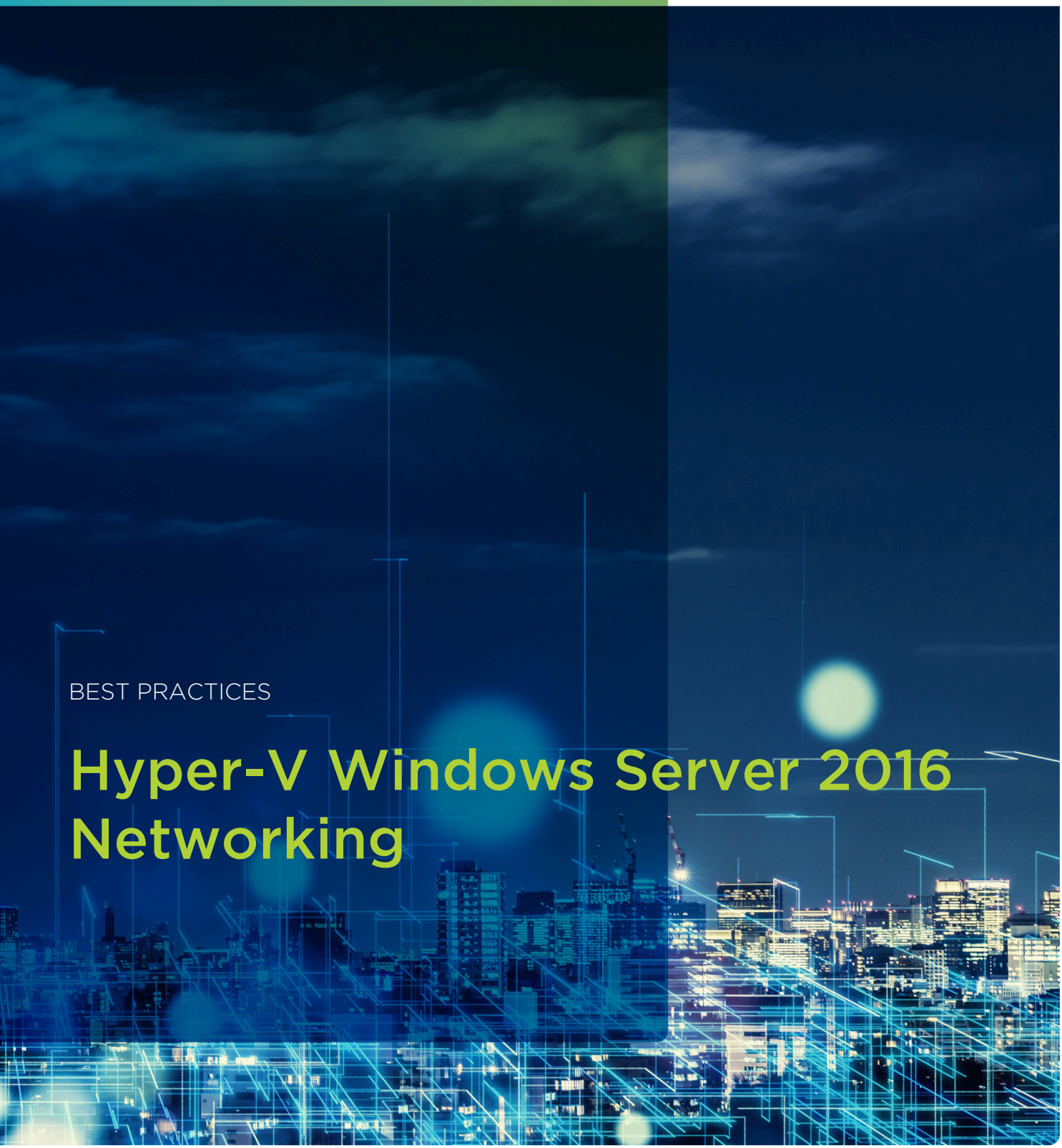
v1.3 | July 2020 | BP-2088



BEST PRACTICES

Hyper-V Windows Server 2016 Networking

NUTANIX
YOUR ENTERPRISE CLOUD

Copyright

Contents

1. Executive Summary

The Nutanix enterprise cloud software is a highly scalable, converged compute and storage platform designed for virtual environments, including Hyper-V with Windows Server 2016. The Nutanix architecture runs a storage controller in each virtual machine (VM)—the Nutanix Controller VM (CVM). Every server node on a Nutanix system runs the CVM, which is central to forming a highly distributed, shared-nothing converged infrastructure.

The network in the Nutanix solution ensures storage high availability and performance. The CVMs in a Nutanix cluster communicate with each other over a set of network interface cards (NICs) that reside in each host. Nutanix comes with redundant 10 Gbps and 1 Gbps NICs. These connections support networking traffic in a variety of ways, such as Nutanix storage, VMs, and Hyper-V management functions like domain communications and live migration.

The default Nutanix configuration for Windows Server 2016 and Hyper-V has a single load balancing and failover (LBFO) NIC team that supports network traffic between the hosts. A specific virtual network switch and set of virtual and physical NICs use the default LBFO team. The default Nutanix networking configuration requires no modification and suits most use cases. However, you can extend this default configuration to include additional LBFO teams, virtual switches, or virtual NICs (VNICs) to segment specific kinds of network traffic in a more deterministic way. System Center Virtual Machine Manager (SCVMM) can help standardize a custom network deployment and manage the overall solution where you need network virtualization.

In this document, we detail the best practices for making changes to the default networking configuration, including when to do it and the effects of the changes.

2. Introduction

Audience

This best practices guide is part of the Nutanix Solutions Library. We intended it for IT administrators and architects who want to understand the networking architecture of Windows Server 2016 and Hyper-V with Nutanix.

Purpose

This best practices guide describes Hyper-V and Windows Server 2016 networking concepts and how to use them in a Nutanix environment to ensure optimal performance and availability. It covers the recommended configuration settings for different Hyper-V networking options, including the use of SCVMM to manage the environment.

Refer to the Nutanix Hyper-V Administration guide for additional topics.

Table 1: Document Version History

Version Number	Published	Notes
1.0	December 2017	Original publication.
1.1	May 2018	Logical switch mode clarification and platform update.
1.2	May 2019	Updated Nutanix overview.
1.3	July 2020	Updated Nutanix overview and Jumbo Frames section and added SET support.

3. Nutanix Enterprise Cloud Overview

Nutanix delivers a web-scale, hyperconverged infrastructure solution purpose-built for virtualization and both containerized and private cloud environments. This solution brings the scale, resilience, and economic benefits of web-scale architecture to the enterprise through the Nutanix enterprise cloud platform, which combines the core HCI product families—Nutanix AOS and Nutanix Prism management—along with other software products that automate, secure, and back up cost-optimized infrastructure.

Available attributes of the Nutanix enterprise cloud OS stack include:

- Optimized for storage and compute resources.
- Machine learning to plan for and adapt to changing conditions automatically.
- Intrinsic security features and functions for data protection and cyberthreat defense.
- Self-healing to tolerate and adjust to component failures.
- API-based automation and rich analytics.
- Simplified one-click upgrades and software life cycle management.
- Native file services for user and application data.
- Native backup and disaster recovery solutions.
- Powerful and feature-rich virtualization.
- Flexible virtual networking for visualization, automation, and security.
- Cloud automation and life cycle management.

Nutanix provides services and can be broken down into three main components: an HCI-based distributed storage fabric, management and operational intelligence from Prism, and AHV virtualization. Nutanix Prism furnishes one-click infrastructure management for virtual environments running on AOS. AOS is hypervisor agnostic, supporting two third-party hypervisors

—VMware ESXi and Microsoft Hyper-V—in addition to the native Nutanix hypervisor, AHV.

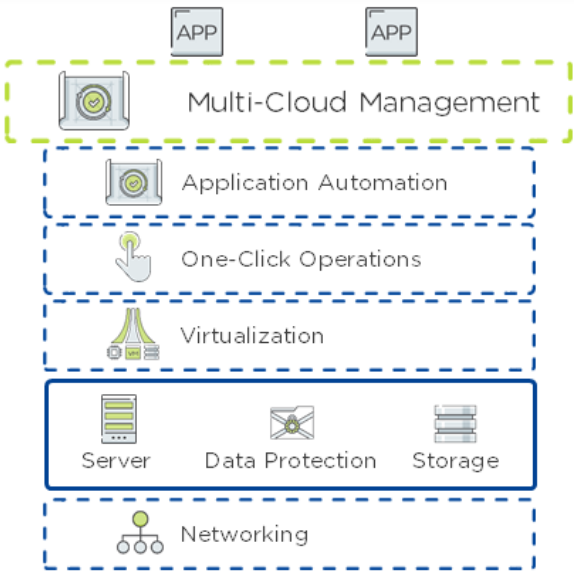


Figure 1: Nutanix Enterprise Cloud OS Stack

Nutanix HCI Architecture

Nutanix does not rely on traditional SAN or network-attached storage (NAS) or expensive storage network interconnects. It combines highly dense storage and server compute (CPU and RAM) into a single platform building block. Each building block delivers a unified, scale-out, shared-nothing architecture with no single points of failure.

The Nutanix solution requires no SAN constructs, such as LUNs, RAID groups, or expensive storage switches. All storage management is VM-centric, and I/O is optimized at the VM virtual disk level. The software solution runs on nodes from a variety of manufacturers that are either entirely solid-state storage with NVMe for optimal performance or a hybrid combination of SSD and HDD storage that provides a combination of performance and additional capacity. The storage fabric automatically tiers data across the cluster to different classes of storage devices using intelligent data placement algorithms. For best

performance, algorithms make sure the most frequently used data is available in memory or in flash on the node local to the VM.

To learn more about Nutanix enterprise cloud software, visit the Nutanix Bible and Nutanix.com.

4. Microsoft Hyper-V Networking

Microsoft provides a variety of network services out of the box with Windows Server 2016. The Hyper-V virtual switch is an extensible switch that supports Hyper-V Network Virtualization (HNV). HNV is a technology that uses network virtualization generic routing encapsulation (NVGRE) to enable datacenters to use a flat network fabric and configure multiple isolated tenant networks on the same physical network.

A variety of networking features are built into Windows 2016 and HNV, including quality of service (QoS), PVLAN support, receive-side scaling (RSS), virtual machine queue (VMQ), and third-party extensibility. Extensions include firewall, intrusion detection, and OpenFlow and you can use them for both ingress and egress traffic.

The following sections give an overview of the Windows 2016 and HNV features relevant to the Nutanix platform, including deployment and support considerations.

Server Message Block (SMB)

SMB is an application-layer network protocol typically used to provide access to shared files in a network. Microsoft supports version 3.0 of the SMB protocol. SMB 3.0 introduced several core features, including SMB Transparent Failover, SMB Direct, and SMB Multichannel, to improve the protocol's availability and performance.

SMB with Nutanix

The Nutanix platform uses SMB 3.0 to present all shared storage in Hyper-V environments. This solution doesn't use Cluster Shared Volumes (CSV), based on SCSI logical unit numbers (LUNs). The Nutanix SMB share, which each CVM exports globally, is presented directly to the Hyper-V server to host VM files. Under most circumstances, the system doesn't present Nutanix SMB shares directly to VMs.

The unique Nutanix architecture processes all SMB 3.0 traffic locally to the Hyper-V server hosting the VM that is performing the I/O operation. This SMB storage I/O traffic occurs over the internal VNIC and internal virtual switch outlined in the following sections. Because of the localized, in-memory SMB traffic, you don't need to implement certain features of the SMB 3.0 protocol, such as SMB Direct or SMB Multichannel, on the Nutanix platform.

One aspect of the SMB 3.0 protocol we implemented on the Nutanix platform is transparent failover. Nutanix enables the continuously available setting (which controls transparent failover and is considered a requirement for Hyper-V environments) by default. If a CVM becomes unavailable on a given Hyper-V server, the routing table for that server updates to reference the SMB server instance running in a CVM on another node in the cluster. Nutanix refers to this CVM storage controller redirection as data path redundancy. Data path redundancy allows VMs to continue to access the SMB share without significant interruption when the local CVM becomes unavailable. For this redirection to work, the file handles associated with the VMs need to be maintained across the CVM instances in the cluster. SMB transparent failover allows this file handle redirection across CVM instances, which ensures minimal interruption to VM storage traffic during CVM failure or upgrade scenarios.

Hyper-V Virtual Switches

The Hyper-V virtual switch is a layer 2 virtual switch that provides programmatically managed capabilities to connect VMs to a physical network. Hyper-V supports several virtual switch types:

- Private

  Virtual switches supporting private networks allow communication only between VMs that reside on the same host.

- Internal

  Virtual switches supporting internal networks allow communication between VMs on the same host and between VMs and the Hyper-V host where they reside.

- External

  Virtual switches supporting external networks allow communication between physical servers and between VMs running on the same or on different Hyper-V hosts.

