NetApp Verified Architecture

FlexPod Datacenter with Microsoft Hyper-V 2025 & NetApp Shift Toolkit

NVA deployment

Ruchika Lahoti, NetApp

June 2025 | NVA-1180-DEPLOY

In partnership with

Abstract

This document describes the design and implementation of FlexPod® data center solution with Microsoft Hyper-V 2025. This document primarily focuses on deploying Hyper-V failover Cluster on FlexPod® data center using iSCSI protocol and migrating VM from vCenter to Microsoft Hyper-V using NetApp Shift.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Solution Overview

It is important that a data center solution embraces technology advancement in various areas, such as compute, network, and storage technologies to address rapidly changing requirements and challenges of IT organizations. The current industry trend in datacenter design is towards shared infrastructures. By using virtualization along with pre-validated IT platforms, enterprise customers have embarked on the journey to the cloud by moving away from application silos and toward shared infrastructure that can be quickly deployed, thereby increasing agility, and reducing costs.

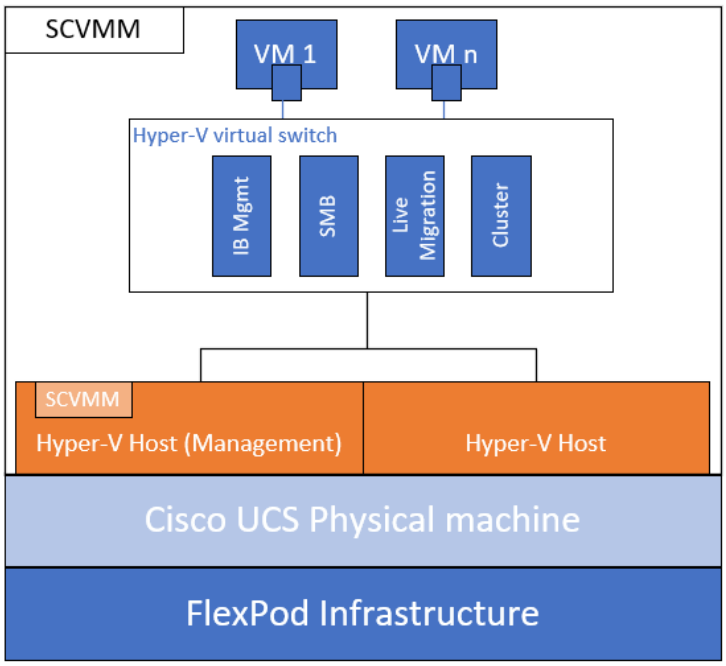
FlexPod® with Microsoft Hyper-V is a comprehensive and integrated IT architecture that combines the strengths of Cisco's Unified Computing System (UCS), NetApp storage, Cisco Nexus Switch and Microsoft's Hyper-V hypervisor to deliver a flexible, scalable, and efficient data center solution. The integration of Hyper-V virtualization enables organizations to maximize resource utilization, improve hardware efficiency, and ensure high availability with features like live migration and failover. The architecture is designed to support diverse workloads, including virtualized applications, databases, and web services, providing high-performance computing, storage, and networking capabilities within a unified platform.

By integrating System Center Virtual Machine Manager (SCVMM), organizations can streamline operations, automate workload management, and enhance overall efficiency while reducing operational costs. SCVMM provides centralized orchestration of virtual machine deployments, network policies, storage classification, and fabric resource pooling across Hyper-V hosts, bringing policy-driven control and simplified infrastructure lifecycle management.

This solution incorporates NetApp Shift Toolkit®, which facilitates cross-platform virtual machine migration. Shift works by replicating VMs, transforming configuration formats, and aligning the virtual hardware with Hyper-V-compatible profiles, all while ensuring data consistency and minimizing downtime. Together, FlexPod® with Hyper-V and NetApp Shift Toolkit delivers a robust, enterprise-ready foundation for next-generation data centers—capable of supporting both current workloads and future cloud integration strategies.

Figure 1 illustrates a generic architecture of FlexPod® with Microsoft Hyper-V®, comprising two hosts configured in a failover cluster to support high availability for multiple virtual machines (VMs). One of the host is designated as the management node, where the SCVMM virtual machine is deployed. A virtual switch has been created on this, hosting multiple logical networks for VM communication and services.

Figure 1) Generic Illustration of FlexPod with Microsoft Hyper-V



Audience

The audience for this document includes, but is not limited to sales engineers, field consultants, professional services, IT managers, partner engineers, and customers. It aims to provide insights into leveraging an infrastructure designed to enhance IT efficiency and foster IT innovation, particularly through the use of Microsoft Hyper-V technology.

Solution Topology

FlexPod® is a defined set of hardware and software that serves as an integrated foundation for both virtualized and non-virtualized solutions. Microsoft Hyper-V built on FlexPod includes NetApp AFF solution, Cisco Nexus networking, Cisco Unified Computing System, and Microsoft Hyper-V software in a single package. The design is flexible enough that the networking, computing, and storage resources can fit in one datacenter rack or be deployed according to a customer's datacenter design.

FlexPod Datacenter with Cisco UCS X-Series supports both IP and Fibre Channel (FC)—based storage access design. This document covers the IP-based solution using Cisco UCS M7 servers. For this solution, iSCSI configuration on Cisco UCS and NetApp AFF C250 is utilized to set up boot from SAN for Hyper-V hosts. The physical connectivity details for IP-based design are explained below.

Figure 2 shows the FlexPod components and the network connections for a configuration with Cisco UCS 6536 Fabric Interconnects. This design can support end to end 100-Gbps Ethernet connections between the NetApp AFF C250 storage array and Cisco UCS X210c M7 compute nodes. Each of the components can be scaled easily to support specific business requirements.

The reference hardware configuration includes:

- One Cisco UCSX-9508 blade chassis with Cisco UCS 9108 25G IFM modules

- Two Cisco UCS X210c M7 compute nodes with the Cisco UCS VIC 15231
- One Cisco UCS X210c M6 compute nodes with the Cisco UCS VIC 15231
- Two Cisco UCS 6536 Fabric Interconnects
- Two Cisco Nexus 9336C-FX2 Switches
- One NetApp AFF C250 (high-availability pair)

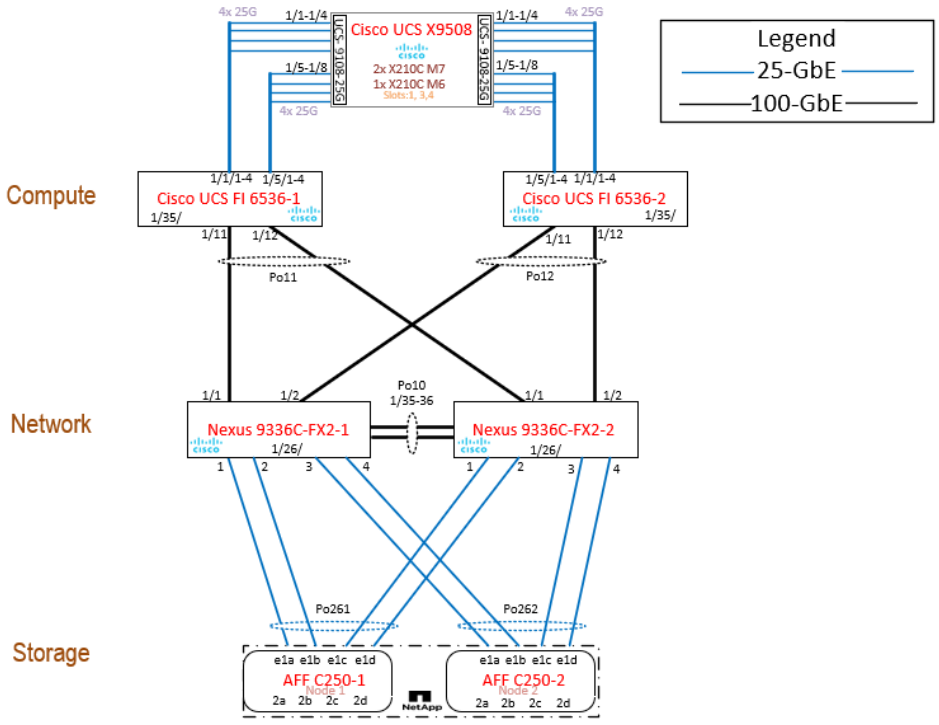


Figure 2) FlexPod Datacenter Physical Topology

To validate the IP-based storage access in this FlexPod configuration, the components are set up as follows:

- Cisco UCS 6536 Fabric Interconnects provide chassis and network connectivity.
- The Cisco UCS X9508 Chassis connects to fabric interconnects using Cisco UCSX-I-9108-25G intelligent fabric modules (IFMs), where eight 25 Gigabit Ethernet ports are used on each IFM to connect to the appropriate FI.
- 2 Cisco UCSX-210c M7 Compute Nodes and 1 Cisco UCSX-210c M6 Compute Nodes contain fifth-generation Cisco 15231 virtual interface cards (VICs) which are used for 100Gbps connectivity on each side of fabric interconnect.
- Cisco Nexus 9336C-FX2 Switches in Cisco NX-OS mode provide the switching fabric. Cisco UCS 6536 Fabric Interconnect 100-Gigabit Ethernet uplink ports connect to Cisco Nexus 9336C-FX2 Switches in a Virtual Port Channel (vPC) configuration.
- The NetApp AFF C250 controllers connect to the Cisco Nexus 9336C-FX2 Switches using four 25 GE ports from each controller configured as an interface group.
- Microsoft Hyper-V is installed on Cisco UCS X210c M7 Compute nodes.
- VMware ESXi is installed on Cisco UCS X210c M6 compute node.

Solution Components

This section describes the components that were used and validated in this solution.

NetApp AFF C250

The NetApp® AFF C250 is an entry-level small form-factor capacity flash model designed for environments that demand space-efficient, high-capacity storage. As part of the NetApp C-Series, it is primarily optimized for capacity, making it ideal for organizations seeking cost-effective flash performance at scale. The 2U dual-controller system supports 24 internal drives for space efficient deployment. The NetApp AFF C250 offers scale-out performance, storage expansion, flexibility in network connectivity, and a rich set of data management and data protection capabilities powered by NetApp ONTAP software.

The NetApp AFF C250 offers both 25 GbE and 100 GbE Ethernet connectivity as well as 32Gb FC connectivity for deploying reliable Ethernet and FC solutions. By adding external NVMe expansion shelves for additional NVMe QLC SSD, the platform is capable of meeting the substantial capacity needs of the data centers.

Key Features:

- High-Density NVMe Technology: Built on high-density NVMe capacity flash technology, the AFF C250 delivers enhanced performance and efficiency.
- Unified Storage: Supports block, file, and object workloads, allowing seamless consolidation and management of diverse data types.
- Scalability: Offers a maximum effective capacity of up to 71PB.
- Energy Efficiency: Compared to hybrid flash storage, the AFF C250 can reduce the storage footprint by up to 99% and energy consumption by up to 97%, contributing to a more sustainable data center.
- Data Protection: Delivers integrated protection with NetApp Snapshot™, SnapMirror®, and SnapVault® technologies, along with AI/ML-powered real-time ransomware detection to proactively safeguard critical data and ensure business continuity.

For more information about the NetApp AFF C series, refer https://www.netapp.com/data-storage/aff-c-series/ , https://www.netapp.com/pdf.html?item=/media/115943-na-1043-asa-aff-datasheet.pdf&v=2024103171

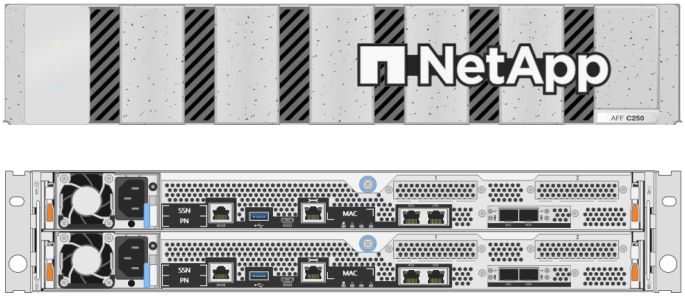


Figure 3) AFF C250 front and rear view

Cisco UCS X9508 Chassis

The Cisco UCS X-Series Modular System begins with the Cisco UCS X9508 Chassis, engineered to be adaptable and future-ready. The X-Series is a standards-based open system designed to be deployed and automated quickly in a hybrid cloud environment. With a midplane-free design, I/O connectivity for the X9508 Chassis is accomplished with front-loading vertically oriented computing nodes that intersect with horizontally oriented I/O connectivity modules in the rear of the chassis. Cisco UCS X-Series is powered by Cisco Intersight, making it simple to deploy and manage at scale.

The Cisco UCS X9508 Chassis provides these features and benefits:

- The Seven-Rack-Unit (7RU) chassis has eight front-facing flexible slots. These can house a combination of computing nodes and a pool of future I/O resources, which may include Graphics Processing Unit (GPU) accelerators, disk storage, and non-volatile memory.
- X9508 Chassis supports two types of Intelligent Fabric Modules (IFMs). One is 9108 25G IFM and the other is 9108 100G IFM.
  - The 100G IFM has eight 100G ports and it provides up to 200 Gbps of unified fabric connectivity per computing node.
  - The 25G IFM has eight 25G ports and it provides up to 100 Gbps of unified fabric connectivity per computing node
- At the bottom of the chassis are slots ready to house future I/O modules that can flexibly connect the computing modules with I/O devices.
- Six 2800W Power Supply Units (PSUs) provide 54V power to the chassis with N, N+1, and N+N redundancy. A higher voltage allows efficient power delivery with less copper and reduced power loss.
- Efficient, 4x100mm, dual counter-rotating fans deliver industry-leading airflow and power efficiency.

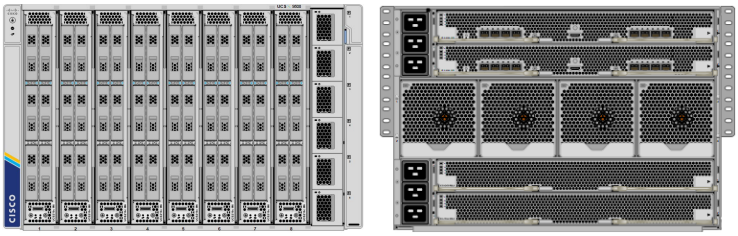


Figure 4) Cisco UCS X9508 Chassis Front and Back view

Cisco UCSX-I-9108 25G Intelligent Fabric Module

For the Cisco UCS X9508 Chassis, the network connectivity is provided by a pair of Cisco UCSX 9108-25G Intelligent Fabric Modules (IFMs). IFMs also host the Chassis Management Controller (CMC) for chassis management. In contrast to systems with fixed networking components, Cisco UCS X9508's midplane-free design enables easy upgrades to new networking technologies as they emerge making it straightforward to accommodate new network speeds or technologies in the future.

Figure 5) Cisco UCSX-I-9108 25G Intelligent Fabric Module

Each IFM supports eight 25Gb uplink ports for connecting the Cisco UCS X9508 Chassis to the FIs and 32 25Gb server ports for the eight compute nodes. IFM server ports can provide up to 200 Gbps of unified fabric connectivity per compute node across the two IFMs. The uplink ports connect the chassis to the UCS FIs, providing up to 400Gbps connectivity across the two IFMs.

Cisco UCS X210c M7 Compute Node

The Cisco UCS X9508 Chassis is designed to host up to 8 Cisco UCS X210c M7 Compute Nodes. The front view of Cisco UCS X210c M7 Compute Node is shown in the below Figure 6.

Figure 6) Cisco UCS X210c M7 Compute Node

The Cisco UCS X210c M7 features:

- **CPU:** Up to 2x 5th Gen or 4th Gen Intel Xeon Scalable Processors with up to 64 cores per processor and up to 320 MB of Level 3 cache per CPU.
- **Memory:** Up to 8TB of main memory with 32x 256 GB DDR5 5600 MT/s or DDR5 4800 MT/s DIMMs depending on the CPU installed.
- **Disk storage:** Up to 6 SAS or SATA drives or NVMe drives can be configured with the choice of an internal RAID controller or passthrough controllers. Two M.2 memory cards can be added to the Compute Node with optional hardware RAID.
- **GPUs:** The optional front mezzanine GPU module allows support for up to two HHHL GPUs. Adding a mezzanine card and a Cisco UCS X440p PCIe Node allows up to four more GPUs to be supported with a Cisco UCS X210c M7.
- **Virtual Interface Card (VIC):** Up to 2 VICs including an mLOM Cisco UCS VIC 15231 or an mLOM Cisco UCS VIC 15420 and a mezzanine Cisco UCS VIC card 15422 can be installed in a Compute Node.
- **Security:** The server supports an optional Trusted Platform Module (TPM). Additional security features include a secure boot FPGA and ACT2 anticounterfeit provisions.

Cisco UCS X210c M6 Compute Node

The Cisco UCS X9508 Chassis is designed to host up to eight Cisco UCS X210c M6 Compute Nodes, offering a high-density modular architecture. The front view of the Cisco UCS X210c M6 Compute Node is shown in Figure 6.

Figure 7) Cisco UCS X210c M6 Compute Node

The Cisco UCS X210c M6 features:

- **CPU:** Up to 2x 3rd Gen Intel® Xeon® Scalable Processors with up to 40 cores per processor and 1.5 MB Level 3 cache per core
- **Memory:** Up to 32x 256 GB DDR4-3200 DIMMs for up to 8 TB of main memory. Configuring up to 16x 512-GB Intel Optane™ persistent memory DIMMs can yield up to 12 TB of memory.
- **Storage:** Up to 6 hot-pluggable, Solid-State Drives (SSDs), or Non-volatile Memory Express (NVMe) 2.5-inch drives with a choice of enterprise-class Redundant Array of Independent Disks (RAIDs) or pass-through controllers with four lanes each of PCIe Gen 4 connectivity and up to 2 M.2 SATA drives for flexible boot and local storage capabilities.
- **GPUs:** The Cisco UCS Front Mezzanine GPU module is a passive PCIe Gen 4 front mezzanine option with support for up to two U.2 NVMe drives and two GPUs.
- **Virtual Interface Card (VIC):** supports Cisco UCS VIC 14425, 15231, 15420 (mLOM), and VIC 14825, 15422 (mezzanine) for 100 Gbps 100 Gbps connectivity per server
- **Security:** The server supports an optional Trusted Platform Module (TPM). Additional features include a secure boot FPGA and ACT2 anti-counterfeit provisions.

Cisco UCS Virtual Interface Card 15231 (VIC)

Cisco UCS X210c M7 Compute Nodes support multiple Cisco UCS VIC cards. In this solution, Cisco UCS VIC 15231 is used for validation.

The Cisco UCS VIC 15231 are 2x100-Gbps Ethernet/FCoE-capable modular LAN on motherboard (mLOM) adapters designed exclusively for the Cisco UCS X210c Compute Node. The Cisco UCS VIC 15231 adapters enable a policy-based, stateless, agile server infrastructure that can present to the host PCIe standards-compliant interfaces that can be dynamically configured as either NICs or HBAs. In this solution, we have used 2 VIC cards per UCS Server.

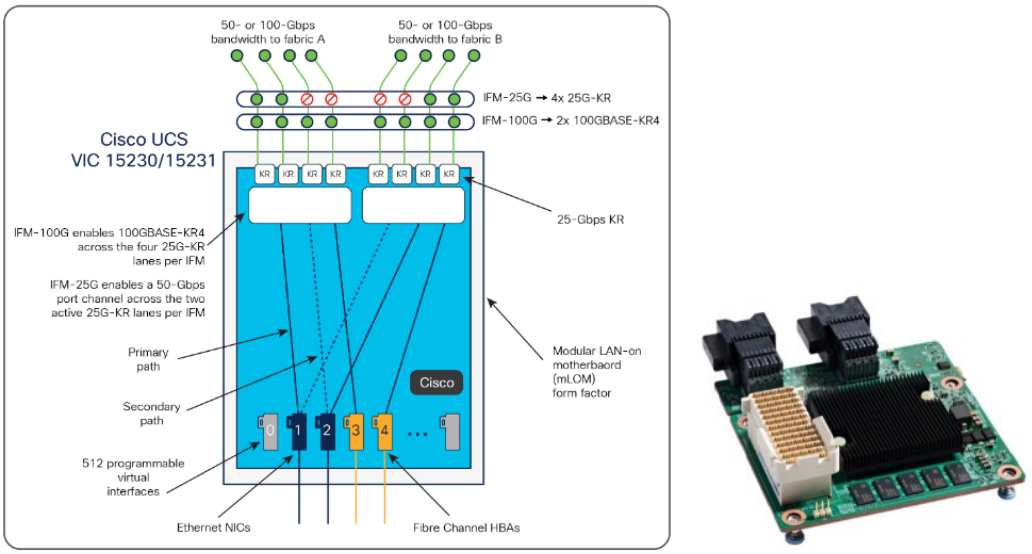


Figure 8) Cisco UCS VIC 15231

Cisco UCS 6536 Fabric Interconnects

The Cisco UCS 6536 Fabric Interconnect (FI) is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. The Cisco UCS 6536 Fabric Interconnect offers line-rate, low-latency, lossless 10/25/40/100 Gigabit Ethernet, Fibre Channel, NVMe over Fabric, and Fibre Channel over Ethernet (FCoE) functions. In addition, by supporting a unified fabric, Cisco UCS 6536 Fabric Interconnect provides both LAN and SAN connectivity for all servers within its domain.

Figure 9) Cisco UCS 6536 Fabric Interconnects

From a networking perspective, the Cisco UCS 6536 uses a cut-through architecture, supporting deterministic, low-latency, line-rate 10/25/40/100 Gigabit Ethernet ports, a switching capacity of 7.42 Tbps per FI and 14.84 Tbps per unified fabric domain, independent of packet size and enabled services. With the X9108-IFM-25G, it enables 400Gbps bandwidth per chassis per FI domain.

Cisco Nexus 9336C-FX2 Switches

The Cisco Nexus 9336C-FX2 switch offers flexible port speeds supporting 1/10/25/40/100 Gbps in a compact 1 RU form factor with cloud-scale technology. It is designed to meet the changing needs of data centers, big data applications, and automated cloud environments.

- All 36 ports support 10/25/40/100 Gbps QSFP28 and wire-rate MACsec encryption.
- Supports 7.2 Tbps of bandwidth and over 2.8 bpps.
- Enhanced Cisco NX-OS Software designed for performance, resiliency, scalability, manageability, and programmability.
- Real-time buffer utilization per port and per queue, for monitoring traffic micro-bursts and application traffic patterns.

Figure 10) Cisco Nexus 9336C-FX2 switch

Cisco Intersight

The Cisco Intersight platform is a Software-as-a-Service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support. The Cisco Intersight platform is designed to be modular, so you can adopt services based on your individual requirements. The platform significantly simplifies IT operations by bridging applications with infrastructure, providing visibility and management from bare-metal servers and hypervisors to serverless applications, thereby reducing costs and mitigating risk. This unified SaaS platform uses a unified Open API design that natively integrates with third-party platforms and tools.

There are two modes of management operations possible with Cisco Intersight: UCSM Managed Mode (UMM) and Intersight Managed Mode (IMM). You can select the native UCSM Managed Mode (UMM) or Intersight Managed Mode (IMM) for fabric-attached Cisco UCS systems during the initial setup of the fabric Interconnects. In this solution, native IMM is used.

Microsoft Hyper-V 2025

Microsoft Hypervisor Server 2025 is an advanced virtualization platform designed to help businesses optimize their IT infrastructure by running multiple virtual machines (VMs) on a single physical server. This technology allows organizations to maximize hardware utilization, reduce operational costs, and simplify IT management by consolidating workloads into fewer physical servers. Hypervisor Server 2025 builds upon previous versions, offering enhanced scalability, security features, and improved performance, making it suitable for both small businesses and large enterprises.

It allows for virtual machine management, where each VM can be easily created, configured, and monitored through management tools like Hyper-V Manager. The system supports virtual networking, allowing VMs to communicate with each other and with external networks. Another key functionality is live migration, which enables VMs to be moved between physical servers without any downtime, ensuring business continuity. Additionally, snapshot and checkpoint features allow users to save the state of a virtual machine, making it easier to roll back to a previous configuration if needed. These basic functions make Hypervisor Server 2025 a powerful tool for improving hardware utilization, simplifying IT management, and supporting various workloads across different environments.

SCVMM

System Center Virtual Machine Manager (SCVMM) is a powerful management tool for overseeing Hyper-V environments, offering centralized control, automation, and optimization of virtualized infrastructure. As a core component of Microsoft's System Center suite, SCVMM is designed to streamline the deployment and administration of Hyper-V hosts, virtual machines (VMs), and related networking and storage resources. It simplifies complex tasks such as provisioning VMs, live migration, and dynamic optimization by providing a single-pane-of-glass management experience. SCVMM enables administrators to create and manage private clouds, automate workflows using PowerShell, and integrate with Microsoft Azure for hybrid cloud management. It supports features like virtual machine replication, failover clustering, and software-defined networking (SDN), making it a crucial tool for enterprise-level Hyper-V environments.

With SCVMM, administrators can efficiently manage large-scale Hyper-V deployments by utilizing features such as Logical Networking, which abstracts physical network components to improve flexibility which allows for software-defined storage management. Additionally, it provides role-based access control (RBAC) to enforce security policies and restrict access to critical resources. By integrating with other Microsoft tools like Windows Admin Center, Active Directory, and System Center Operations Manager (SCOM), SCVMM enhances monitoring, reporting, and automation capabilities within a Hyper-V environment, helping organizations maximize performance, reliability, and cost-efficiency.

