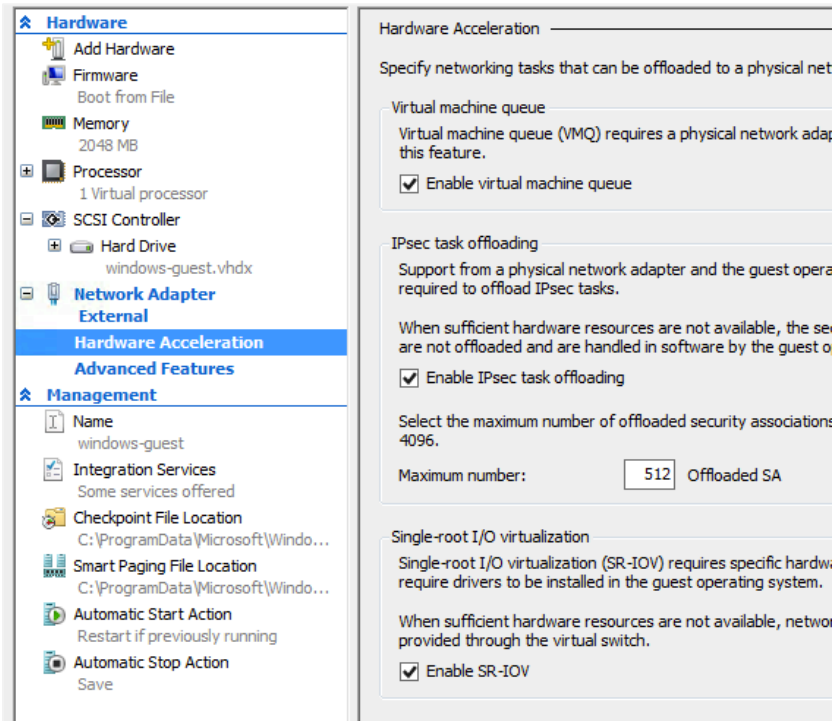
For details about AVMA, see the [Hyper-V Automatic Virtual Machine Activation in Windows Server 2016](#) blog post at altaro.com.

Create the Base Helper Guests

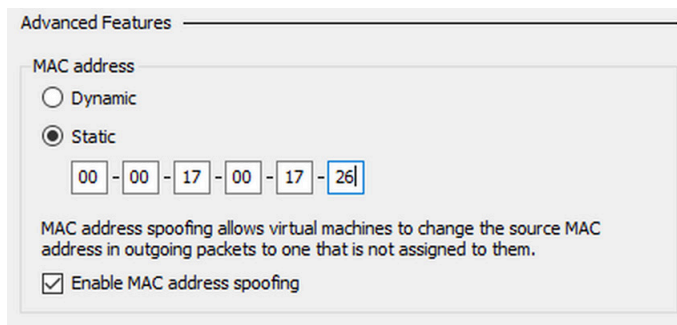
1. Open Hyper-V Manager and create two new VMs, one named **hvnat** and one named **hvrouter**. Define the following characteristics for the VMs:
 - Generation 2 VM
 - Minimum memory of 4196 MB (dynamic memory)
 - Network connection to the external vSwitch
 - 100G of space for the VHDX, on the block storage device (typically the **D:** drive)
2. After the hvnat VM is created, select the VM and select **Settings**.
3. Get the information for the NAT helper (hvnat) VNIC, and then perform the following steps in the **Settings** dialog box:
 - A. In the left navigation pane, select **Network Adapter External**.
 - B. Select the **Enable virtual LAN identification** check box.
 - C. Enter the VLAN ID of the secondary VNIC.



- D. In the left navigation pane, select **Hardware Acceleration** (under **Network Adapter External**), and then select the **Enable SR-IOV** check box.



- E. In the left navigation pane, click **Advanced Features** (under **Network Adapter External**). In the **MAC Address** section on the right, select the **Static** option, and then enter the MAC address associated with the secondary vNIC being used. Select the **Enable MAC address spoofing** check box.



- F. In the left navigation pane, select **Add Hardware** and then select **Network Adapter**.
- G. Add an internal network adapter, keeping all the default settings.
- H. Save the configuration.

- I. Repeat the preceding steps for the hvrouter VM, except selecting the information for the Traffic Forwarder (hvrouter) VNIC.

Install and Configure Windows for the hvnat and hvrouter Hyper-V Guests

Install Windows 2012 R2 on both the hvnat VM and the hvrouter VM, and then perform the following steps on each guest:

1. Identify the interface associated with the secondary VNIC, by looking at the MAC address of the virtual NIC in the instance.
2. Configure the IP address, subnet mask, and default gateway of the secondary VNIC with the information identified for the particular instance.
3. Configure the second interface with the IP address selected for the function.
 - The hvnat guest should *not* be the route target for the VCN and should get the Hyper-V address associated with the default gateway/NAT.
 - The hvrouter guest should have the secondary VNIC associated with the route target address and should get the Hyper-V address associated with the VCN gateway/router.
 - The interface with the Hyper-V address should *not* get a default gateway configured, but should have the DNS address assigned. The DNS address should be the internal address associated with the DNS/DHCP function for Hyper-V.
4. Verify that each instance can ping the subnet default gateway on the VCN and the internal DNS/DHCP address, and can get to the internet.
5. Apply all current Windows patches to the operating system.

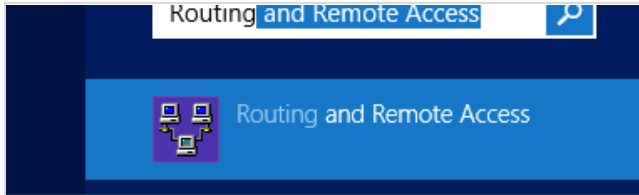
Configure the hvnat Guest

Before performing these steps, ensure that all networking on the hvnat guest has been configured and is functional. Tests of the network should include being able to communicate with both instances on the VCN side of the hvnat guest and network targets on the internal Hyper-V side. A simple ping test should suffice.

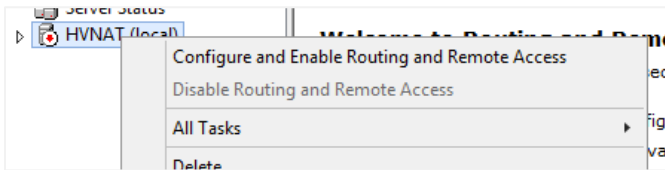
1. On the hvnat instance, install the Routing and Remote Access service (RRAS), routing only. Perform this step by using the following PowerShell command, run as Administrator:

```
Install-WindowsFeature -Name "Routing" -IncludeSubFeature -  
IncludeManagementTools -Confirm:$false
```

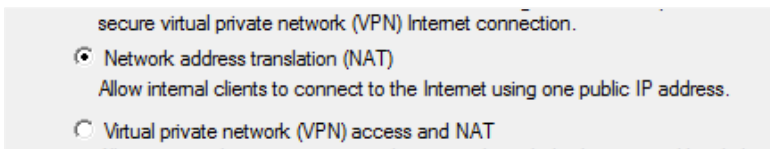
2. Open the Routing and Remote Access tool.



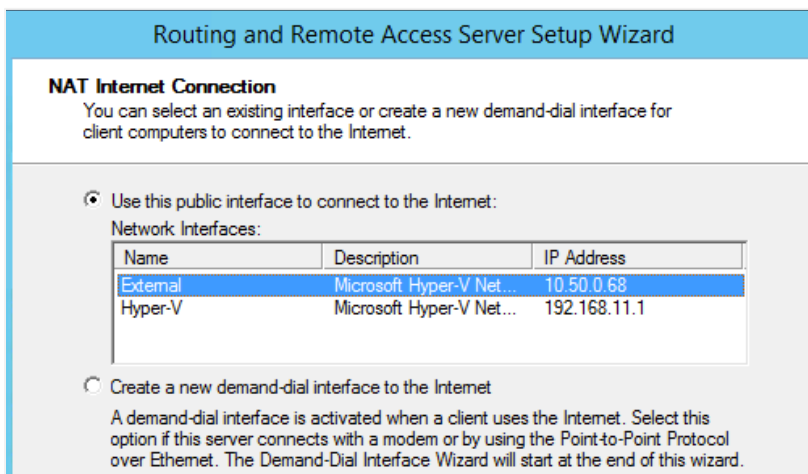
3. Right-click the server and select **Configure and Enable Routing and Remote Access**.



4. On the welcome page of the wizard, click **Next**.
5. On the **Configuration** page, select **Network address translation (NAT)**, and then click **Next**.