Hyper-V Virtual Switches with Nutanix

The Nutanix imaging process with Hyper-V creates two virtual switches on every host. One switch manages network communication between the Nutanix CVM and the Hyper-V host. This switch is called InternalSwitch and configured as an internal virtual switch type. The second switch manages external communication between the VMs and between the Hyper-V hosts. Its networking traffic also includes CVM replication traffic that maintains the replication factor, as well as any DSF traffic that can't be processed locally. This second switch, configured as an external virtual switch, is called ExternalSwitch. The external switch is assigned a network adapter team to provide connectivity outside the host. Assuming that the system uses the 10 Gbps NICs, the following diagram details the default Nutanix virtual switch configuration.

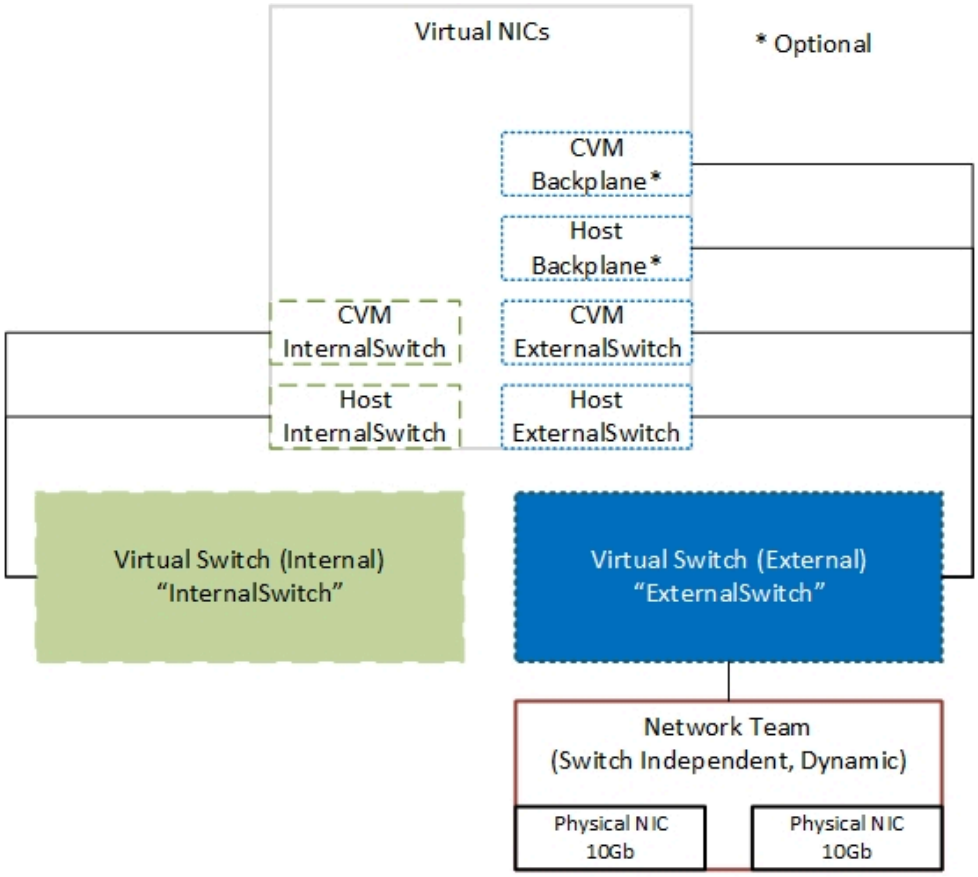


Figure 2: Default Nutanix Networking with Hyper-V

By default, the system uses a management OS VNIC named ExternalSwitch for external host communication. You can enable an optional backplane network that uses a backplane management OS VNIC. The backplane network separates the Nutanix storage traffic from the management traffic, as required for security purposes.

You can view the default Nutanix networking configuration using standard Windows tools, including Hyper-V Manager or PowerShell. The following PowerShell commands manage the virtual switches:

```
Add | Get | New | Remove | Rename | Set-VMSwitch
```

The following PowerShell example shows how to view the default configuration, including the switch type and default bandwidth reservation mode.


```
PS C:\> Get-VMSwitch | fl Name, SwitchType, BandwidthReservationMode, NetAdapter
InterfaceDescription

Name                                : ExternalSwitch
SwitchType                          : External
BandwidthReservationMode            : Absolute
NetAdapterInterfaceDescription      : Microsoft Network Adapter Multiplexor Driver

Name                                : InternalSwitch
SwitchType                          : Internal
BandwidthReservationMode            : Absolute
NetAdapterInterfaceDescription      :
```

Figure 3: Default Nutanix Virtual Switch Configuration

Hyper-V Virtual Switches with SCVMM

When using SCVMM, Hyper-V supports a standard switch and a logical switch. Each Hyper-V host contains a standard switch and maintains a unique configuration on a host-by-host basis. Underlying the standard switch is a Hyper-V virtual switch that administrators can modify with PowerShell, Hyper-V Manager, or SCVMM. The virtual switch created during the Nutanix installation process is a standard switch.

The logical switch construct acts as a container for all virtual switch settings. Like the standard switch described previously, this logical switch is based on a Hyper-V virtual switch. The main benefit of a logical switch is that it enables network management through SCVMM, including the use of NVGRE-based virtual networks. For more detailed information on Hyper-V virtual networks, refer to Hyper-V Network Virtualization Technical Details in Windows Server 2016.

The design Nutanix recommends for SCVMM is similar to the default configuration, in which a single logical switch conjoins with a network team to manage the dual 10 Gbps NICs. Administrators can then create multiple VNICs through SCVMM for live migration and management traffic. For Nutanix to support the configuration, you must name the management VNIC ExternalSwitch to match the name used with the default configuration. You can find additional information on using SCVMM to manage networking on Nutanix in the Deployment Models section.

Hyper-V VNICs

VNICs connect VMs or the Hyper-V host (also referred to as the management OS) to the virtual switches for either internal or external networking traffic. The VNICs for VMs are configured as a part of the VM creation process. Administrators create the VNICs the Hyper-V server uses either through PowerShell, in the case of standard virtual switches, or through SCVMM when using logical switches.

Hyper-V VNICs with Nutanix

The default Nutanix configuration creates one management OS VNIC for each of the two default virtual switches, as depicted in the Default Nutanix Networking with Hyper-V figure. You can also configure an optional backplane VNIC. To help separate network traffic and apply QoS, most notably for live migration, you can create additional VNICs for the Hyper-V server. The Deployment Models section provides details for virtual switch and VNIC customization.

The following PowerShell commands manage VNICs:

```
Add | Connect | Disconnect | Get | Remove | Rename | Set | Test-
VMNetworkAdapter
```

The following example shows the default Nutanix configuration for the CVM.

```
PS C:\> Get-VM | where {$_.name -like "NTNX*"} | Get-VMNetworkAdapter | ft name,
 switchname, VMName -AutoSize

Name     SwitchName     VMName
----     ----------     ------
External ExternalSwitch NTNX-13SM35190018-B-CVM
Internal InternalSwitch NTNX-13SM35190018-B-CVM
```

Figure 4: Default CVM VNICs

The following example shows the default Nutanix configuration for the host (management OS).


```
PS C:\> Get-VMNetworkAdapter -ManagementOS | ft Name, Switchname, MacAddress, St
atus -AutoSize

Name           SwitchName     MacAddress   Status
----           ----------     ----------   ------
InternalSwitch InternalSwitch 00155D1E4800 {Ok}
ExternalSwitch ExternalSwitch 002590E170C9 {Ok}
```

Figure 5: Default Hyper-V Host VNICs

NIC Teaming Overview

Microsoft introduced native NIC teaming (also referred to as LBFO) with Windows Server 2012. NIC teaming provides network fault tolerance and continuous availability. It also aggregates bandwidth from multiple network adapters.

Windows Server 2016 with Hyper-V offers two teaming options: traditional NIC teaming and Switch Embedded Teaming (SET). Traditional NIC teaming support is similar to the architecture available with Windows Server 2012 and Windows Server 2012 R2, where a NIC team is set as an uplink for a virtual switch. SET, new with Server 2016, integrates the teaming function into the virtual switch.

Nutanix with Windows Server 2016 defaults to the traditional teaming model. AOS 5.17 and later versions support SET as the teaming model with Windows Server 2016 and Hyper-V. Configuration of SET with Windows Server 2016 and Hyper-V is outside the scope of this document. Refer to the Nutanix Hyper-V Administration guide for more details.

Windows NIC teaming supports two modes of operation, generally referred to as switch independent and switch dependent. Switch-independent teaming, as the name implies, does not depend on the underlying physical switches to form the network team.

Switch-dependent teaming requires you to configure the underlying switches using either static teaming or dynamic teaming with Link Aggregation Control Protocol (LACP). The specific modes for the NIC team in this case are either static teaming or LACP.

Microsoft also offers several load-balancing algorithms, including Hyper-V switch port, address hashing, and dynamic mode. Combining NIC teaming and

load distribution modes determines the overall capabilities and interoperability of the NIC team. Details on these combinations are outside the scope of this document. For more information, refer to Microsoft's detailed whitepaper on Windows Server 2016 NIC teaming.

NIC Teaming with Nutanix

The default Nutanix configuration uses an LBFO team in switch-independent mode with dynamic load balancing. Switch-independent mode does not require any unique switch configuration to implement the Nutanix solution, which simplifies setup and maintenance. Switch-independent mode also allows for active-standby mode teams (one active NIC and one standby NIC), as well as the ability to aggregate the VM queues across all NICs.

Dynamic load balancing uses a combination of the address hashing and Hyper-V switch port load distribution algorithms. Microsoft recommends the dynamic distribution configuration for most use cases. Overall, the combination of switch-independent mode and dynamic distribution supports for the broadest range of configurations while optimizing performance.

For performance-intensive environments, we recommend using Hyper-V Port as the load-balancing algorithm. Set Hyper-V Port with the following command:

```
Set-NetLbfoTeam NetAdapterTeam -LoadBalancingAlgorithm HyperVPort
```

You can view and modify the NIC teaming configuration using the lbfoadmin.exe utility. Launch this utility from the command line or open it from Server Manager, as shown in the following figure.

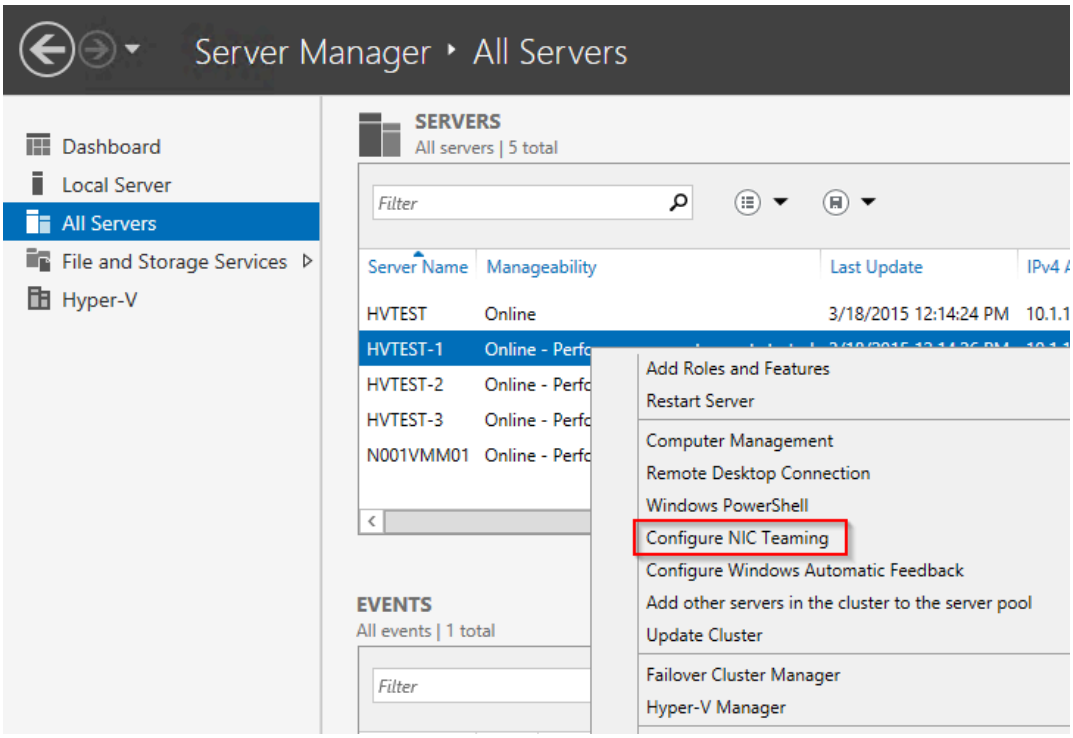


Figure 6: Configure NIC Teaming from Server Manager

Once you have opened the utility, you can view or modify the team settings and members. You can also view the team health status.