Microsoft Windows Server 2025

Microsoft® Windows Server 2025 is the latest version of Microsoft’s enterprise operating system, bringing enhanced security, performance, and hybrid cloud capabilities. It builds upon the strengths of Windows Server 2022, introducing improved virtualization through Hyper-V, deeper Azure integration, and advanced security features.

NetApp Shift Toolkit

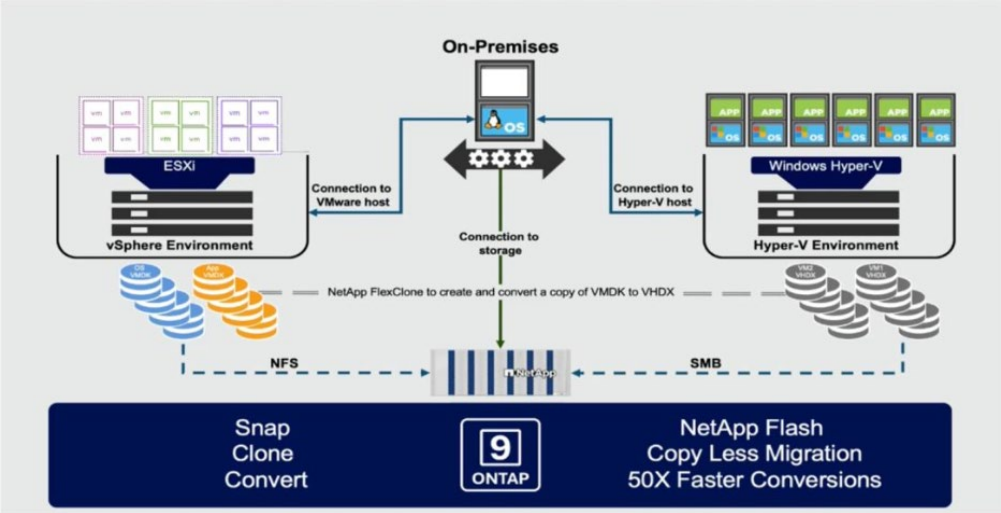
The NetApp Shift Toolkit® is a standalone, user-friendly GUI solution designed to facilitate rapid and efficient migration of virtual machines (VMs) between different hypervisors, notably from VMware ESXi to Microsoft Hyper-V. It utilizes NetApp FlexClone® technology to quickly convert VM hard disks like VMDK to VHDX. Additionally, the toolkit manages the creation and configuration of destination VMs. For instance, converting a 1TB VMDK file, which traditionally takes hours, can be completed in seconds using the Shift Toolkit.

Shift toolkit provides flexibility in a multi-hypervisor environment by supporting bidirectional conversion between the following hypervisors:

- VMware ESXi to Microsoft Hyper-V
- VMware ESXi to KVM compatible hypervisor
- Microsoft Hyper-V to VMware ESXi (Upcoming release)

Benefits of Shift toolkit:

- Helps minimize downtime and enhances business productivity.
- Offers choice and flexibility by reducing licensing costs, lock-in, and commitments to a single vendor.
- Enables organizations looking to optimize VM licensing costs and extend IT budgets.
- Reduces virtualization costs with VM portability and is offered free from NetApp.



NetApp SMI-S Provider

The NetApp SMI-S Provider is a standards-based interface that enables integration of NetApp storage systems with management tools like Microsoft System Center Virtual Machine Manager (SCVMM). It implements the Storage Management Initiative Specification (SMI-S), allowing SCVMM to discover, classify, and manage NetApp storage resources such as volumes and SMB shares. Once registered in SCVMM, the SMI-S Provider allows administrators to provision file shares directly from the VMM console, assign them to host clusters, and manage storage capacity more efficiently. This integration helps automate VM deployment workflows, enforces storage policies, and simplifies storage administration in environments that leverage NetApp as back-end storage for Hyper-V.

For more information about the NetApp SMI-S Provider, refer https://docs.netapp.com/us-en/smis-provider/index.html

Hardware and Software Revisions

This solution can be extended to any FlexPod environment running supported software, firmware, and hardware versions as defined in the NetApp Interoperability Matrix Tool, UCS Hardware and Software Compatibility, Broadcom Compatibility Guide The following table shows the FlexPod hardware and software revisions used in this solution.

Table 1) Hardware and software version

Component	Product	Version
Compute	Cisco UCSX-210C-M7 Compute Node	5.3(0.250001)
	Cisco UCSX-210C-M6 Compute Node	5.3(0.250001)
	Cisco UCS	4.3(5.240032)
	Cisco UCS VIC 15231	5.3(4.84)
	Cisco eNIC (Cisco VIC Ethernet NIC Driver)	5.15.17.4
Network	Cisco Nexus 9336C-FX2 NX-OS	10.5(2)
Storage	NetApp AFF C250	ONTAP 9.16.1P3
Software	Microsoft Hyper-V	2025
	Microsoft Windows Server	2025
	Microsoft System Center Virtual Machine Manager	2025 (10.25.1200.0)

	Microsoft SQL Server	2022
	Microsoft SQL Server Management Studio	20.2.30.0
	NetApp Host Utilities for Windows	7.2
	NetApp Shift Toolkit	2.0
	VMware vSphere	8.0.3
	VMware vCenter Appliance	8.0.3
	VMware ESXi nenic Ethernet driver	2.0.15.0
	NetApp SMI-S Provider	5.2.7
	HammerDB	5.0

Installation and Configuration

This section describes the set of steps that were followed to prepare the solution infrastructure for validation.

FlexPod Setup

Refer the following IaC document to setup the base FlexPod:
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_imm_m7_iac.html

VLAN Configuration

Table 2 lists the VLANs configured for setting up the IP-based FlexPod environment along with their usage.

Table 2) Configured VLANs and their usage

Name	VLAN ID	Usage
Native-VLAN	2	VLAN to which untagged frames are assigned
IB-MGMT	2210	VLAN for in-band management interfaces
NFS	2211	VLAN for NFS
VM	2212	VLAN for VM traffic
Infra-iSCSI-A	101	VLAN for iSCSI Boot on Fabric A & datastore access
Infra-iSCSI-B	102	VLAN for iSCSI Boot on Fabric B & datastore access
MS-LVMN	103	VLAN designated for the movement of VMs from one physical host to another.
MS-Cluster	104	VLAN for cluster connectivity
Infra-SMB	500	VLAN for SMB

The below sections only explain the changes to ONTAP and UCS w.r.t Microsoft Hyper-V.

ONTAP Storage Configuration

This section provides details on the additional step required for Hyper-V and NetApp Shift Toolkit setup.

Create the CIFS Service

Configure the DNS for your SVM.

```
dns create -vserver Infra-SVM -domains <<domain_name>> -name-servers <<dns_server_ip>>
```

Add a default route for the SVM to reach the Active Directory domain controller via the in-band management network.

```
a02-affa300::> net route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway 172.22.10.1
  (network route create)

AI-C250::> net route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
AI-C250
                    0.0.0.0/0       172.22.10.1     20
Infra-SVM
                    0.0.0.0/0       172.22.10.1     20
2 entries were displayed.
```

Create the CIFS service.

```
vserver cifs create -vserver Infra-SVM -cifs-server Infra-CIFS -domain flexpod.local

In order to create an Active Directory machine account for the CIFS server, you must supply the
name and password of a Windows account with sufficient privileges to add computers to the
"CN=Computers" container within the
"FLEXPOD.LOCAL" domain.

Enter the user name: Administrator@flexpod.local

Enter the password:
```

Create NetApp FlexVol Volumes

```
volume create –vserver Infra-SVM –volume iscsi_datastore_1 -aggregate aggr1_node01 -size 500GB -
state online -policy default -security-style ntfs -space-guarantee none -percent-snapshot-space 0

volume create –vserver Infra-SVM –volume iscsi_datastore_2 -aggregate aggr1_node02 -size 500GB -
state online -policy default -security-style ntfs -space-guarantee none -percent-snapshot-space 0

volume create –vserver Infra-SVM –volume ESXi_datastore -aggregate aggr1_node02 -size 500GB -
junction-path /Esxi_infra_datastore -state online -policy default -security-style unix -space-
guarantee none -percent-snapshot-space 0

volume create -vserver Infra-SVM -volume witness -aggregate aggr1_node01 -size 5GB -state online
-policy default -security-style ntfs -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra-SVM -volume HV_boot -aggregate aggr1_node01 -size 500GB -state
online -policy default -security-style ntfs -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra-SVM -volume SQL_data -aggregate aggr1_node01 -size 1TB -state online
-policy default -security-style ntfs -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra-SVM -volume SQL_log -aggregate aggr1_node01 -size 500GB -state
online -policy default -security-style ntfs -space-guarantee none -percent-snapshot-space 0
```

Create Qtree

Create a Qtree on the volume that will be used for hosting the VMs to be converted from VMware to Hyper-V

```
qtree create -vserver Infra-SVM -volume ESXi_datastore -qtree ESXi_qtree -security-style ntfs
```

Create CIFS Shares

Create a share where the converted VM data will be stored.

Note: Make sure that the NFS share (used to store the VMs to be converted) and the destination share (used to store the converted VMs) reside on the same volume. Shift toolkit does not support spanning on multiple volumes.

```
cifs share create -vserver Infra-SVM -share-name ESXi_share -path /ESXi_datastore -share-
properties oplocks,browsable,continuously-available,showsnapshot,show-previous-
versions,changenotify
```

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables to control the level of access to a share for users and groups.

```
cifs share access-control create -vserver Infra-SVM -share ESXi_share -user-or-group fpmc\Mgmt-
01-Host$ -user-group-type windows -permission Full_Control

cifs share access-control create -vserver Infra-SVM -share ESXi_share -user-or-group fpmc\Mgmt-
02-Host$ -user-group-type windows -permission Full_Control

cifs share access-control create -vserver Infra-SVM -share ESXi_share -user-or-group
fpmc\scvmmrunas -user-group-type windows -permission full_Control

cifs share access-control create -vserver Infra-SVM -share ESXi_share -user-or-group fpmc\HV-
MGMT-Cluster$ -user-group-type windows -permission full_Control
```

Create Gold Management Host Boot LUN

To create one boot LUN, run the following command:

```
lun create -vserver Infra-SVM -volume HV_boot -lun MGMT-Win2025-Gold -size 200GB –ostype
windows_2008 -space-reserve disabled
```

Create Witness, SQL and iSCSI Datastore LUNs

A witness LUN is required in a Hyper-V cluster to ensure continuous cluster operation if some nodes go down.

To create LUN, run the following command:

```
lun create -vserver Infra-SVM -volume witness -lun witness -size 1GB –ostype windows_2008 -space-
reserve disabled

lun create -vserver Infra-SVM -volume iscsi_datastore_1 -lun iscsi_datastore_1 -size 500GB –
ostype windows_2008 -space-reserve disabled

lun create -vserver Infra-SVM -volume iscsi_datastore_2 -lun iscsi_datastore_2 -size 500GB –
ostype windows_2008 -space-reserve disabled

lun create -vserver Infra-SVM -volume SQL_data -lun SQL_data -size 500GB –ostype windows_2008 -
space-reserve disabled

lun create -vserver Infra-SVM -volume SQL_log -lun SQL_log -size 200GB –ostype windows_2008 -
space-reserve disabled
```

Cisco UCS Configuration using Cisco Intersight

We have deployed VMware ESXi on a Cisco UCS X210c M6 compute node using standard FlexPod architecture and this section provides more details on the specific Cisco UCS policies and settings used for configuring Cisco UCS X210c M7 compute nodes for hosting Microsoft windows server 2025 to create Hyper-V setup. It is important to use the correct network policy here to be able to successfully install windows server 2025.

Create LAN Connectivity Policy for iSCSI Boot

We will be using Win-HPN-v2 policy for 00-vSwitch0-A & 01-vSwitch0-B and iSCSI boot & we will use windows policy for VM network. To know more about these policies, refer to: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/unified-computing-system-adapters/ucs-vic-15000-series-ether-fabric-wp.html

vNICs	Switch ID	PCI Order	VLANs	Ethernet adapter policy
00-vSwitch0-A	A	0	IB_Mgmt, NFS, MS_LVMN, MS_Cluster, Infra_SMB	Win-HPN-v2

01-vSwitch0-B	B	1	IB_Mgmt, NFS, MS_LVMN, MS_Cluster, Infra_SMB	Win-HPN-v2
02-iSCSI-5G-A	A	2	iSCSI_A	Win-HPN-v2
03-iSCSI-5G-B	B	3	iSCSI_B	Win-HPN-v2
04-VM-5G-A	A	4	VM_traffic	Windows
05-VM-5G-B	B	5	VM_traffic	Windows

NetApp ONTAP Boot Storage Setup

Create igroups

To create igroups, run the following commands:

```
igroup create –vserver Infra-SVM –igroup Hyper-V-MGMT-01 –protocol iscsi –ostype windows –
initiator <hyper-v-mgmt-01-iqn>
igroup create –vserver Infra-SVM –igroup Hyper-V-MGMT-02 –protocol iscsi –ostype windows –
initiator <hyper-v-mgmt-02-iqn>
igroup create –vserver Infra-SVM –igroup Hyper-V-MGMT-All –protocol iscsi –ostype windows –
initiator <hyper-v-mgmt-01-iqn>,<hyper-v-mgmt-02-iqn>
```

To get the management host IQNs, log in to Cisco intersight and go to Configure > Profiles > UCS Server Profiles > Profile > General > Configuration > Identifiers. The required IQN can be found to the right of IQN.

Map LUNs to igroups

To map LUNs to igroups, run the following commands:

```
lun map –vserver Infra-SVM –volume HV_boot –lun MGMT-Win2025-Gold –igroup Hyper-V-MGMT-01 –lun-id
0
lun map –vserver Infra-SVM –volume witness –lun witness –igroup Hyper-V-MGMT-All –lun-id 1

lun map –vserver Infra-SVM –volume iscsi_datastore_1 –lun iscsi_datastore_1 –igroup Hyper-V-MGMT-
All –lun-id 2

lun map –vserver Infra-SVM –volume iscsi_datastore_2 –lun iscsi_datastore_2 –igroup Hyper-V-MGMT-
All –lun-id 3

lun map –vserver Infra-SVM –volume SQL_data –lun SQL_data –igroup Hyper-V-MGMT-All –lun-id 4

lun map –vserver Infra-SVM –volume SQL_log –lun SQL_log –igroup Hyper-V-MGMT-All –lun-id 5
```

Microsoft Windows Server 2025 Hyper-V Deployment Procedure

Setting Up Microsoft Windows Server 2025

This section provides detailed instructions for installing Microsoft Windows Server 2025 in a FlexPod® environment. After the procedures are completed, two booted Windows Server 2025 hosts will be provisioned.

Several methods exist for installing Microsoft Windows Server 2025. These procedures focus on how to use the built-in keyboard, video, mouse (KVM) console and virtual media features in Cisco intersight to map remote installation media to individual servers and connect to their boot logical unit numbers (LUNs).

Log in to the Cisco Intersight and complete the following steps:

1. Click ‘Servers’ to find the target server.
2. Click the triple dots (…) to the right of the target and Select ‘Launch vKVM’
3. Click ‘Launch’ and ‘Load KVM Certificate’.
4. In the ‘Virtual Media’ area, click KVM Mapped vDVD and browse to the windows Server 2025 installation ISO image file and click Open.

5. Map the image that you just added by selecting Map Device.
6. To boot the server, click on the power system.

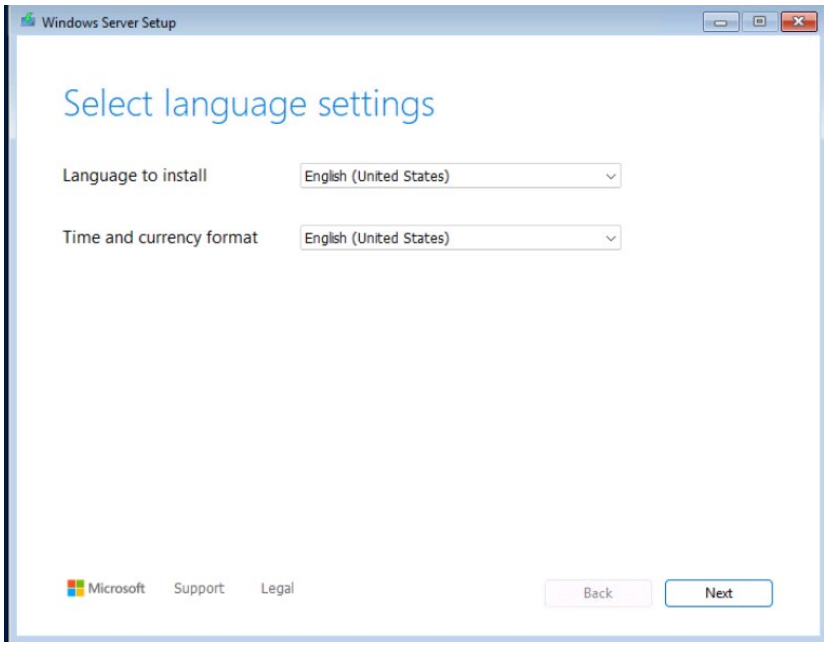
Install Windows Server 2025

Before proceeding with windows Server 2025 installation on the first management host, we need to make sure to have a single iSCSI path.

> **Note:** Multipath configurations may cause installation failures. To avoid this issue, we will use a separate template with a single NIC specifically for the installation process. Once the installation is successfully completed, we can update the template.

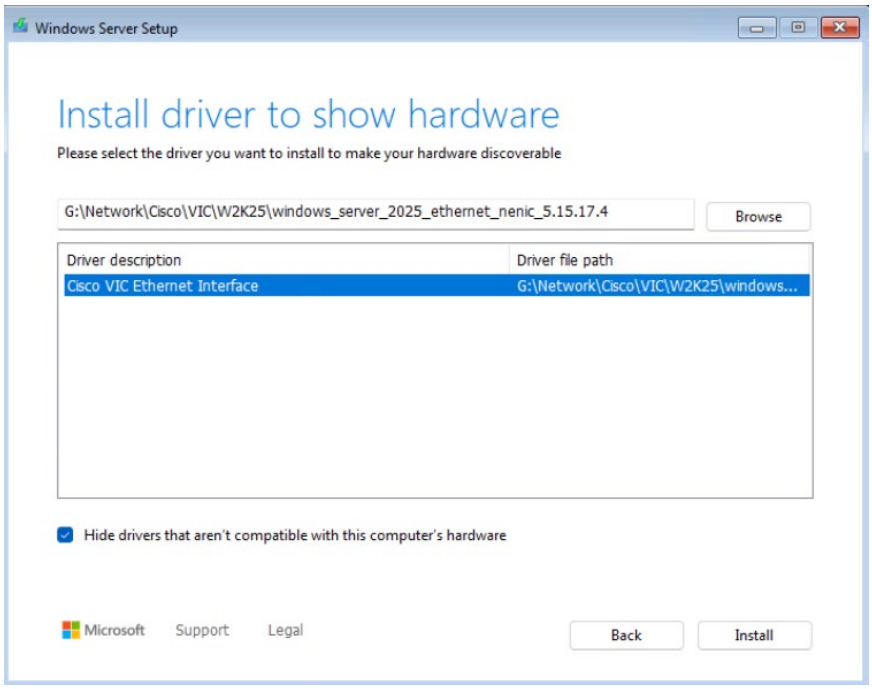
On boot, the machine detects the presence of the Windows installation media.

1. After the installer has finished loading, select the relevant region information and click Next.

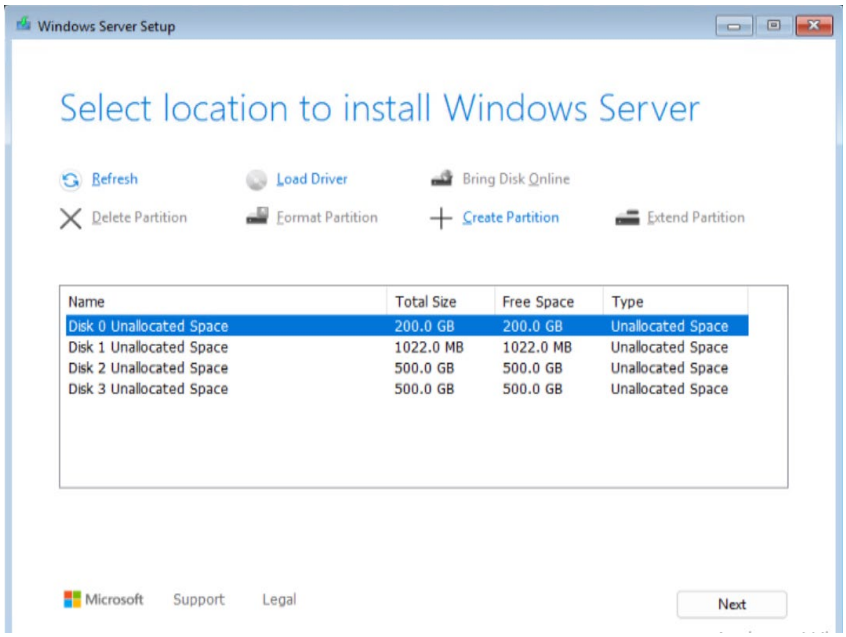


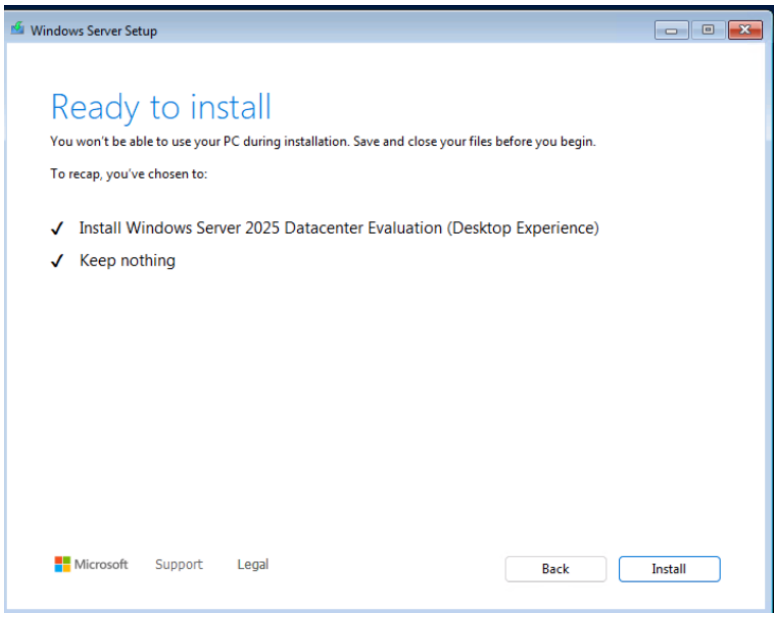
2. Click Install Windows Server.
3. Enter the Product Key and click Next.
4. Select Windows Server 2025 Datacenter (Desktop Experience) and click Next.

   Note: You may optionally remove the GUI after the Hyper-V cluster is operational.
5. After reviewing the EULA, accept the license terms and click Next.
6. Select Custom: Install Windows only (advanced).
7. In the Windows Setup window, select Load driver.
8. Under Virtual Media, select the Windows Server 2025 item to unmap it. Click Yes to complete the unmapping.
9. Under Virtual Media, select map CD/DVD.
10. Click Browse and browse to the UCSX-drivers-windows.5.3.0d iso. Select this iso and click Open. Click Map Device to map this iso.
11. In the Load driver window, click Browse.
12. Browse to the CD Drive and expand Network > Cisco > VIC > W2K25. Select windows_server_2025_ethernet_nenic_5.15.17.4 under W2K25. Click Ok.



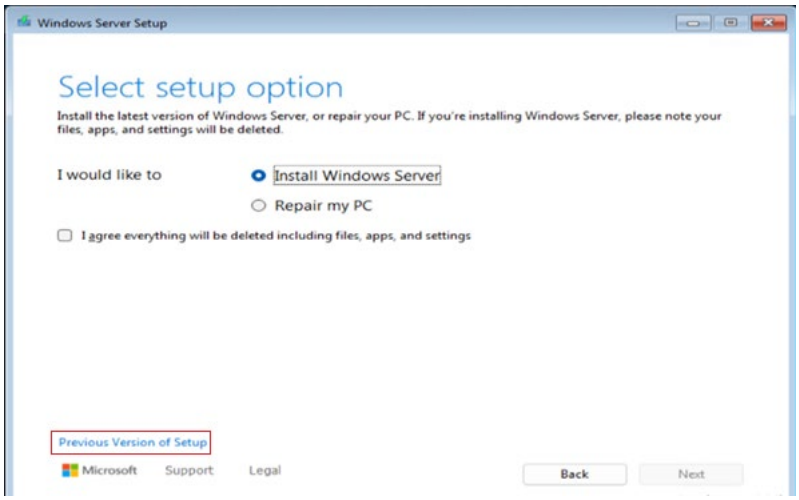
13. Back in the Windows Setup window, make sure Cisco VIC Ethernet Interface is selected and click Install.
14. The drives should now appear in the Windows Setup window. In the Virtual Media menu, unmap the UCSX-drivers-windows.5.3.0d iso and remap the Windows Server 2025 installation iso.
15. In the Windows Setup window, click Refresh. Make sure the 200 GB drive is selected and click Next.