6. On the **NAT Internet Connection** page, select the interface that has the VCN IP address for the internet-facing interface, and then click **Next**.



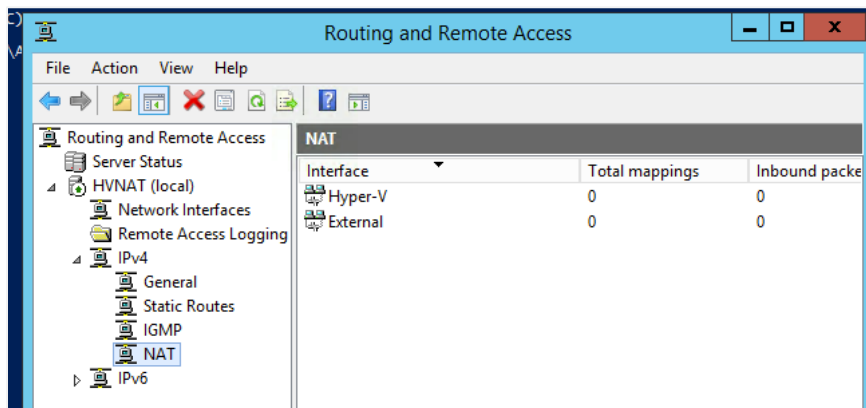
7. Click **Finish**. If you get a warning that the service is unable to open ports for Routing and Remote Access in Windows Firewall service, you can ignore it and click **OK**.

A dialog box is displayed, indicating that the configuration is being initialized.

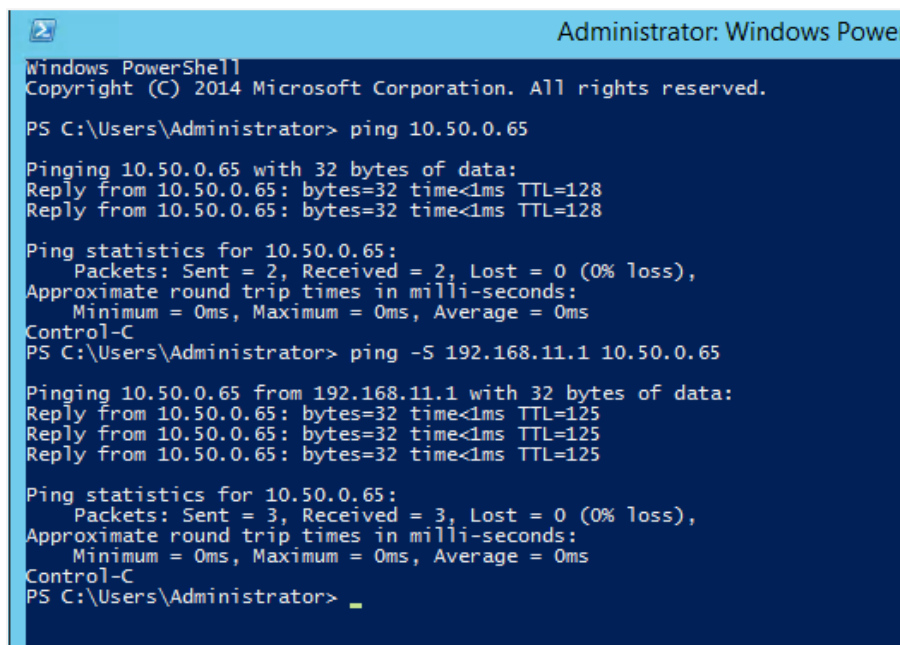
This process might stop responding. If the dialog box does not disappear after 10 or so minutes, restart the instance.

8. In the Routing and Remote Access tool, expand the server and click **NAT**.

The right side of the window should display entries similar to the following ones:



9. Verify that you can still ping the VCN subnet default gateway via the Hyper-V address. In the following example, the VCN gateway is 10.50.0.65 and the Hyper-V address for hvnat is 192.168.11.1. You can open a PowerShell window to issue the commands.



The `ping -S` command sends the ping from the designated interface.

Configure the hvrouter Guest

Before performing these steps, ensure that all networking on the hvrouter guest has been configured and is functional. Tests of the network should include being able to communicate with both instances on the VCN side of the hvrouter guest and network targets on the internal Hyper-V side. A simple ping test should suffice.

1. Log in to the hvrouter instance.
2. Open a PowerShell window as Administrator.
3. Identify the interface index numbers by running the following command:

```
Get-NetAdapter
```

4. Note the `ifIndex` numbers for each of the Hyper-V interfaces.
5. Configure forwarding on each interface by running the following command for each interface number identified:

```
Set-NetIPInterface -InterfaceIndex <ifIndex_number> -Forwarding Enabled
```


6. Test to ensure that you can ping the Hyper-V interface from an instance on the VCN subnet.

Add Routes to VCN Route Tables

For Citrix Virtual Apps and Desktops to access Oracle Cloud Infrastructure services and communicate with outside targets, the route tables of the VCN must include information about the internal networks created within the Hyper-V instances. Perform the following steps for each Hyper-V instance deployed:

1. Open the route table of the VCN where the Hyper-V server is being configured, and add a route rule. Enter the private IP address that you just selected as the route target for the IP address range selected for the Hyper-V deployment.

For example, 192.168.11.0/24 was selected as the address space for Hyper-V. A secondary VNIC on the Hyper-V server was selected with an IP address of 10.50.0.69. The resulting route table entry would look as follows:

DESTINATION CIDR BLOCK	TARGET TYPE	TARGET SELECTION	
192.168.11.0/24	Private IP	10.50.0.69	
		OCID: ...2qgn4a	

For information about managing route tables, see the [Route Tables topic](#) in the Networking service documentation.

2. Open the security list for the subnet. If you have configured a global security list for the VCN, consider using that security list instead.
3. Add an entry that allows traffic from the Hyper-V internal network to be accepted by instances within the VCN. For example, if the VCN has a global security list that covers the entire VCN, the entry added to the global security list would look as follows:



The screenshot shows a configuration interface for a security list entry. On the left, there is a red 'X' icon and a checked checkbox. The entry name is 'STATELESS'. Below the name is a link '(more information)' and the text 'Allows all traffic for all ports'. To the right, there are two input fields: 'SOURCE CIDR' with the value '192.168.11.0/24' and 'IP PROTOCOL' with a dropdown menu set to 'All Protocols'. Below the 'IP PROTOCOL' dropdown is another link '(more information)'.

For information about how to manage and update security lists, see the [Security Lists topic](#) in the Networking service documentation.

Add Hyper-V Hosts to SCVMM

After all Hyper-V hosts are configured to this point, add them to SCVMM. Before adding the hosts, ensure that the following prerequisites are completed.

Note: This section does *not* provide a comprehensive list of the steps needed to configure or use SCVMM. For a complete description of planning, installing, and configuring SCVMM, we *strongly* recommend that you consult [System requirements for System Center Virtual Machine Manager](#).

- Ensure that the security lists on the subnets that host the *primary NIC* for the Hyper-V hosts and the SCVMM instance have at least the following ports configured for use on the subnets:
 - TCP ports 22, 80, 135, 139, 443, 445, 2179, 5985, 5986, 8100, 8101, 8102, 8103
 - If you are running a separate SQL Server instance, TCP 1433 is also required between the SCVMM instance and the target SQL Server instance.

For more information about the port configuration for SCVMM, see [Identify VMM ports and protocols](#) in the Microsoft documentation.

- The Hyper-V host needs to have the Windows Firewall configured to allow the following applications for all network types (Domain, Private, Public):
 - File and Printer Sharing
 - Hyper-V
 - Hyper-V Management Clients

- Hyper-V Replica HTTP/HTTPS
- Windows Remote Management (normal and compatibility)
- Virtual Machine Monitoring
- WinRM HTTPS
- Ensure that the PowerShell remote execution is enabled by running the following commands *as Administrator* in a PowerShell session on each Hyper-V host:

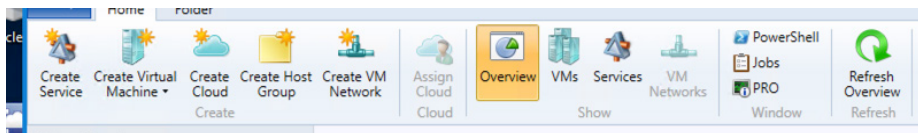
```
winrm quickconfig
```

```
Enable-PSRemoting -Force
```

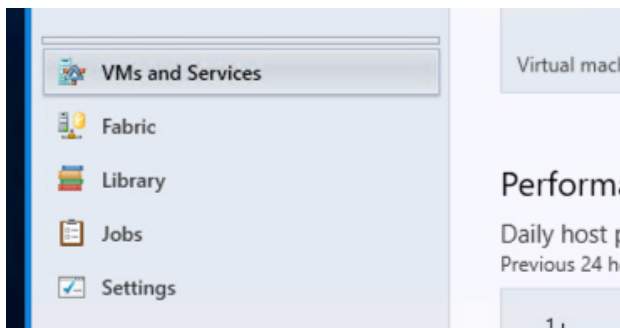
- Create two service accounts in Active Directory for SCVMM. One is an operational account, and the other is a RunAs account.