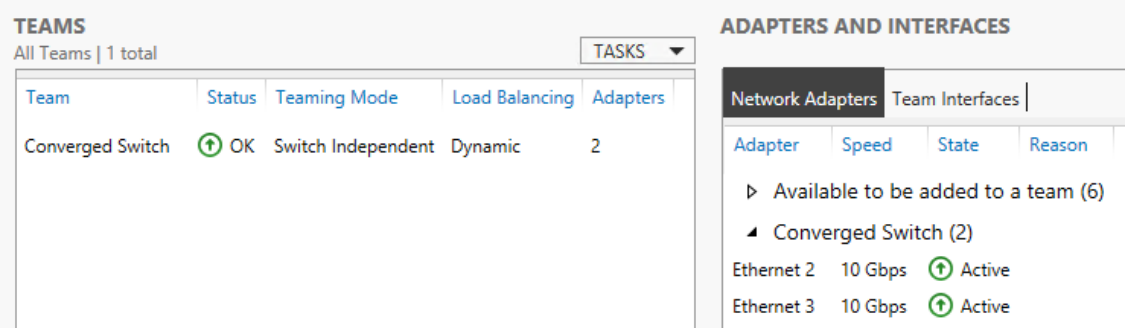


Figure 7: NIC Teaming Admin

The corresponding PowerShell commands for managing traditional NIC teaming with Windows 2016 are:

```
[Add|Get|Remove|Set]-NetLbfoTeamMember
[Add|Get|Remove|Set]-NetLbfoTeamNic
```



```
[Get|New|Remove|Rename|Set]-NetLbfoTeam
```

The following PowerShell example shows the default network team configuration with two members.

```
PS C:\> Get-NetLbfoTeam

Name                       : NetAdapterTeam
Members                    : {Ethernet 3, Ethernet 2}
TeamNics                   : NetAdapterTeam
TeamingMode                : SwitchIndependent
LoadBalancingAlgorithm     : Dynamic
Status                     : Up
```

Figure 8: Default Network Team Configuration

Dynamic Virtual Machine Queue Overview

The virtual machine queue (VMQ), with supported NICs, enables separate queues on the network adapter, with each queue mapped to an individual VM. These are the same hardware queues that RSS uses, so you can't use VMQ with the RSS feature. VMQ allows different host CPUs to service the network traffic, which improves performance and more evenly distributes CPU load on the host. Windows 2012 introduced dynamic VMQ, which automatically increases or decreases the number of cores VMQ uses depending on the workload.

VMQ assignment is on a first-come, first-served basis, but the allocation of processor cores is dynamic. The queues can move between logical processors on the fly based on load. As the load drops, the queues can fall back to fewer cores. A downside of VMQ is that a single VNIC only uses a single VMQ and therefore a single processor core. From a performance perspective, using a single processor core means that the maximum throughput for a single VNIC is limited by the frequency of that core, which can vary depending on processor type.

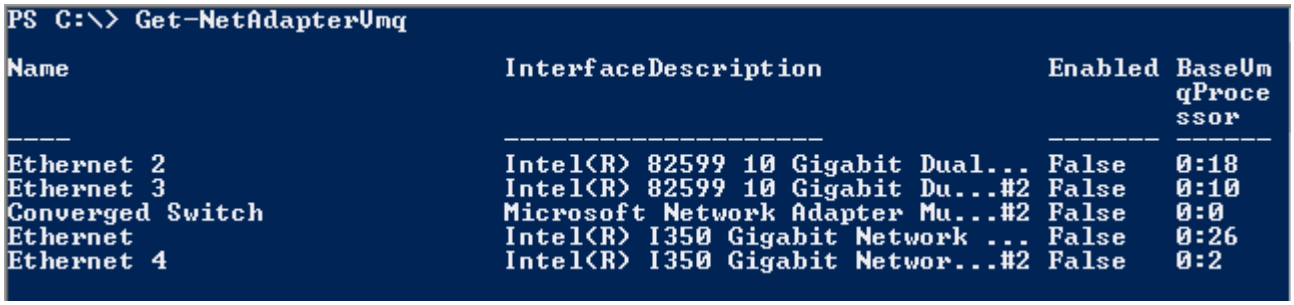
VMQ with Nutanix

Nutanix supports VMQ. VMQ support requires an updated Intel NIC driver, included with the Nutanix Foundation imaging software. VMQ is enabled by default. The corresponding PowerShell commands are:

```
[Disable|Enable|Get]-NetAdapterVmq
```


As an example, the Intel 82599 NIC has 63 queues per NIC, for a total of 126 queues servicing both 10 Gbps NICs. Combining switch-independent NIC teaming with dynamic load balancing uses the sum of both NIC queues. In this configuration, up to 125 VMs (assuming a single NIC per VM and a single management OS VNIC) on a Nutanix node each get their own network queue.

The next figure shows the result of running Get-NetAdapterVmq on a Nutanix 3050 platform.



```
PS C:\> Get-NetAdapterVmq

Name                            InterfaceDescription                Enabled BaseVmq
                                                                            Processor
----                            --------------------                ------- -------
Ethernet 2                      Intel(R) 82599 10 Gigabit Dual...   False   0:18
Ethernet 3                      Intel(R) 82599 10 Gigabit Du...#2   False   0:10
Converged Switch                Microsoft Network Adapter Mu...#2   False   0:0
Ethernet                        Intel(R) I350 Gigabit Network ...   False   0:26
Ethernet 4                      Intel(R) I350 Gigabit Networ...#2   False   0:2
```

Figure 9: Get-NetAdapterVmq Example

You can also control the VM's VMQ settings using PowerShell:

```
[Get|Set]-VMNetworkAdapter
```

You can set the --vmqweight option to 0 to disable VMQ or to another value to enable it. The default is 100 (enabled).

You can also use Hyper-V Manager to view or modify the VMQ setting for a VM. The VMQ setting is under the Hardware Acceleration heading in the VNIC options for the VM.

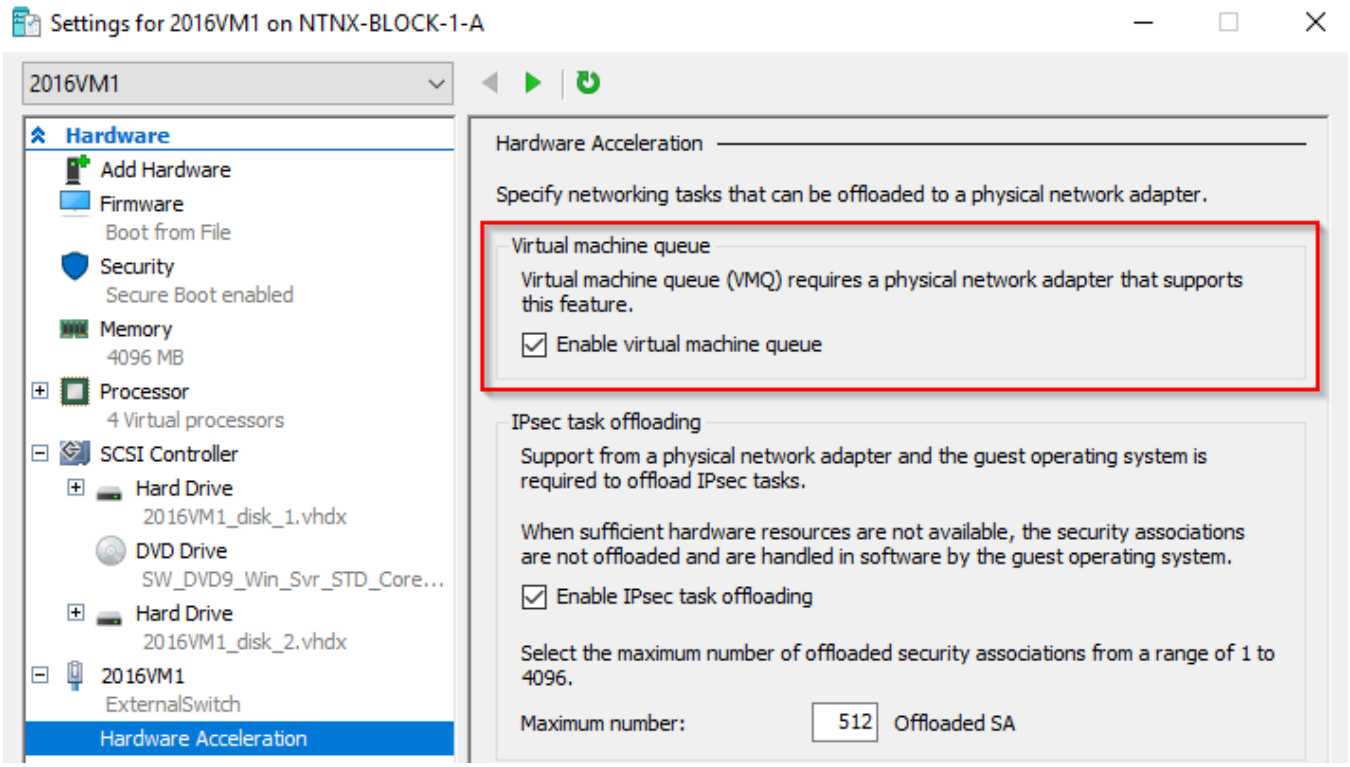


Figure 10: Enabling VMQ in Hyper-V Manager

When you configure a NIC team to support sum-queue mode with VMQ, as in the default Nutanix configuration, Microsoft recommends specifying nonoverlapping processor ranges for the NICs in the team. This Microsoft Support article contains detailed information on configuring VMQ processor ranges.

In an environment where VMQ is enabled, you can use PowerShell to check which VMs are using VMQ. You can run the Get- NetAdapterVmqQueue command on the Hyper-V host that owns the VM, as in the following figure.


```
PS C:\> Get-NetAdapterVmqQueue | ft -AutoSize

Name                QueueID MacAddress        VlanID Processor VmFriendlyName
----                ------- ----------        ------ --------- --------------
Ethernet 2          0                                 0:0       HVTEST-1
Ethernet 2          1       00-1D-D8-B7-1C-2B         0:18      HVTEST-1
Ethernet 2          2       00-15-5D-92-B8-00         0:18      NTNX-14SM3609008...
Ethernet 2          3       00-15-5D-4F-4C-48         0:18      WIN2012R2_VM-1
Ethernet 2          4       00-15-5D-4F-4C-25         0:18      WIN2012R2_VM-4
Ethernet 3          0                                 0:0       HVTEST-1
Ethernet 3          1       00-15-5D-92-B8-27         0:10      HVTEST-1
Ethernet 3          2       00-1D-D8-B7-1C-28         0:10      HVTEST-1
Ethernet 3          3       00-15-5D-4F-4C-39         0:10      WIN2012R2_VM-2
Ethernet 3          4       00-15-5D-94-E4-31         0:10      WIN2012R2_VM-3
Ethernet 3          5       00-15-5D-4F-4C-33         0:10      WIN2012R2_VM-5
Converged Switch 0                                    0:0       HVTEST-1
Converged Switch 1  00-1D-D8-B7-1C-2B                 0:18      HVTEST-1
Converged Switch 2  00-15-5D-92-B8-27                 0:10      HVTEST-1
Converged Switch 3  00-1D-D8-B7-1C-28                 0:10      HVTEST-1
Converged Switch 4  00-15-5D-92-B8-00                 0:18      NTNX-14SM3609008...
Converged Switch 5  00-15-5D-4F-4C-48                 0:18      WIN2012R2_VM-1
Converged Switch 6  00-15-5D-4F-4C-39                 0:10      WIN2012R2_VM-2
Converged Switch 7  00-15-5D-94-E4-31                 0:10      WIN2012R2_VM-3
Converged Switch 8  00-15-5D-4F-4C-25                 0:18      WIN2012R2_VM-4
Converged Switch 9  00-15-5D-4F-4C-33                 0:10      WIN2012R2_VM-5
```

Figure 11: VMQs Used by VMs and Host VNICs

Virtual Receive-Side Scaling (vRSS) Overview

vRSS spreads network traffic on two levels: inside the host and inside the VM. Without vRSS, network processing is restricted to core 0 of CPU 0 inside the VM and limited in throughput based on the frequency of that core. Enabling vRSS inside the guest VM distributes network packet processing across all virtual processors assigned to the VM once CPU 0 reaches 80 percent utilization.

vRSS is not enabled by default and you should only turn it on for network-intensive VMs (with high network throughput requirements). You must provision vRSS-enabled VMs with multiple vCPUs, with four or more in virtual NUMA mode recommended for maximum throughput. Only enable vRSS for these high-traffic VMs, as it adds CPU overhead.

To enable vRSS using the GUI in the guest OS, open the advanced properties of the VNIC and enable RSS, as shown in the following figure below.

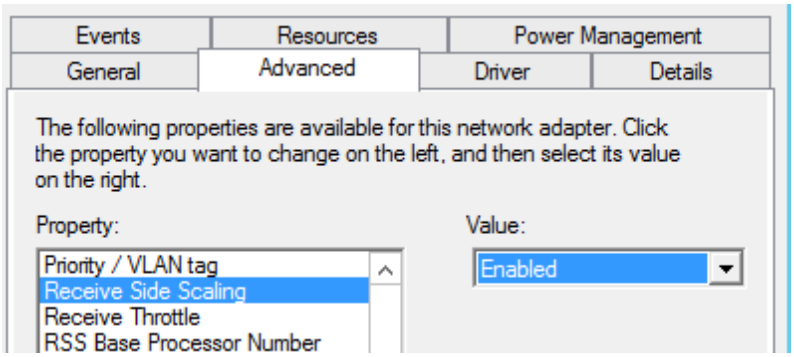


Figure 12: Virtual Machine RSS Setting

You can also use these commands to configure vRSS in the guest VM using PowerShell:

```
[Get|Enable|Disable]-NetAdapterRss
```

```
PS C:\> get-netadapterrss

Name                                            : Ethernet
InterfaceDescription                            : Microsoft Hyper-V Network Adapter
Enabled                                         : True
NumberOfReceiveQueues                           : 16
Profile                                         : NUMAStatic
BaseProcessor: [Group:Number]                   : :0
MaxProcessor: [Group:Number]                    : :
MaxProcessors                                   : 16
RssProcessorArray: [Group:Number/NUMA Distance] :
IndirectionTable: [Group:Number]                :
```

Figure 13: Virtual Machine RSS Setting Using PowerShell

vRSS with Nutanix

vRSS uses VMQ to help distribute the networking workload across available processors. You can enable vRSS without VMQ, but in this case the processor utilization benefits are only realized in the VM and not on the host. The Nutanix platform supports vRSS, but you only see the complete benefits if you enable VMQ.