16. When Windows is finished installing, enter an administrator password on the settings page and click Finish.
17. Under Virtual Media, unmap the Windows Server 2025 Installation iso.

    Note: In case of a windows 2025 installation failure, try installing with the “Previous Version of Setup” method as highlighted in the below screenshot



Host Renaming and Join to Domain

To rename host and join to a domain, complete the following steps:

1. Login to the host and open PowerShell.
2. Rename the host.

```
Rename-Computer -NewName Win2025-Gold -restart
```

3. Set the MTU of the current management interface to 1500.

```
netsh interface ipv4 set subinterface 00-vSwitch0-i-5G-A mtu=1500 store=persistent
```

4. Assign an IP address to the management interface.

```
Get-NetAdapter – determine the ifIndex of the 00-vSwitch0-i-5G-A adapter
new-netipaddress –interfaceindex <UInt32> -ipaddress <string> -prefixlength <Byte> -
DefaultGateway <string>
```

5. Assign DNS server IP address to the above management interface

```
Set-DnsClientServerAddress -InterfaceIndex <UInt32> -ServerAddresses <String>
```

6. Add the host to Active Directory.

```
Add-Computer -DomainName <domain_name> -Restart
```

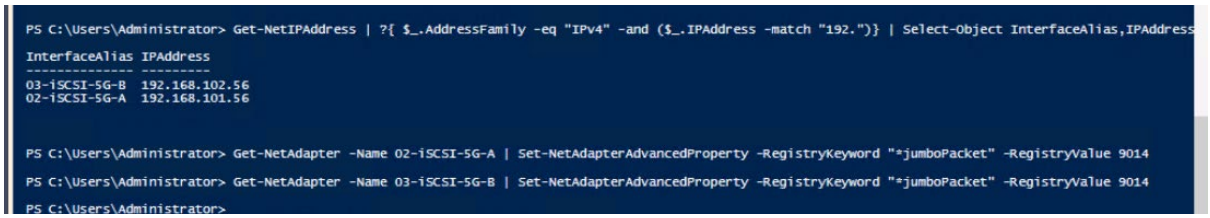
7. Set the timezone of the host to the appropriate timezone through server manager GUI.

Enable Jumbo frames on Storage Network Interfaces

1. Check the adapter details using the below command

```
PS C:\Users\Administrator> Get-NetAdapter
Name                      InterfaceDescription                    ifIndex Status       MacAddress
LinkSpeed
----                      --------------------                    ------- ------       ----------
---------
01-vSwitch0-i-5G-B        Cisco VIC Ethernet Interface #4              26 Up           00-15-5D-
66-38-00         50 Gbps
02-iSCSI-5G-A             Cisco VIC Ethernet Interface #2              22 Up           00-25-B5-
03-1A-10         50 Gbps
00-vSwitch0-i-5G-A        Cisco VIC Ethernet Interface #3              20 Up           00-25-B5-
03-1A-09         50 Gbps
04-VM-5G-A                Cisco VIC Ethernet Interface #5              19 Up           00-25-B5-
03-1A-0A         50 Gbps
03-iSCSI-5G-B             Cisco VIC Ethernet Interface                 17 Up           00-25-B5-
03-1B-10         50 Gbps
05-VM-5G-B                Cisco VIC Ethernet Interface #6              15 Up           00-25-B5-
03-1B-0A         50 Gbps
```

2. Execute the steps below to set the jumbo frames to 9000 on the ethernet adapter.



3. After enabling jumbo frames, make sure the virtual machine can reach the storage with the maximum packet size without fragmenting the packets.

```
PS C:\Windows\system32> ping 192.168.101.121 -l 8958 -f -S 192.168.101.56

Pinging 192.168.101.121 from 192.168.101.56 with 8958 bytes of data:
Reply from 192.168.101.121: bytes=8958 time<1ms TTL=64
Reply from 192.168.101.121: bytes=8958 time<1ms TTL=64
Reply from 192.168.101.121: bytes=8958 time<1ms TTL=64
Reply from 192.168.101.121: bytes=8958 time<1ms TTL=64

Ping statistics for 192.168.101.121:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Configure multipath software

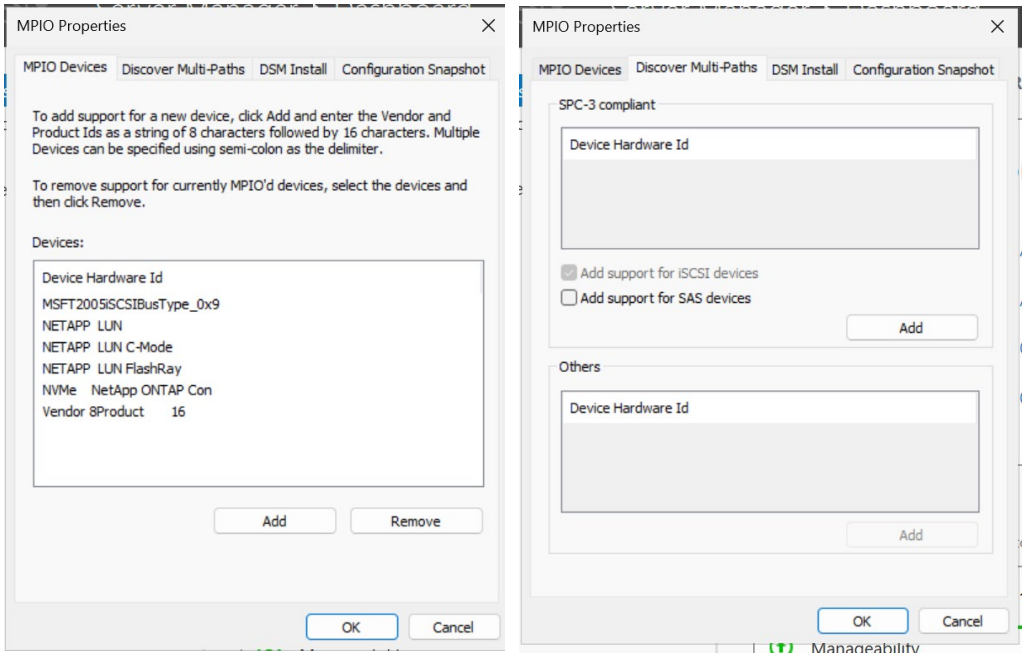
1. After installing multipath-io feature, enable Microsoft Device Specific Module (MSDSM) to automatically claim SAN disks for Microsoft Multipath I/O (MPIO) for the iSCSI bus type.
2. Restart the virtual machine to make the changes take effect.

```
PS C:\Users\Administrator> Install-WindowsFeature -Name multipath-io

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    Yes            SuccessRest... {Multipath I/O}
WARNING: You must restart this server to finish the installation process.


PS C:\Users\Administrator> Enable-MSDSMAutomaticClaim -BusType iSCSI

VendorId ProductId
-------- ---------
MSFT2005 iSCSIBusType_0x9
```

Install NetApp Windows Unified Host Utilities

After enabling the MPIO feature in Windows, download and install NetApp Windows Unified Host Utilities. To download and install the host utilities, complete the following steps:

1. Download NetApp Host Utilities Version 7.2 for Windows from this link: https://mysupport.netapp.com/site/products/all/details/hostutilities/downloads-tab/download/61343/7.2/downloads
2. Unzip the file and run the executable file. The NetApp Windows Unified Host Utilities setup wizard is launched. Click Next.
3. Click Yes, install support for Multipath I/O, and click Next.
4. Accept the default destination folder and click Next.
5. Click Next and then click Install to start the installation of the host utilities.
6. After the installation is complete, click Finish and restart the virtual machine.
7. After the virtual machine is restarted, verify that appropriate device drivers are added in the MPIO utility as shown below:



Configure iSCSI Software Initiator

This procedure provides the steps for configuring the in-guest iSCSI initiator for virtual machines to directly access the NetApp storage LUNs.

1. Run the following PowerShell commands on the server to start the Microsoft iSCSI initiator service and set it to start automatically .

```
PS C:\Users\Administrator> Start-Service msiscsi
PS C:\Users\Administrator> Set-Service msiscsi -StartupType "automatic"
```

2. Next step is to establish connections to the NetApp target iSCSI IP addresses. For each virtual machine, you need to replace InitiatorPortalAddress with the appropriate guest iSCSI IP address:

```
New-IscsiTargetPortal -TargetPortalAddress 192.168.101.122 -InitiatorPortalAddress 192.168.101.56
New-IscsiTargetPortal -TargetPortalAddress 192.168.102.122 -InitiatorPortalAddress 192.168.102.56
```

3. Connect to the NetApp targets using the following PowerShell commands:

```
$target = Get-IscsiTarget
Connect-IscsiTarget -TargetPortalAddress 192.168.101.122 -InitiatorPortalAddress 192.168.101.56 -
NodeAddress $target.NodeAddress -IsMultipathEnabled $true -IsPersistent $true
Connect-IscsiTarget -TargetPortalAddress 192.168.102.122 -InitiatorPortalAddress 192.168.102.56 -
NodeAddress $target.NodeAddress -IsMultipathEnabled $true -IsPersistent $true
```

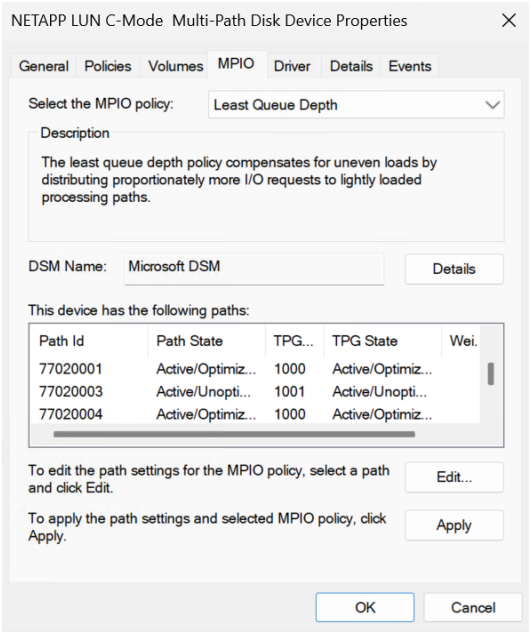
4. Verify the connections using below command:

```
Get-IscsiConnection
```

Configure Server for Cloning

To configure the server for cloning, complete the following steps:

1. Under Windows Administrative tools, open the Computer Management tool.
2. On the left, select Disk Management. Click Cancel on the Disk 1 initialization window. Near the bottom middle of the window, right-click Disk 0 and select Properties.
3. Select the MPIO tab and verify the disk now has two Active/Optimized paths and two Active/Un-optimized paths. Click OK to close the Disk Device Properties window and close the Computer Management tool.



4. Install all available Windows Updates on the server.

5. Open Windows PowerShell and enter SCONFIG to configure the server.
6. Select Remote Desktop by typing 7 and pressing Enter.
7. Enter E to enable Remote Desktop.
8. Enter 2 to allow any version of Remote Desktop. Click OK to acknowledge Remote Desktop enablement.
9. Enter 14 to shut down the server. Click Yes to complete shutdown.

Note: The boot LUN cloning procedure used in this document will only work when the clones are applied to the same server hardware. If the clone source image was created on a Cisco UCS B200 M4, and you want to apply the image to a Cisco UCS C220 M4, you will need to follow the steps above to install Windows on the Cisco UCS C220 M4.

Clone and Remap Server LUNs for Sysprep Image

To clone and remap the server LUNs for the sysprep image, complete the following steps:

1. In the storage cluster interface, unmap the MGMT-Win2025-Gold LUN.

```
lun unmap -path /vol/HV_boot/MGMT-Win2025-Gold -igroup Hyper-V-MGMT-01
```

2. Make a clone of the MGMT-Win2025-Gold LUN for the Sysprep clone.

```
clone start -source-path /vol/HV_boot/MGMT-Win2025-Gold -destination-path /vol/HV_boot/MGMT-
Win2025-Gold-Sysprep
```

3. Map the Sysprep clone boot LUN to the first Hyper-V management host.

```
lun map -path /vol/HV_boot/MGMT-Win2025-Gold-Sysprep -igroup Hyper-V-MGMT-01 -lun-id 0
```

Boot and Set Up Sysprep Clone

To boot and set up the sysprep clone, complete the following steps:

1. Back in the cisco intersight KVM Console for Hyper-V-MGMT-Host-01, click power cycle system to boot the Sysprep Clone LUN.
2. Once the server boots up, log in as the local machine Administrator.
3. Open the Windows Powershell prompt and enter C:\Windows\System32\Sysprep\sysprep /generalize /oobe /shutdown to reset the machine's security id. The server will shut down.

Clone and Remap Server LUNs for Production Images

To clone and remap server LUNs for production images, complete the following steps:

1. In the storage cluster interface, unmap the MGMT-Win2025-Gold-Sysprep LUN.

```
lun unmap -path /vol/HV_boot/MGMT-Win2025-Gold-Sysprep -igroup Hyper-V-MGMT-01
```

2. Make two clones of the MGMT-Win2025-Gold-Sysprep LUN for the Hyper-V-MGMT hosts.

```
clone start -source-path /vol/HV_boot/MGMT-Win2025-Gold-Sysprep -destination-path
/vol/HV_boot/Hyper-V-MGMT-01
clone start -source-path /vol/HV_boot/MGMT-Win2025-Gold-Sysprep -destination-path
/vol/HV_boot/Hyper-V-MGMT-02
```

3. Map the Hyper-V-MGMT LUNs to the hosts.

```
lun map -path /vol/HV_boot/Hyper-V-MGMT-01 -igroup Hyper-V-MGMT-01 -lun-id 0
lun map -path /vol/HV_boot/Hyper-V-MGMT-02 -igroup Hyper-V-MGMT-02 -lun-id 0
```

Boot and Set Up Clones

To boot and set up clones, complete the following steps:

1. Back in the cisco intersight KVM Console for Hyper-V-MGMT-Host-01, click power cycle system to boot Hyper-V-MGMT-Host-01.

2. When the server boots up, select the appropriate Regional and Language information and click Next.
3. Enter the server Product Key and click Next.
4. Click Accept to Accept the License terms.
5. Log into the server as Administrator and open Powershell.
6. Rename the host.

```
Rename-Computer -NewName Hyper-V-MGMT-01 -Restart
```

7. The server will reboot. Return to Powershell. Assign an IP address to the management interface.

```
Get-NetAdapter – determine the ifIndex of the 00-vSwitch0-i-5G-A adapter
new-netipaddress –InterfaceIndex <UInt32> -ipaddress <string> -prefixlength <Byte> -
DefaultGateway <string>
```

8. Assign DNS server IP address to the above management interface

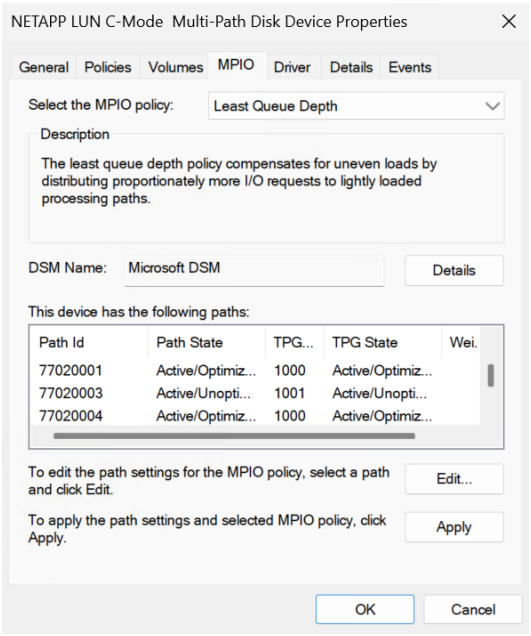
```
Set-DnsClientServerAddress -InterfaceIndex <UInt32> -ServerAddresses <String>
```

9. Add the host to Active Directory.

```
Add-Computer -DomainName <domain_name> -Restart
```

10. Enter the appropriate Domain Admin credentials and click OK. The server will reboot. Login to the server as a Domain Admin.
11. Follow configure iSCSI Software Initiator step and verify the iscsi Connection.
12. Under Windows Administrative tools, open the Computer Management tool.
13. Select Disk Management.
14. Only on the first Hyper-V Management host, on the Initialize Disk window, make sure Disks 1-5 are selected and select the GPT radio button. Click OK.
15. Only on the first Hyper-V Management host, for Disk 1 (the 1GB disk), right-click the Unallocated area and select New Simple Volume. Click Next. Leave the size at default maximum and click Next. Select “Do not assign a drive letter or drive path” and click Next. Change the Volume label to Quorum and click Next. Click Finish.
16. Only on the first Hyper-V Management host, for Disk 2 (the first 500GB disk), right-click the Unallocated area and select New Simple Volume. Click Next. Leave the size at default maximum and click Next. Select “Do not assign a drive letter or drive path” and click Next. Change the Volume label to iscsi_datastore_1 and click Next. Click Finish.
17. Only on the first Hyper-V Management host, for Disk 3 (the second 500GB disk), right-click the Unallocated area and select New Simple Volume. Click Next. Leave the size at default maximum and click Next. Select “Do not assign a drive letter or drive path” and click Next. Change the Volume label to iscsi_datastore_2 and click Next. Click Finish.
18. Only on the first Hyper-V Management host, for Disk 4 (the 1TB disk), right-click the Unallocated area and select New Simple Volume. Click Next. Leave the size at default maximum and click Next. Select “Do not assign a drive letter or drive path” and click Next. Change the Volume label to SQL_data and click Next. Click Finish.
19. Only on the first Hyper-V Management host, for Disk 5 (the third 500GB disk), right-click the Unallocated area and select New Simple Volume. Click Next. Leave the size at default maximum and click Next. Select “Do not assign a drive letter or drive path” and click Next. Change the Volume label to SQL_log and click Next. Click Finish.
20. Only on the second Hyper-V Management host, launch Disk Management. At the Initialize Disk window, click Cancel. Under the Action Menu, select Rescan Disks. Verify that Disks 1-5 now show a status of Online.
21. Near the bottom middle of the window, right-click Disk 0 and select Properties.

22. Select the MPIO tab and verify the disk now has two Active/Optimized paths and two Active/Un-optimized paths. Click OK to close the Disk Device Properties window and close the Computer Management tool.



23. Open a second UCS KVM console and repeat steps 1-20 for the Hyper-V-MGMT-02 host.

Install Roles and Features Required for Hyper-V

To install roles and features on both Hyper-V-MGMT Hosts, complete the following steps:

1. Log in with a Domain Administrator User ID.
2. Open PowerShell with elevated rights (Run as Administrator) and add Hyper-V and Windows Failover Clustering by entering the following command:

```
Add-WindowsFeature Hyper-V, Failover-Clustering –IncludeManagementTools –Restart
```

3. The servers will reboot two times. When the reboots have completed, log in with a Domain Administration User ID.

Set Up Hyper-V Networking

To set up networking on both Hyper-V-MGMT Hosts from a UCS KVM Console, complete the following steps:

1. Open Powershell with elevated rights (Run as Administrator). Set the MTU of the 00-vSwitch0-i-5G-A network interface back to 9000.

```
netsh interface ipv4 set subinterface 00-vSwitch0-i-5G-A mtu=9000 store=persistent
netsh interface ipv4 show subinterface
```

2. Run the Get-NetAdapter command to confirm the vNIC names.
3. Create a Hyper-V virtual switch for management, storage, and VM traffic.

```
New-VMSwitch –Name HV-Infra-vSwitch –NetAdapterName 00-vSwitch0-i-5G-A, 01-vSwitch0-i-5G-B -
AllowManagementOS $false -EnableEmbeddedTeaming $true

New-VMSwitch -Name VM_traffic_switch -NetAdapterName 04-VM-5G-A,05-VM-5G-B -AllowManagementOS
$false -EnableEmbeddedTeaming $true
```

4. Create Virtual NIC.

```
Add-VMNetworkAdapter –ManagementOS –Name MS-IB-MGMT –SwitchName HV-Infra-vSwitch
```

5. Make sure MTU of MS-IB-MGMT virtual adapter is 1500.

```
netsh interface ipv4 show subinterface
```

6. Set IP Address for MS-IB-MGMT host virtual NIC.

```
New-NetIPAddress –InterfaceAlias “vEthernet (MS-IB-MGMT)” –IPAddress <host-mgmt-ip> -
DefaultGateway <mgmt-gateway> -PrefixLength <mgmt-net-prefix>
```

Note: You will not add a VLAN to this interface since the IB-MGMT-VLAN <418> is the native VLAN for the UCS VIC vNIC interfaces used in the team for the virtual switch.

7. Disable DNS registration for all NICs

```
Set-DnsClient –InterfaceAlias * -Register $false
```

8. Turn registration back on and configure DNS for the Management NIC