After all the preceding items are complete, following these steps to add the Hyper-V hosts to SCVMM.

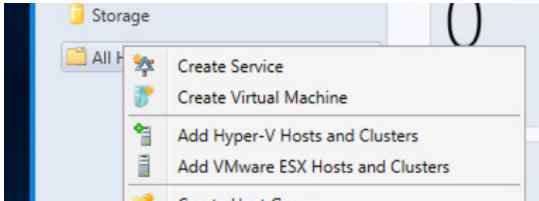
1. Connect to the SCVMM Management Console either by using RDP to the SCVMM instance or by using the console remotely.
2. On the **Home** tab at the top of the window, click **Overview**.



3. In the bottom-left navigation pane, click **VMs and Services**.



4. In the upper-left navigation pane, right-click **All Hosts** and select **Add Hyper-V hosts and Clusters**.



5. Follow the wizard to add the Hyper-V hosts to the **All Hosts** host group.

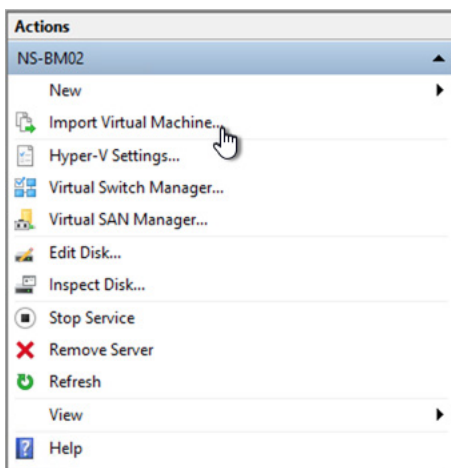
Monitor the **Add virtual machine host** jobs to ensure completion and correct any problems before continuing.

Install and Configure the Citrix ADC Instance

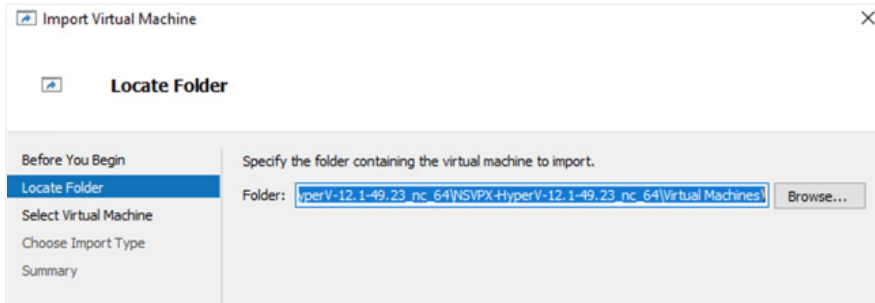
This process applies only for single or dual Citrix ADC architectures, and for Hyper-V instances that will contain an ADC. If you're performing a Storefront Only implementation, or if the Hyper-V instance won't contain an ADC, skip this section.

Installing the Citrix ADC Instance in Hyper-V

1. Copy the Citrix ADC image to the Hyper-V server. Unpack the file to the previously configured NVMe storage.
2. Import the image to Hyper-V.
 - A. Open Hyper-V Manager.
 - B. In the **Actions** pane, select **Import Virtual Machine**.



- C. On the **Locate Folder** page of the Import Virtual machine wizard, select the folder that contains the Citrix ADC download, and then click **Next**.

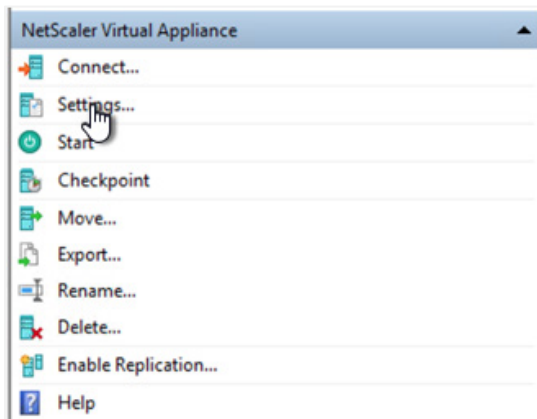


- D. On the **Select Virtual Machine** page, select **NetScaler Virtual Appliance**, and then click **Next**.
- E. On the **Choose Import Type** page, select **Register the virtual machine in-place (use the existing unique ID)**. Then, click **Next** and **Finish**.

The Citrix ADC should be imported. Don't start the virtual machine at this point. If it starts automatically, stop the virtual machine before continuing.

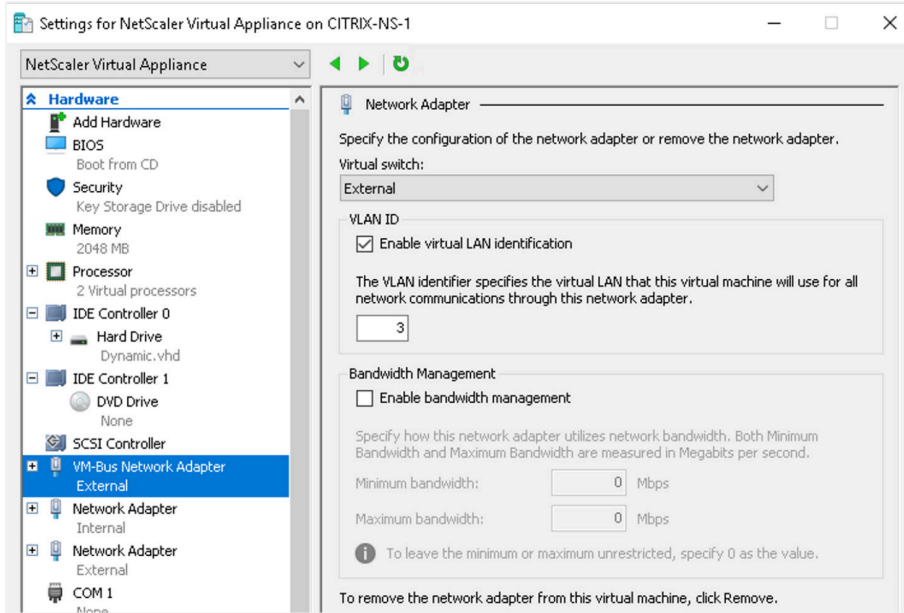
Configuring the Citrix ADC with Oracle Cloud Infrastructure VNICs

1. In Hyper-V Manager, select the **NetScaler Virtual Appliance** guest.
2. In the bottom section of the **Actions** pane, click **Settings**.

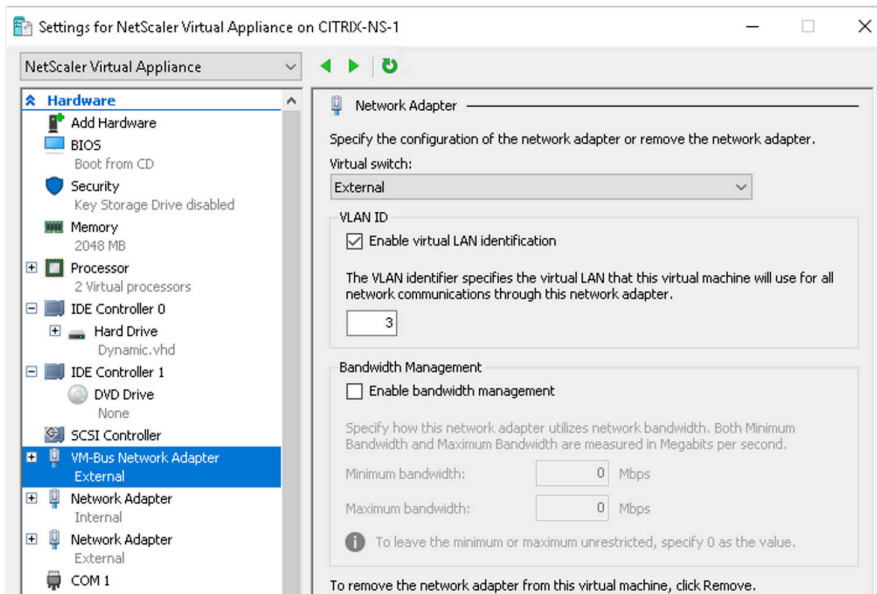


3. In the **Settings** dialog box, select the existing **VM-Bus Network Adapter**. Using the information from the VNIC selected as the NSIP as part of the provisioning process of the bare metal instance, modify the virtual adapter as follows:

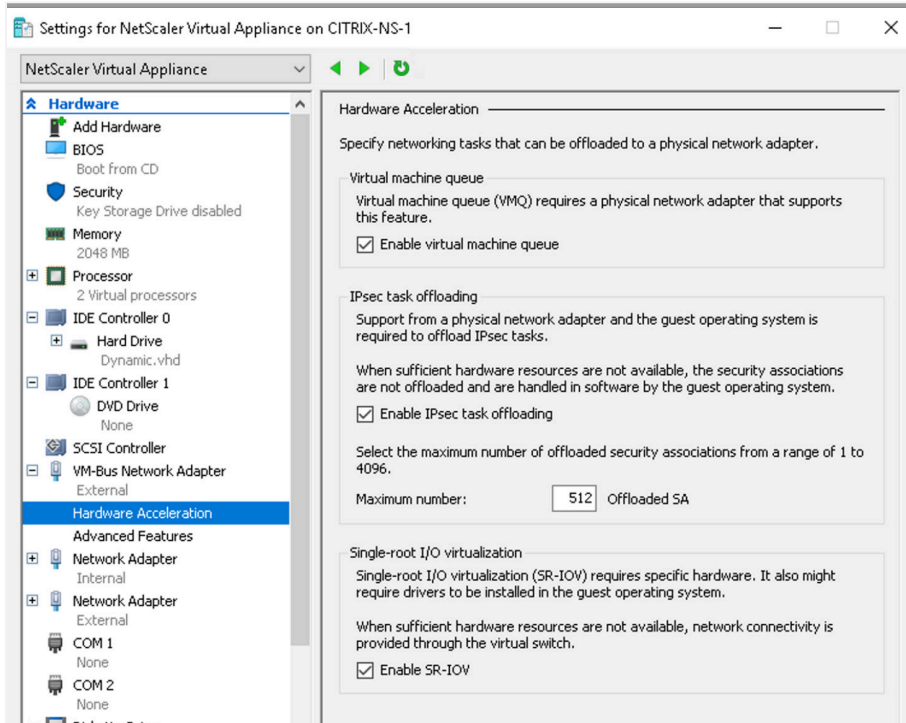
A. Change the **Virtual switch** value to **External**.



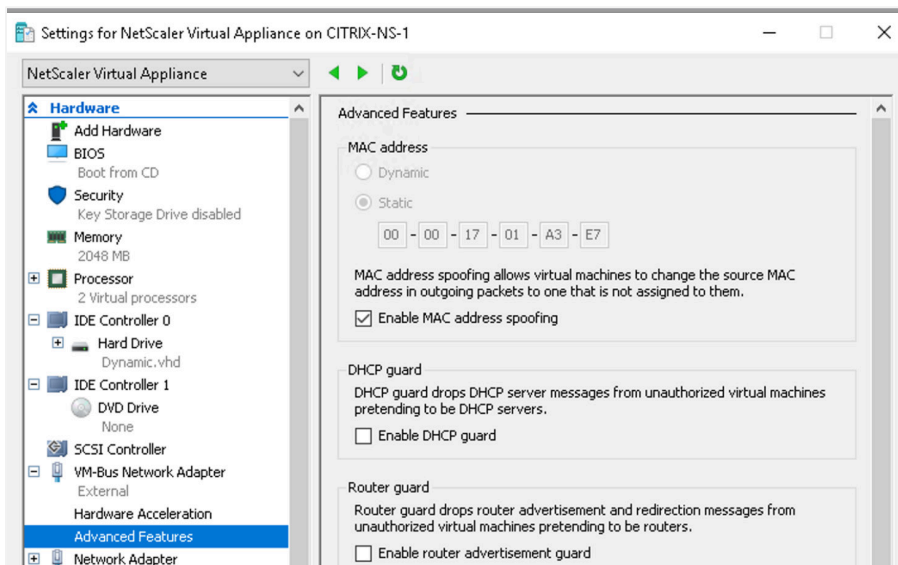
B. Select the **Enable virtual LAN identification** check box, and enter the VLAN tag from the VNIC being used to configure the network interface



- C. Expand the settings for the network interface by clicking the + sign next to the adapter and then select **Hardware Acceleration**. Then, select the **Enable SR-IOV** check box.



- D. Click **Advanced Features**. In the **MAC address** box, select **Static** and enter the MAC address of the VNIC being used to configure this interface. Select the **Enable MAC address spoofing** check box.

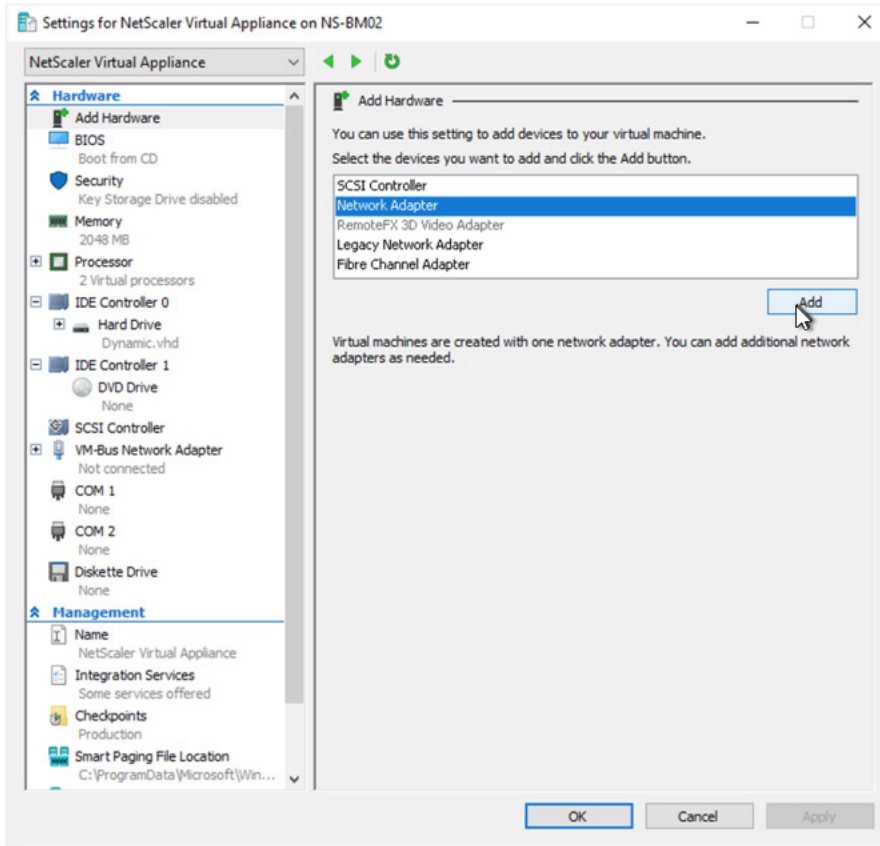


E. Click **Apply** to save the configuration.

4. Using the information from the VNICs created for the ADC Gateway interface, and as part of the provisioning process of the Oracle Cloud Infrastructure bare metal instance, create another network adapter by using the following steps:

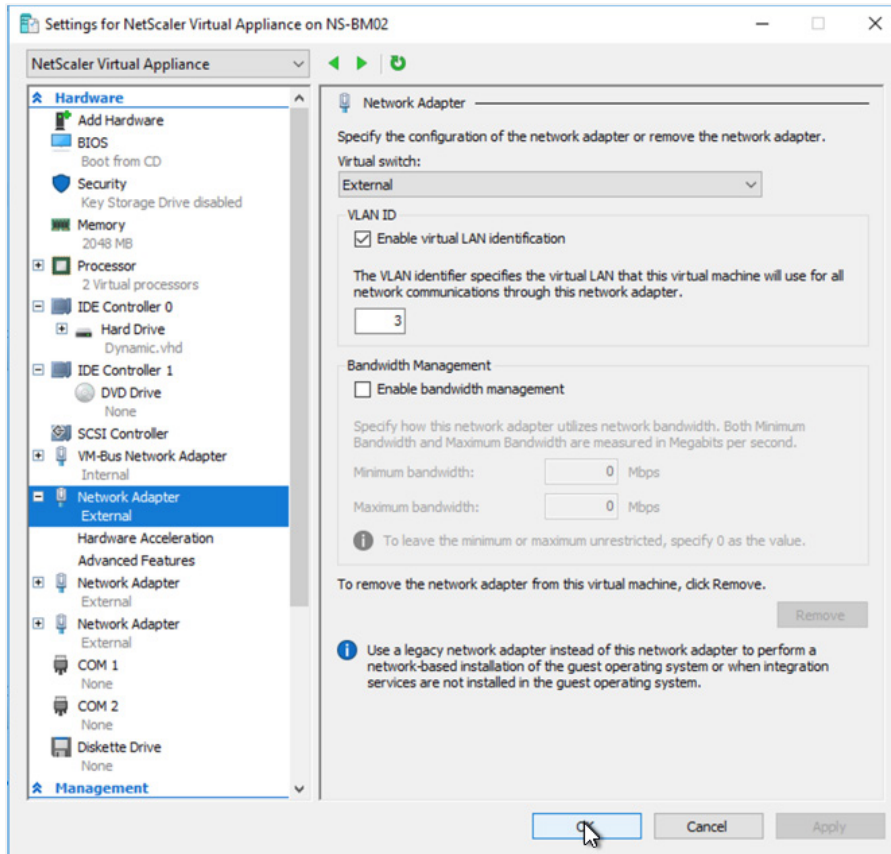
A. At the top of the **Settings** dialog box, click **Add Hardware**.

B. Select **Network Adapter**, and click **Add**.

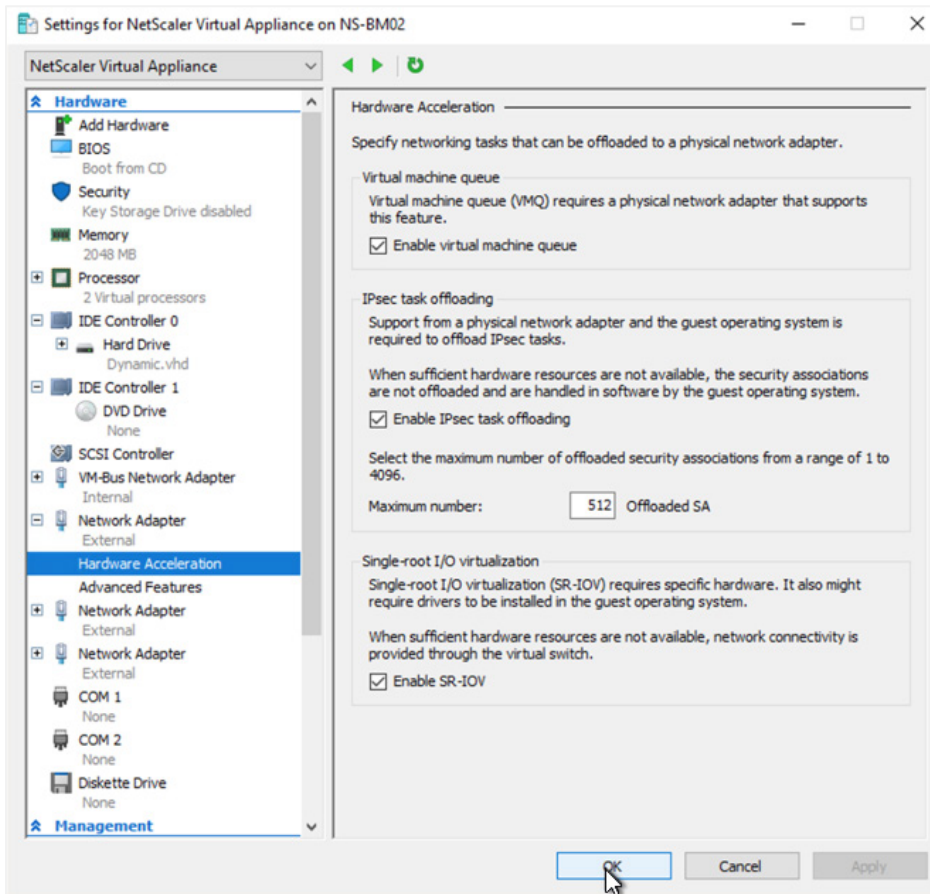


C. Select the new network adapter, and change the **Virtual switch** value to **External**.

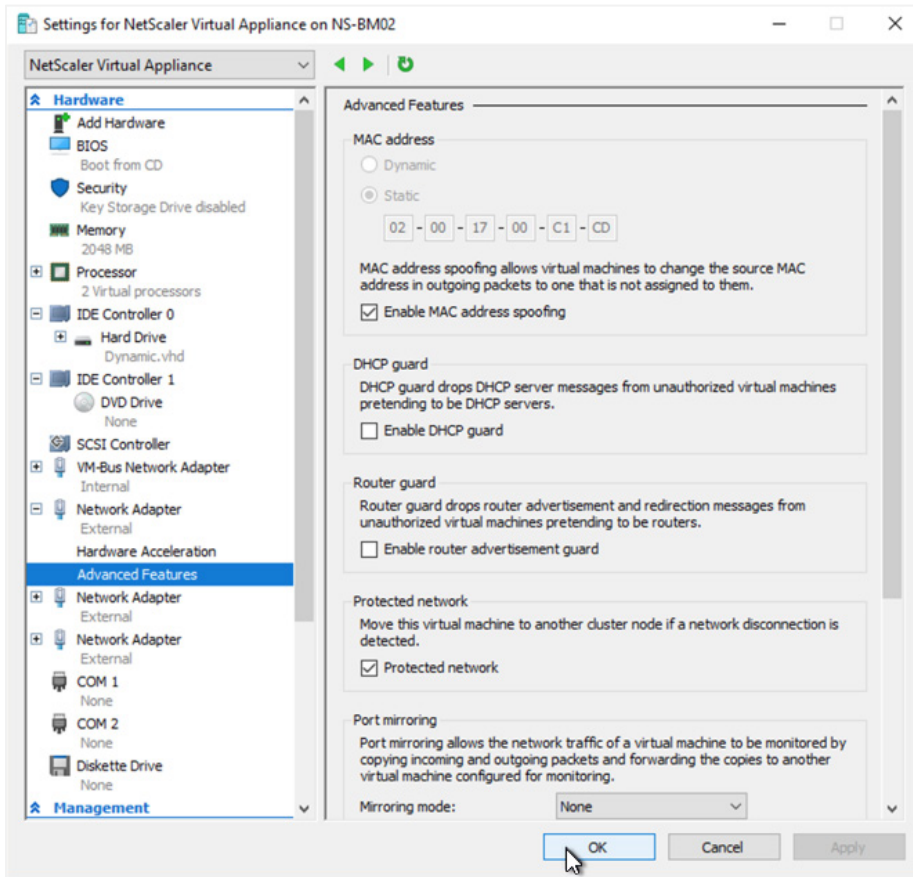
- D. Select the **Enable virtual LAN identification** check box, and enter the VLAN tag from the VNIC being used to configure the network interface



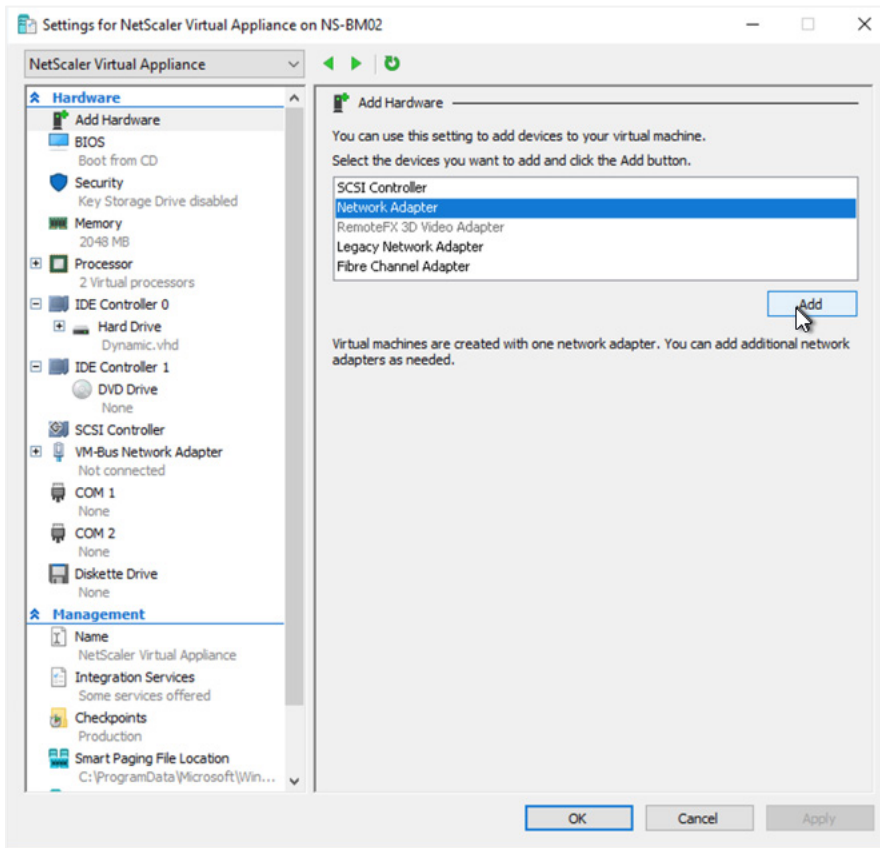
- E. Expand the settings on the network interface by clicking the + sign next to the adapter and then select **Hardware Acceleration**. Then, select the **Enable SR-IOV** check box.