Jumbo Frames

The Nutanix CVM uses the standard Ethernet MTU (maximum transmission unit) of 1,500 bytes for all the network interfaces by default. The standard

1,500-byte MTU delivers excellent performance and stability. Nutanix does not support configuring the MTU on a CVM's network interfaces to higher values.

You can enable jumbo frames (MTU of 9,000 bytes) on the physical network interfaces of AHV, ESXi, or Hyper-V hosts and user VMs if the applications on your user VMs require them. If you choose to use jumbo frames on hypervisor hosts, be sure to enable them end to end in the desired network and consider both the physical and virtual network infrastructure impacted by the change.

Large Send Offload (LSO) Overview

Large send offload (LSO) is a way to get the NIC, rather than the host CPU, to segment a packet. The NIC receives a large packet, but it sends out multiple packets that fit within the specified MTU. Having the NIC segment the packets is more efficient than having the host process multiple packets. LSO is compatible with all other Windows networking features.

LSO with Nutanix

Nutanix supports LSO. LSO is enabled by default and should not be disabled. The corresponding PowerShell commands related to LSO are:

```
[Get|Set]-NetAdapterLso
```

```
PS C:\> Get-NetAdapterLso

Name                                    Version          V1IPv4Enabled  IPv4Enabled  IPv6 Enabled
----                                    -------          -------------  -----------  ----
vEthernet (Internal)                    LSO Version 2    False          True         True
vEthernet (External)                    LSO Version 2    False          True         True
NetAdapterTeam                          LSO Version 2    False          True         True
Ethernet 3                              LSO Version 2    False          True         True
Ethernet 2                              LSO Version 2    False          True         True
Ethernet 4                              LSO Version 2    False          True         True
Ethernet                                LSO Version 2    False          True         True
```

Figure 14: Default Nutanix LSO Settings

Bandwidth Management

Managing the bandwidth in a virtualized environment can be important, especially when you're using a converged networking architecture. Some traffic,

like live migration, can potentially saturate multiple 10 Gbps NICs. Bandwidth management can help preserve network resources for storage and VM traffic.

Microsoft offers two modes of bandwidth management for Hyper-V virtual switches, expressed in minimum bandwidth modes based on weights or absolute values. Absolute values are defined as bits per second. Weight values are an integer between 1 and 100, where total bandwidth available for a given VNIC is a percentage calculated based on the total of all weights.

Microsoft best practices for software QoS are as follows:

- If using weights, the lowest weight should not be extremely different from the highest weight.
- If using absolute bandwidth, the lowest bandwidth should not be orders of magnitude less than the highest bandwidth.
- Know what type of QoS mode you want to use (relative weight, absolute bandwidth) when you create a switch, as you can't change it.
- You can't migrate VMs between weight-based and absolute bandwidth switches.

Using weights ensures that burst workloads, such as live migration (in this example, the migration of a VM to a different Hyper-V host), can complete as quickly as possible where bandwidth is available. Bandwidth weights prevent available bandwidth limitations from significantly impacting other workloads. When using SCVMM, configuring port profiles control bandwidth weights, linking the port profiles to port classifications and assigning those classifications to VNICs. You can configure VMs to use the appropriate port classification and associated QoS policies in the linked port profile.

You can assign VNICs a specific bandwidth or weight, or you can leave them in a default pool. The default pool, commonly called the default flow, is assigned a specific bandwidth or weight, and the members of the pool share equally in the bandwidth reservation. The default flow configuration is set on the virtual switch using the default flow minimum bandwidth properties (either weight or absolute).

Bandwidth Management with Nutanix

The default minimum bandwidth mode set for virtual switches in the Nutanix environment depends on the version of Foundation used for cluster deployment. Prior to Foundation 4.3.3, the default bandwidth mode is absolute. With Foundation 4.3.3 or higher, the default is weight.

Don't set minimum bandwidth settings for the default VNICs used by the Hyper-V host or the Nutanix CVM. Many environments do not require bandwidth management. However, if you want to manage bandwidth, take the following workloads into account.

Management Traffic

Management traffic supports such network activity as remote desktop, remote PowerShell, domain communications, DNS lookups, and backups. Additionally, if CVM maintenance invokes data path redundancy, Nutanix storage I/O—specifically the SMB 3.0 traffic—occurs across the management network (assuming the backplane network is not configured) until the local CVM is available. In the default Nutanix configuration, management traffic occurs over the ExternalSwitch VNIC assigned to the Hyper-V host. Set any bandwidth reservations for management traffic against this ExternalSwitch VNIC.

SMB Traffic

Hyper-V hosts use SMB shares, presented by the Nutanix CVM, to host vDisks for VM storage. SMB traffic is therefore essential to VM storage performance in Nutanix environments. Under normal operation, the CVM services SMB traffic locally over the internal network using the InternalSwitch VNICs presented to both the Nutanix CVM and the Hyper-V host. Because this traffic occurs across the internal virtual switch, it does not impact the physical network cards except when the Nutanix CVM is offline for maintenance or in the event of a failure. In either of these offline scenarios, SMB traffic uses either the management network as discussed in the Management Traffic section or the backplane network if configured.

Under normal circumstances, no SMB traffic crosses the physical NICs. For QoS purposes, the network handles SMB traffic the same way it handles CVM traffic.

Nutanix CVM Traffic

The Nutanix distributed storage fabric requires connectivity between the CVMs in the cluster to function. This connectivity enables tasks such as synchronously writing I/O across the cluster and Nutanix cluster management. Nutanix data locality helps keep VM read I/O local to each node; however, read traffic may also occur between the CVMs to service VM requests. Additionally, a CVM may have to process remote SMB requests, as discussed in the previous section. All this traffic occurs by default over the CVM's ExternalSwitch VNIC. In environments configured with a backplane network, CVM-to-CVM communication occurs over this network instead.

In the unlikely event that both 10 Gbps adapters are saturated, an administrator can set the external network for each CVM to receive a higher relative bandwidth reservation to ensure storage performance.

Live Migration

Live migration is a burst-type workload that uses no bandwidth until dynamic optimization or an administrator starts a live migration. As such, it is unlikely to have any ongoing impact on the network traffic. In the Nutanix default configuration, live migration traffic uses the ExternalSwitch VNIC of the Hyper-V host.

If you want to apply QoS to live migration traffic, you can configure additional VNICs. The Deployment Models section provides additional information on configuring additional VNICs, including the use of SMB Multichannel. SMB Multichannel for live migration enables traffic to use both 10 Gbps NICs more fully, decreasing the time needed to perform live migrations and increasing the potential bandwidth utilization. Assigning a lower relative bandwidth weight to the live migration VNICs can help limit the performance impact on other applications while live migrations occur.

Virtual Machine Traffic

VM traffic is why we have datacenters in the first place, so this traffic is always important, if not critical. If VM network connectivity slows, it can quickly impact end users and reduce productivity. It is important to ensure that this traffic has a significant share of the available bandwidth during periods of contention.

You can assign VM traffic bandwidth reservations either directly on a per-VNIC basis or using the virtual switch default flow. Assigning every VM NIC the same weight (1, for example) is a possible approach to sharing bandwidth evenly between VMs.

In dynamic environments where you are creating or migrating VMs frequently, assigning bandwidth reservations per VM may make it difficult to maintain balanced reservation settings between hosts. Assigning a weight to the default flow but not to VMs allows VMs to share equally against the default flow minimum bandwidth setting. This common configuration can aid in balancing dynamic environments. If a given VM has a required SLA, you can still set a minimum bandwidth reservation for that specific VM's NICs.

iSCSI Traffic

By default, a Hyper-V configuration doesn't use iSCSI; all storage traffic occurs through SMB 3.0. Nutanix supports using iSCSI through the Nutanix Volumes feature. We do not address iSCSI traffic specifically in this document; see the Nutanix Volumes best practices guide for more detail.

Bandwidth Management Setting Example

Not all environments require network bandwidth reservations for managing their Nutanix clusters. Consider the likely benefit along with the administrative overhead of configuring and managing these settings before making unnecessary modifications. For administrators who wish to apply bandwidth management for the workloads described in the Bandwidth Management with Nutanix section, the following table provides a general example of settings to use when specifying weights.

Table 2: Bandwidth Weights Example

Network Traffic Type	Weight	Native Port Profile
Management traffic	15	Host management
Live migration	20	Live migration
VM traffic (per VM)	1	Low bandwidth adapter

Network Traffic Type	Weight	Native Port Profile
Nutanix CVM	35	Nutanix CVM

Security

Hyper-V offers several network security features, as shown in the following table. You can configure these settings per VNIC using PowerShell or Hyper-V Manager. SCVMM also allows you to modify these security settings through port profiles and classifications. SCVMM offers predefined port profiles, each of which has security-related settings. Each customer environment is unique, so review your security settings with the appropriate resources from your organization's security department. Additionally, some security settings, such as DHCP guard and router guard, may have a slight performance overhead when enabled. Consider this overhead before determining the default security settings for a particular environment.

Table 3: Default Security Settings

Security Option	Default Setting
Allow MAC spoofing	Off
Enable DHCP guard	Off
Allow router guard	Off
Allow guest teaming	Off
Allow IEEE priority tagging	Off
Allow guest-specified IP addresses	Off

5. Deployment Models

As discussed previously, the default Nutanix networking configuration suits most environments without modification, including when you run SCVMM. However, in the following section we outline how customers who want to use SCVMM to manage the networking components directly can do so. Additionally, you can extend the default configuration without SCVMM by using native Hyper-V tools such as PowerShell. The Hyper-V Without SCVMM Network Architecture section describes this option.

Hyper-V with SCVMM Network Architecture

The following figure shows the supported Nutanix architecture where SCVMM directly manages the networking components. This configuration is similar to the default Nutanix configuration that uses a converged network architecture. A single NIC team manages the 10 Gbps network adapters. For SCVMM to manage the environment fully, the NIC team is configured and applied as an uplink port profile. The SCVMM logical switch construct also applies a single external virtual switch. With a logical switch created, you can use SCVMM to add multiple VNICs, including one for live migration traffic. You must name the management VNIC, which represents the network interface registered with the Nutanix cluster, ExternalSwitch. You can use SCVMM port profiles and classifications to apply QoS and security settings to the VNICs.

SCVMM 2016 supports the online conversion of standard switches to logical switches. You must create a logical switch and an uplink port profile that match the existing virtual switch and NIC team settings on Nutanix. For more details on using SCVMM to convert a virtual switch to a logical switch, refer to the Microsoft article Create Logical Switches. We include the full procedures for implementing this supported Nutanix configuration in the appendix.

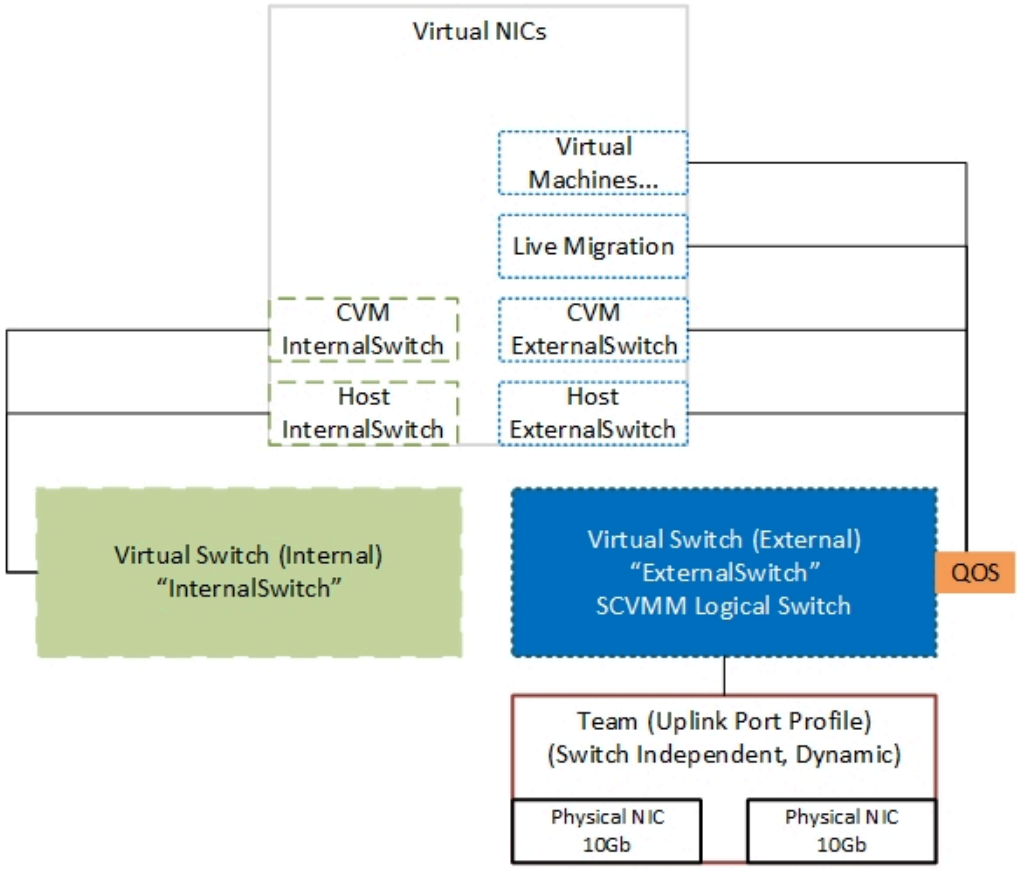


Figure 15: Networking with SCVMM

Features of this SCVMM design include:

- SCVMM logical switch.
- SCVMM uplink port profile for network teaming.
- SCVMM-manageable VNICs for the management OS.
- Separate live migration VNIC for QoS management.
- SMB Multichannel used for live migration.