```
Set-DnsClient –InterfaceAlias “vEthernet (MS-IB-MGMT)” –Register $true –ConnectionSpecificSuffix
<dns-domain-name>
Set-DnsClientServerAddress –InterfaceAlias “vEthernet (MS-IB-MGMT)” –ServerAddresses <dns-server-
ip>
```

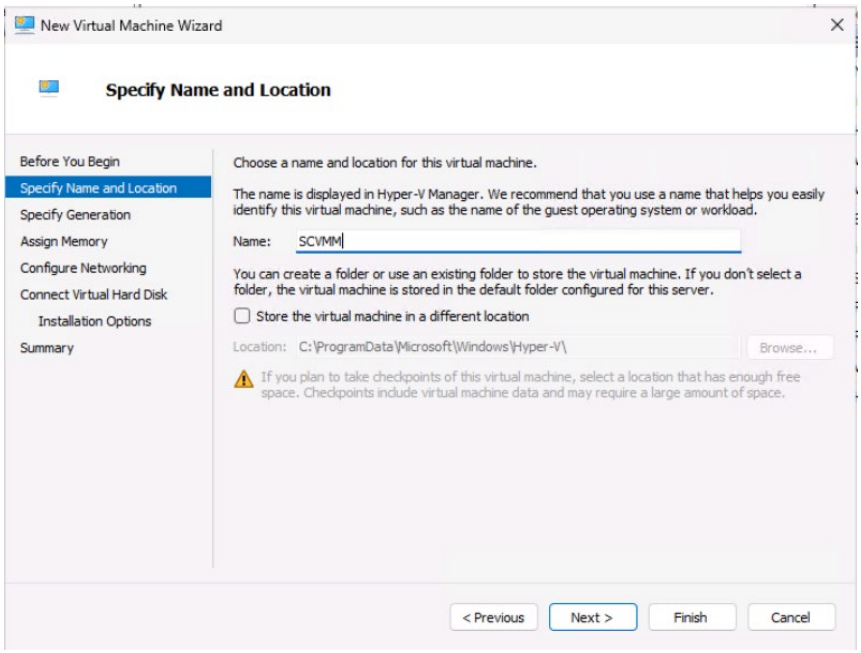
Note: Now that the host networking setup is complete, a Microsoft Remote Desktop session can be used on both hosts going forward.

Build System Center Virtual Machine Manager (SCVMM) Virtual Machine (VM)

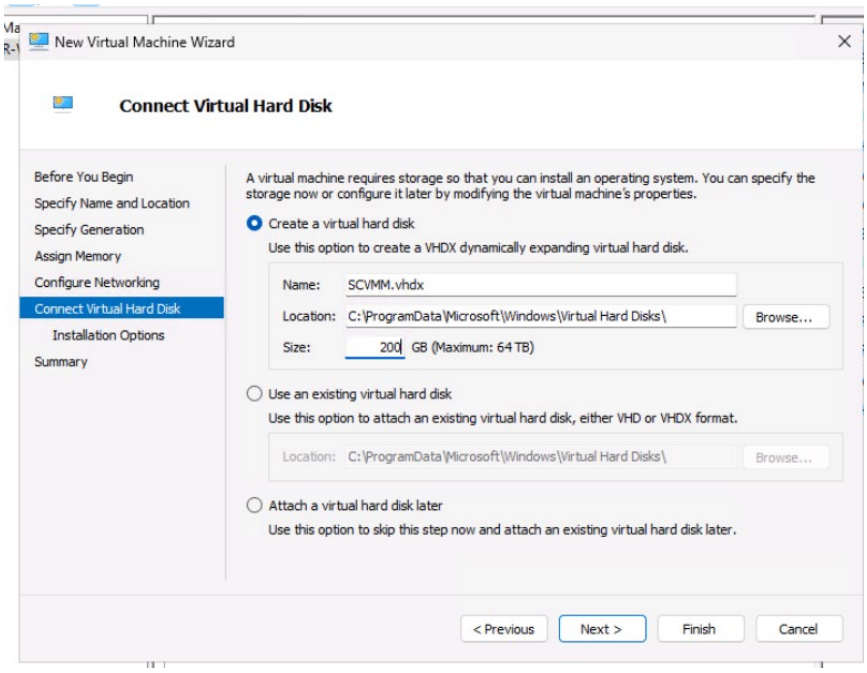
To build SCVMM virtual machine, complete the following steps:

First Hyper-V Management Host Only

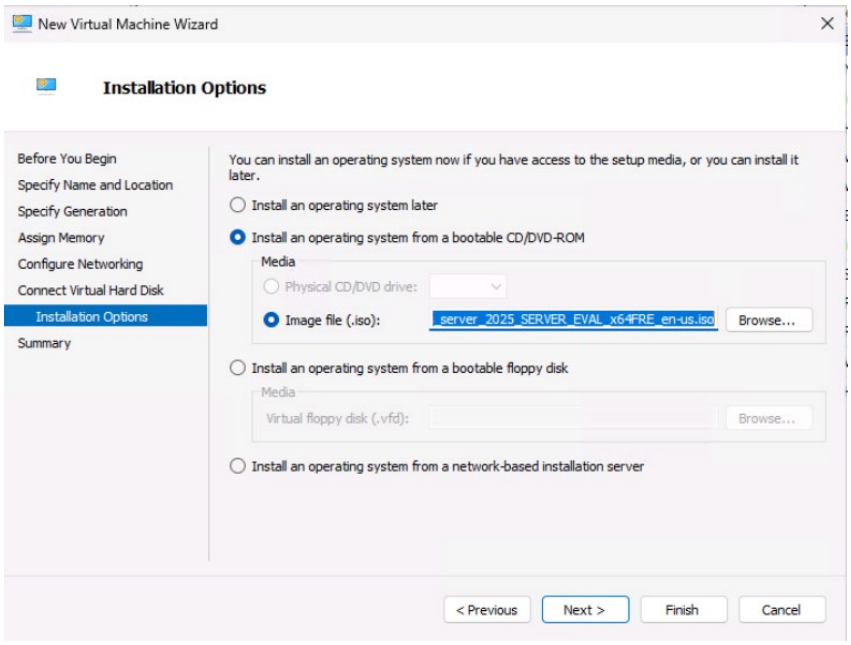
1. Connect to the first Hyper-V Management Host with Windows Remote Desktop.
2. Copy the Windows Server 2025 Installation ISO and the SQL Server 2022 ISO to the host desktop.
3. From the Start Menu under Windows Administrative Tools, open Hyper-V Manager.
4. On the left, right-click the host and select New Virtual Machine.
5. In the New Virtual Machine Wizard, click Next.
6. Name the virtual machine SCVMM and leave the default location for the virtual machine selected. Click Next.



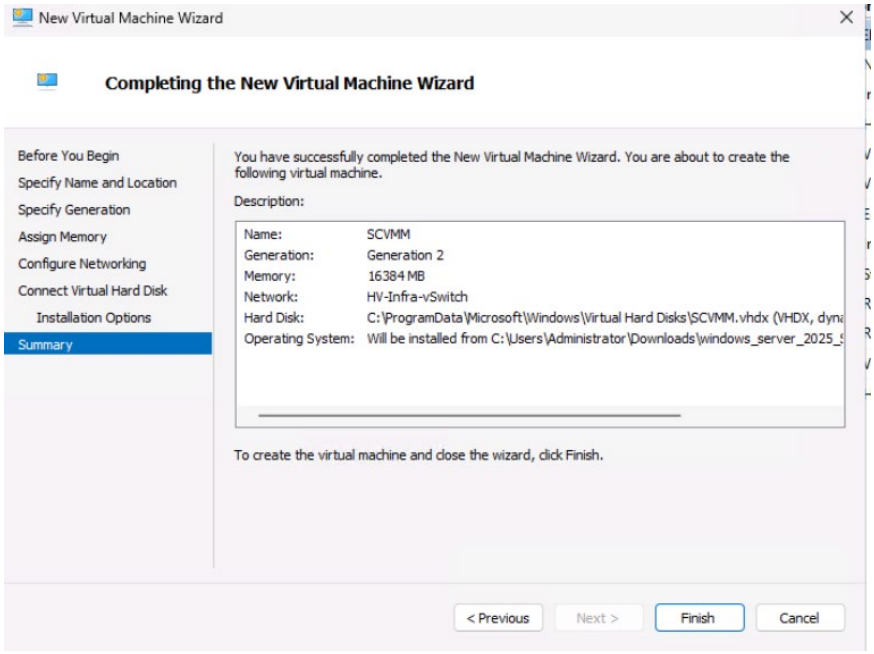
7. Select Generation 2 and click Next.
8. Enter 16384 for the Startup memory and select the checkbox for “Use Dynamic Memory for this virtual machine”. Click Next.
9. For the Networking Connection, select HV-Infra-vSwitch. Click Next.
10. Set the virtual hard disk size to 200GB and click Next.



11. Select “Install an operating system from a bootable image file”. Click Browse and browse to the Windows Server 2025 Installation ISO. Select the ISO and click Open. Click Next.

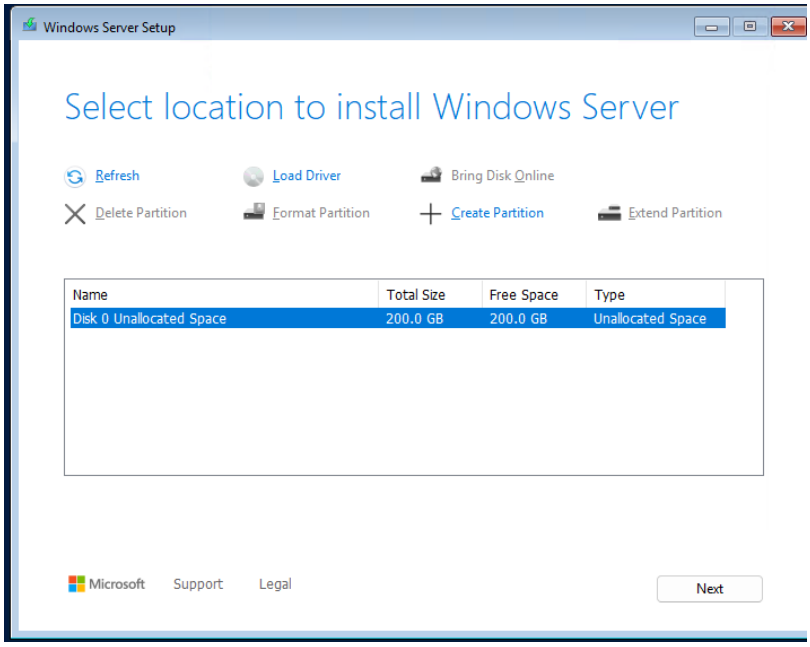


12. Verify all information and click Finish.



13. The SCVMM VM should now appear in Hyper-V Manager when the host is selected. Select the VM and on the right select Settings.
14. Under Memory, change the Minimum RAM to 4096 MB.
15. Under the Processor change the Number of virtual processors to 8.
16. Since the UCS IB-MGMT VLAN is set as the default VLAN on the virtual switch network uplinks, it is not necessary to set a VLAN for this VM.
17. Click Apply then OK to complete changing the VM settings.
18. Right-click the SCVMM VM and click Connect.

19. In the SCVMM Virtual Machine Connection window, under the Action menu, select Start. Immediately press a key when you see “Press any key to boot from CD or DVD”. If the VM tries to boot from the network, use Action > Reset to reset the VM and immediately press a key when you see “Press any key to boot from CD or DVD”.
20. In the Windows Setup Window, select the appropriate language and regional format and click Next.
21. Click Install now.
22. In the Activate Windows window, enter product key.
23. Select Windows Server 2025 Datacenter (Desktop Experience) and click Next.
24. Click to accept the license terms and click Next.
25. Select Custom: Install Windows only (advanced).
26. Select Drive 0 Unallocated Space and click Next.

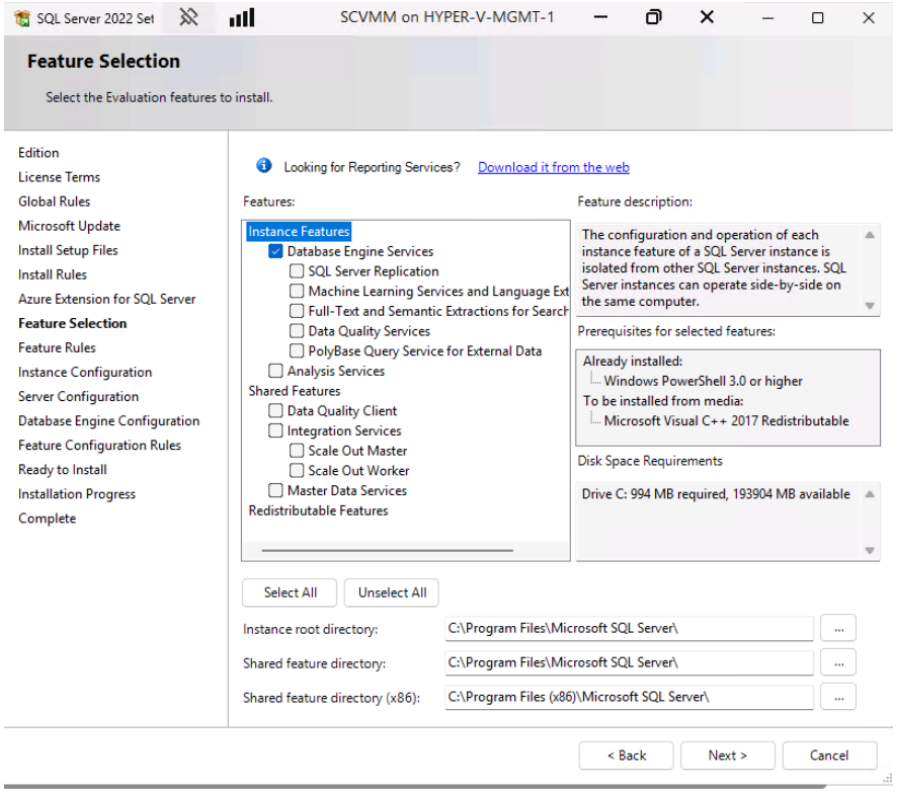


27. Windows Installation will complete and the VM will reboot.
28. After reboot, set the Administrator password on the SCVMM VM and log into the VM as Administrator.
29. Rename the computer name.
30. Set an IP address on the VM in the IB-MGMT subnet and join the machine to the AD Domain. On reboot, login as the local machine administrator.
31. Set the correct time zone in the VM and enable Remote Desktop.
32. Verify that the server has been Activated (this may require a Product Key to be entered).
33. In Server Manager under Local Server, turn Internet Explorer Enhanced Security Configuration Off for Administrators and click OK.

Install SQL Server 2022 on SCVMM VM

1. In the Virtual Machine Connection window, select Media > DVD Drive > Eject Windows Installation ISO.
2. Select Media > DVD Drive > Insert Disk.
3. Browse to the SQL 2022 Installation ISO and click Open.

4. Open Windows Explorer and browse to the DVD Drive where the SQL 2022 Installation ISO is mounted.
5. Double-click setup.
6. When the SQL Server Installation Center has loaded, click Installation on the left, then New Server standalone installation.
7. On the Product Key window, enter your product key and click Next.
8. On the License Terms screen, read the license terms, then click the checkbox next to “I accept the license terms”. Click Next.
9. On the Global Rules window, a system check runs.
10. On the Microsoft Update window, check the box to check for updates and click Next.
11. Click Next.
12. Setup files will be installed and an Install Rules check will be run. The Windows Firewall warning can be disregarded. Click Next.
13. On the Feature Selection window, select the checkbox next to “Database Engine Services” under Instance Features. Click Next.



14. A Features Rules check will run.
15. On the Instance Configuration window, click Next unless a different instance id is needed. If a different instance id is needed, change the Instance ID field and click Next.
16. At the Server Configuration Window, click Next.
17. At the Database Engine Configuration window, click Add Current User to add the SCVMM local Administrator as a SQL Server Administrator. Click Next.
18. Click Install to install SQL Server 2022 Database Engine.
19. Once the installation has completed, click Close to close the Setup window.

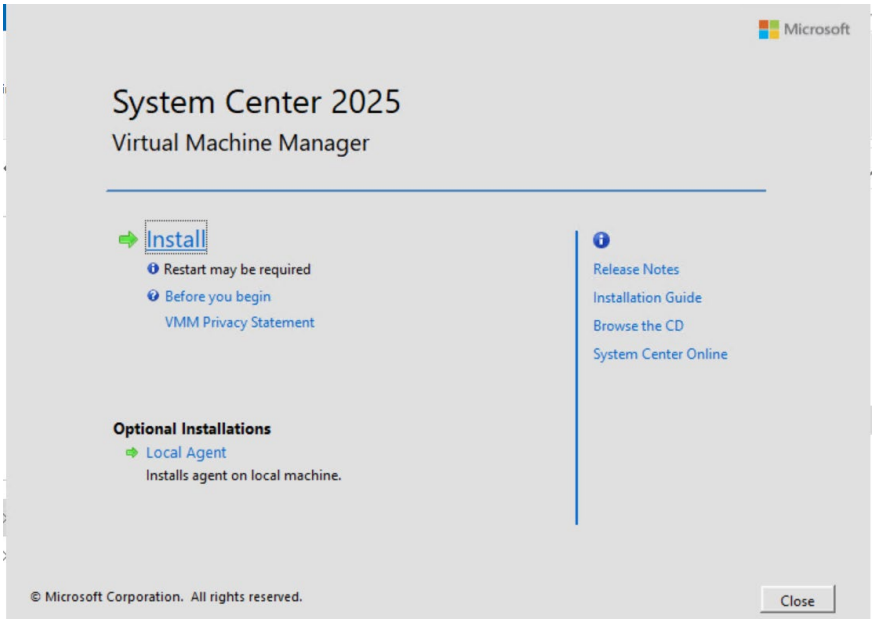
Install SQL Server Management Tools

1. Back at the SQL Server Installation Center window, click Install SQL Server Management Tools. A web browser will launch to download the tools. Click OK to use default Internet Explorer settings. Click to Download SQL Server Management Studio.
2. Click Run to install the SQL Server Management Tools. Click Install.
3. When the installation is complete, click Restart to restart the SCVMM VM.

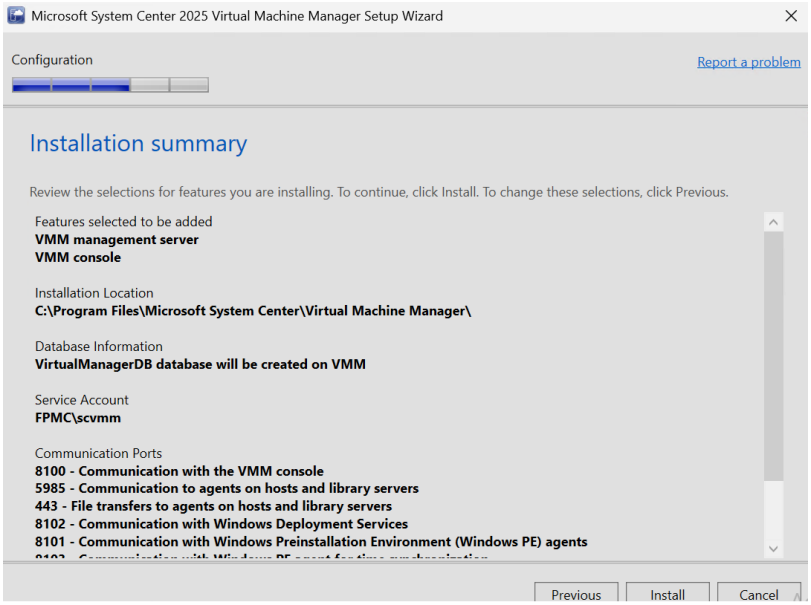
Install System Center Virtual Machine Manager 2025

1. Log in as the local Administrator.
2. Download and install the x64 version of Microsoft Command Line Utilities 15 for SQL Server from https://go.microsoft.com/fwlink/?linkid=2230791.
3. Select the option to run SqlCmdLnUtils.msi.
4. At the Welcome window, click Next.
5. Accept the terms in the license agreement and click Next.
6. Click Install.
7. Click Finish.
8. Install the Windows Assessment and Deployment Kit (ADK) after downloading it from the following URL. Download the Windows ADK for Windows 11, version 24H2. https://go.microsoft.com/fwlink/?linkid=2289980
9. Click Run to install the ADK.
10. Click Next to install the ADK in the default location.
11. Respond to the Privacy prompt and click Next.
12. Click Accept to accept the license agreement.
13. Ensure that Deployment Tools is selected. Click Install.
14. When the installation completes, click Close to close the installation window.
15. Install the ADK windows preinstalltion environment add-on https://go.microsoft.com/fwlink/?linkid=2289981
16. Click Run to install the ADK add-on.
17. Click Next to install the ADK in the default location.
18. Respond to the Privacy prompt and click Next.
19. Click Accept to accept the license agreement.
20. Ensure that Windows Preinstallation Environment (Windows PE) is selected. Click Install
21. Close the Web Browser Window.
22. In the AD server, create an SCVMM user and place it in the Domain Admins group.
23. Log out and log back into the SCVMM VM as the SCVMM user just created.
24. Download and start installing SCVMM 2025 execution file https://www.microsoft.com/en-us/evalcenter/download-system-center-2025
25. Click Next at the Welcome window.
26. Click to accept the license agreement and click Next.
27. Change the location to “C:\System Center 2025 Virtual Machine Manager” and click Next.
28. Click Extract to extract the SCVMM files.
29. Click Finish to close the file extractor.
30. Open Windows Explorer and navigate to C:\System Center 2025 Virtual Machine Manager.
31. Double-click the setup application. Click Yes to allow the app to make changes.

32. Click Install to begin the installation.



33. Select both the VMM management server and VMM console features. Click Next.
34. Enter a Name, Organization, and the SCVMM Product key and click Next.
35. Click to accept the license agreement and click Next.
36. Click Next.
37. Click Next to install in the default location.
38. A hardware and software check will run. If a Pending Restart is necessary, restart the machine and return to this point.
39. At the Database configuration window, use the Browse button to browse AD for the local computer name. This will populate the database Instance Name. Select the checkbox next to “Use the following credentials”. Enter “servername\Administrator” as the User name and the local Administrator password. Click Next.
40. At the Configure service account and distributed key management window, click Select and select the domain SCVMM user created above. Enter the password for this user. Do not select the checkbox next to “Store my keys in Active Directory”. Click Next.
41. At the Port configuration window, click Next.
42. At the Library configuration window, leave the default settings and click Next.



43. Click Install.
44. When installation has completed, follow any instructions in the window and click Close and click Close again to close the installer.
45. If it is not already opened, open Virtual Machine Manager and Connect with the current Microsoft Windows session identity.
46. In Server Manager, under Manage, select Add Roles and Features and under the feature Remote Server Administration Tools > Role Administration Tools, install the Hyper-V Management Tools feature.
47. Install all available Windows Updates on the SCVMM VM.

Deploying and Managing the Management Hyper-V Cluster Using System Center 2025 VMM

This section will focus only on configuring the Networking, Storage and Servers in VMM to deploy and manage Hyper-V failover clusters.

Create Run As accounts in VMM

A Run As account is a container for a set of stored credentials. In VMM a Run As account can be provided for any process that requires credentials. Administrators and Delegated Administrators can create Run As accounts. For this deployment, a Run As account should be created for adding Hyper-V hosts. To create a Run As account in VMM, complete the following steps:

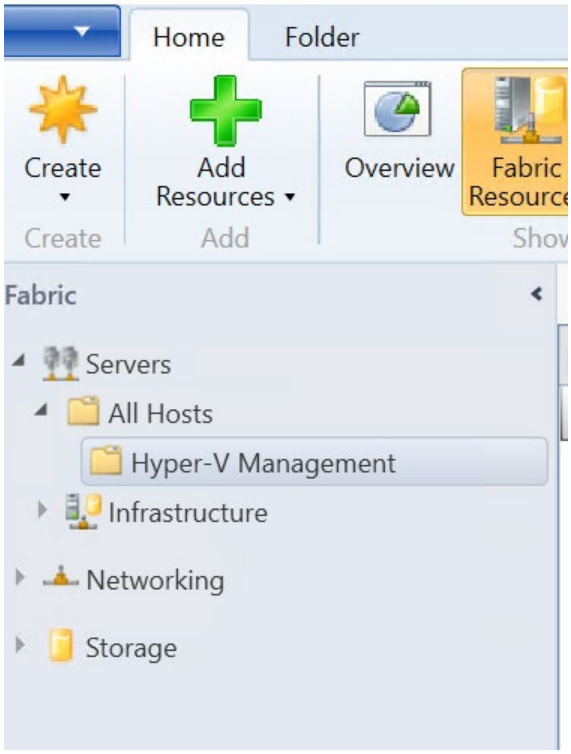
1. Connect to the AD Domain and create a scvmmrunas account and place in the Domain Admins group.
2. Click Settings, and at the top of the window, click Create Run As Account.
3. In Create Run As Account specify name and optional description to identify the credentials in VMM.
4. In User name and Password specify the credentials. The credentials can be a valid Active Directory user or group account, or local credentials. The scvmmrunas account created in step 1 should be used here.
5. Clear Validate domain credentials if you don't need it and click Finish to create the Run As account.

Set up host groups in the VMM compute fabric

You can use host groups to group virtual machine hosts in meaningful ways, often based on physical site location and resource allocation.

To create a host group structure in Virtual Machine Manager (VMM) for the Hyper-V Management Cluster, complete the following steps:

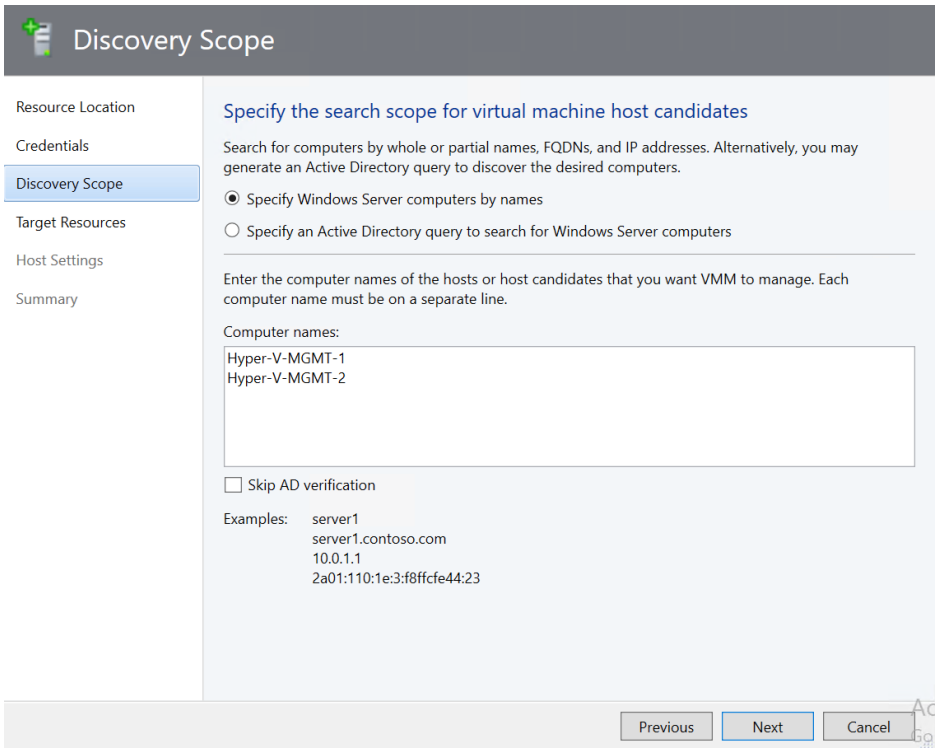
1. To create a host group structure, open the Fabric workspace.
2. In the Fabric pane, expand Servers.
3. Right-click All Hosts, and then click Create Host Group. VMM creates a new host group that is named New host group, with the host group name highlighted.
4. Type Hyper-V Management for the name and then press Enter.



Add Windows servers as Hyper-V hosts in the Host Group

When the Host Group is created, to add the Hyper-V hosts to Virtual Machine Manager, complete the following steps:

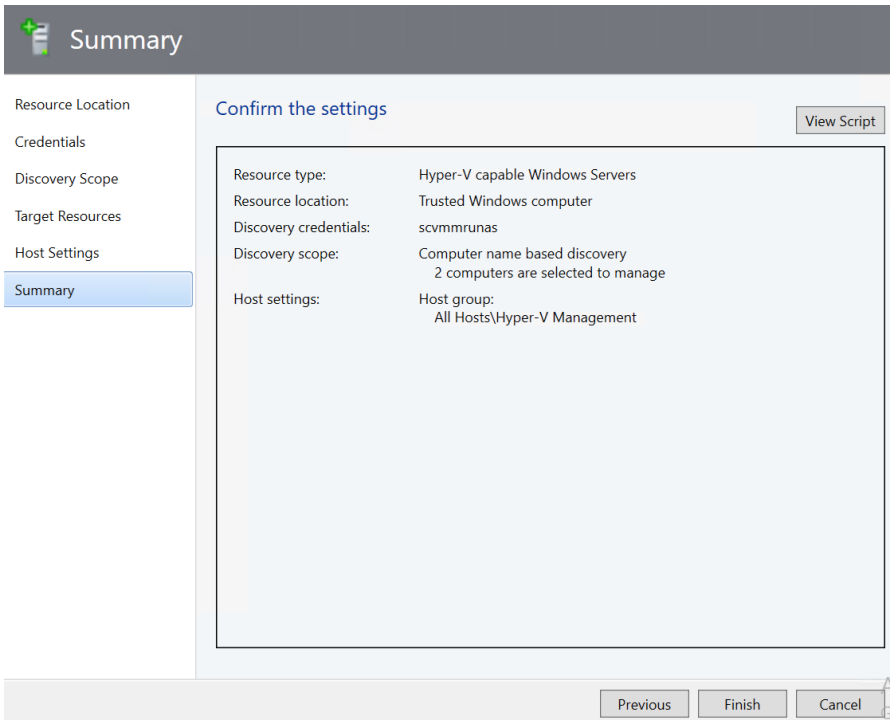
1. Open the Fabric workspace.
2. Select the just created host group, and On the Home tab, in the Add group, click Add Resources, and then click Hyper-V Hosts and Clusters. The Add Resource Wizard starts.
3. On the Resource location page, click Windows Server computers in a trusted Active Directory domain, and then click Next.
4. On Credentials page, select Use an Run As account, click Browse and add the Run as account created earlier. Click Next.
5. On Discovery scope, select Specify Windows Server computers by names and enter the Computer names. Click Next.



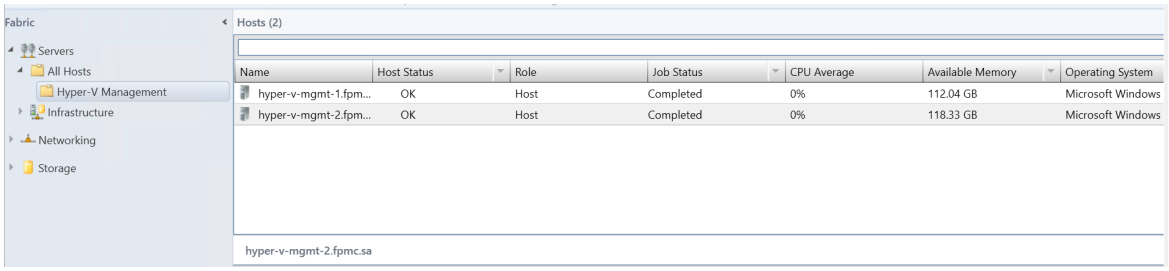
6. Under Target Resources, select the check boxes next to the two Hyper-V management hosts that need to be added. Click Next.

   Note: If the Hyper-V role is not enabled on a selected server, you receive a message that VMM will install the Hyper-V role and restart the server. Click OK to continue.

7. On the Host settings page, In the Host group list, use the pulldown to select the Hyper-V Management Host Group.
8. On the Summary page, confirm the settings, and then click Finish.



9. A Jobs log window will open showing completion status. It may be necessary to reboot the two Hyper-V Management hosts. If the log indicates a reboot of the two hosts is required, on the left, select VMs and Services. In the expanded Host Group and Cluster, select the second Hyper-V-MGMT host. Right-click the host and select Restart. Shutdown the SCVMM VM. Then connect to either a console or RDP session on the first host and reboot it. Finally, once the first host has rebooted, used Hyper-V Manager to restart the SCVMM VM.



Set up VM networks in the VMM fabric

The below figure provides an overview of the fabric networking configuration within VMM 2025. We'll now dive deeper into the configuration of each part.