- F. Select **Advanced Features**. In the **MAC address** box, select **Static** and enter the MAC address of the VNIC being used to configure this interface. Select the **Enable MAC address spoofing** check box.



- G. Click **Apply** to save the configuration.
5. Add the internal SNIP adapter to the Citrix ADC
- A. If the **Settings** dialog closed during the previous process, reopen the dialog box.
- B. Click **Add Hardware** at the top of the box.
- C. Select **Network Adapter**, and click **Add**.



- D. Select the new network adapter, and change the **Virtual switch** value to **Internal**.
- E. Keep all the default settings, and click **OK**.

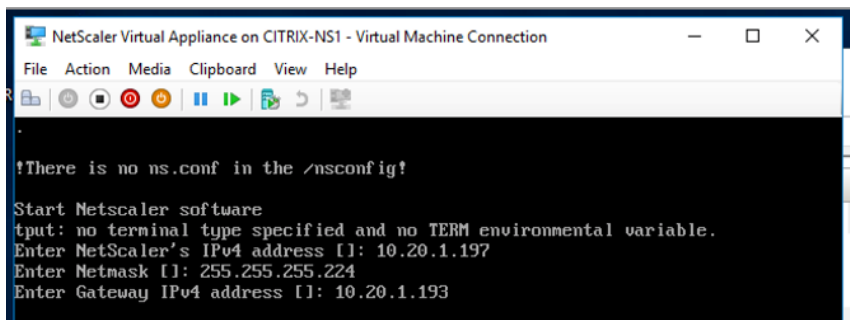
Configure the Citrix ADC

1. After all the networking is completed, start the Citrix ADC instance in Hyper-V Manager. Connect to the console of the instance.

The console should show the initial configuration screen for the Citrix ADC. The prompt on the console asks for the NetScaler's IPv4 address.

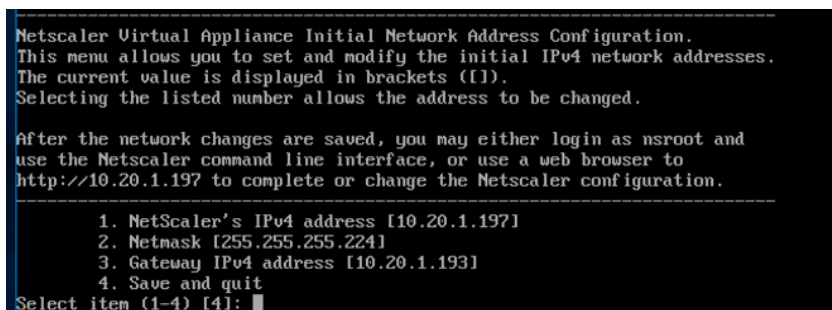
2. At the console prompts, enter the following information:

- **NetScaler's IPv4 address:** IP address of the Citrix ADC NSIP VNIC
- **Netmask:** Netmask of the subnet for the NSIP VNIC
- **Gateway IPv4 address:** Gateway address of the subnet, typically the first address in the CIDR range



```
NetScaler Virtual Appliance on CITRIX-NS1 - Virtual Machine Connection
File Action Media Clipboard View Help
!There is no ns.conf in the /nsconfig!
Start Netscaler software
tput: no terminal type specified and no TERM environmental variable.
Enter NetScaler's IPv4 address [ ]: 10.20.1.197
Enter Netmask [ ]: 255.255.255.224
Enter Gateway IPv4 address [ ]: 10.20.1.193
```

3. Verify that all information is correct, and then press **Return**.



```
-----
Netscaler Virtual Appliance Initial Network Address Configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ( []).
Selecting the listed number allows the address to be changed.

After the network changes are saved, you may either login as nsroot and
use the Netscaler command line interface, or use a web browser to
http://10.20.1.197 to complete or change the Netscaler configuration.
-----
 1. NetScaler's IPv4 address [10.20.1.197]
 2. Netmask [255.255.255.224]
 3. Gateway IPv4 address [10.20.1.193]
 4. Save and quit
Select item (1-4) [4]:
```

4. Wait for the boot sequence to complete, and then open a browser to the NSIP IP address. Because the NSIP is typically on a private subnet, you will likely have performed this step from an instance inside the VCN.

5. Log in to the Citrix ADC with the default credentials, as provided by Citrix.

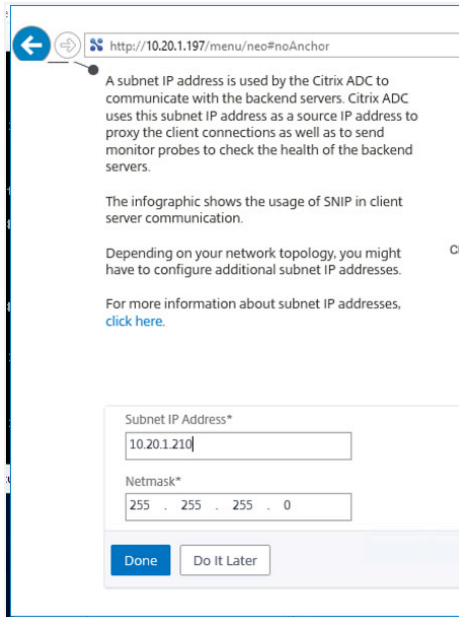
6. Click the **Configuration** tab.

7. Click the **Subnet IP Address** option.

8. In the **Subnet IP Address** box, perform the following steps:

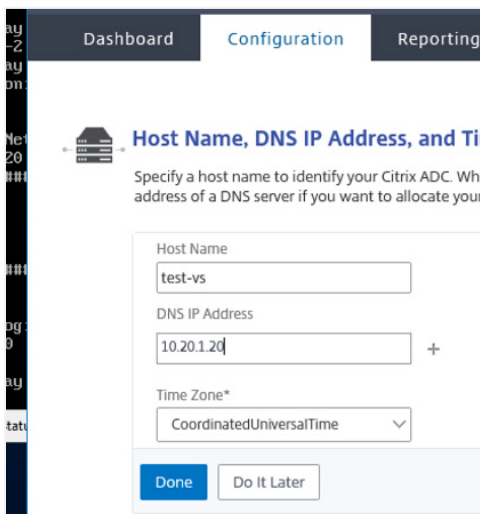
- A. Enter in the secondary IP address that you assigned to the NSIP VNIC during the provisioning process.
- B. Enter the netmask of the subnet for the VNIC.

C. Click **Done**.



9. Click the **Host Name, DNS IP Address, and Time Zone** option.

10. Enter a hostname for the ADC, the IP address of the Windows DNS server, and the time zone being used. Then, click **Done**.

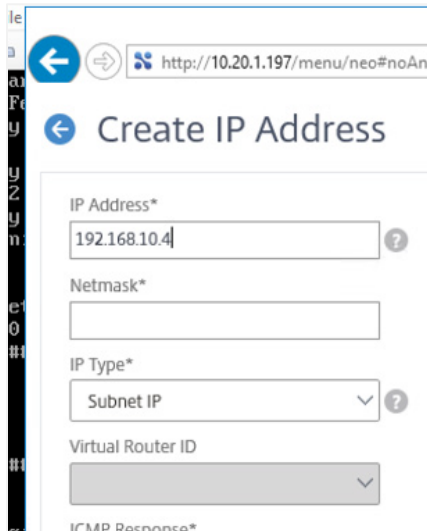


11. Click **Continue**.

12. In the navigation pane, click **System > Network > IPs**.

13. Click **Add**.

14. Add the internal IP address and netmask identified in the prerequisites for this Hyper-V instance. Keep all the remaining selections default, and then click **Create**.