The following figure relates many of the Hyper-V and SCVMM networking components to each other, with the manually configured items in orange. At the bottom of the diagram are the two 10 Gbps NICs, which connect the Hyper-V host to the physical network. These two NICs use an uplink port profile to the converged logical switch, managed by SCVMM.

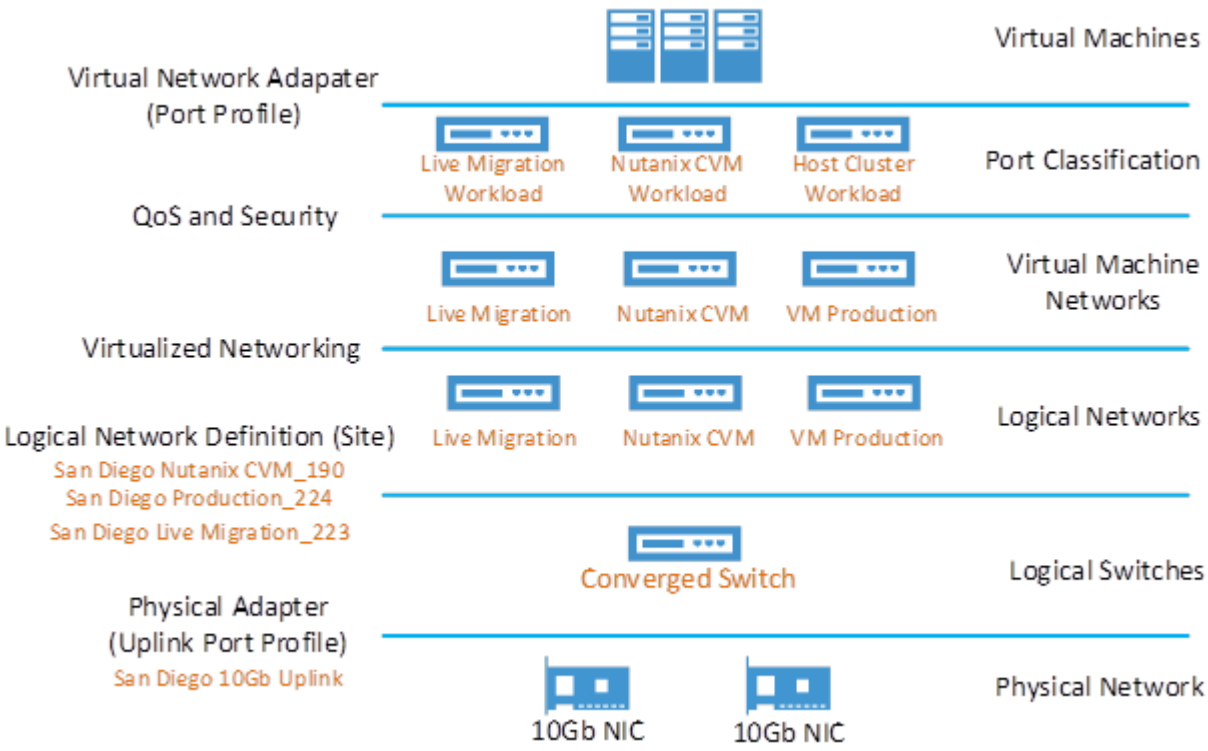


Figure 16: SCVMM Networking Components

Every environment has different logical network requirements, but in this example three logical networks correspond to IP address spaces used for VMs, live migration, and the Nutanix CVMs on top of the logical switch. Each logical network has a corresponding VM network.

To enforce software QoS and security settings, we created three port classifications, one for each of the major workload types: live migration, Nutanix CVM, and general VM production traffic. We then configured all VMs to use the logical switch and the appropriate port classification.

The appendix contains a full step-by-step guide to configuring Hyper-V using SCVMM, QoS, and logical switches.

Hyper-V Without SCVMM Network Architecture

Some customers may not use SCVMM or may use SCVMM but do not need it to fully manage the networking components. Nutanix supports Hyper-V deployments that don't use SCVMM to manage the host networking components directly.

In certain environments, you may want to extend the default configuration to include additional components, either to apply QoS or to isolate specific kinds of network traffic. In this case, PowerShell allows you to customize the deployment. The following figure shows a modification to the default Nutanix configuration. This modification creates additional VNICs for a live migration network so you can apply bandwidth QoS to that workload. The user does not need to do any additional virtual switch or network teaming configuration. The appendix provides the steps for configuring this setup.

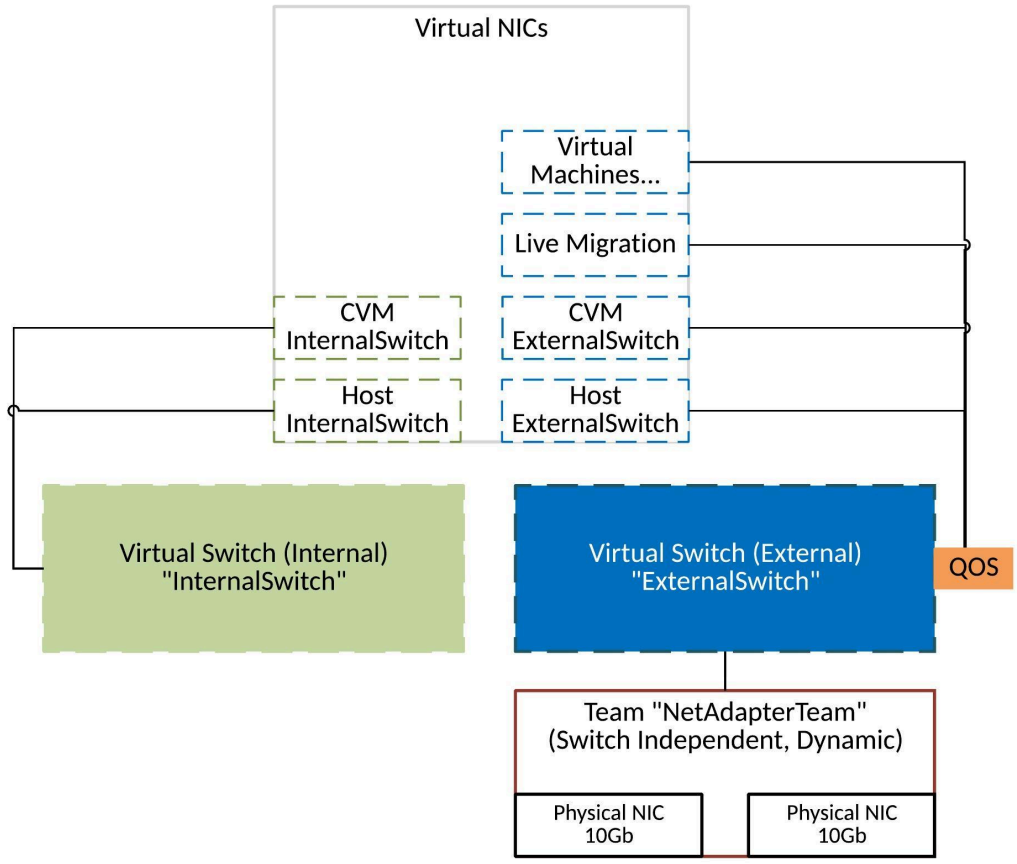


Figure 17: Default Nutanix Configuration with Additional VNICs

Features of this Hyper-V-only design include:

- Default Nutanix network team.
- Default Nutanix virtual switch (standard switch from SCVMM perspective).
- Default Nutanix VNICs.
- Additional VNICs for live migration traffic.
- SMB Multichannel used for live migration.
- QoS configured using PowerShell.

6. Architectural Summary

The following table summarizes the Nutanix default settings for several Hyper-V and Server 2016 technologies.

Table 4: Feature Summary

Feature	Hyper-V Hosts 10 Gbps	1 Gbps	Guest VM
Large send offload	Enabled (Default)	N/A	N/A
Receive-side scaling (RSS)	Disabled (Default)	N/A	N/A
Virtual receive-side scaling (vRSS)	N/A	N/A	VMs with >4 CPUs and high throughput requirements
VMQ	Enabled (Default)	N/A	Enabled (Default)
NIC teaming	Enabled (Default)	N/A	N/A
Jumbo frames	Disabled (Default)		
Host management	Enabled (Default)	N/A	N/A

7. Conclusion

In this best practices guide we described Hyper-V networking concepts and how to use them in a Nutanix environment to ensure optimal performance and availability. We also provided two alternative solutions beyond the default Nutanix configuration. One option allows SCVMM to control the host networking components; the other is a slightly modified extension to the Nutanix default configuration. Nutanix fully supports both deployment options.

Continue the conversation on the Nutanix NEXT online community. For more information on Microsoft Hyper-V or to review other Nutanix documents, visit the Nutanix Support Portal.

Appendix

Configuring an Environment with SCVMM, QoS, and Logical Switches

This section walks through best practices for configuring an environment with SCVMM, QoS, and logical switches. We assume you followed the applicable Nutanix Acropolis setup guide.

Create Logical Networks and IP Pools in SCVMM

- Disable automatic creation of logical networks after installing SCVMM and prior to adding Hyper-V hosts. In SCVMM, go to Settings > General > Network Settings. Clear the box as shown in the following figure.

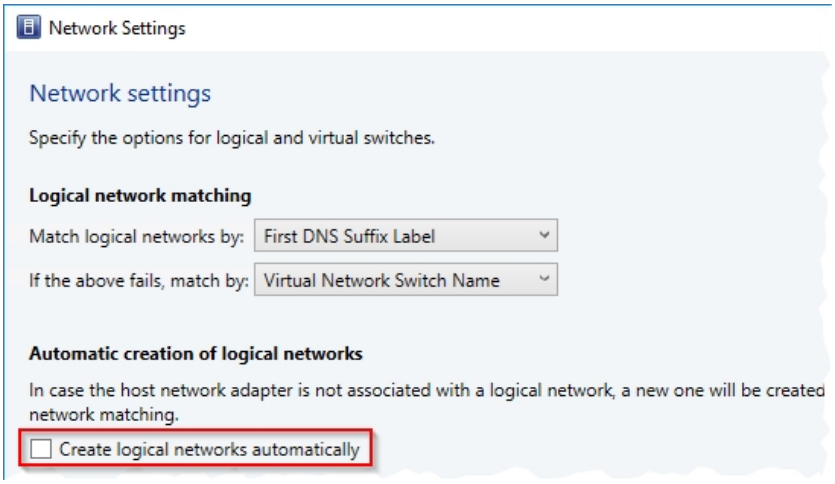


Figure 18: Network Settings

- In SCVMM, create a logical network using an appropriate description, such as VM Production.

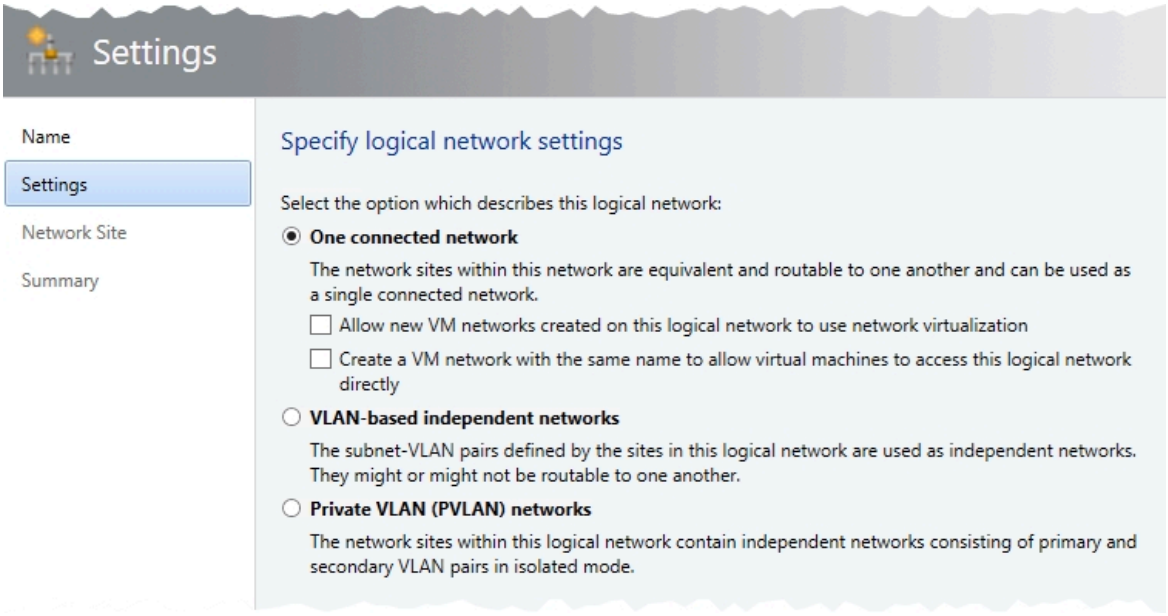


Figure 19: Create Logical Network

- Configure network sites as appropriate by adding VLANs and IP addresses. In this example, we are creating the production VM network; use the applicable settings for your environment.

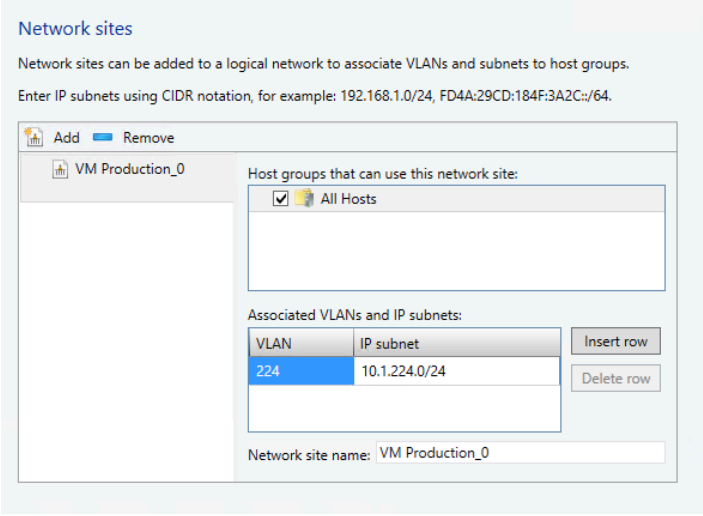


Figure 20: Network Sites

- Repeat the process for a logical network called Live Migration, using the applicable VLAN and IP subnet.
- Repeat the process for a logical network called Nutanix, using the applicable VLAN and IP subnet.
- Under Logical Networks, right-click your VM production network and select Create IP Pool. Enter a name and select the logical network.

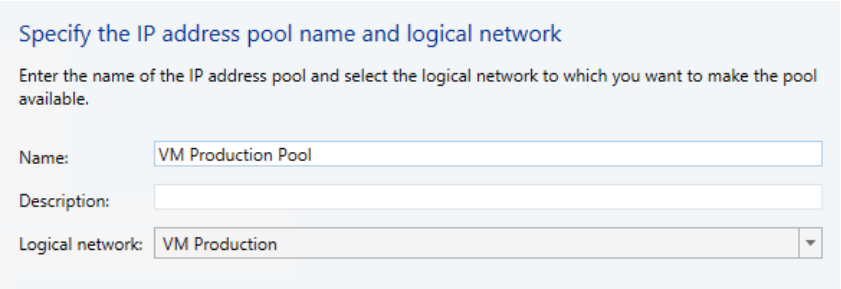


Figure 21: Specify IP Address Pool Name and Logical Network

- Select the appropriate network site and IP subnets.

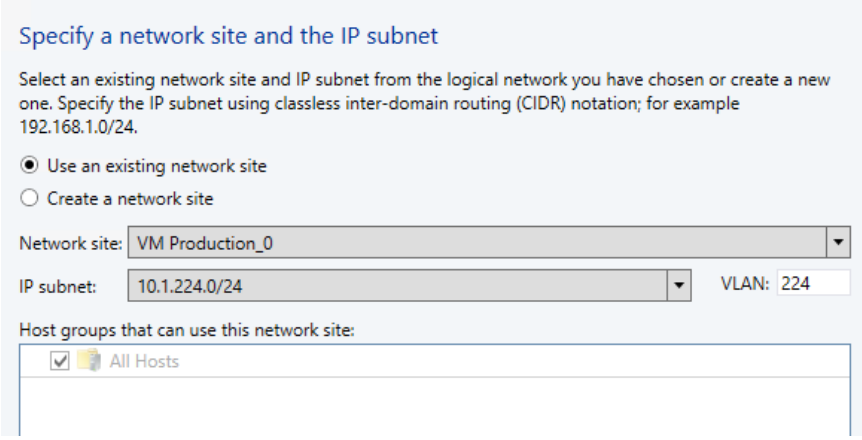


Figure 22: Specify Network Site and IP Subnet

- Go through the rest of the wizard and provide network details as needed.
- Create an IP pool for the live migration logical network as well. Do not create an IP pool for the Nutanix CVM logical network.
- After you create all three networks, the results should resemble the following figure.

Name	Network Complian...	Subnet
VM Production	Fully compliant	
VM Production Pool	Fully compliant	10.1.224.0/24
Nutanix	Fully compliant	
Live Migration	Fully compliant	
Live Migration Pool	Fully compliant	192.168.11.0/24

Figure 23: Results of Creating All Three Networks

Create VM Networks

- Navigate to VMs and Services. Create VM networks to match each logical network you just created.

Tip: You could have created these networks when you created the logical network if you selected the Create a VM network with the same name... option.

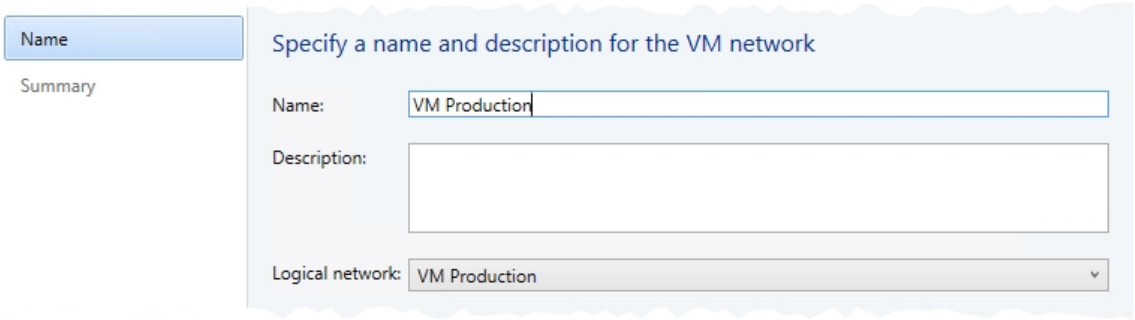


Figure 24: Create VM Network Wizard

- After you have created all VM networks, your screen should resemble the following figure.

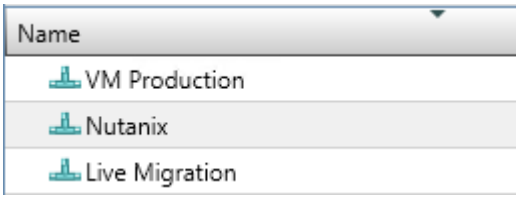


Figure 25: Results of VM Network Creation

Create Port Profiles

- In SCVMM, navigate to Fabric > Port Profiles and create an uplink port profile for the two 10 Gbps NICs. Select Dynamic load balancing and Switch Independent teaming mode.

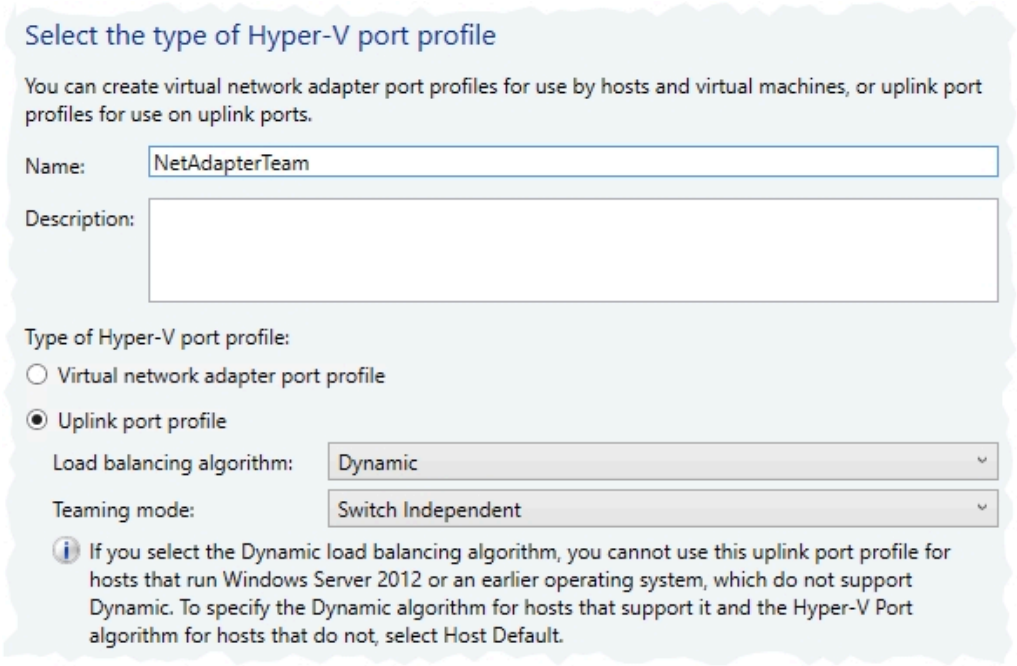


Figure 26: Select Uplink Port Profile

- Select all networks that should use the 10 Gbps NICs. In this case, select all three networks.

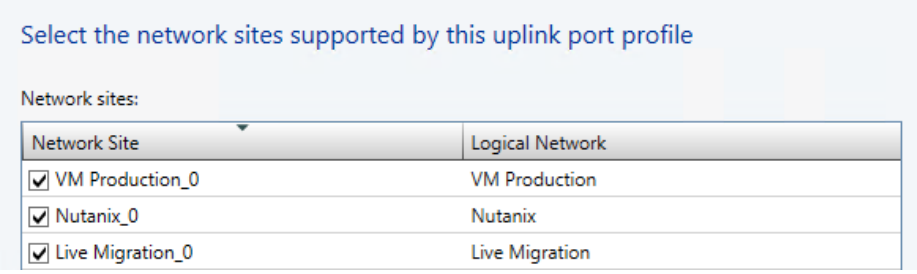


Figure 27: Select Networks for Uplink Port Profile

- Create a new virtual network adapter port profile called Nutanix CVM.

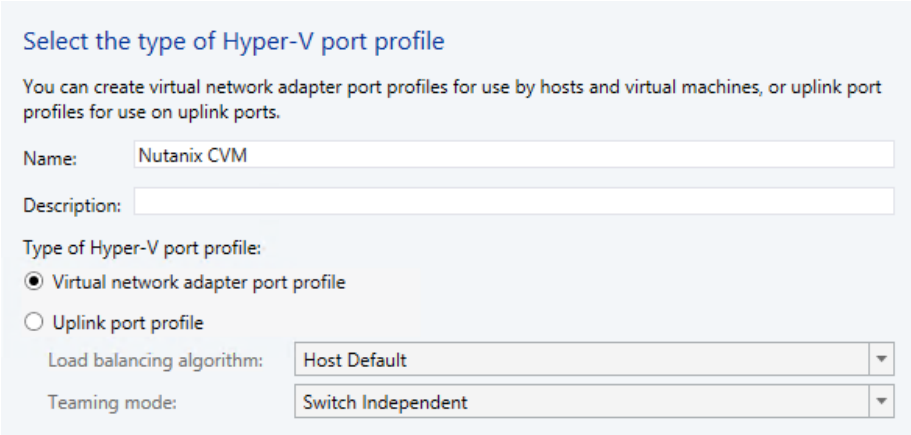


Figure 28: Create Virtual Network Adapter Port Profile

- Enable VMQ and configure the minimum bandwidth as desired. The conversion to logical switch with SCVMM 2016 sets the Nutanix ExternalSwitch to use the Absolute minimum bandwidth mode.
- Modify the existing live migration port profile bandwidth setting and change the minimum bandwidth as desired.
- Modify the host management profile and change the bandwidth as desired.

Create the Logical Switch

- In the Fabric pane, navigate to Logical Switches and create a new logical switch. Enter ExternalSwitch as the name to match the existing ExternalSwitch virtual switch.
- Choose uplink mode Team. Choose Absolute as the minimum bandwidth mode. Leave the default extensions.
- Add the appropriate virtual ports and include port classifications, to be associated with virtual network adapter port profiles as needed.

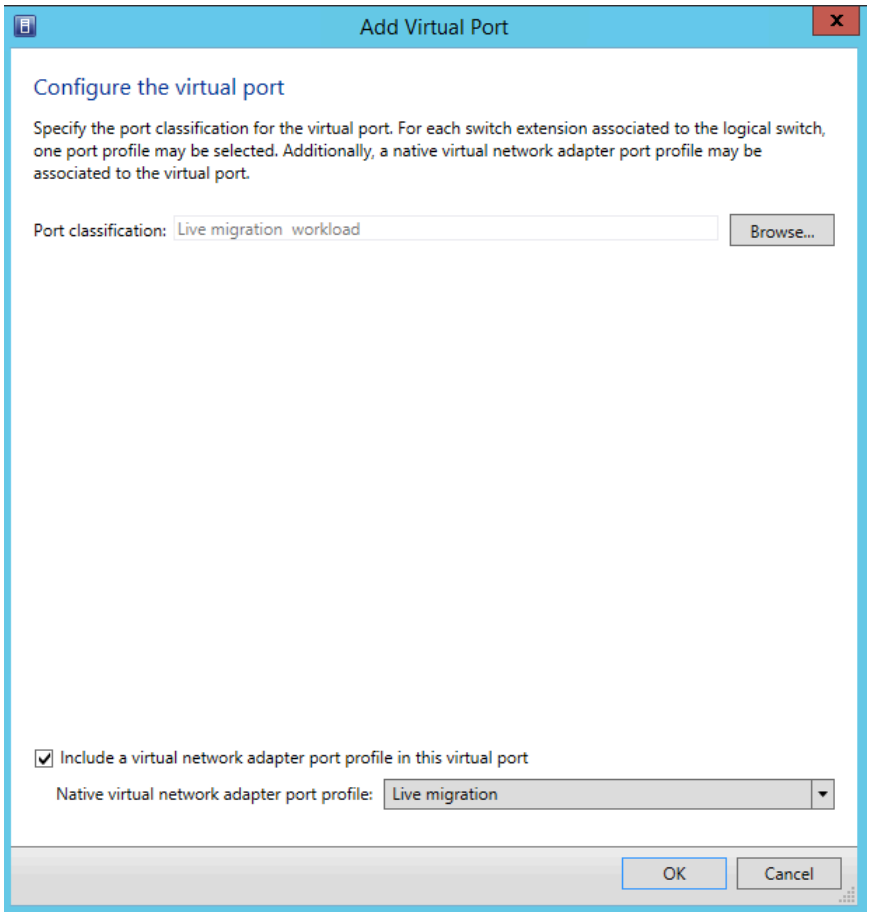


Figure 29: Configure the Virtual Port

- Add the uplink port profile NetAdapterTeam to the logical switch.

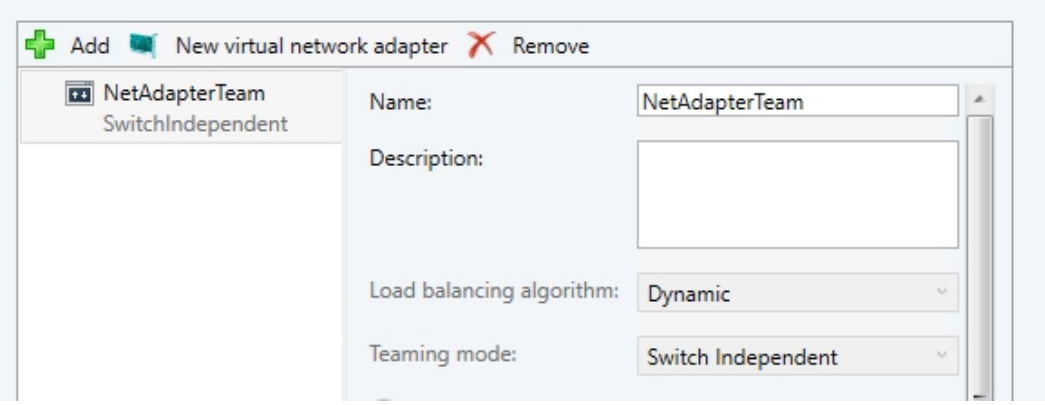


Figure 30: Add Team to Logical Switch

Convert the Standard Switch to a Logical Switch

- Navigate to the properties of a cluster node in SCVMM.
- Click Virtual Switches.
- Click ExternalSwitch, then click Convert to Logical Switch.

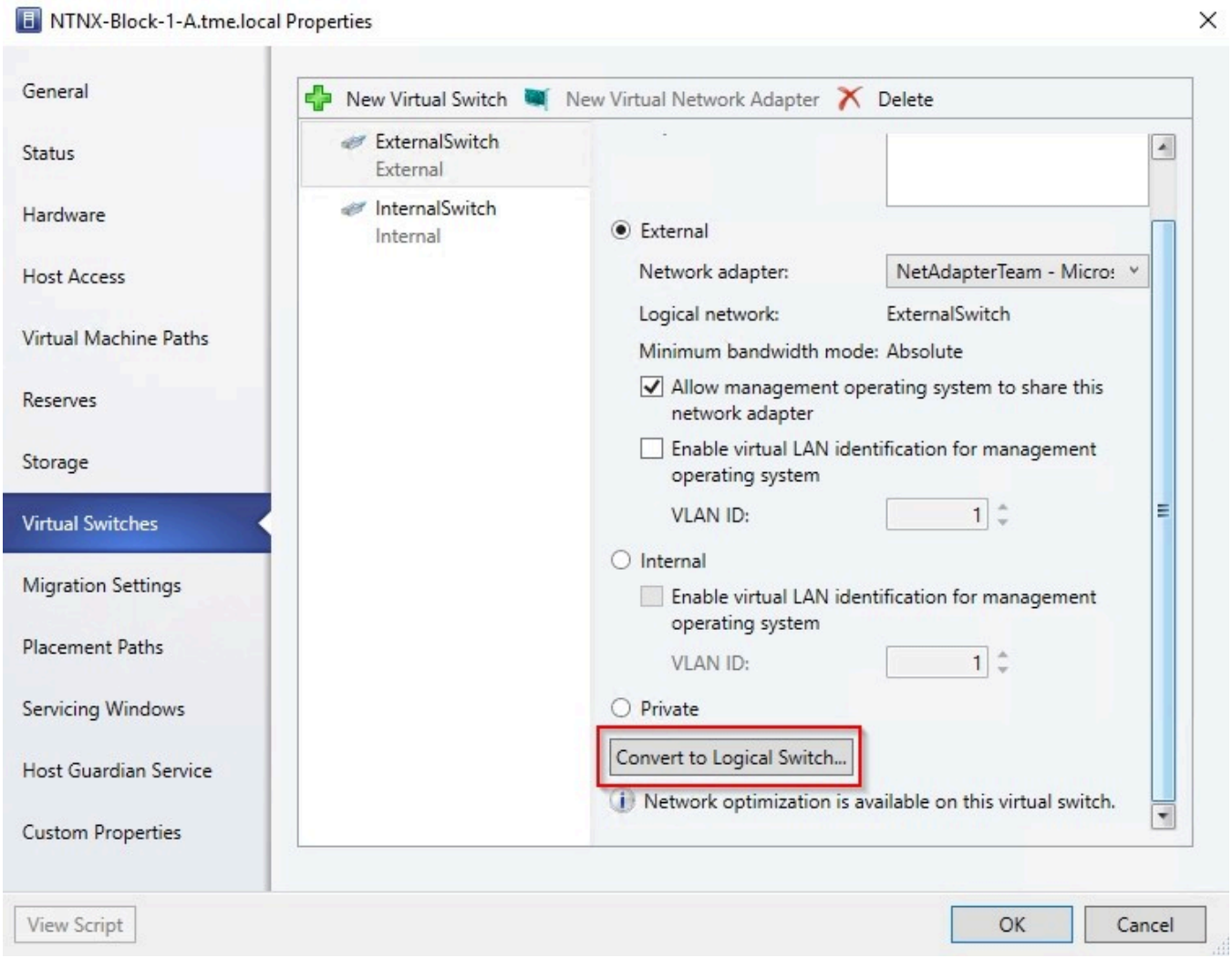


Figure 31: Convert to Logical Switch

- Select the ExternalSwitch logical switch and the NetAdapterTeam uplink port profile, then click Convert.

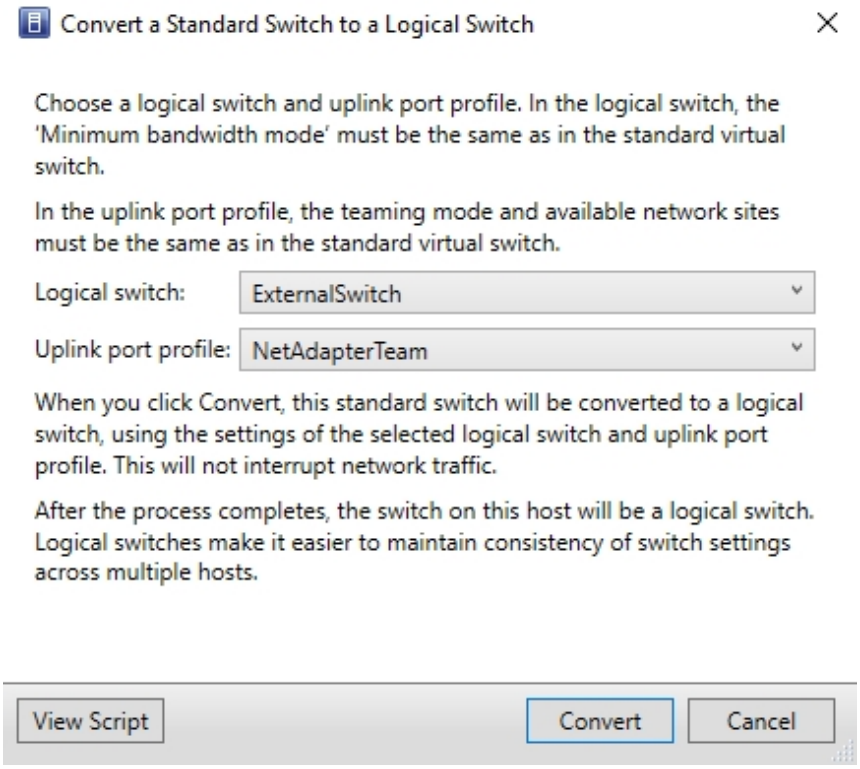


Figure 32: Logical Switch and Uplink Selection

- The process completes in a few seconds and does not disrupt the environment.
- Repeat the conversion on each node.

Add the Live Migration Network

- Click New Virtual Network Adapter and add a VNIC for the live migration network. Select the live migration workload classification and configure the IP address information as appropriate for your environment. The following figure shows an example using automated SCVMM IP addressing.

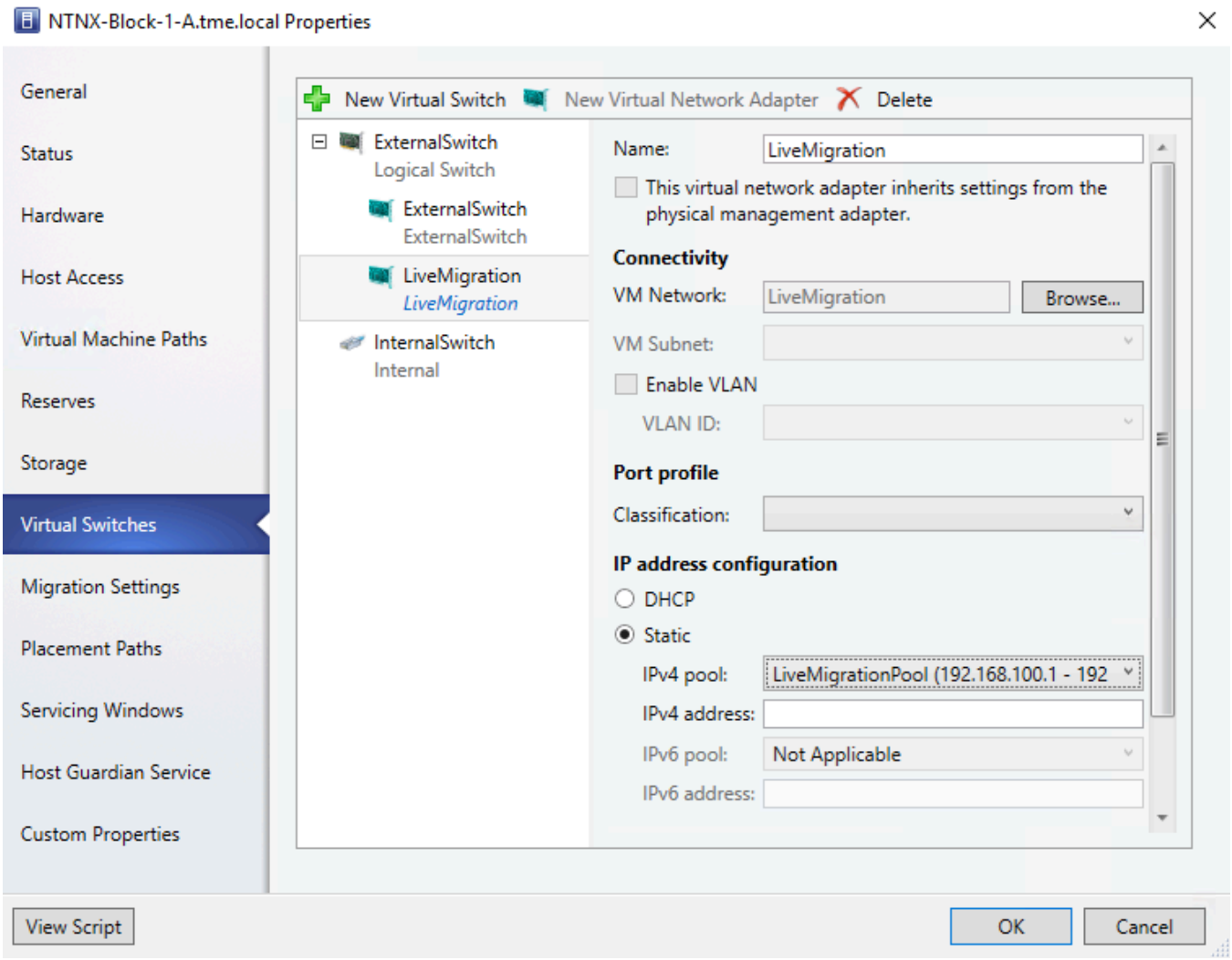


Figure 33: Live Migration Adapter

- Add the Live Migration adapter on the remaining Hyper-V hosts.

Configure Live Migration with SCVMM

- In SCVMM, open the properties of the first Nutanix node. Go to the virtual switches and note both of the live migration IP addresses SCVMM assigned. Navigate to the Migration Settings pane and configure the options as shown in the following figure. Change the performance option to Use SMB as transport, then enter the live migration IP addresses you previously noted.

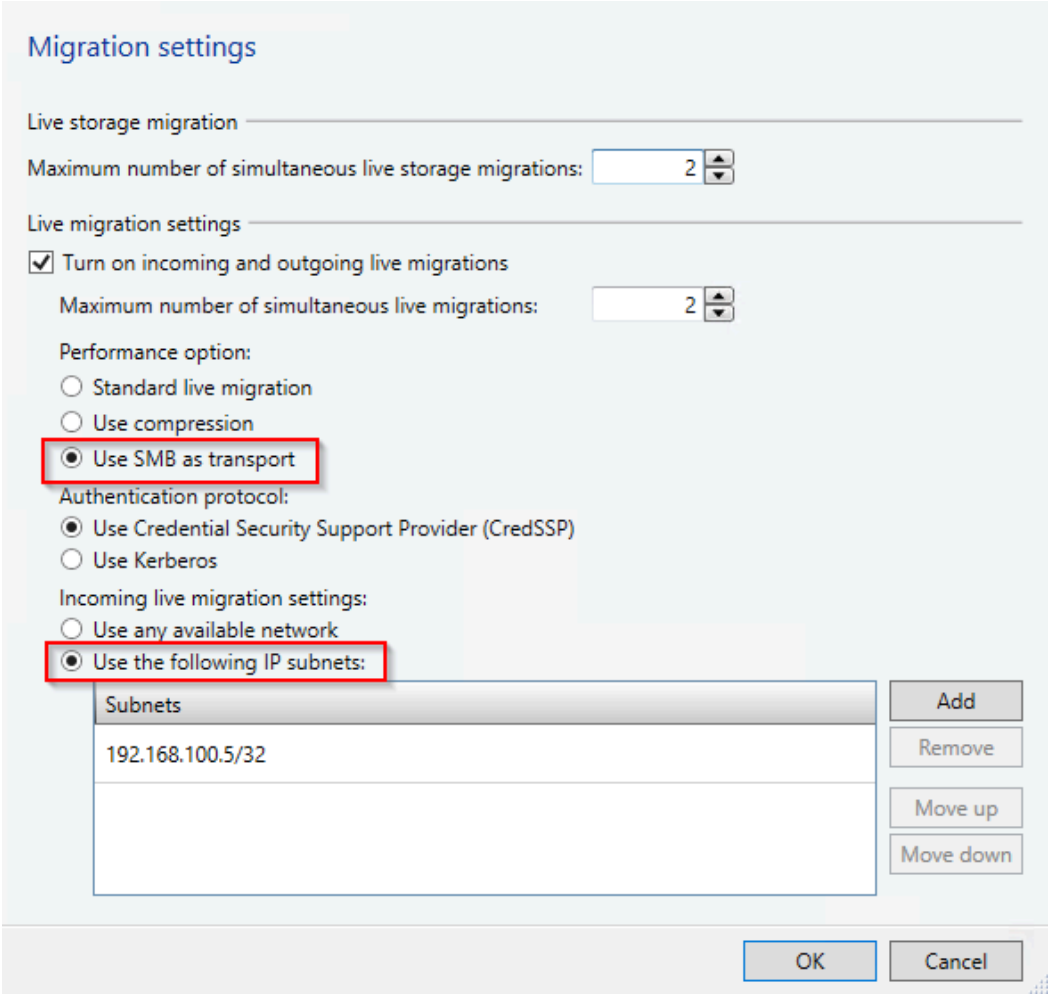


Figure 34: Migration Settings

- Repeat the previous step on all other Nutanix nodes.
- Open the Failover Cluster Manager. Review the various networks and locate the one with the live migration subnet (probably Cluster Network 3). In the right pane, click Live Migration Settings and check only the one network associated with the live migration subnet.

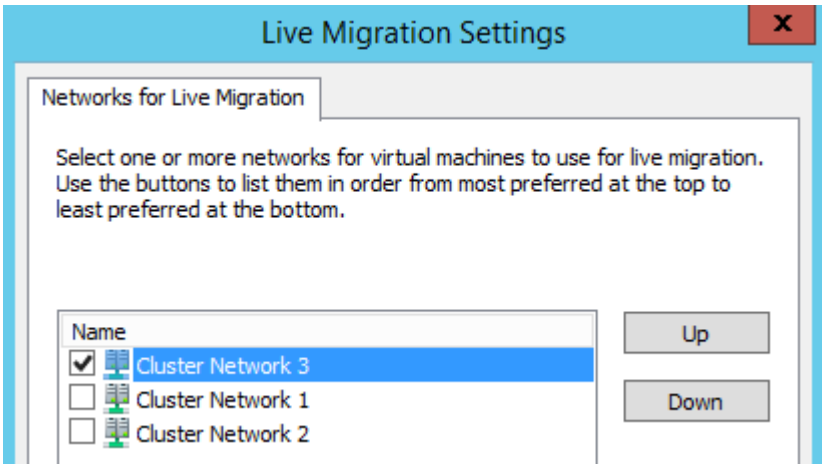


Figure 35: Live Migration Settings

Configure Cluster Networks

- Locate the live migration cluster network and rename it Migration_Network.
- Locate the cluster network with subnet 192.168.5.0 and rename the network Nutanix_CVM.
- Locate the cluster network associated with the management subnet and rename it Management_Network. The names should then look like the following figure.

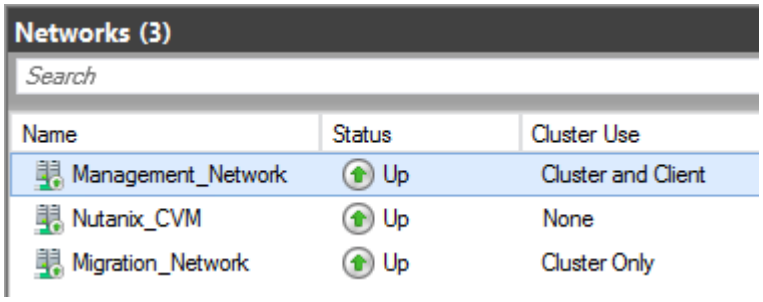


Figure 36: Configure Cluster Networks

- Open a PowerShell window and enter the following commands:

```
(Get-ClusterNetwork -Name "Management_Network").Role = 3
(Get-ClusterNetwork -Name "Migration_Network").Role = 1
(Get-ClusterNetwork -Name "Nutanix_CVM").Role = 0
```


Note: The roles specified above map to the capabilities in the following table.

Table 5: Cluster Network Capabilities

Name	Value	Description
Disabled for cluster communication	0	No cluster communication sent over this network.
Enabled for cluster communication only	1	Internal cluster communication can be sent over this network, including live migration.
Enabled for client and cluster communication	3	External clients can use this network to connect to the server. Cluster communication can also occur over this network.

Modifying the Default Nutanix Configuration Without SCVMM

This section walks you through modifying the default Nutanix configuration without using SCVMM. You can use the default configuration created during the Nutanix installation process as it is, but if you want to add SMB Multichannel to enhance live migration performance and enable QoS, perform the following steps. This process assumes you followed the applicable Nutanix Acropolis setup guide and configured a specific VLAN for the live migration traffic.

The default minimum bandwidth mode for virtual switches in the Nutanix environment is Absolute. Therefore, you must specify the minimum bandwidth settings for the VNICs created in this section in absolute values, such as MB or GB per second, rather than in weights as outlined in the previous sections. You also have the option to set a maximum bandwidth.

Note: We intend these bandwidth numbers as examples only; modify them to suit your specific environment.

Create Live Migration VNIC

- From PowerShell on all hosts:

```
Add-VMNetworkAdapter -ManagementOS -Name "Live Migration" -SwitchName
 "ExternalSwitch"
```


Set VLANs for the Live Migration VNIC

- From PowerShell on all hosts:

```
Set-VMNetworkAdapterVlan -ManagementOS -VMNetworkAdapterName "Live Migration" -
Access -VlanId xxx
```

Set Live Migration Bandwidth Minimum and Maximum Values

- From PowerShell on all hosts:

```
Set-VMNetworkAdapter -ManagementOS -Name "Live Migration" -
MinimumBandwidthAbsolute=1GB
```

Set the Bandwidth Minimum for the Default Flow

- From PowerShell on all hosts:

```
Set-VMSwitch ExternalSwitch -DefaultFlowMinimumBandwidthAbsolute 3GB
```

Set the Bandwidth Minimum for the Nutanix CVM External Adapter

- From PowerShell on all hosts:

```
$localcvm=get-vm | where Name -like "NTNX*" | Get-VMNetworkAdapter | where Name -
eq "External" | Set-VMNetworkAdapter -MinimumBandwidthAbsolute 4GB
```

Set the IP Addresses for the Live Migration VNICs

- From PowerShell, on all hosts (replace with unique IP addresses for each host):

```
new-netipaddress -interfacealias "vEthernet (Live Migration)" -IPAddress 10.0.0.1
 -PrefixLength "24"
```

Configure Live Migration Without SCVMM

- From PowerShell, on all hosts, set the live migration performance option to SMB:

```
Set-VMHost -VirtualMachineMigrationPerformanceOption SMB
```

- Open the Failover Cluster Manager. Review the various networks and locate the one with the live migration subnet (probably Cluster Network 3). In the right pane, click Live Migration Settings and only check the one network associated with the live migration subnet.

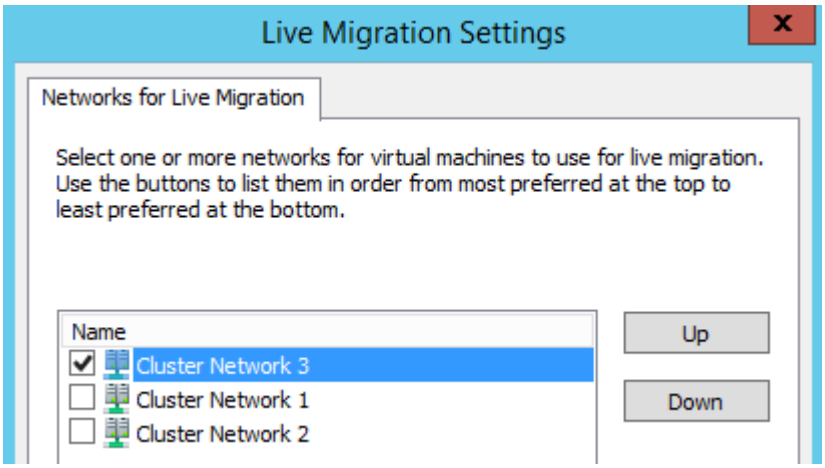


Figure 37: Live Migration Settings in the Failover Cluster Manager

Set Up Cluster Networks

See the instructions in the section Configure Cluster Networks.

References

1. Nutanix Hyper-V Administration Guide
2. Windows Server 2016 NIC and Switch Embedded Teaming User Guide
3. Event ID 106 when a Hyper-V virtual switch is bound to an LBFO team
4. Create Logical Switches
5. Nutanix Volumes best practices guide

About Nutanix

Nutanix makes infrastructure invisible, elevating IT to focus on the applications and services that power their business. The Nutanix enterprise cloud software leverages web-scale engineering and consumer-grade design to natively converge compute, virtualization, and storage into a resilient, software-defined solution with rich machine intelligence. The result is predictable performance, cloud-like infrastructure consumption, robust security, and seamless application mobility for a broad range of enterprise applications. Learn more at www.nutanix.com or follow us on Twitter @nutanix.

List of Figures

List of Tables