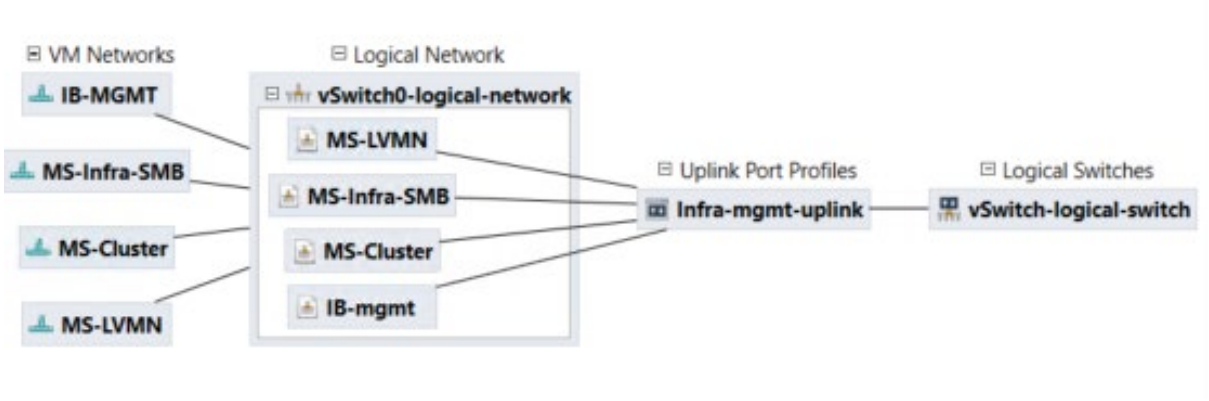
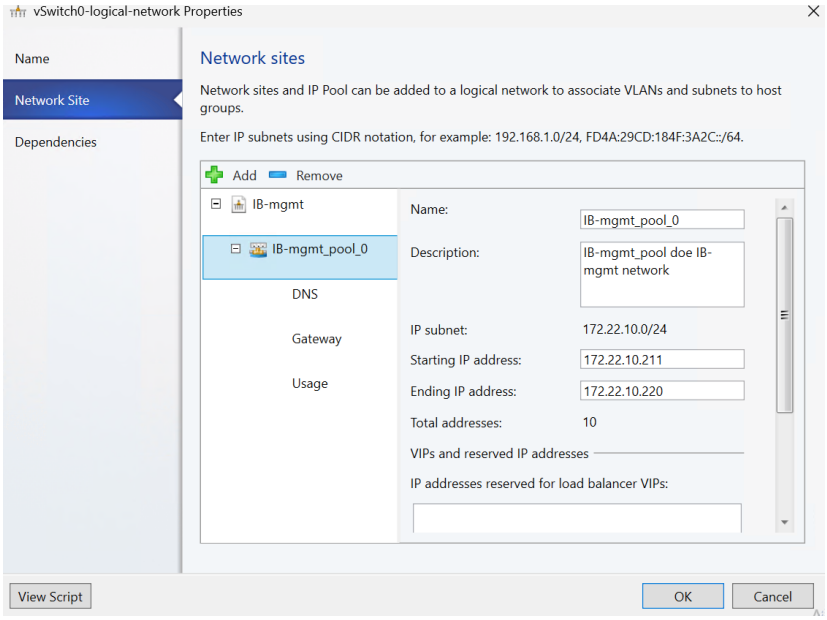


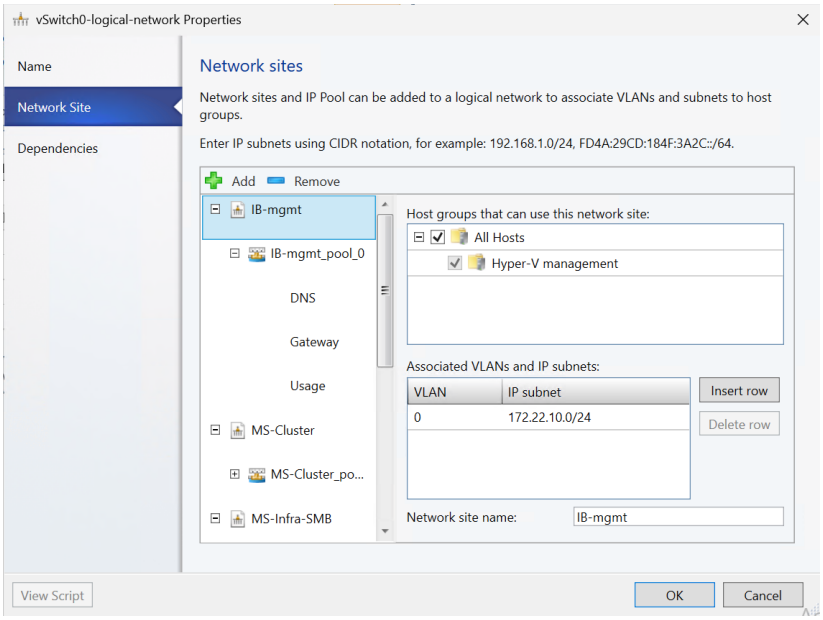
Figure 11) Overview of Fabric networking configuration in VMM 2025

Set up logical network

1. In VMM console, go to Fabric > Home > Show > Fabric Resources. In Fabric, expand Networking > Logical Networks > Home > Create > Create Logical Network.
2. In the Create Logical Network Wizard, select Name, and specify a name and description.
3. Under settings, select VLAN based Independent Network, click next.
4. In Network Site, add all the network sites to the logical network.
5. Click add > Network Site .
6. choose the Hyper-V Management host group in which the existing Hyper-V hosts are located
7. update network site name
8. click on insert row under “Associated VLANs and IP subnets” and update the VLAN id and ip subnet detail. Make sure to update IB-mgmt vlan id as 0.
9. Click on add ip pool under the network site.
10. Enter name, description, starting and ending IP address.
11. In DNS, specify DNS information, including DNS servers, the default DNS suffix for the connection, and the list of DNS search suffixes.
12. In Gateway, select Insert to specify default gateway

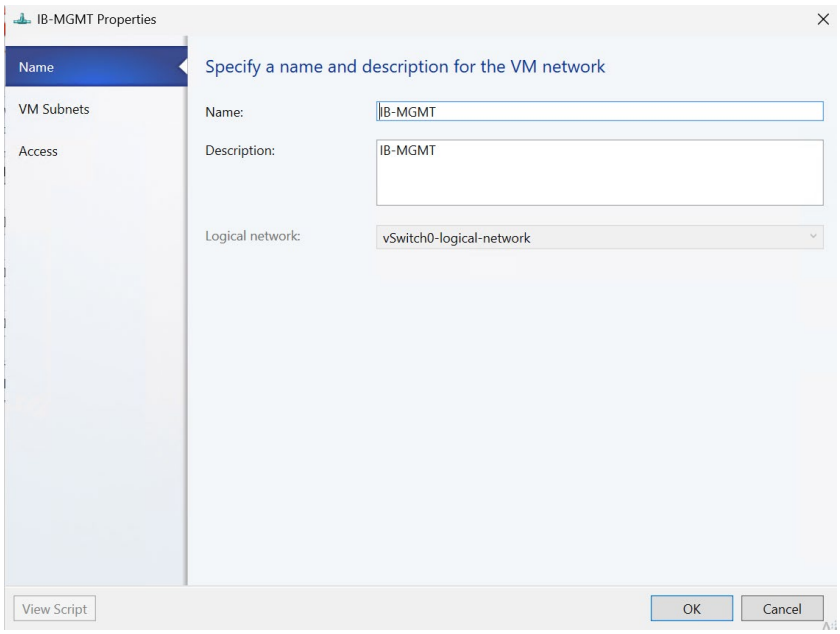


13. Repeat steps 5 to 12 for all the VLANs.



Setup VM networks

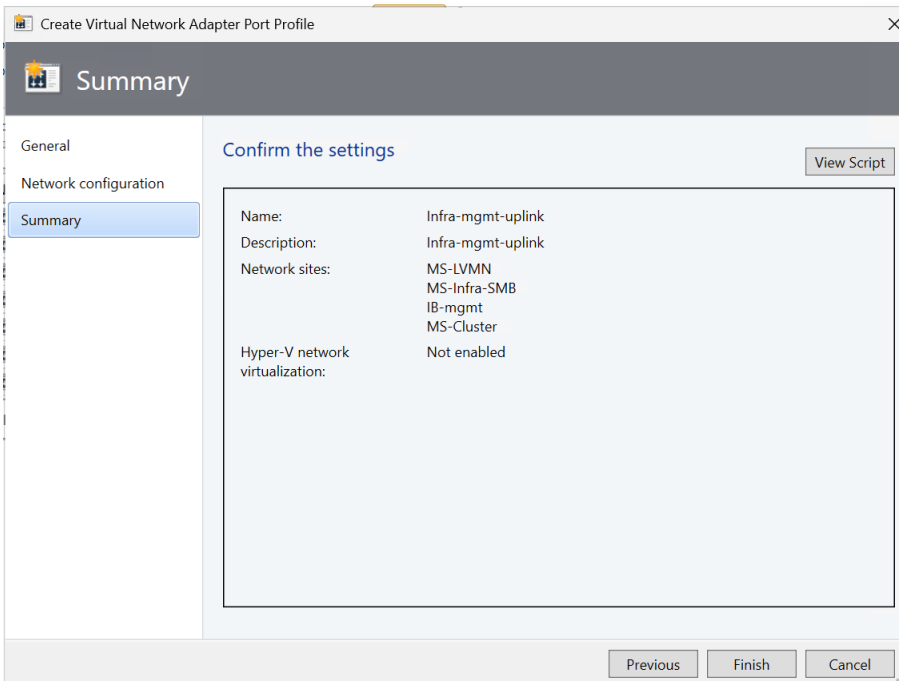
1. Select VMs and Services > VM Networks > Home > Create > Create > Create VM Network.
2. In Create VM Network Wizard > Name, enter a name and description and select a logical network on which to base the VM network.



3. On the Isolation Options page, select a network site and specify a VLAN to configure isolation manually.
4. On the Summary page, verify settings and select Finish.
5. Repeat the above steps to add all the networks.

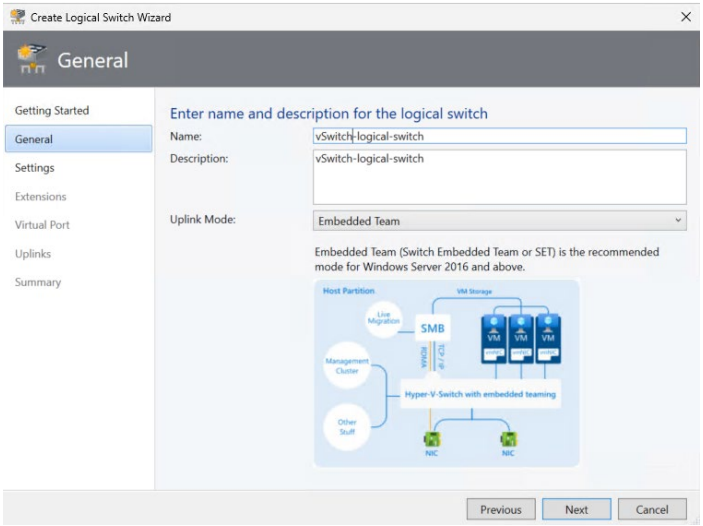
Set up port profile

1. Select Fabric > Home > Show > Fabric Resources. Select the Fabric tab > Networking > Port Profiles > Hyper-V Port Profile.
2. In Create Hyper-V Port Profile Wizard > General, enter a name and description, and select Uplink Port Profile. Select the Hyper-V port as the load balancing algorithm and Switch Independent as teaming mode.
3. On the Network Configuration page, select all the network sites.
4. On the Summary page, review the settings and select Finish.



Set up a logical switch

1. Select Fabric > Networking
2. Right-click Logical Switches, and then select Create Logical Switch.
3. In Create Logical Switch Wizard > Getting Started, review the information.
4. In General - Specify a name, description
5. In Uplink Mode, select Embedded Team

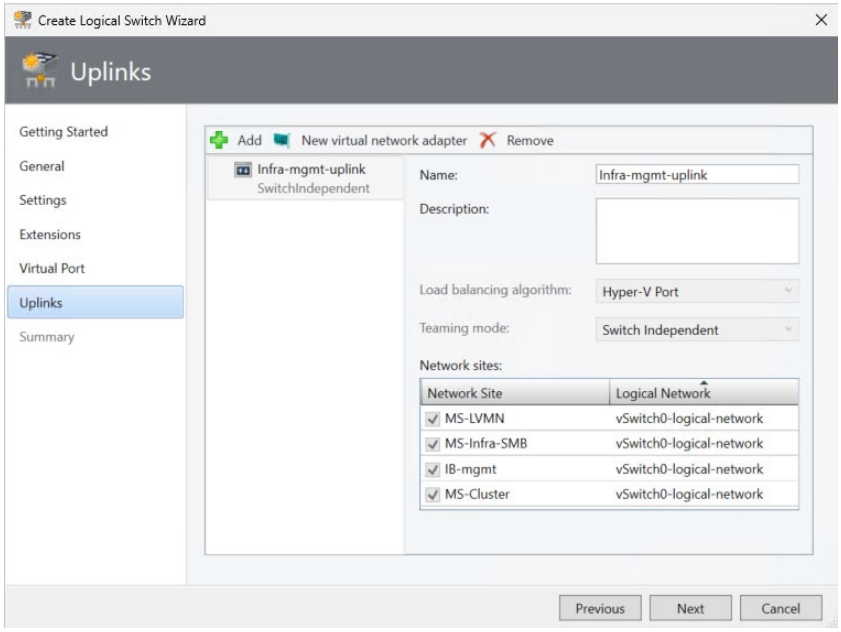


6. In Settings, select the minimum bandwidth mode as Absolute

   Note: If the bandwidth mode is not set as absolute then Convert to logical switch option would be greyed out

7. Skip adding entries under extensions and virtual ports page.

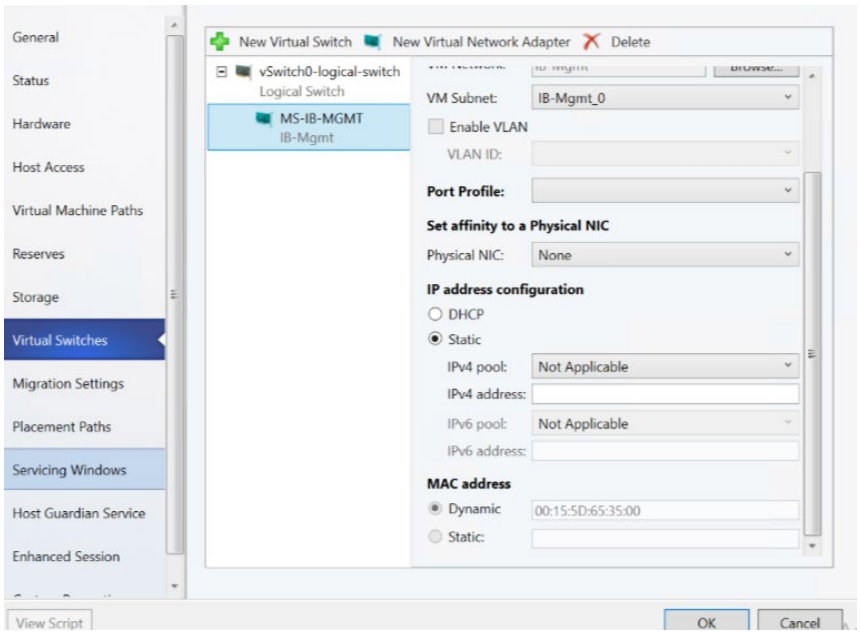
8. On the Uplink page, click add existing port profile.



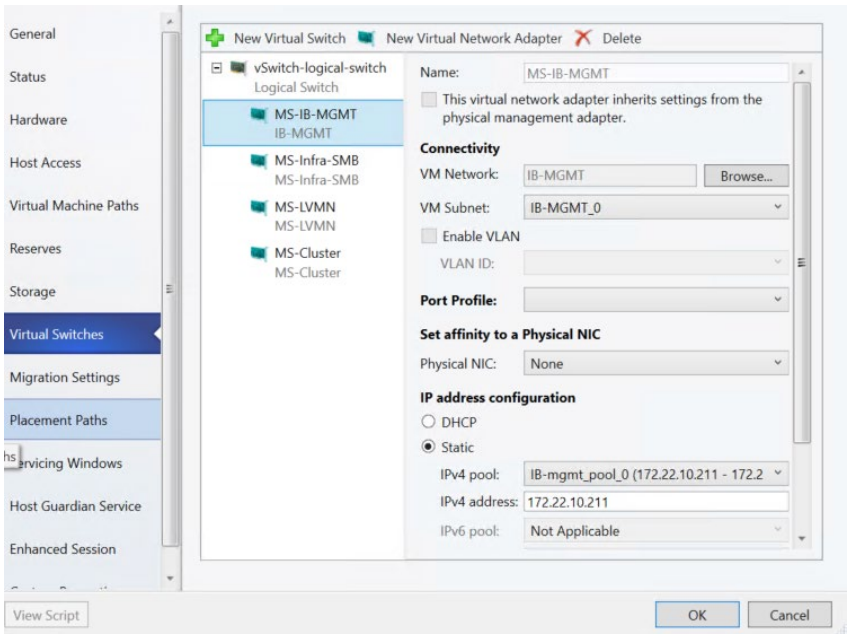
9. On the Summary page, review the settings and select Finish. Verify if the switch created appears in Logical Switches.

Convert virtual switch to logical switch

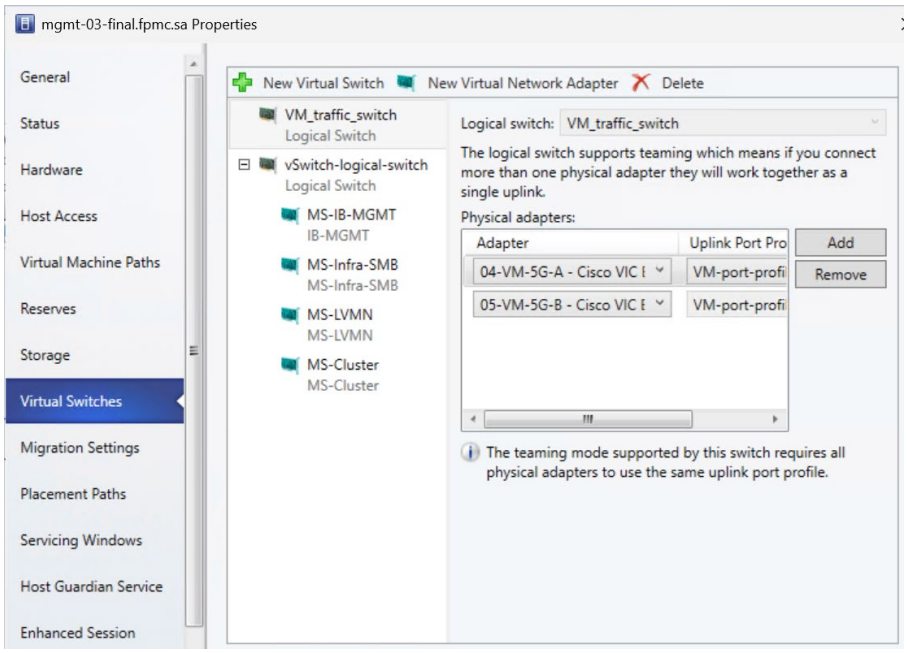
1. In the VMM console > Fabric > Servers > All Hosts, right-click the host > Properties.
2. On the Virtual Switches tab, select Convert to Logical Switch.
3. Select the logical switch which was created in the earlier stage, select the uplink port profile and select Convert.
4. Ensure the job has a status of Completed and then close the dialog.
5. To verify that the switch was converted, right-click the host, select Properties, and then select the Virtual Switches tab.



6. Connect to the host using the vKVM console and update the IP address for IB-Mgmt network. Make sure the DNS entry is updated as well
7. Login back to VMM console and select the IPv4 pool under IP address configuration and mention the IP address, click OK.
8. Click on add “New Virtual Network Adapter” and update the VM network and add static IPv4 address for all other networks.



9. Repeat the above steps to convert the external switch to logical switch on the other Hyper-V host.
10. Created a logical switch in a similar way for VM traffic which is mapped with vNICs which contains VM vlans.

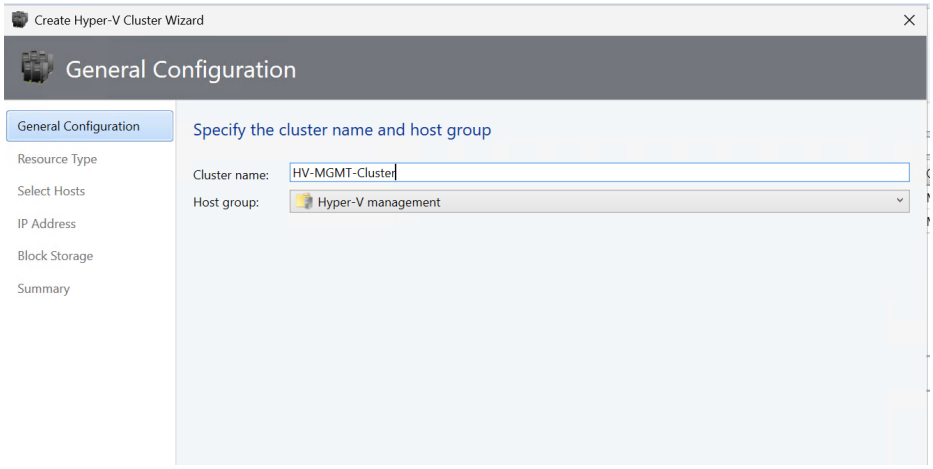


Create Windows Failover Cluster

To create a Windows Failover Cluster, complete the following steps:

Note: Be sure to create DNS records for the Cluster name. The IP address for cluster management should be on the IB-MGMT Subnet.

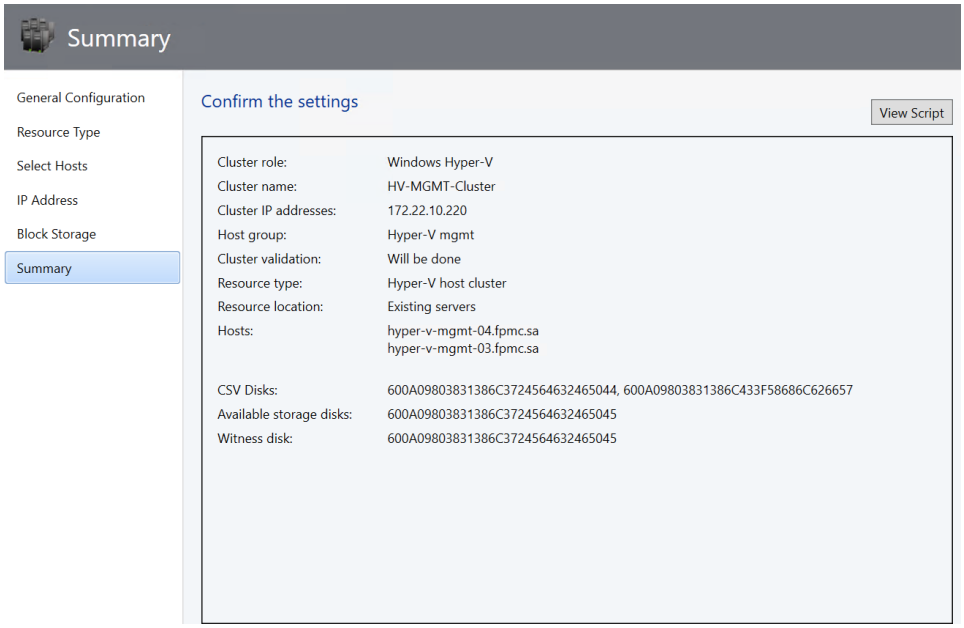
1. In the VMM console, click Fabric > Create > Hyper-V Cluster to open the Create Hyper-V Cluster wizard.
2. In General Configuration, specify a cluster name and choose the Hyper-V Management host group in which the existing Hyper-V hosts are located. Click Next.



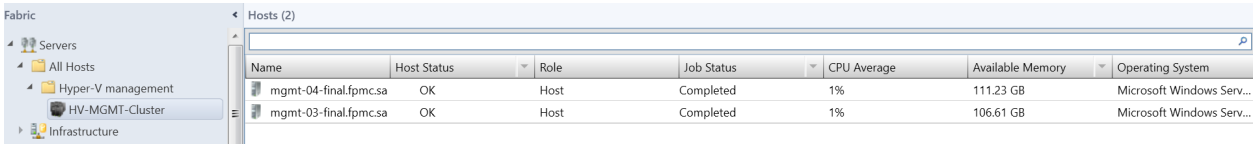
3. In Resource Type, select the SCVMM Run As account that you'll use to create the cluster. Make sure “Existing servers running a Windows Server operating system” is selected and click Next.

Note: The accounts that you use must have administrative permissions on the servers that will become cluster nodes, and must belong to the same domain as the Hyper-V hosts that you want to cluster. Also, the account requires Create Computer objects permission in the container that is used for Computer accounts in the domain. Ensure that the option Existing Windows servers is selected.

4. In Nodes, select the Hyper-V host servers that you want to include in the cluster. Click Next
5. In IP address, select the IB-MGMT subnet and type in the IP address you want to use for the cluster. Click Next.
6. In Block Storage, for the two 500GB disks, select the GPT partition style, Quick Format, and CSV. For the 500 GB disk with the Name closest to the name for the 1 GB disk, make the Volume Label Infra-iSCSI-01. Make the Volume Label for the other 500GB disk Infra-iSCSI-02. Update the Volume Label for the two 200GB disks of SQL_data and SQL_log as well. Click Next.
7. In Summary, confirm the settings and then click Finish.



8. You can go to the jobs workspace and click on “Install Cluster” job to see the status of cluster installation. Fix and troubleshoot any errors or warnings and revalidate the cluster.
9. After the cluster is installed, a new cluster icon is seen after expanding the Servers > All Hosts > Hyper-V Management host group in the fabric workspace. Right-click on the cluster and click on properties to view the status and other information about the cluster.



Hyper-V Cluster Communication Network Configuration

A failover cluster can use any network that allows cluster network communication for cluster monitoring, state communication, and for CSV-related communication.

The following table shows the recommended settings for each type of network traffic.

To configure a network to allow or not to allow cluster network communication, you can use Failover Cluster Manager or Windows PowerShell.

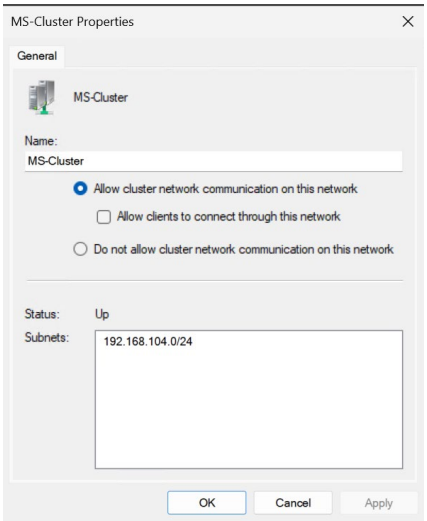
Table 3) Recommended Settings for Network Traffic

Network Type	Recommended Setting
Management	Both of the following: - Allow cluster network communication on this network - Allow clients to connect through this network
Cluster	Allow cluster network communication on this network Note: Clear the Allow clients to connect through this network check box.
Live migration	Allow cluster network communication on this network Note: Clear the Allow clients to connect through this network check box.
Storage	Do not allow cluster network communication on this network

1. On the SCVMM VM, open Failover Cluster Manager and connect to the Failover Cluster just created. Click Networks in the navigation tree.

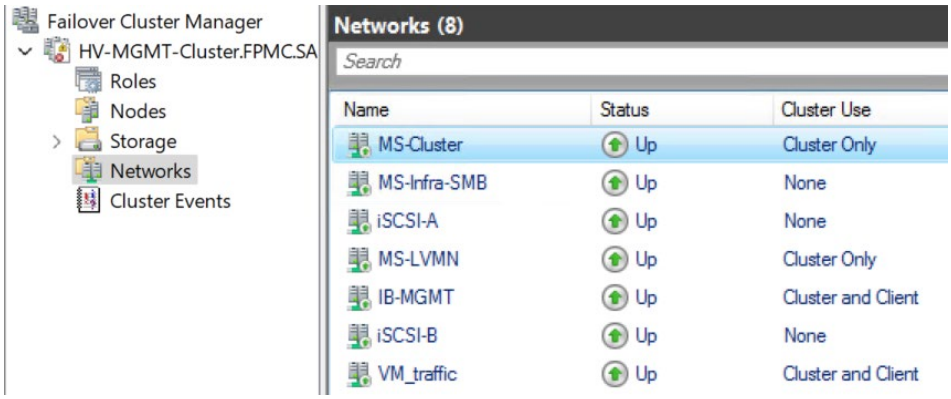
Note: It may be necessary to install the Failover Clustering Tools Feature under Features > Remote Server Administration Tools > Feature Administration Tools in the Add Roles and Features Wizard to install Failover Cluster Manager.

2. In the Networks pane, right-click a network, and then click Properties.



3. Using the subnet information reset the Name of the Cluster Network to the appropriate name, adjust the communication setting and click OK. It may be necessary to edit the network two times to get the name and Cluster Use setting correctly input.

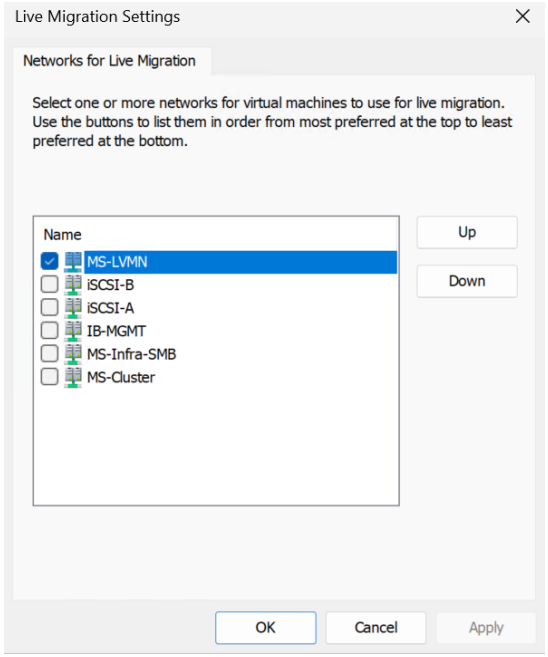
4. Repeat step 3 to assign a descriptive name to all Cluster Networks.



Live Migration Network Settings

By default, live migration traffic uses the cluster network topology to discover available networks and to establish priority. However, you can manually configure live migration preferences to isolate live migration traffic to only the networks that you define. Complete the following steps:

1. Open Failover Cluster Manager.
2. In the navigation tree, right-click **Networks**, and then click **Live Migration Settings**.
3. Select only the Live Migration network (MS-LVMN).

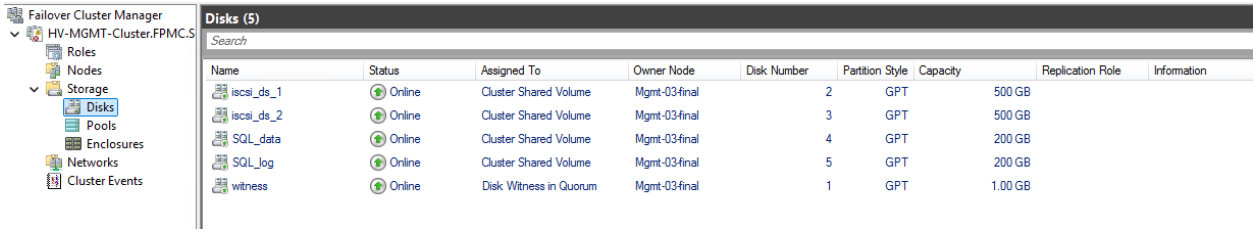


4. Click Apply and OK to save this setting.

Cluster Storage Settings

1. On the left, expand Storage and select Disks.
2. Right-click the Witness disk and select Properties.
3. Change the Disk Name to Witness and click OK.

4. Looking at the volume names for the Cluster Shared Volumes, rename them to match to storage volume names. Note, the mount pointy for each CSV.



Make SCVMM a Highly Available VM

1. In Virtual Machine Manager, in the VMs and Services workspace, select the first Hyper-V Management host and in the VMM pane, right-click the SCVMM VM and select Migrate Storage.

2. Browse to C:\ClusterStorage\Volume1. Select the radio button to Automatically place all VHDs with the configuration. Click Next.

3. Click Move. The migration will take several minutes.

4. Right-click the SCVMM VM again and select Properties. Select Hardware Configuration. Ensure that Availability is High.

Build a Virtual Machine & Install NetApp SMI-S Provider

1. In Virtual Machine Manager, in the Library workspace, at the top select Import Physical Resource. Click “Add resource” and browse to the location of the Windows Server 2025 ISO. Select the ISO and click Open. Back in the Import Library Resources window, click Browse, select the MSSCVMMLibrary, and click OK. Click Import. When the resource is successfully imported, close the Jobs window.
2. On the SCVMM VM use Windows Explorer to navigate to C:\ProgramData. Add the Everyone user to the Sharing on the Virtual Machine Manager Library Files” folder with Read-only permissions.
3. In Virtual Machine Manager, in the VMs and Services workspace, select the HV-MGMT-Cluster. Right-click the cluster and select Create Virtual Machine.
4. Under Select Source, select “Create the new virtual machine with a blank virtual hard disk” and click Next.
5. Under Identity, name the virtual machine SMI-S-Provider, select Generation 2, and click Next.
6. Under Configure Hardware, select the Hyper-V Cloud Capability Profile, 2 Processors, 8192 MB Virtual machine memory, a new Dynamic 120 GB Virtual Hard Disk that contains the operating system, the Windows Server 2025 Installation ISO connected to the Virtual DVD drive with “Share file instead of copying it” selected, Network Adapter 1 connected IB-Mgmt and Availability set to “Make the virtual machine highly available. Click Next.
7. Under Select Destination, select “Place the virtual machine on a host” and make sure the “Hyper-V Management” Destination is selected. Click Next.
8. Under Select Host, allow the placement process to run, accept the recommendation, and click Next.
9. Under Configure Settings, Virtual Machine Location, browse to C:\ClusterStorage\Volume1. Also under Machine Resources, browse to C:\ClusterStorage\Volume1 for the Destination path of the Virtual Hard Disk. Click Next.
10. Under Add Properties, select the Windows Server 2025 Datacenter Operating system and click Next.
11. Under Summary, click Create.
12. When the virtual machine is successfully created, close the Jobs window.

13. In Virtual Machine Manager, in the VMs and Services workspace, right-click the newly created SMI-S-Provider VM and select Power On. Then right-click the VM and select Connect or View > Connect via Console. Click the icon to send Ctrl-Alt-Del to the VM and press Enter when you see “Press any key to boot from CD or DVD”.
14. Install Windows Server 2025 Datacenter with Desktop Experience on the VM, assign it an IP address and hostname and join the VM to the Windows Domain, and install all Windows Updates on the VM.
15. Download the NetApp SMI-S Provider version 5.2.7 to the local desktop from http://mysupport.netapp.com. Save the file as smisprovider-5-2-7.msi.
16. Navigate to the directory that contains the NetApp SMI-S Provider software package. Double-click the package name.
17. Complete the steps in the setup wizard to complete the install.
18. Using the search icon, enter run and open the Run application.
19. Open the Local Users and Groups window by entering lusrmgr.msc and pressing Enter.
20. Add a user named SMIS-User as a local Administrator

Configure the NetApp SMI-S Provider

1. In the Start Menu, navigate to NetApp SMI-S Provider.
2. Right click and select Run as Administrator. A command line prompt should open.
3. Run the command smis cimserver status to ensure the NetApp SMI-S Provider is running

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin>smis cimserver status

NetApp SMI-S Provider is running.
```