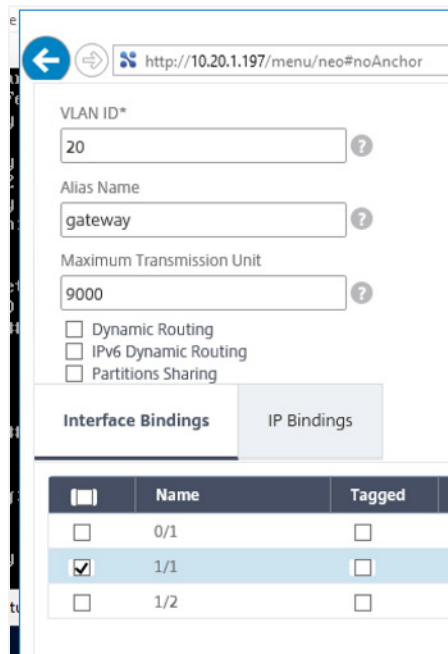


The screenshot shows a web browser window with the address bar displaying `http://10.20.1.197/menu/neo#noAn`. The page title is "Create IP Address". The form contains the following fields:

- IP Address***: Text input field containing "192.168.10.4".
- Netmask***: Empty text input field.
- IP Type***: Dropdown menu with "Subnet IP" selected.
- Virtual Router ID**: Dropdown menu (partially obscured).
- ICMP Response***: Label for a field that is mostly obscured.

15. Click **Add** again, and add the ADC VNIC Gateway address in the same way.
16. Select **System > Network > Interfaces**.
17. Note the MAC addresses, and correlate them back to the VNICs that were created. The MAC address that doesn't correlate is for the internal IP address.
18. Select **System > Network > VLANs**.
19. Click **Add**.
20. Select a VLAN ID that is meaningful.
This does not correlate to an 802.1q VLAN, but is used internally.
21. Change the **MTU** to **9000**.

22. Select the interface that correlates to the ADC Gateway VNIC MAC address, and select the check box for it. Don't select the **Tagged** check box.



The screenshot shows a web browser window with the URL <http://10.20.1.197/menu/neo#noAnchor>. The page contains several input fields: 'VLAN ID*' with the value '20', 'Alias Name' with 'gateway', and 'Maximum Transmission Unit' with '9000'. Below these are three unchecked checkboxes: 'Dynamic Routing', 'IPv6 Dynamic Routing', and 'Partitions Sharing'. There are two tabs: 'Interface Bindings' (selected) and 'IP Bindings'. Under 'Interface Bindings' is a table:

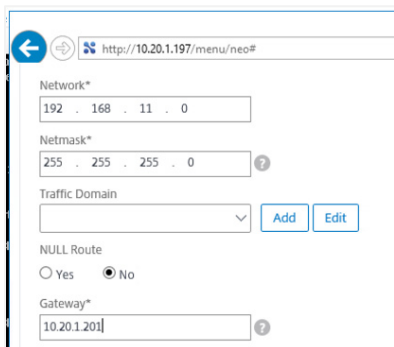
<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	0/1	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/1	<input type="checkbox"/>
<input type="checkbox"/>	1/2	<input type="checkbox"/>

23. Click the **IP Bindings** tab. Select the IP address of the ADC Gateway VNIC, and then click **Create**.
24. Repeat this process for the internal interface.
25. Select **System > Network > Routes**.

Note: The next steps require you to obtain all hvrouter VNIC addresses and internal IP address ranges/CIDRs used for any additional Hyper-V instances that will be used in this configuration. It establishes the route between the ADC and any additional Hyper-V instances

26. Click **Add**.


27. Enter in the internal Hyper-V network address, the netmask, and the IP address of the VNIC being used for hvrouter on the remote Hyper-V instance.



The screenshot shows a web browser window with the URL `http://10.20.1.197/menu/neo#`. The page contains a configuration form with the following fields and values:

- Network***: 192 . 168 . 11 . 0
- Netmask***: 255 . 255 . 255 . 0
- Traffic Domain**: A dropdown menu is currently empty, with **Add** and **Edit** buttons to its right.
- NULL Route**: Radio buttons for **Yes** and **No**, with **No** selected.
- Gateway***: 10.20.1.201

28. Click **Create**.

29. Save the running configuration to the device by clicking the Save button .

Note: When you configure the gateway service on the ADC, it is important to use the *private IP address* of the VNIC assigned to the gateway interface, not the public address. The ADC doesn't know about the public IP address and responds only to traffic directed at the private address. Oracle Cloud Infrastructure backend services transparently handle the translation of traffic from the public IP address to the private IP address.

Conclusion

The initial configuration of the Citrix ADC is complete at this point. Continue the configuration of the Citrix Virtual Apps and Desktops environment (both the CVADS and non-CVADS implementations), including any additional configuration required for setting up the ADC as a desktop gateway, by using the processes documented on <https://docs.citrix.com/>. If you selected the dual ADC architecture option, repeat this process for all Hyper-V servers that are deployed as part of the second set that is related to the second ADC. For more information about completing this process, see Appendix A: Deploying Dual Citrix ADCs.

Deploying Citrix Virtual Apps and Desktops on Oracle Cloud Infrastructure allows enterprise applications to smoothly interact with data sources within Oracle Cloud Infrastructure and to effectively interact with the data stored there. User experience is maintained in a consistent manner, and end users can be productive because they can predictably perform the tasks that are encapsulated in the virtual app or desktop.

This paper provided the following information:

- Gave you the rationale behind Oracle's and Citrix's implementation of Citrix Virtual Apps and Desktops on the Oracle Cloud Infrastructure

- Guided you through the various architectural options and explained the decision points for selecting the appropriate one for your environment and requirements
- Walked you through the implementation of the infrastructure required to successfully install Citrix Virtual Apps and Desktops

The information provided should inform your decisions and allow you to successfully move virtual application and/or desktops to Oracle Cloud Infrastructure using Citrix Virtual Apps and Desktops as the management and provisioning tool while maintaining the operational experience gained when running the Citrix suite in an on-premises environment.

Appendix A: Deploying Dual Citrix ADCs

As indicated previously in this paper, one of the options for using Citrix Virtual Apps and Desktops in the Oracle Cloud Infrastructure environment is to deploy two Citrix ADCs, spread across two different Hyper-V instances. Figure 7 shows the architecture of the resulting deployment of a dual-ADC environment.

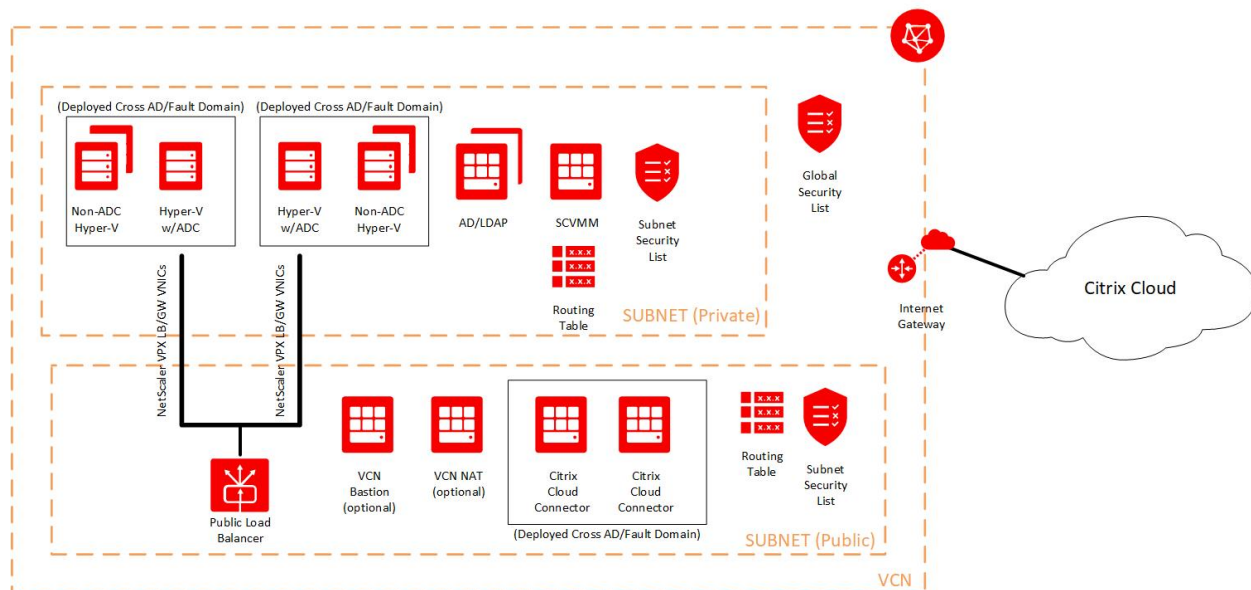



Figure 7: Dual Citrix ADC Deployment Architecture

Although the deployment mechanism for the Hyper-V instance itself is the same as described earlier, you must meet additional requirements and perform additional configuration steps to support this type of deployment.



One of the main items is that each ADC must manage its own set of Hyper-V instances. Having two different ADCs place apps or desktops on a common Hyper-V instance is not supported. Therefore, when you calculate the number of required bare metal instances, if an odd number is returned, you must round up to the nearest even number.

For example, suppose that you decide initially, based on the calculation earlier in the paper, that four bare metal instances are required, including the one that contains the ADC. Adding another ADC results in a requirement of five bare metal servers. However, because the two ADC servers can't share a common non-ADC Hyper-V instance, an additional bare metal server would be required to balance the load between the two ADC instances. As a result, you need six bare metal servers.

Note, that this outcome achieves only a balanced load, not a full failover. To achieve a full failover, the preceding scenario would require eight bare metal instances to fully take on the load of a single ADC.

In either case, after the second ADC/non-ADC set of instances is deployed and configured, these instances should be configured as two different delivery groups within the Citrix environment, each having their own set of machine catalogs. The machine catalogs should be clones of each other (that is, each should have the same templates and configuration), so that the desktop templates created for one set of machine catalogs match *exactly* that of the other. This ensures that users of a particular set of desktops have a consistent experience regardless of which ADC set they are assigned to.

Additional Requirements for Dual ADC deployment

The following items are required for the dual ADC deployment model:

- Minimum of two BM.DenseIO2.52 instances running Windows 2016 Datacenter Edition. The actual number is based on the preceding calculation, rounded up to the next even number.
- Minimum 400Mbps Oracle Cloud Infrastructure regional load balancer. If this deployment is using Citrix Virtual Apps and Desktops Service, the load balancer must be public; if not, it can be public or private.
- Two Citrix ADC licenses (one for each initial bare metal instance), each with the required throughput. We recommend that both Citrix ADCs are licensed to the same capacity.

Configuration Procedure

When deploying the dual ADC model, you deploy a second ADC Hyper-V instance, along with all attendant non-ADC instances as detailed previously. Configure the machine catalogs and delivery groups for each set of Hyper-V ADC/non-ADC instances. You must use the same SSL certificate for both ADCs and retain that certificate for the load balancer configuration.

After the environment is configured, set up the load balancer.

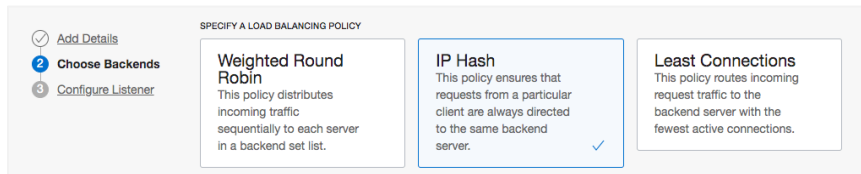
1. In the Oracle Cloud Infrastructure Console main menu, select **Networking > Load Balancers**.
2. Click **Create Load Balancer**.
3. On the **Add Details** page, specify the following values:
 - A. Give the load balancer a meaningful name.
 - B. If it will provide services to the internet, select **Public**; otherwise, select **Private**.
 - C. Select either the **Medium** or **Large** bandwidth, depending on your requirement. Citrix requires a minimum of a 400Mbps.
 - D. Select the VCN used for the ADCs.
 - E. Select a subnet appropriate to your configuration. If you selected a public load balancer, only public subnets are shown.

The screenshot shows the 'Create Load Balancer' page in the Oracle Cloud Infrastructure Console. The page is titled 'Create Load Balancer' and has a breadcrumb trail 'Networking > Load Balancers'. The page is divided into three steps: 'Add Details', 'Choose Backends', and 'Configure Listener'. The 'Add Details' step is currently active and shows a form with the following fields:

- Name:** lb_2019-0716-1341
- CHOOSE VISIBILITY TYPE:** Public (selected), Private
- CHOOSE THE MAXIMUM TOTAL BANDWIDTH:** Small (100Mbps), Medium (400Mbps, selected), Large (8000Mbps)
- CHOOSE NETWORKING:** VIRTUAL CLOUD NETWORK in c2 (Change Compartment), SUBNET in c2 (Change Compartment)
- USE NETWORK SECURITY GROUPS TO CONTROL TRAFFIC

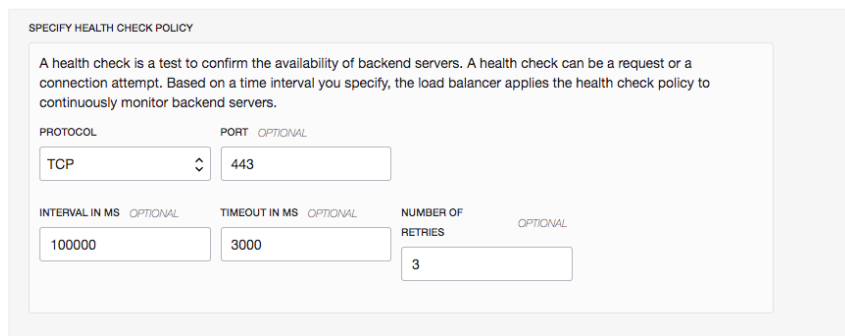
At the bottom of the form, there are 'Next Step' and 'Cancel' buttons.

4. Click **Next Step**.
5. On the **Choose Backends** page, specify the following values:
 - A. Select **IP Hash**.



Note: *Don't* click **Add Backends**. The backends and backend sets are created after the load balancer is deployed.

- B. Change the Health Check Policy to use TCP instead of the default HTTP. Specify port 443 as the health check port. Leave all the other settings as default.



6. Click **Next Step**.
7. On the **Configure Listener** page, ensure that port 443 is set for the listener, and upload the certificate used for the ADCs.

Create Load Balancer

A listener is a logical entity that checks for incoming traffic on the load balancer's IP address. To handle TCP, HTTP and HTTPS traffic, you must configure at least one listener per traffic type. You can configure additional listeners after you create your load balancer.

Add Details
 Choose Backends
 Configure Listener

SPECIFY THE TYPE OF TRAFFIC YOUR LISTENER HANDLES

HTTPS HTTP TCP

SPECIFY THE PORT YOUR LISTENER MONITORS FOR INGRESS TRAFFIC

443

SELECT AN SSL CERTIFICATE

Drop a file or [select one](#)
Certificates must be in PEM format and must be signed

testcert_pub.pem

SPECIFY CA CERTIFICATE
 SPECIFY PRIVATE KEY
 CHOOSE PRIVATE KEY FILE PASTE PRIVATE KEY

PRIVATE KEY

Drop a file or [select one](#)
Private key must be in PEM format

testcert.pem

8. Click **Create Load Balancer**.
9. After the load balancer is deployed, open the load balancer configuration, and click **Backend Sets** in the lower-left pane.
10. Select the default backend set that was created as part of the load balancer deployment.
11. In the lower-left pane, select **Backends**.
12. When the backend set console appears, click **Add Backends**.
13. Change the selection criteria by selecting IP Addresses. Enter the IP address of the first ADC Gateway VNIC, and select port 443.


Add Backends [help](#) [cancel](#)

Choose how to add backend servers by selecting compute instances or by entering IP addresses.

COMPUTE INSTANCES **IP ADDRESSES**

IP ADDRESS	PORT	WEIGHT
10.20.1.20	443	1

+ Additional Backend

- 
14. Click **+Additional Backend** and repeat for the second ADC gateway VNIC.
 15. Click **Add**.
 16. In the Work Request dialog box, click **Close**.
 17. After the backend set is created and running, the load balancer configuration is complete.
Consult your Citrix documentation for any additional configuration needed to allow the load balancer to work.





As described, this configuration provides a method for implementing dual ADCs that can potentially serve the same type of virtual applications or desktops. This implementation can fulfill the requirements of scaling out bandwidth between a number of ADCs, providing a highly available environment, or both, depending on the size of the environment.



Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0819

Implementing Citrix Virtual Apps and Desktops in Oracle Cloud Infrastructure
August 2019
Author: Steven B. Nelson, Oracle, Inc.
Contributing Authors: Albert Lee, Citrix, Inc.