4. Add a user to the CIM server by running the following command:

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin>cimuser -a -u SMI-S-Provider\smis
Please enter your password: ********
Please re-enter your password: ********
User added successfully.
```

5. Add the Infrastructure SVM to the SMI-S Provider using the following command:

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin>smis addsecure 172.22.10.150 vsadmin
Enter password: ********
Returned Path  ONTAP_FilerData.hostName="172.22.10.150",port=443

Successfully added 172.22.10.150
```

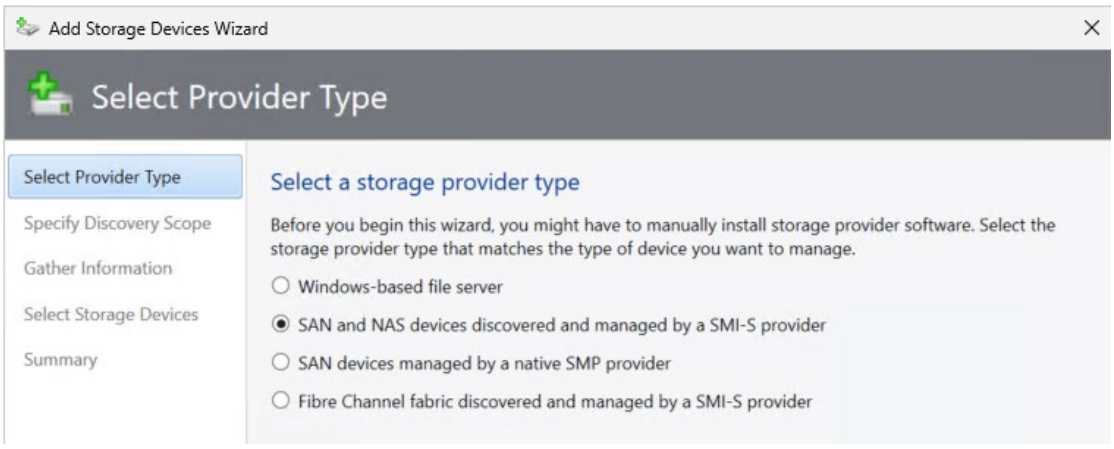
NetApp SMI-S Integration with VMM

1. To add a remote storage device in Virtual Machine Manager (VMM), you can add and discover external storage arrays that are managed by Storage Management Initiative – Specification (SMI-S) or Store Management Provider (SMP) providers.
2. To add an SMI-S storage device, make sure that you have installed the SMI-S provider for the array on a server that the VMM management server can access over the network by IP address or by fully qualified domain name (FQDN).

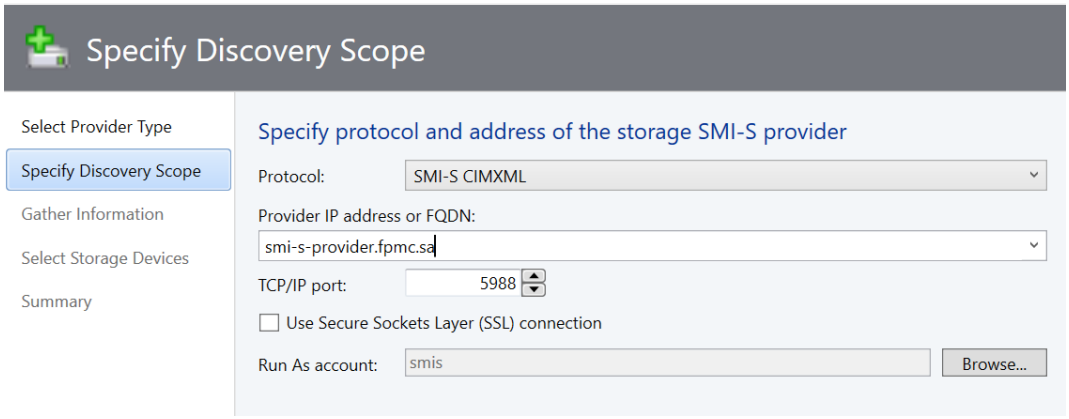
Note: Do not install the SMI-S provider on the VMM management server. This configuration is not supported.

Add a storage device

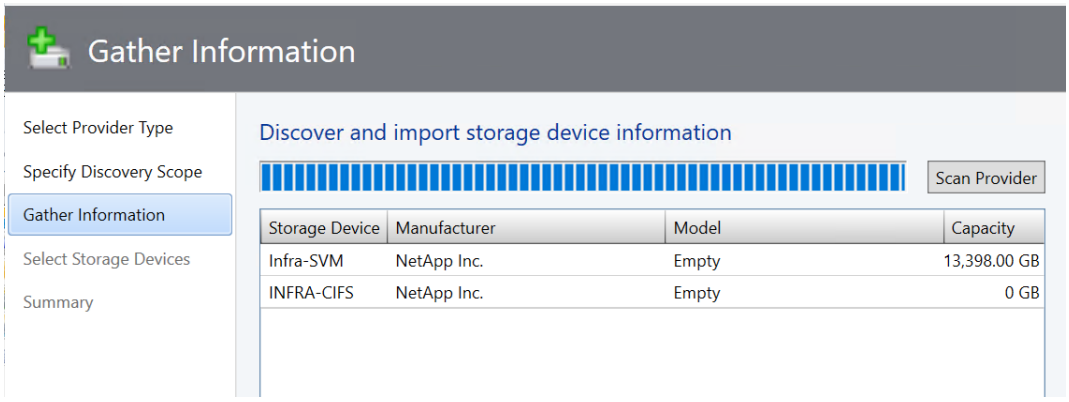
1. In Virtual Machine Manager, click Fabric > Storage > Providers >Add Storage Devices.
2. In Add Storage Devices Wizard > Select Provider Type, select to add a storage device with SMI-S. Click Next.



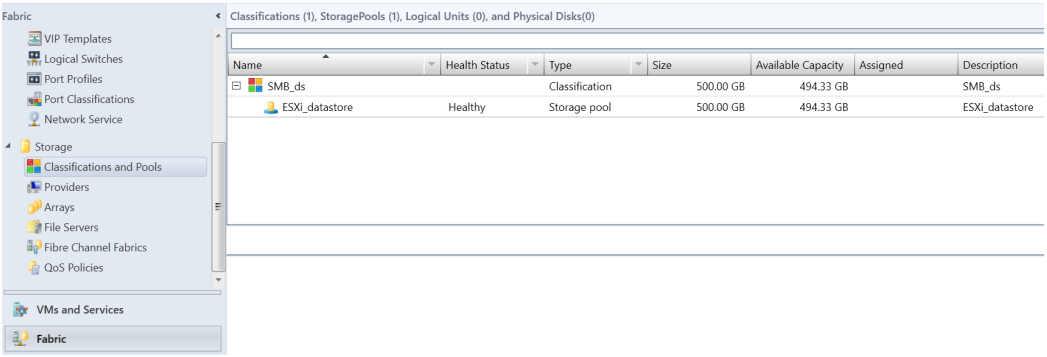
3. In Specify Discovery Scope, select Protocol - SMI-S CIMXML, add the IP address/FQDN of the SMI-S Provider, and add the port used to connect to the provider on the remote server. You can enable SSL if you're using CIMXML. Then specify an account which was created earlier for connecting to the provider. Click Next.



4. In Gather Information, VMM automatically tries to discover and import the storage device information. You will need to import the security certificate.
5. If the discovery process succeeds, the discovered storage arrays, storage pools, manufacturer, model, and capacity are listed as shown in the below figure. When the process finishes, click Next.

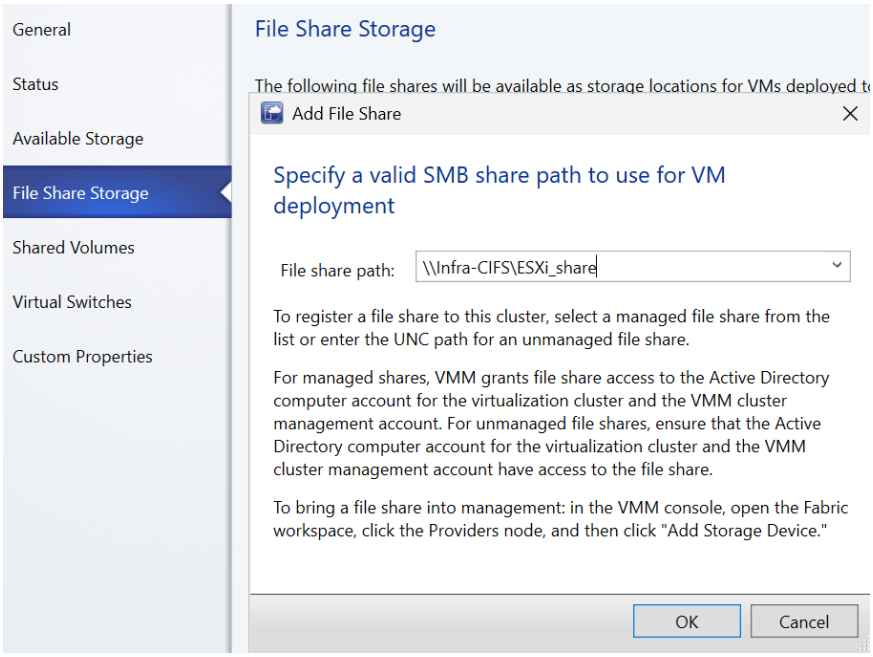


6. In Select Storage Devices, specify a classification and host group from the drop-down list for each storage pool. Create storage classifications if none exists to group storage pools with similar characteristics. Only select storage where VMs will be stored. Click Next.
7. On the Summary page, confirm the settings, and then click Finish. The Jobs dialog box appears. When status is Completed you can verify the storage in Fabric > Storage > Classifications and Pools.



Add SMB file share to the Hyper-V host clusters

1. In Virtual Machine Manager, click servers > All Hosts > [Host Group]. Locate and right-click the Cluster name.
2. right-click and select properties.
3. Go to "File Share Storage" Tab. Click on add and enter the SMB path as shown in below screenshot.

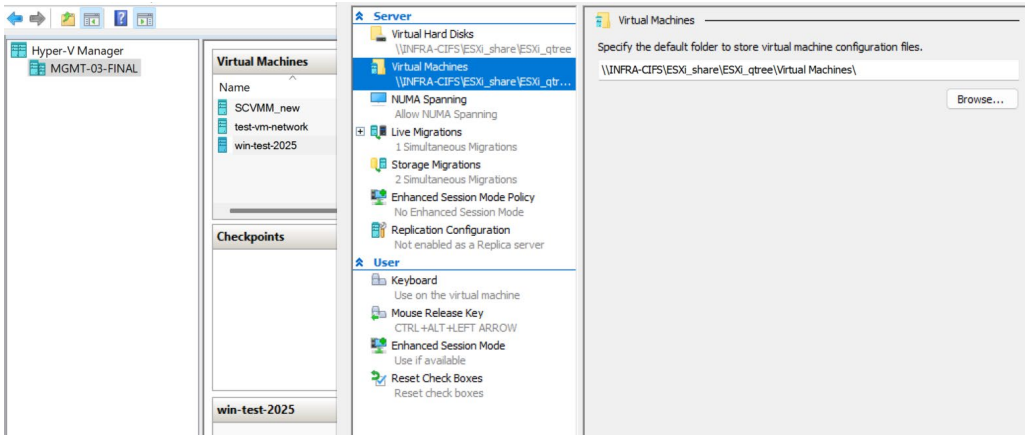


Update Default Virtual Machine and Virtual Hard Disk Storage Paths

To ensure all new virtual machines and their associated virtual hard disks are stored on the designated SMB file share, follow the steps below to update the default paths on the Hyper-V host:

1. Open Hyper-V Manager on the Hyper-V management host.
2. In the left pane, right-click the Hyper-V host and select Hyper-V Settings.
3. Under Server section, Click Virtual Hard Disks and update the path to the desired SMB share.

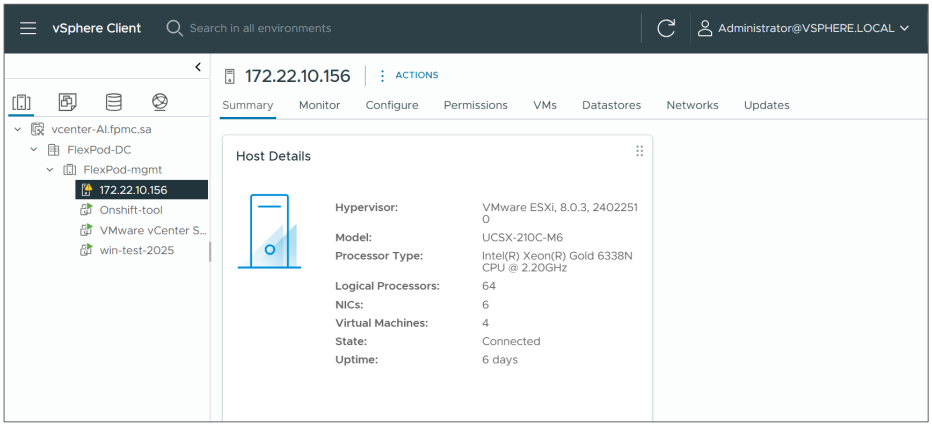
4. Click Virtual Machines and similarly change the default location for virtual machine configuration files to the same SMB path or a subfolder if preferred.



VMware vSphere 8.0U3 Setup

NetApp Shift toolkit doesn't support NFS4.1 datastore so update the var value of nfs_datastore_type (roles/VMware/ESXIhosts/defaults/main.yml) to nfs3 and after that execute the ansible playbook.

Once the setup is done, create a test VM on vSphere which we will be migrating to Hyper-V using NetApp Shift toolkit.



NetApp Shift toolkit

This section will focus on installing & configuring the NetApp Shift Toolkit. After that we will migrate a test VM from vCenter to Hyper-V.

Installation

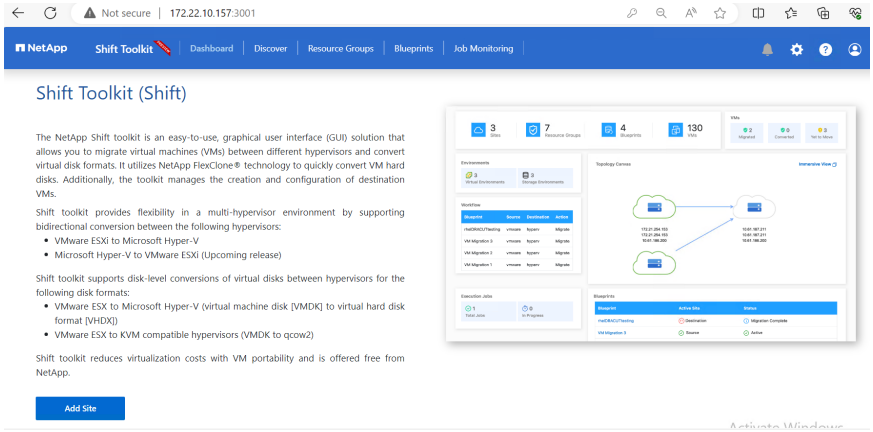
1. Download the Shift toolkit package from NetApp Toolchest and unzip it.
2. Run the exe to install and start the service
3. Using the browser, access Shift toolkit UI by entering the http://<IP address specified during installation>:3001

   Note: If you have configured proxy in your setup then make sure to add Shift IP in the exclusion list

4. Access the UI using default credentials as below:
   Username: admin
   Password: admin

Note: The admin credential can be changed using “Change Password” option.

5. Accept the legal EULA by clicking on “Accept and Continue”
6. Installation is completed.



Shift Toolkit Configuration

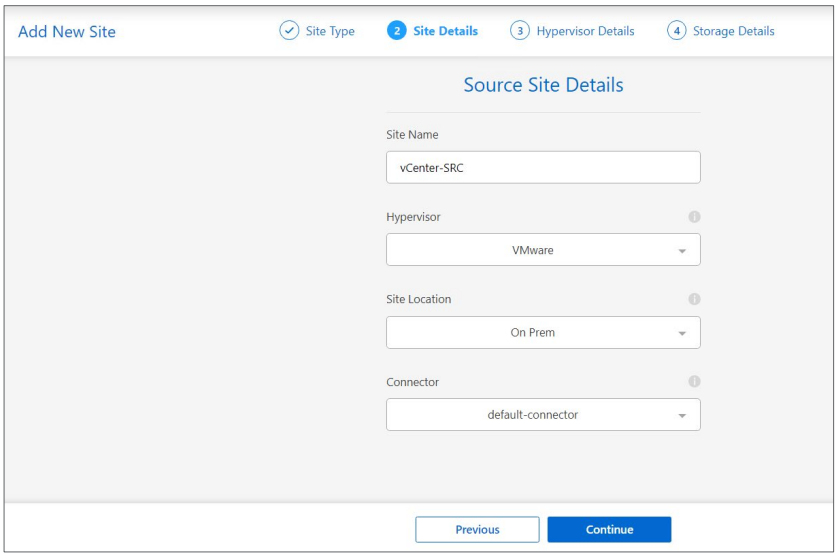
Below are the key steps planned for Shift Toolkit configuration:

- Add Source/Destination site: Configured vCenter as source and SCVMM as destination.
- Create Resource Group: Grouped relevant compute and storage resources.
- Define Blueprint: Standardized VM, network, and storage settings.
- Migration: Verified setup for solution validation phase.

Add Source/Destination site

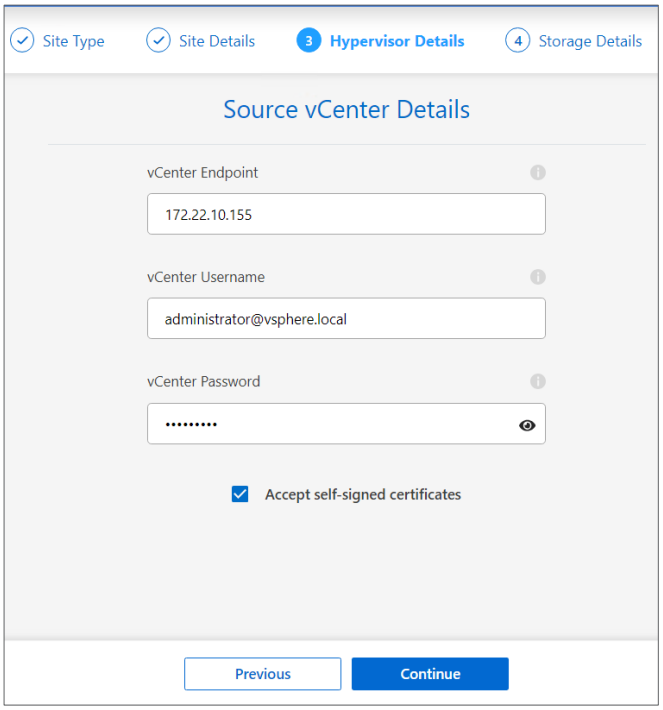
1. Click on add site to add the source into the Shift toolkit.
2. Enter source site details:
    - Site Name - Provide a name for the site
    - Hypervisor – Select VMware as the source
    - Site Location – Select the default option
    - Connector – Select the default selection

      Once filled, click Continue.



3. Enter Source vCenter details:
   - Endpoint - Enter the IP address or FQDN of the vCenter server
   - Username - username to access the vCenter
   - vCenter Password – Password to access vCenter
   - vCenter SSL Thumbprint (optional)

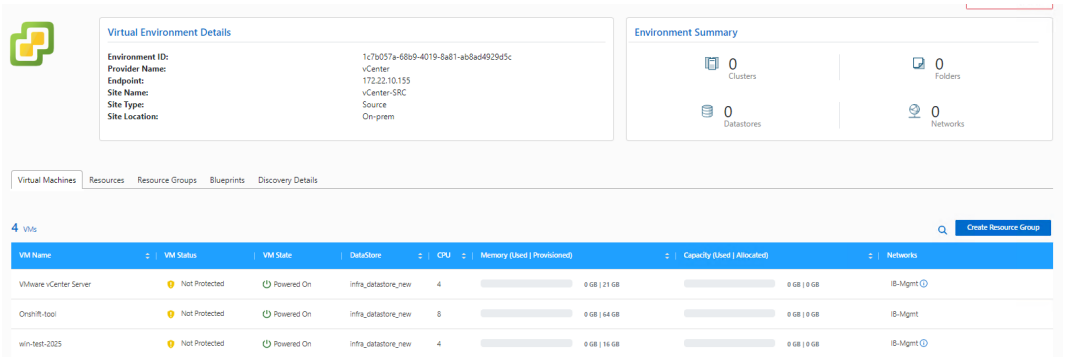
     Select “Accept Self signed certificate” and click Continue.



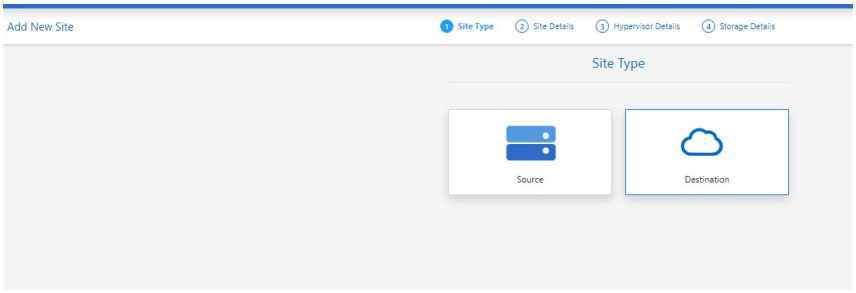
4. Enter ONTAP Storage system credentials

5. Once added, Shift toolkit will perform an automatic discovery and display the VMs along with the relevant metadata information. Shift toolkit will automatically detect the networks and port groups used by the VMs and will populate them.

To view the data for a specific vCenter, go to the dashboard, click on “View VM List” against the appropriate site name. The page will display the VM inventory along with the VM attributes.

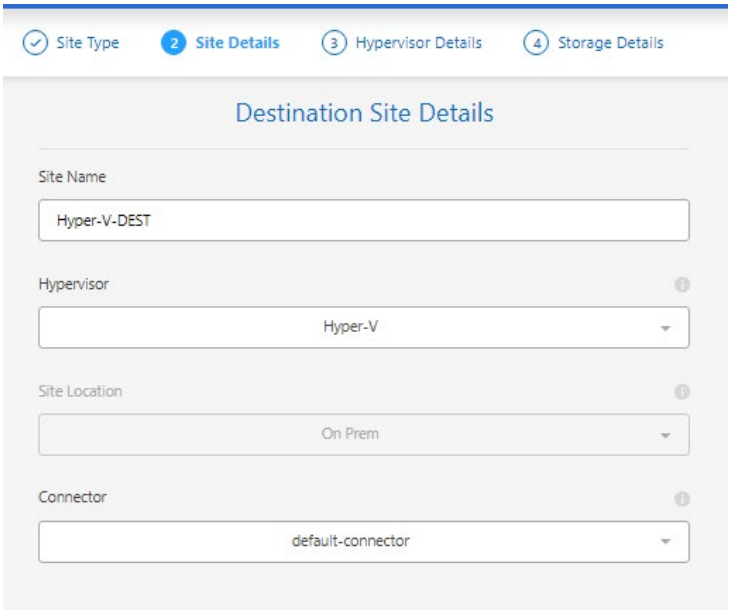


6. Next step is to add the destination hypervisor.



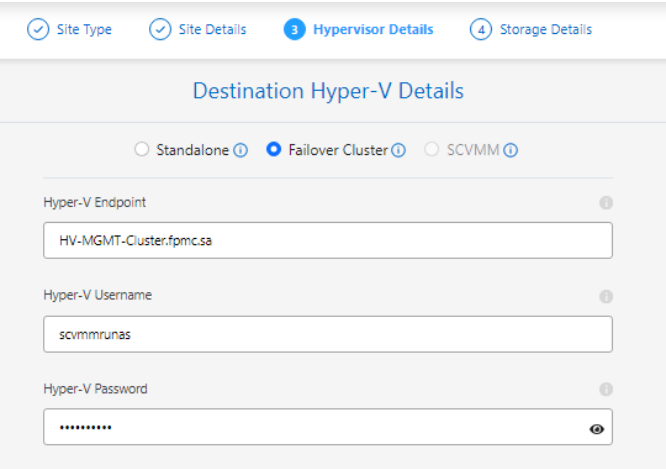
7. Enter Destination Site Details
   - Site Name - Provide a name for the site
   - Hypervisor – Select Hyper-V as the target
   - Site Location – Select the default option
   - Connector – Select the default selection

   Once filled, click Continue.



8. Destination Hyper-V details
   - select failover cluster and enter Hyper-V FQDN
   - Username - username to access Hyper-V
     Password – Password to access Hyper-V for performing inventory of the resources.

   Once done, Click Continue



9. Enter ONTAP Storage system details

Note: The source and destination storage system should be the same as the disk format conversion happens at the volume level.

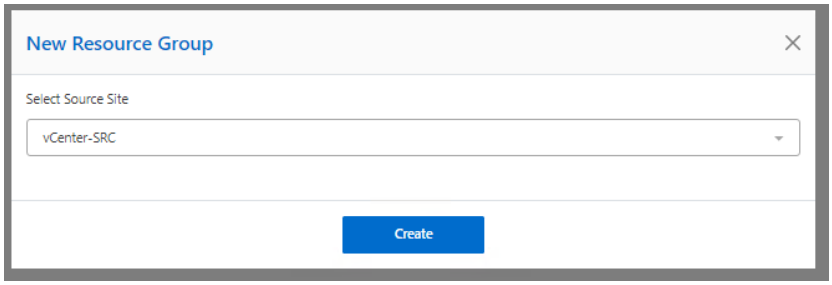
Create Resource Group

Once the platforms have been added, group the VMs you want to migrate or convert into resource groups. Shift toolkit resource groups allow you to group set of dependent VMs into logical groups that contain their boot orders and boot delays.

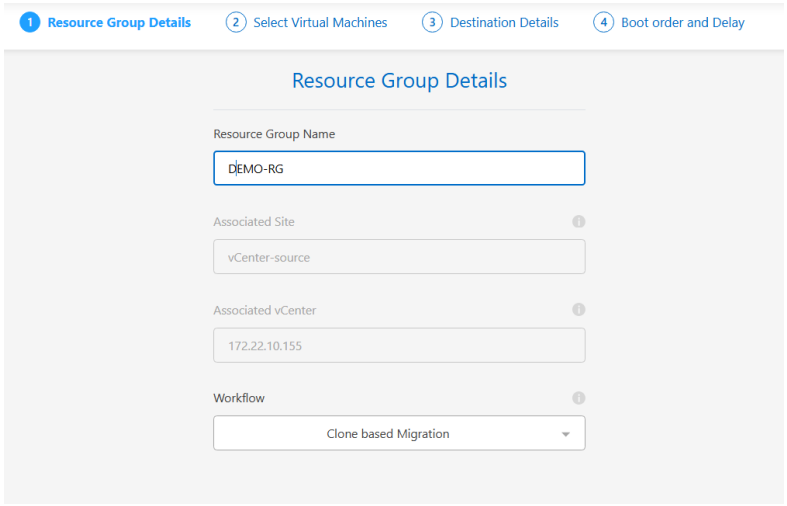
Note: Ensure the Qtrees are provisioned before creating the resource groups.

To start creating resource groups, click on the “Create New Resource Group” menu item.

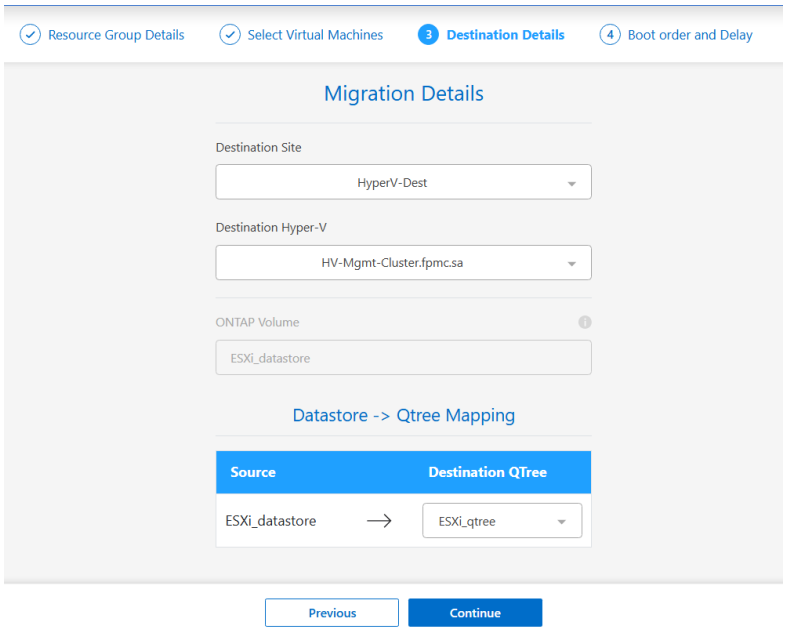
1. Access Resource groups, click on “Create New Resource Group”.
2. On the “New resource group”, select the Source site from the dropdown and click “Create”



3. Provide Resource Group Details and select the workflow as “Clone based Migration”, which performs end to end migration of the VM from source hypervisor to destination hypervisor.



4. Click on “Continue”
5. Filter the datastore where VM is placed and Select appropriate VMs using the search option.
6. Update the migration details by selecting “Destination Site”, “Destination Hyper-V entry” and Datastore to Qtree mapping.



7. Select the Boot Order and Boot delay (secs) for all the selected VMs. Set the order of power on sequence by selecting each virtual machine and setting up the priority for it. 3 is the default value for all virtual machines.

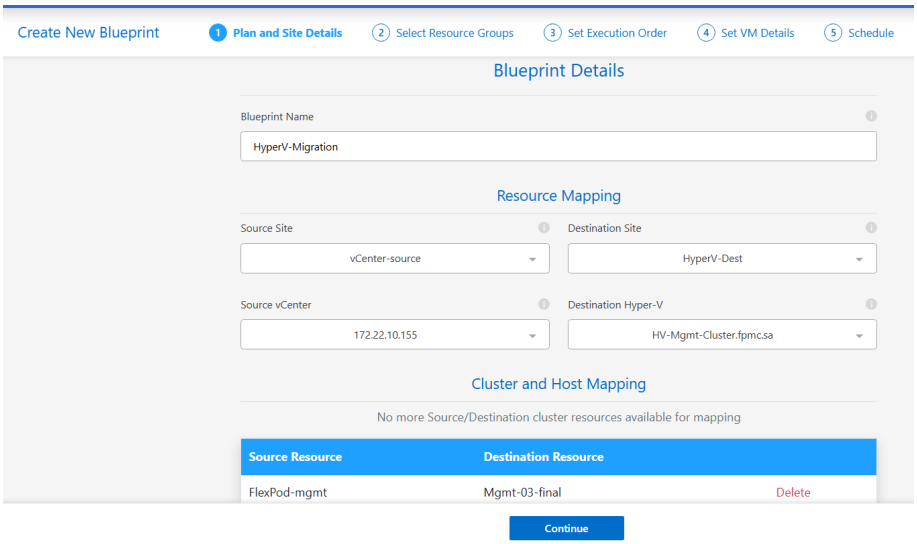
   Options are as follows:

   1 – The first virtual machine to power on
   3 – Default
   5 – The last virtual machine to power on

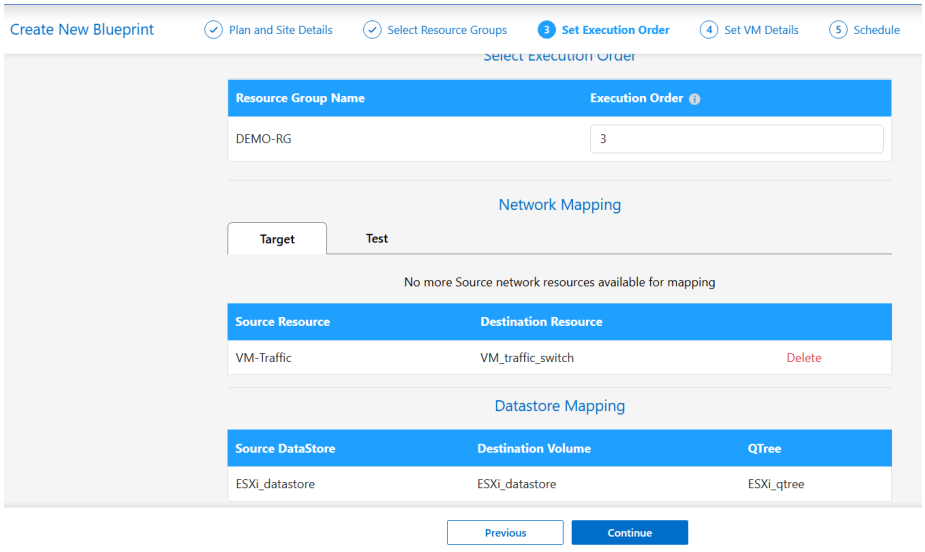
8. Click on “Create Resource Group”.

Define Blueprints

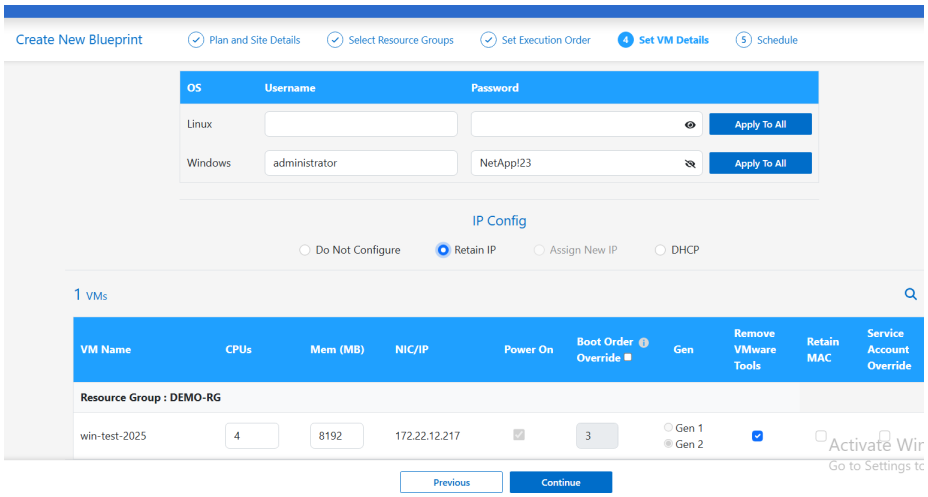
1. To start creating blueprint, click on the “Create New Blueprint”.
2. On the “New Blueprint”, provide a name for plan and add necessary host mappings by selecting Source Site, associated vCenter, Destination Site and associated Hyper-V hypervisor.
3. Once the mappings are done, select the cluster and host mapping.



4. Select Resource Group Details and click on “Continue”
5. Keep the Execution Order value for Resource Group as default value.
6. Select Network Mapping to the appropriate virtual switch. The virtual switches should already be provisioned within Hyper-V.
7. Based on the selection of VMs, storage mappings will be automatically selected.



8. Under VM details, provide username and password details for each OS type under Service Account section
9. Select Retain IP under IP config
10. Under VM configuration details, update any parameters if required like CPU, memory etc.



11. Click on “Create Blueprint”.

The base setup is now completed, and we will proceed to the solution validation phase to verify the environment’s functionality. As part of our validation process, we will also perform a cross-platform migration of a VM from VMware to Hyper-V using Shift

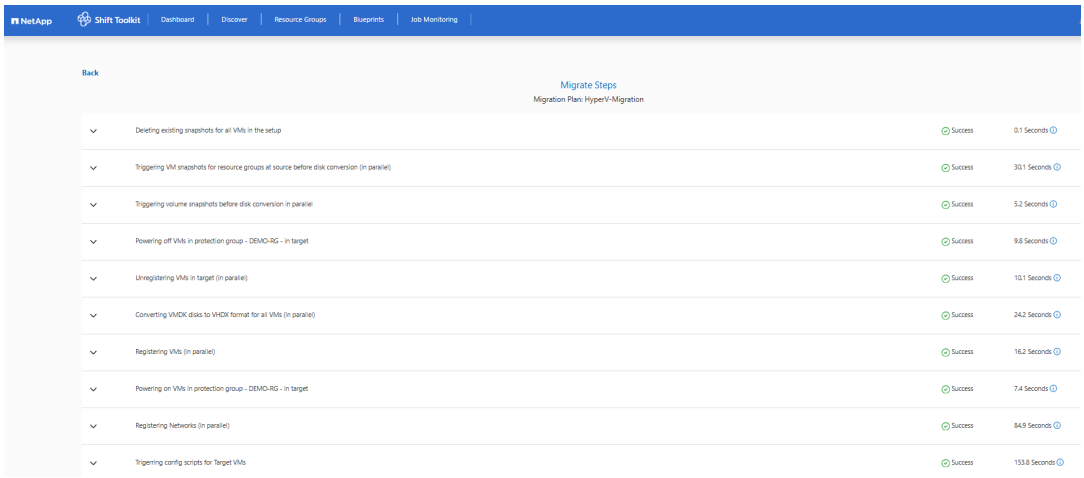
Solution validation

The following scenarios were validated as part of the solution testing:

- VM Migration using Shift Toolkit
- Build a test VM on Hyper-V
- Database workload simulation
- Live VM Migration
- Host Maintenance Operations

VM Migration using Shift Toolkit

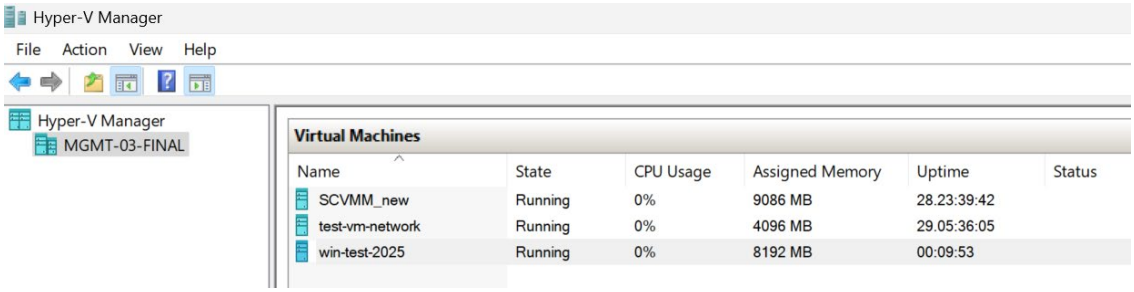
1. Power off the test VM before we begin with migration.
2. To trigger Migrate workflow with the configuration specified in Blueprint as it is, click on Migrate.
3. Once triggered, the preparation stage kicks in and the conversion process runs through all the steps as shown in the screenshot below



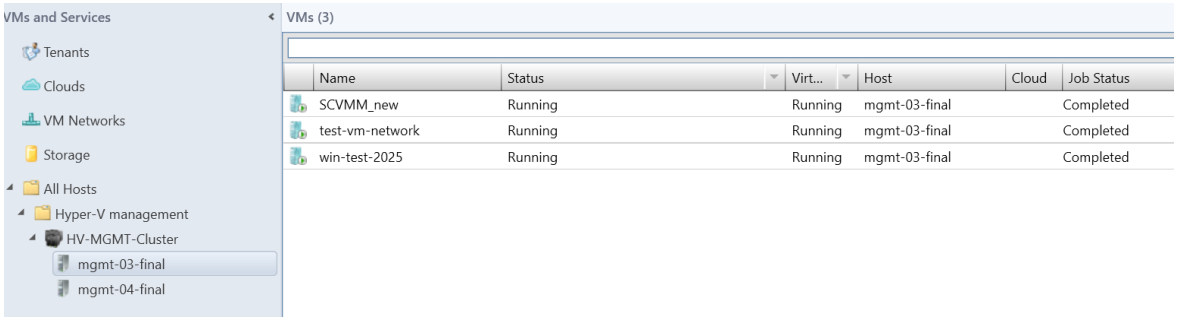
Note: It is recommended that no more than ten conversions be triggered parallelly from the same ESXi source to the same Hyper-V destination

Once the job is completed, the status of the blueprint changes to “migration Complete”.

With migration complete, it’s time to validate the VMs on Hyper-V side. Below screenshot shows the VMs running on the Hyper-V host that was specified during the blueprint creation.



You can verify the same on SCVMM as well.

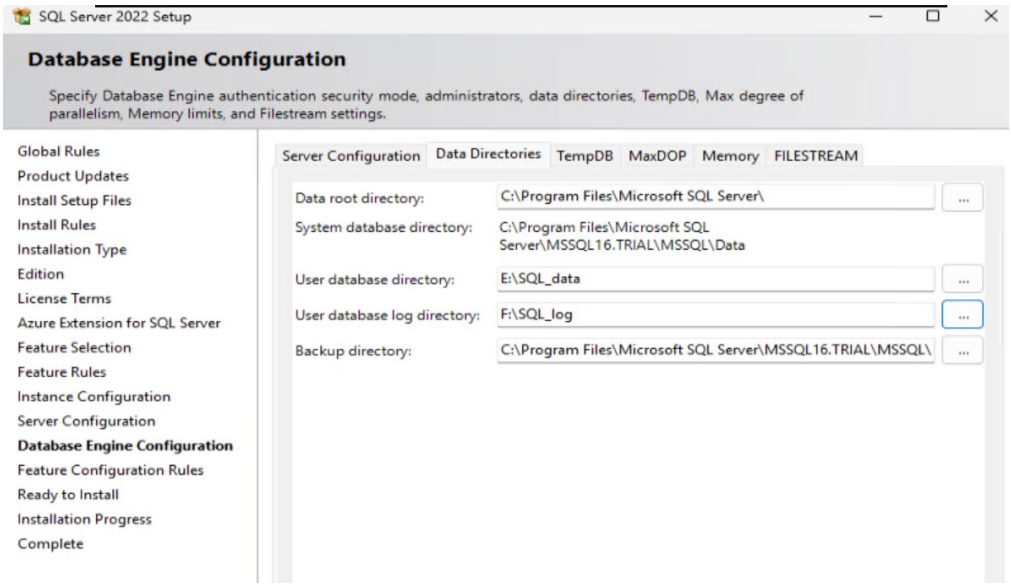


Build a Windows Server 2025 Virtual Machine on Hyper-V

4. In Virtual Machine Manager, in the Library workspace, at the top select Import Physical Resource. Click “Add resource” and browse to the location of the Windows Server 2025 ISO. Select the ISO and click Open. Back in the Import Library Resources window, click Browse, select the MSSCVMMLibrary, and click OK. Click Import. When the resource is successfully imported, close the Jobs window.

5. On the SCVMM VM use Windows Explorer to navigate to C:\ProgramData. Add the Everyone user to the Sharing on the Virtual Machine Manager Library Files" folder with Read-only permissions.
6. In Virtual Machine Manager, in the VMs and Services workspace, select the HV-MGMT-Cluster. Right-click the cluster and select Create Virtual Machine.
7. Under Select Source, select "Create the new virtual machine with a blank virtual hard disk" and click Next.
8. Under Identity, name the virtual machine Win2025-DC-GUI", select Generation 2, and click Next.
9. Under Configure Hardware, select the Hyper-V Cloud Capability Profile, 2 Processors, 4096 MB Virtual machine memory, a new Dynamic 120 GB Virtual Hard Disk that contains the operating system, the Windows Server 2025 Installation ISO connected to the Virtual DVD drive with "Share file instead of copying it" selected, add 2 more disks for SQL_data and SQL_log, Network Adapter 1 connected VM_network and Availability set to "Make the virtual machine highly available. Click Next.
10. Under Select Destination, select "Place the virtual machine on a host" and make sure the "Hyper-V Management" Destination is selected. Click Next.
11. Under Select Host, allow the placement process to run, accept the recommendation, and click Next.
12. Under Configure Settings, Virtual Machine Location, browse to C:\ClusterStorage\Volume1. Also under Machine Resources, browse to C:\ClusterStorage\Volume1 for the Destination path of the Virtual Hard Disk. Click Next.
13. Under Add Properties, select the Windows Server 2025 Datacenter Operating system and click Next.
14. Under Summary, click Create.
15. When the virtual machine is successfully created, close the Jobs window.
16. In Virtual Machine Manager, in the VMs and Services workspace, right-click the newly created Win2025-DC-GUI VM and select Power On. Then right-click the VM and select Connect or View > Connect via Console. Click the icon to send Ctrl-Alt-Del to the VM and press Enter when you see "Press any key to boot from CD or DVD".
17. Install Windows Server 2025 Datacenter with Desktop Experience on the VM, assign it an IP address and hostname and join the VM to the Windows Domain, and install all Windows Updates on the VM.
18. Download SQL 2022 Installation ISO file and double click the setup.
19. Refer the steps mentioned under Install SQL Server 2022 and SQL server management tools to install it on the the VM.

    Note: Make sure to update User database directory & User database Log directory under database engine configuration tab while installing SQL Server 2022.



20. Install the ODBC driver 18 for SQL server after downloading it from the following URL: https://learn.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server?view=sql-server-ver16#download-for-windows
21. At the Welcome window, click Next.
22. Accept the terms in the license agreement and click Next.
23. Click Install.

Database workload simulation

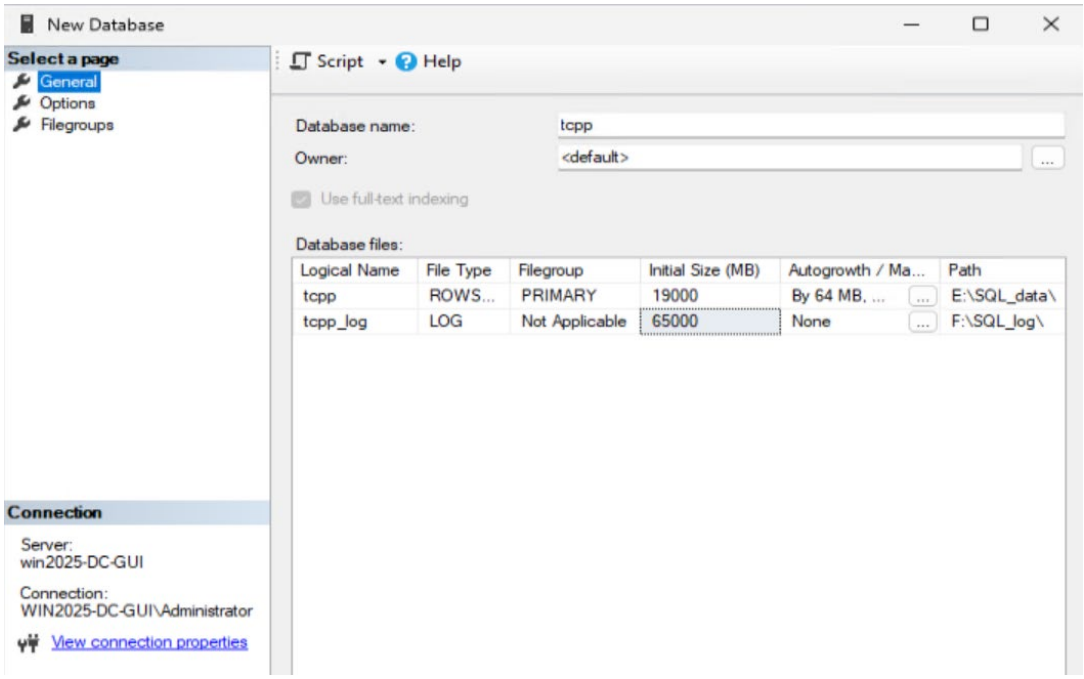
A sample transactional database was created using HammerDB's built-in TPC-C workload generation. Configuration parameters such as the number of warehouses, virtual users, and connection settings were customized to reflect realistic enterprise usage patterns. This database was then used to execute benchmark tests and measure system performance under load.

Creating Sample Database

This section describes how to create a database in SQL Server by using SQL Server Management Studio.

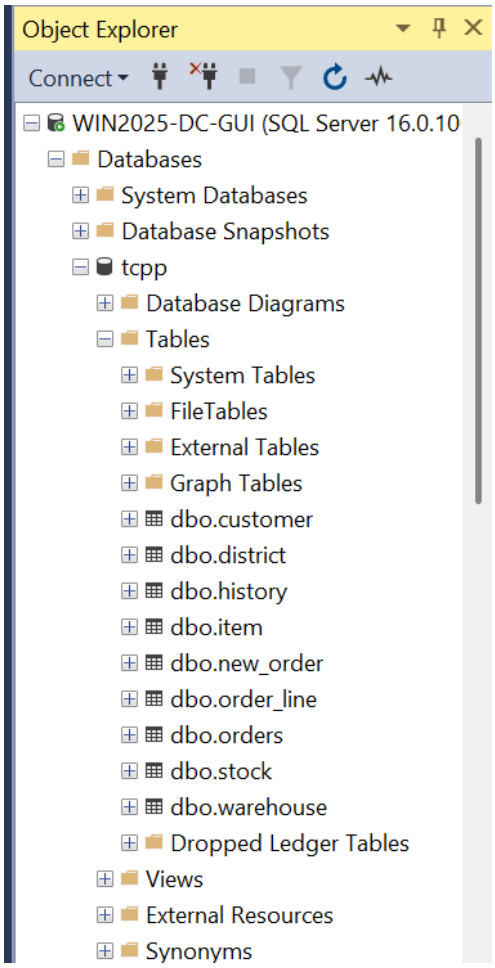
1. Launch the SQL Server Management Studio.
2. In Object Explorer, connect to the instance of the SQL Server Database Engine and then expand that instance.
3. Right-click Databases, and then select New Database.
4. In New Database, enter a database name (here we have given name "tcpp").
5. To create the database by accepting all default values, select OK; otherwise, continue with the following optional steps:
    - To change the owner name, select (…) to select another owner.
    - To change the default values of the primary data and transaction log files, in the Database files grid, select the appropriate cell and enter the new value. For more information, see Add Data or Log Files to a Database.
        - For this solution, we have set the initial size of the data file to 190,000 MB and the log file to 65,000 MB.
        - We have set the data file to grow by 64 MB to unlimited size. Set the log file to disable auto-growth. Click OK.

- Users can set these values depending upon their requirements and type of applications/ workloads they would like to run.



- To change the collation of the database, select the Options page, and then select a collation from the list.
- To change the recovery model, select the Options page and select a recovery model from the list. By default, this is set to Full.
- As we have installed SQL Server 2022, so by default the Compatibility level is set to SQL Server 2022 (160).
- To add a new filegroup, select the Filegroups page. Select Add and then enter the values for the filegroup.
- To add an extended property to the database, select the Extended Properties page.
  - In the Name column, enter a name for the extended property.
  - In the Value column, enter the extended property text. For example, enter one or more statements that describe the database.

6. Click OK to create the database, which can take a few minutes to complete.
7. Database (tpcc) gets created and shows under Databases tab in Object Explorer as shown in following diagram.



Installing HammerDB & configuring and running HammerDB

This section describes HammerDB installation & execution of benchmark test

Download & launch HammerDB 5.0 for windows

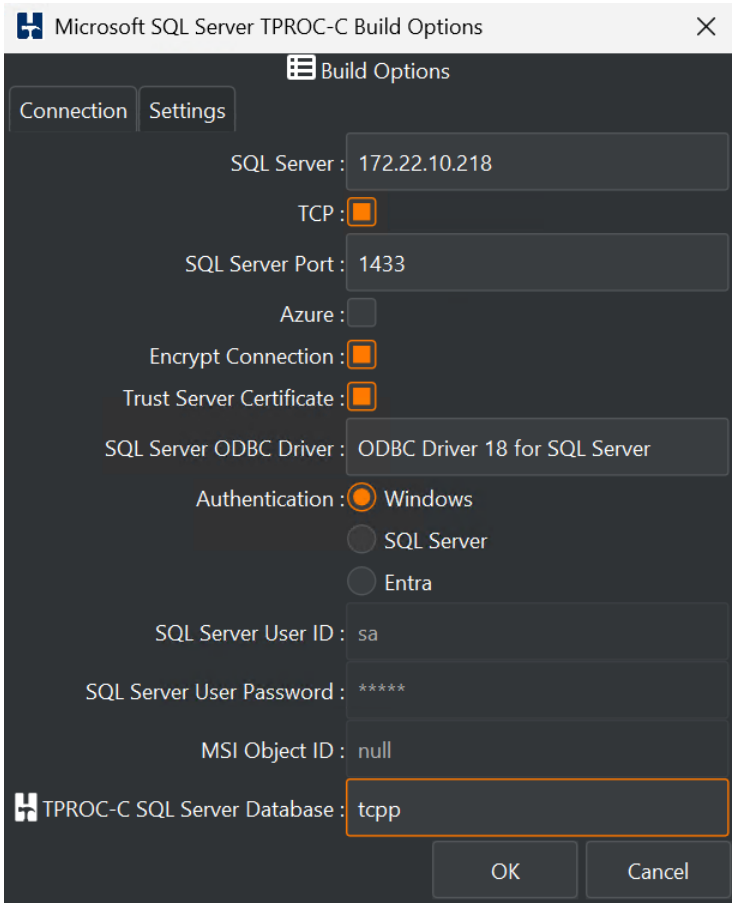
1. Go to: https://www.hammerdb.com/download.html and download HammerDB-5.0-Windows setup file.
2. Double click on setup file, click next
3. Accept the agreement license, click next
4. Do not change the installation directory path, Click next and click finish.
   Launch Hammer
5. Go to C:\Program Files\HammerDB-5.0
6. Double-click hammerdb.bat to launch the GUI

Configure HammberDB

Setup your Benchmark:

7. In the GUI, select:
   Benchmark → Choose SQL Server → TPROC-C
8. To Build the Schema (Test DB Setup), select:
   Schema → Options

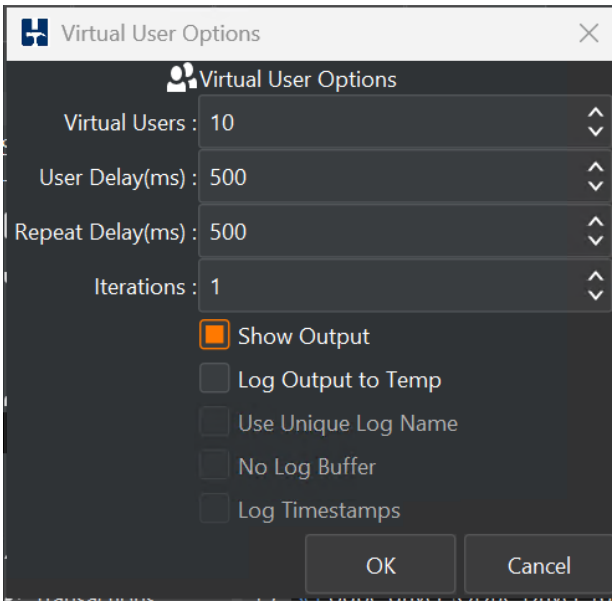
9. Update SQL Server IP, select TCP, update SQL server database details:



10. Click Build — HammerDB will connect to the DB and create schema & data

    Note: Ensure your DB user has privileges to create schema and insert data.

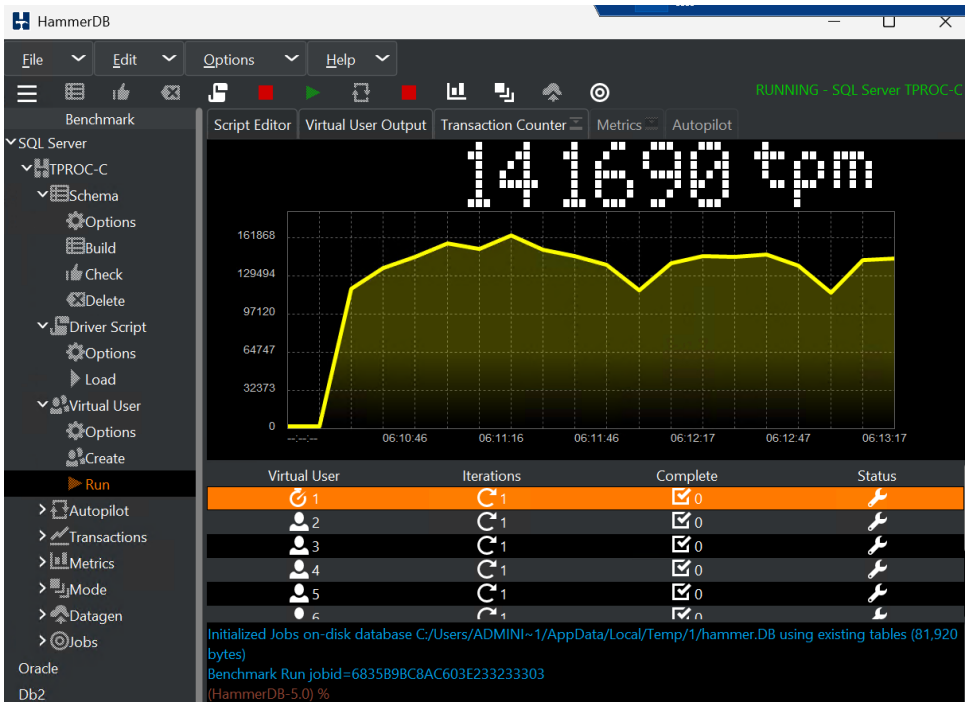
11. Create Virtual Users (Simulated Load)
    - Go to Driver Script → Load
    - Then go to Virtual User → Options & Choose number of Virtual Users (threads)



- Click Virtual User → Run to begin the benchmark

12. Monitor Performance

Monitor Transactions Per Minute (TPM) and other stats in real time in the output window.

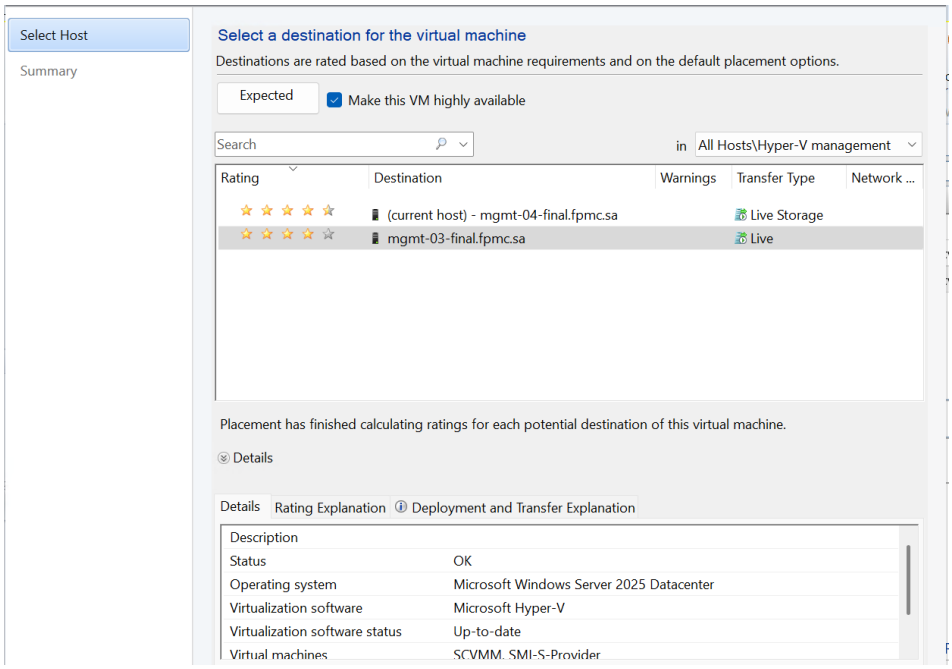


Live Migration Validation

Here we will test seamless virtual machine mobility across hosts. This test ensures that active workloads remained unaffected with minimum downtime and performance impact.

1. Open System Center VMM 2025 Console.

2. Go to VMs and Services and select the VM to migrate.
3. Right-click the VM and choose Migrate Virtual Machine.
4. In the wizard, select Destination Host from the same cluster.



5. Review compatibility checks and any placement warnings.
6. Click Move to start the migration.

Validating VM mobility during Host maintenance

We will verify VM migration during planned host maintenance to ensure continuous application availability:

1. Navigate to Fabric > Servers > All Hosts.
2. Right-click the target Hyper-V host and select Enter Maintenance Mode.
3. Confirm the action in the dialog box. VMM will begin migrating VMs off the host.
4. Check the Jobs tab in VMM for successful live migration entries.
5. Verify that all VMs are now running on different hosts.
6. Confirm VM uptime and application availability during and after the migration.
7. Host appears with a wrench icon and “In Maintenance Mode” status.
8. This endures a smooth live migration, allowing infrastructure updates without downtime.

Conclusion

The integration of Microsoft Hyper-V 2025 with the FlexPod® architecture delivers a highly resilient, scalable, and efficient virtualization platform designed to meet the demands of modern enterprise workloads. By combining Cisco UCS compute, NetApp unified storage, and Cisco networking with the advanced virtualization and management capabilities of Hyper-V 2025, organizations benefit from seamless VM mobility, robust high availability, and simplified operations.

This document illustrates the implementation of FlexPod infrastructure with Microsoft Hyper-V 2025, configured with Windows Failover Clustering. Few failover scenarios were validated like live migration and host maintenance mode testing. Additionally, a sample test VM was created to run HammerDB workloads, providing insights into performance and application behavior within the solution stack. Customers can utilize this validated framework as a foundation for deploying FlexPod with Hyper-V 2025, and further leverage NetApp Shift Toolkit to accelerate and simplify the migration of VMs from VMware to Hyper-V.

Acknowledgement

Roney Daniel – Technical Marketing Engr, NetApp

Abhinav Singh – Sr. Technical Marketing Engr, NetApp

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- FlexPod Home Page: https://www.flexpod.com
- NetApp Interoperability Matrix Tool: http://support.netapp.com/matrix/
- Cisco UCS Hardware and Software Interoperability Tool: http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html
- NetApp Product Documentation: https://www.netapp.com/support-and-training/documentation/
- Cisco Validated Design and deployment guides for FlexPod: https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html
- NetApp Shift Toolkit: https://docs.netapp.com/us-en/netapp-solutions/vm-migrate/shift-toolkit-overview.html
- NetApp SMI-S Provider: https://docs.netapp.com/us-en/smis-provider/index.html

Version history

As an option, use the NetApp Table style to create a Version History table. Do not add a table number or caption.

Version	Date	Document version history
Version 1.0	June 2025	Initial release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp