What is Virtual Machine Manager?

Article • 07/10/2024

Welcome to System Center Virtual Machine Manager (VMM)! VMM is part of the System Center suite used to configure, manage, and transform traditional datacenters. It helps to provide a unified management experience across on-premises, service provider, and the Azure cloud. VMM capabilities include:

- **Datacenter**: Configure and manage your datacenter components as a single fabric in VMM. Datacenter components include virtualization servers, networking components, and storage resources. VMM provisions and manages the resources needed to create and deploy virtual machines and services to private clouds.
- **Virtualization hosts**: VMM can add, provision, and manage Hyper-V and VMware virtualization hosts and clusters.
- **Networking**: Add networking resources to the VMM fabric, including network sites defined by IP subnets, virtual LANs (VLANs), logical switches, static IP address, and MAC pools. VMM provides network virtualization, including support for creating and managing virtual networks and network gateways. Network virtualization allows multiple tenants to have isolated networks and their own IP address ranges for increased privacy and security. Using gateways, VMs on virtual networks can connect to physical networks in the same site or in different locations.
- **Storage**: VMM can discover, classify, provision, allocate, and assign local and remote storage. VMM supports block storage (fiber channel, iSCSI, and Serial Attached SCSI (SAS) storage area networks (SANs)).
- **Library resources**: The VMM fabric retains a library of file-based and non-file-based resources that are used to create and deploy VMs and services on virtualization hosts. File-based resources include virtual hard disks, ISO images, and scripts. Non-file-based resources include templates and profiles that are used to standardize the creation of VMs. Library resources are accessed through library shares.

Resources

- To read blog posts from the VMM engineering team, see System Center Blog ↗.

Next steps

- Learn about system requirements.
- Get started with Arc-enabled SCVMM.

Virtual Machine Manager network object fundamentals

Article • 07/10/2024

System Center Virtual Machine Manager (VMM) is part of the System Center suite used to configure, manage, and transform traditional datacenters. It helps provide a unified management experience across on-premises, service provider, and the Azure cloud.

This article covers the basics that you need to understand before you move on to topics such as advanced VMM features and functions, and planning and designing private and public clouds.

Networking objects

The following VMM networking objects are used to build the basic networking infrastructure of Microsoft's Software Defined Networking (SDN) used in private and public clouds:

- Hosts and host group

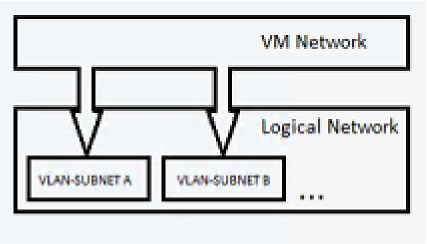
  Hyper-V hosts that VMM manages, organized into groups based on location or purpose.

- Logical network

  Logical objects that mirror your physical networks.

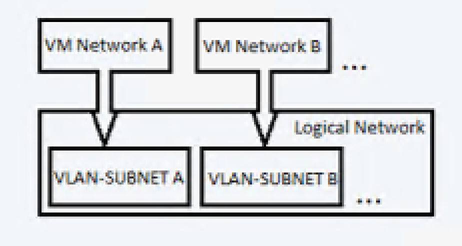
- One connected logical network

  A single VM network is created on top of this logical network, and this VM network provides access to all the underlying VLAN-subnet pairs.

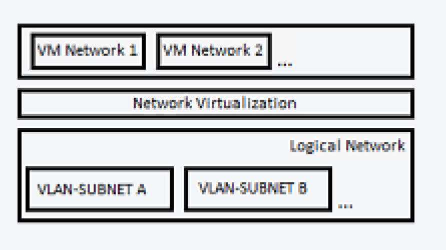
- Independent logical network

  Multiple VM networks can be created on top of this logical network. Each VM network created provides access to a specific VLAN-subnet pair. The VM networks are independent of each other.



- Virtualized network

  This is the fabric network. Multiple virtualized VM networks can be created on top of this logical network. Each VM network has its own virtualized address space.

- Network sites

  Logical groupings of hosts, IP Subnets, and/or VLANs.

- IP address pools (logical networks)

  A static pool of IP addresses used for the associated network sites' IP subnet/VLAN pairs.

- VM networks

  Abstract objects that act as an interface to logical networks.

- IP address pools (VM Networks)

  A static pool of IP addresses for the VM network.

- Uplink port profile

  Defines the load balancing algorithm and teaming mode for physical adapters. Uplink port profiles can be applied to physical network adapters when you deploy switches.

- Virtual network adapter port profile

  Defines the virtual network adapter properties for the virtual network adapters available with the logical switch.

- Port classification

  A label to abstract the virtual network adapter port profile settings.

- Logical Switch

  Brings virtual switch extensions, port profiles, and port classifications together.

- Gateway

  Used to connect a Hyper-V Network Virtualization (HNV) VM network to an external network.

For more information about Microsoft SDN, see Software Defined Networking.

Next steps

To get started with VMM, see What's New in SCVMM and Install.

Feedback

About Arc-enabled System Center Virtual Machine Manager

Article • 06/27/2024

Azure Arc-enabled System Center Virtual Machine Manager (SCVMM) empowers System Center customers to connect their VMM environment to Azure and perform VM self-service operations from Azure portal. Azure Arc-enabled SCVMM extends the Azure control plane to SCVMM-managed infrastructure, enabling the use of Azure security, governance, and management capabilities consistently across System Center-managed estate and Azure.

Azure Arc-enabled System Center Virtual Machine Manager also allows you to manage your hybrid environment consistently and perform self-service VM operations through Azure portal. For Microsoft Azure Pack customers, this solution is intended as an alternative to perform VM self-service operations.

Arc-enabled System Center Virtual Machine Manager allows you to:

- Perform various VM lifecycle operations such as start, stop, pause, and delete VMs on SCVMM-managed VMs directly from Azure.
- Empower developers and application teams to self-serve VM operations on demand using Azure role-based access control (RBAC).
- Browse your VMM resources (VMs, templates, VM networks, and storage) in Azure, providing you with a single pane view for your infrastructure across both environments.
- Discover and onboard existing SCVMM-managed VMs to Azure.
- Install the Azure connected machine agents at scale on SCVMM VMs to govern, protect, configure, and monitor them.
- Procure Extended Security Updates (ESUs) for the WS 2012 and 2012 R2 VMs managed by SCVMM.

Discover Arc-enabled SCVMM from SCVMM console

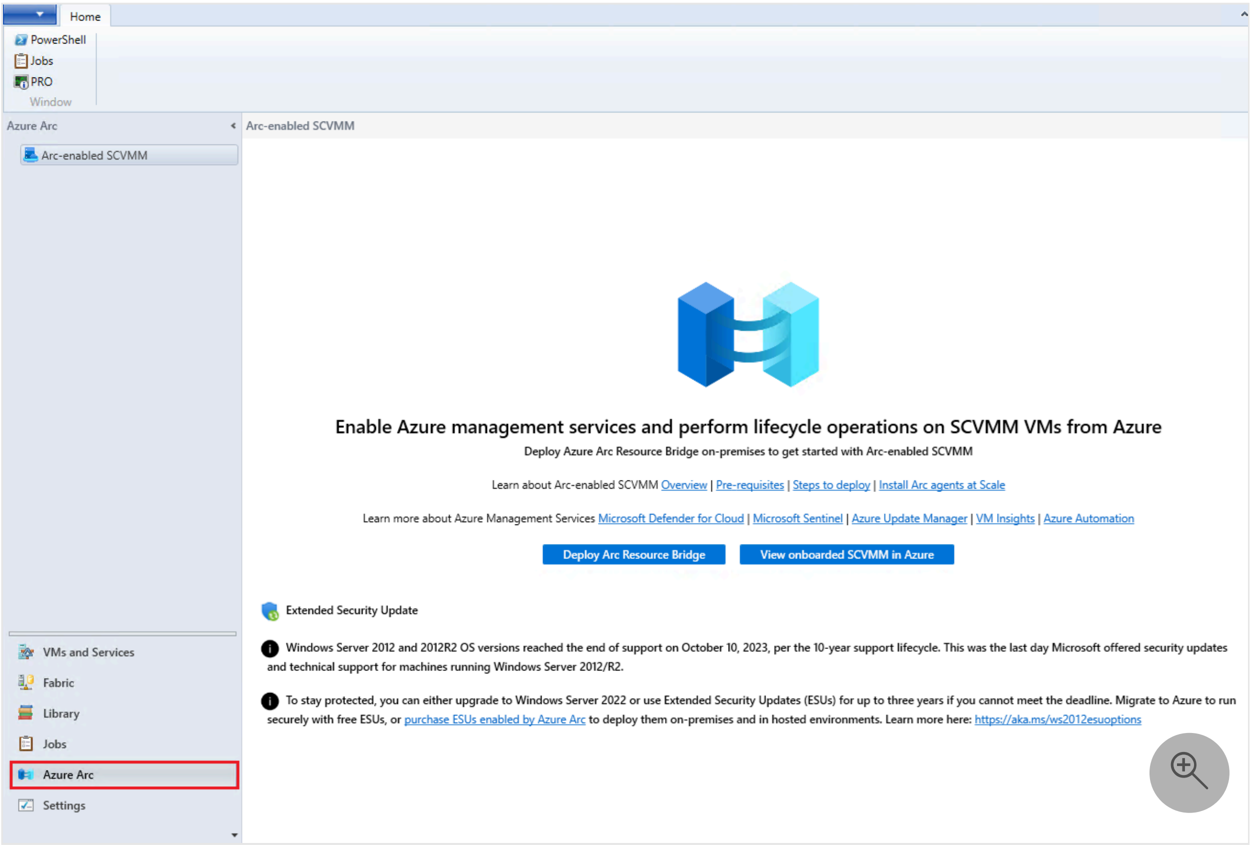
You can discover and learn about Arc-enabled SCVMM from the **Azure Arc** blade in the SCVMM console.

Navigate to **Azure Arc** in the administrator **SCVMM Console** and do the following:

- **Overview**: Read the overview of Arc-enabled SCVMM.

- **Pre-requisites**: Review the prerequisites of Arc-enabled SCVMM.
- **Steps to deploy**: View steps to Arc-enable your SCVMM-managed estate.
- **Install Arc agents at scale**: View steps to install Azure Connected Machine agents at scale to your SCVMM VMs from Azure.
- **Azure Management Services**: Learn about the popular Azure management services to govern, protect, configure, and monitor your SCVMM VMs through Azure Arc.
- **Deploy Arc Resource Bridge**: Deploy Arc resource bridge.
- **View onboarded SCVMM in Azure**: Navigate to your SCVMM inventory page on the Azure Arc portal from the default web browser.

You need appropriate credentials on the Azure portal with the necessary permissions to onboard or use Azure Arc-enabled SCVMM.



Enable Azure management services and perform lifecycle operations on SCVMM VMs from Azure

Deploy Azure Arc Resource Bridge on-premises to get started with Arc-enabled SCVMM

Learn about Arc-enabled SCVMM Overview | Pre-requisites | Steps to deploy | Install Arc agents at Scale

Learn more about Azure Management Services Microsoft Defender for Cloud | Microsoft Sentinel | Azure Update Manager | VM Insights | Azure Automation

Extended Security Update

Windows Server 2012 and 2012R2 OS versions reached the end of support on October 10, 2023, per the 10-year support lifecycle. This was the last day Microsoft offered security updates and technical support for machines running Windows Server 2012/R2.

To stay protected, you can either upgrade to Windows Server 2022 or use Extended Security Updates (ESUs) for up to three years if you cannot meet the deadline. Migrate to Azure to run securely with free ESUs, or purchase ESUs enabled by Azure Arc to deploy them on-premises and in hosted environments. Learn more here: https://aka.ms/ws2012esuoptions

Next steps

Get started with Arc-enabled SCVMM.

Feedback

Was this page helpful? Yes No

Provide product feedback ↗ | Get help at Microsoft Q&A

What's new in System Center Virtual Machine Manager

Article • 07/10/2024

This article details the new features supported in System Center 2022 - Virtual Machine Manager (VMM). It also details the new features in VMM 2022 UR1 and UR2.

New features in VMM 2022

See the following sections for new features and feature updates supported in VMM 2022.

Compute

Windows Server 2022 and Windows Server 2022 Guest OS support

VMM 2022 can be used to manage on Windows Server 2022 hosts and Windows Server 2022 Guest OS hosts.

Windows 11 support

VMM 2022 supports Windows 11 as guest operating system.

Support for Azure Stack HCI clusters 21H2

With VMM 2022, you can manage Azure Stack HCI, 21H2 clusters.

Azure Stack HCI, version 21H2 is the newly introduced hyper-converged infrastructure (HCI) Operating system that runs on on-premises clusters with virtualized workloads.

Most of the operations to manage Azure Stack clusters in VMM are similar to managing Windows Server clusters.

> ⓘ **Note**
>
> Management of Azure Stack HCI stretched clusters is currently not supported in VMM.

See Deploy and manage Azure Stack HCI clusters in VMM.

Register and unregister Azure Stack HCI cluster using PowerShell cmdlets

VMM 2022 supports **register** and **unregister** PowerShell cmdlets for Azure Stack HCI cluster. See Register-SCAzStackHCI and Unregister-SCAzStackHCI.

Support for dual stack SDN deployment

VMM 2022 supports dual stack SDN deployment.

In VMM 2019 UR2, we introduced support for Ipv6 based SDN deployment. VMM 2022 supports dual stack (Ipv4 + Ipv6) for SDN components.

To enable Ipv6 for SDN deployment, do the required changes in the network controller, gateway, and SLB setup.

For more information about these updates, see Network controller, Gateway, SLB, and Set up NAT.

New features in VMM 2022 UR1

The following sections introduce the new features and feature updates supported in VMM 2022 Update Rollup 1 (UR1).

For problems fixed in VMM 2022 UR1, and installation instructions for UR1, see the KB article .

Support for Azure Stack HCI clusters 22H2

With VMM 2022 UR1, you can manage Azure Stack HCI, 22H2 clusters.

Azure Stack HCI, version 22H2 is the newly introduced hyper-converged infrastructure (HCI) Operating system that runs on on-premises clusters with virtualized workloads.

Most of the operations to manage Azure Stack clusters in VMM are similar to managing Windows Server clusters.

See Deploy and manage Azure Stack HCI clusters in VMM.

Support for VMware vSphere 7.0, 8.0 and ESXi 7.0, 8.0

VMM 2022 UR1 supports VMware vSphere 7.0, 8.0 and ESXi 7.0, 8.0. Learn more.

Support for SQL Server 2022

VMM 2022 UR1 supports SQL Server 2022. Learn more.

Support for Smart card sign in in SCVMM Console

VMM 2022 UR1 supports Smart card sign in with enhanced session mode in SCVMM Console.

SR-IOV support for Network Controller managed NICs

With VMM 2022 UR1, SR-IOV supports Network Controller managed NICs.

Removed VMM dependencies on deprecated Operations Manager Management Pack

With VMM 2022 UR1, removed VMM dependencies on deprecated SCOM Management Packs. If you have an active SCOM - VMM integration, follow the steps listed in KB article before you upgrade to VMM 2022 UR1.

Discover Arc-enabled SCVMM from VMM console

VMM 2022 UR1 allows you to discover Arc-enabled SCVMM from console and manage your Hybrid environment and perform self-service VM operations through Azure portal. Learn more.

Support for 64 virtual networks for Windows Server 2019 or later

VMM 2022 UR1 supports 64 virtual networks for Windows Server 2019 or later.

New features in VMM 2022 UR2

The following sections introduce the new features and feature updates supported in VMM 2022 Update Rollup 2 (UR2).

For problems fixed in VMM 2022 UR2, and installation instructions for UR2, see the KB article .

Improved V2V conversion performance of VMware VMs to Hyper-V VMs

You can now convert your VMware VMs to Hyper-V with close to four times faster conversion speed and support for VMware VMs with disk sizes greater than 2 TB. Learn more about how to use this enhancement.

Improved Arc-enabled SCVMM Discovery tab

The **Azure Arc** tab now highlights the latest feature additions to Arc-enabled SCVMM which includes support for Azure management services such as Microsoft Defender for Cloud, Azure Update Manager, Azure Monitor, Microsoft Sentinel, and more. Learn more ↗.

If you are running WS 2012 and 2012R2 host and guest operating systems, the Azure Arc blade now provides guidance to continue remaining in support state.

Support for latest Linux Guest Operating Systems

With VMM 2022 UR2, you can run Ubuntu Linux 22, Debian 11, Oracle Linux 8 and 9 based Linux VMs.

Next steps

- Know the VMM system requirements
- Plan VMM installation

System Center – Virtual Machine Manager build versions

Article • 07/10/2024

This article describes how to determine your current Microsoft System Center – Virtual Machine Manager version number and the corresponding update rollup (UR). Each update rollup release has a link to a support article describing the UR changes and links to the package downloads.

> ⓘ Note
>
> All System Center Virtual Machine Manager update rollups are cumulative. This means, you do not need to apply the URs in order; you can always apply the latest update. If you have deployed System Center – Virtual Machine Manager and never applied an update rollup, you can proceed to install the latest one available.

Virtual Machine Manager 2022 build versions

The following table lists the release history for Virtual Machine Manager 2022.

Expand table

Build Number	KB	Release Date	Description
10.22.1287.0	n/a	March 2022	System Center 2022 Virtual Machine Manager RTM
10.22.1508.0	5019202	November 2022	Update Rollup 1
10.22.1711.0	5032369	November 2023	Update Rollup 2

Next steps

What's New in VMM

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Release notes for System Center Virtual Machine Manager

Article • 07/10/2024

Virtual Machine Manager (VMM) 2022 doesn't have any known issues.

For new features in VMM 2022, see What's new.

Next steps

What's new in Virtual Machine Manager

Feedback

Was this page helpful? 👍 **Yes** 👎 **No**

Provide product feedback | Get help at Microsoft Q&A

Manage telemetry settings in VMM

Article • 07/10/2024

This article provides information about how to turn on/off the telemetry settings in System Center Virtual Machine Manager (VMM).

> ⓘ **Note**
>
> Microsoft does not collect any personal data from the customers. We only listen to events that would help diagnostics in VMM. Learn more

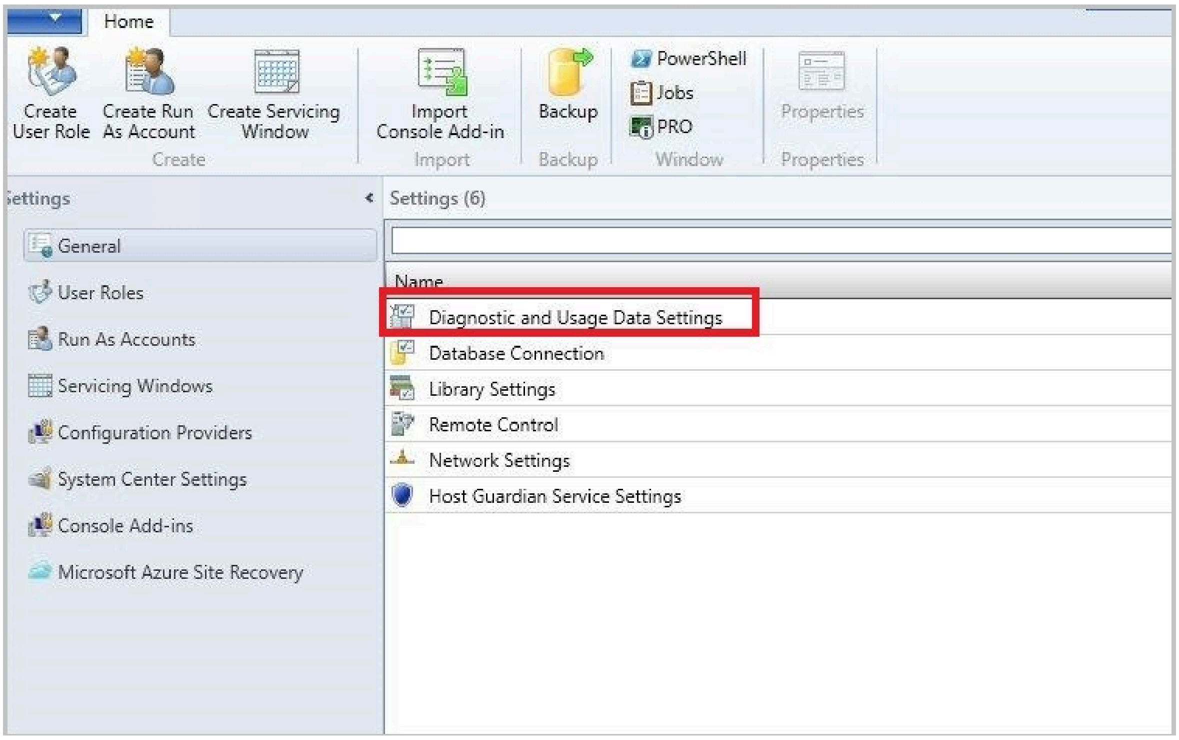
Turn on/off telemetry in VMM

Use the following procedure:

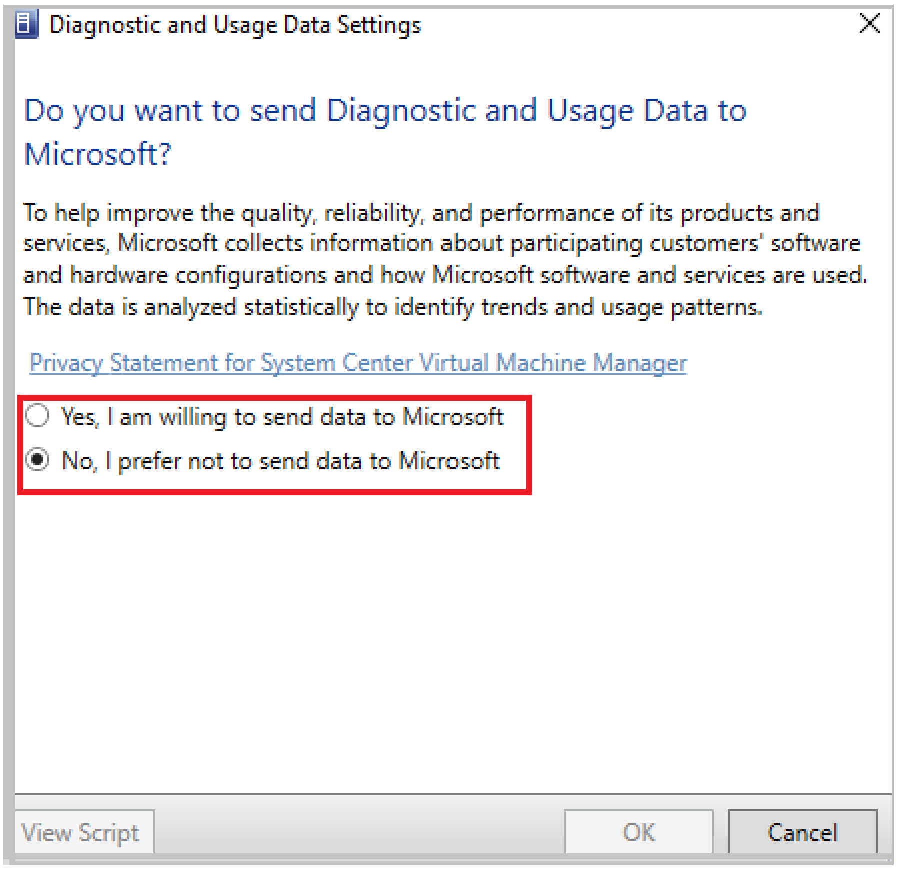
1. On the VMM console, select **Settings**.

   General settings window appears with the available list of settings.

2. Select **Diagnostics and Usage Data Settings**.

   Page with **Do you want to send Diagnostics and Usage Data to Microsoft** message appears with an option to select either Yes or No.



Do you want to send Diagnostic and Usage Data to Microsoft?

To help improve the quality, reliability, and performance of its products and services, Microsoft collects information about participating customers' software and hardware configurations and how Microsoft software and services are used. The data is analyzed statistically to identify trends and usage patterns.

Privacy Statement for System Center Virtual Machine Manager

○ Yes, I am willing to send data to Microsoft

● No, I prefer not to send data to Microsoft

ⓘ Note

We recommend you to go through the privacy statement provided on this page before making a selection.

3. To turn on telemetry, select **Yes, I am willing to send data to Microsoft**.

4. To turn off telemetry, select **No, I prefer not to send data to Microsoft**.

Telemetry data collected

Expand table

Data related To	Data collected
Census Data	Unique ID generated for the VMM deployment VMM build version ID used for correlation with other System Center products
Assurance Data	Information about the VMM deployment - whether guardian service deployment or not Count of guarded hosts being managed

Data related To	Data collected
	Count of hosts being managed Count of shielded VM templates Count of VM templates Count of shielded VMs Count of VMs Count of shielded clouds Count of guarded hosts in a cluster Count of guarded hosts in standalone deployments Count of code integrity policy in Global Settings Count of Physical Computer Profile (PCP) with host guarding set If the VMM deployment is a guardian service deployment and OM integrated If the VMM deployment is a guardian service deployment and WSUS integrated Count of hosts with attestation mode as TPM Count of hosts with attestation mode as AD Count of CI policies existing in a library Count of hosts being managed Count of DMZ hosts being managed Count of Hyper-V hosts Count of clusters Count of nontrusted hosts being managed Information if customer is managing the VMware hosts Minimum, maximum, and average host cluster size Minimum, maximum, and average host memory size

Data related To	Data collected
	Minimum, maximum, and average VMware cluster size
Job related	Indication if jobs are user initiated or background jobs Count of the number of times a job description type has failed Number of times job has run Maximum, minimum, and average number of jobs run per day
Dynamic Optimization Settings	Count of hosts considered for dynamic optimization Count of hosts considered for power optimization Minimum, maximum, and average frequency to run dynamic optimization
Network	Count of Edge NAT instances Count of Edge forwarding instances Count of Edge S2S instances Count of VPN connections Count of tenants per multitenant gateway Count of Edge load balancers Count of Edge load balancer VIP templates Count of NC managed VPN connections Count of NC managed IPsec VPN connections Count of NC managed GRE VPN connections Count of NC managed L3 VPN connections
IP Pool	Count of IPV4 and IPV6 address pools Maximum size of IPV4 and IPV6 pools Total reserved IPV4 and IPV6 addresses Average pool usage size

Data related To	Data collected
	Count of NC managed IPV4 and IPV6 addresses
Library	Count of library shared being managed Count of VHDs and VHDXs registered in the library Count of service templates registered in the library Count of VM templates registered in the library Count of host groups belonging to the library Count of equivalent resources registered in the library
Logical Network	Count of Logical networks Count of logical network definitions Count of one connected network managed by network controller Count of VLAN based independent networks Count of private VLAN networks
Policy Distribution	Minimum and maximum policy RTT Policy errors
Service Objects	Count of service instances Count of deployed service instances Count of failed service instances Count of servicing failed service instances Count of service instances deployed to non Hyper-V host groups Count of VM roles Count of applications Count of script applications Maximum, minimum, and average tiers per service Count of services using application hosts

Data related To	Data collected
	Count of services using SQL application Count of services using Web deploy application Maximum, minimum, and average number of applications per customer, computer tier Count of service tiers with load balancers Count of services deployed on VMware
VM	Count of HA VM instances Count of Non-HA VM instances Count of HA VM instances on clustered storage Count of HA VM instances on SMB share Count of DiffDisk VM instances Count of Hyper-V VM instances Count of VMware VM instances Count of OS type, OS name, OS edition, OS version on VMs List of possible VM states Count of VMs per state
VM OS	OS version of VMs OS name of the VMs OS edition of VMs OS Type of VMs Count of VMs for various OS List of possible VM states Count of VMs for each state
VMM Settings	Indication of highly available installation of VMM

Data related To	Data collected
	Indication if VMM is upgraded VMM SKU type Indication of VMM running as domain account Indication if VMM DB is on remote server Indication if VMM is running on a VM Indication if VMM is running on a default path Count of VM networks Count of VM subnets Count of NC managed VM networks and VM subnets
Host OS	OS version on the host OS name of the host SKU type of host Indication of Nano type host Number of hosts with specific OS
Storage Inventory	Count of all storage providers Count of SMIS CIMXML, SMIS WMI, Native Windows, SMP WMI storage providers Count of providers managing arrays Count of providers managing file shares Count of providers managing both arrays and file shares Count of providers managing FC fabric Count of storage classification defined by user Count of discs where custom classification is used to override inherited disk classification Count of disks where custom classification is used to override pool derived classification

Data related To	Data collected
	Count of fabric classifications Count of primary VMs for which HVR is enabled out of band Count of VMs for which HVR is enabled in band Count of LUN based protected replication groups created Out of Band Count of volume-based protected replication groups created Out of Band Count of volume-based protected replication groups created through Azure Site Recovery Indication if VMM is configured to be connected to Azure Site Recovery Count of QoS policies created in VMM Count of VMs with QoS policies applied
Storage Hyper Converged cluster	Count of Hyper converged clusters Count of pools Count of virtual discs Count of volumes Count of local discs attached Average local disc size attached
SAN Arrays	Count of pools in storage array Count of managed pools in storage array Count of managed LUNs in all managed pools per array List of array capabilities Indication if array also has associated file share
Storage Hosts	Count of storage hosts or clusters Name of storage aggregate collection

Data related To	Data collected
	Maximum, minimum, average, median, and mode values of storage aggregate of collector
File server storage	List of total file shares on file server List of managed shares on file server Indication if there is Calabria file share capability List of associated storage array capabilities List of SMB file share dialect supported by file server
Telemetry Opt out	Indication if Telemetry is opted out

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Deploy a private VMM cloud

Article • 07/17/2024

This article provides an overview of System Center Virtual Machine Manager (VMM) private clouds.

A private cloud is a cloud that is provisioned and managed on-premises by an organization. It's deployed using an organization's own hardware to take the advantages of a private cloud model.

You can use VMM to create and deploy private cloud components, and to manage access to the private cloud and the underlying physical resources. VMM provides the following benefits:

- **Self-service** - Self-service admins can delegate management and usage of the private cloud while having no knowledge of the underlying physical resources. They don't have to ask the private cloud provider for administrative changes, except to request increased capacity and quotas as required.
- **Opacity** - Self-service admins don't need any knowledge of the underlying physical resources.
- **Resource pooling** - Administrators can collect and present an aggregate set of resources, such as storage and networking resources. Resource usage is limited by the capacity of the private cloud and by user role quotas.
- **Elasticity** - Administrators can add resources to a private cloud to increase the capacity.
- **Optimization** - Usage of the underlying resources is continually optimized without affecting the overall private cloud user experience.

You can create a private cloud from either:

- VMM host groups that contain resources from virtualization hosts
- A VMware resource pool

You can deploy a private cloud by configuring fabric resources, setting up library paths for private cloud users, and setting the cloud capacity.

Next steps

- Create a private cloud in VMM

Create a VMM private cloud

Article • 07/17/2024

This article provides instructions for creating a private cloud in System Center Virtual Machine Manager (VMM).

You can create a private cloud from a host group or from a VMware resource pool. Host groups can contain a single host type or a mix of Hyper-V and VMware ESX hosts.

> ⓘ Note
>
> You must be a VMM administrator or a member of the delegated Administrators user group with a scope that includes the host groups you'll use for the cloud.

Before you start

- You need to have the VMM fabric in place. Learn more.
- You should have one or more Hyper-V or VMware virtualization hosts in the fabric. If you're creating a cloud from a VMware resource pool, a vCenter Server and the VMware ESX host or host cluster that contains the VMware resource pool must be available in the VMM fabric.
  - If you want to provide self-service users the ability to store virtual machines to the VMM library, then create a library share or create a folder in a library share that will serve as the storage location. Learn more.

    > ⓘ Note
    >
    > Self-service users must have the **Store and re-deploy** permission to store their virtual machines.

  - You can add independently created library shares as read-only library shares in the VMM when you run the Create Cloud Wizard. For example, outside the VMM, you can't create the **\\VMMServer01\Finance\StoredVMs** path and then add the **\\VMMServer01\Finance** library share to the VMM library.
  - The self-service user role data path is specified when you create a self-service user role or modify the properties of a self-service user role.

- If you want to assign read-only shares to the private cloud, where administrators can store read-only resources such as .iso files that they want to make available to self-service users, make sure that one or more library shares exist that you can assign as the read-only library shares.

  > ⓘ **Note**
  >
  > Self-service users must have the **Author** permission to access the resources.

- The library shares that you designate as read-only resource locations for the private cloud must be unique when compared to the library share or shares that are used for stored virtual machines and for the user role data path that is specified for a self-service user role. For example, if the user role data path for a self-service user role is **\\VMMServer01\Finance**, you can't create a stored virtual machine path of **\\VMMServer01\Finance\StoredVMs**. However, if the user role data path is **\\VMMServer01\Finance\FinanceUserRoleData**, you could specify **\\VMMServer01\Finance\StoredVMs** as the stored virtual machine path, as the full path is unique. You could also create entirely separate library shares.

Create a private cloud from a host group

1. Select **VMs and Services** > **Create** > **Create Cloud** to open the Create Cloud Wizard.

2. In **General**, specify a **Name** and optional description for the cloud.

3. Specify whether the cloud will support shielded VMs.

4. In **Resources** > **Host groups**, select the groups you want to add to the cloud. Then select **Next**.

5. In **Logical Networks**, select each logical network that you want to make available to the private cloud, and then select **Next**.

   > ⓘ **Note**
   >
   > Only logical networks that are associated with the physical network adapters on hosts in the selected host groups appear in the list.

6. In **Load Balancers**, select each load balancer that you want to make available to this private cloud, and then select **Next**.

   > ⓘ Note
   >
   > Only load balancers that are associated with the selected host groups appear in the list.

7. In **VIP Templates**, select each VIP template that you want to make available to the private cloud, and then select **Next**.

8. In **Port Classifications**, select each port classification that you want to make available to the cloud, and then select **Next**.

9. In **Storage**, if you have storage managed by VMM, select each storage classification that you want to make available to the private cloud, and then select **Next**.

   > ⓘ Note
   >
   > Only storage classifications for storage pools that are assigned to the selected host groups appear in the list.

10. In **Library** > **Stored VM path**, browse and select the library share you want to use for the self-service users to store VMs. Select **OK**.

11. In **Read-only library shares** > **Add**, select one or more library shares where administrators can provide read-only resources to cloud users. Select **OK** and then select **Next**.

12. In **Capacity**, set capacity limits for the private cloud, and then select **Next**. You can either accept the default values, or clear the **Use Maximum** checkboxes and set quotas for the following resources:

    Expand table

Quota Type	Description
Virtual CPUs	Sets a limit on processing capacity within the private cloud that is equivalent to the capacity that can be provided by a specified number of CPUs. Applied against running virtual machines. Setting a CPU quota doesn't guarantee

Quota Type	Description
	contiguous capacity; it only guarantees total CPU capacity available among hosts in the private cloud.
Memory	Sets a quota on memory (in gigabytes) that is available for virtual machines that are deployed on the private cloud. Applied against running virtual machines only. Setting a memory quota doesn't guarantee contiguous capacity. For example, the private cloud might have 2 GB of memory available on one host and 2 GB of memory on the other.
Storage	Sets a quota on storage capacity (in gigabytes) that is available to virtual machines that are deployed on the private cloud. For dynamic virtual hard disks, quota calculations are based on maximum size.
Custom quota (points)	Sets a quota on virtual machines that are deployed on the private cloud based on the total quota points that are assigned to the virtual machines through their virtual machine templates. Quota points are an arbitrary value that can be assigned to a virtual machine template based on the anticipated size of the virtual machines. Custom quotas are provided for backward compatibility with self-service user roles that were created in VMM.
Virtual machines	Limits the total number of virtual machines that can be deployed on the private cloud.

13. In **Capability Profiles**, select each virtual machine capability profile that you want to add, and then select **Next**. Select the capability profiles that match the type of hypervisor platforms that are running in the selected host groups. The built-in capability profiles represent the minimum and maximum values that can be configured for a virtual machine for each supported hypervisor platform.

14. In **Replication Groups**, select the replication groups for the private cloud, and select **Next**.

15. In **Summary** page, confirm the settings, and then select **Finish**.

View status in **Jobs** and ensure the job is complete.

To verify that the private cloud was created, check **VMs and Services** > **Clouds**. You can also verify in **Library** > **Cloud Libraries**, to view the read-only library shares.

Assign Storage QoS Policies while creating a cloud

1. Follow the steps until 14 in the above procedure.

2. In **Storage QoS Policies**, select the policies that you want to assign to this cloud.

3. Proceed with the rest of the steps and complete the wizard.

Create a private cloud from a VMware resource pool

1. Select **VMs and Services** > **Create** > **Create Cloud** to open the Create Cloud Wizard.
2. In **General**, specify a **Name** and optional description for the cloud.
3. In **Resources**, select **VMware resource pools** > **Next**.
4. In **Logical Networks**, select each logical network that you want to make available to the private cloud, and then select **Next**.
5. In **Load Balancers**, select each load balancer that you want to make available to the private cloud, and then select **Next**. Only load balancers that are associated with the selected host groups appear in the list.
6. In **VIP Templates**, select each VIP template that you want to make available to the private cloud, and then select **Next**.
7. In **Storage**, select **Next**. VMM doesn't manage or assign storage classifications assigned to ESX hosts.
8. In **Library** > **Stored VM path**, browse and select the library share you want to use for self-service users to store VMs, and select **OK**.
9. In **Read-only library shares** > **Add**, select one or more library shares where administrators can provide read-only resources to cloud users. Select **OK** and then select **Next**.
10. In **Capacity**, set capacity limits for the private cloud, and then select **Next**. You can either accept the default values, or clear the **Use Maximum** checkboxes and set quotas for the following resources:

Expand table

Quota Type	Description
Virtual CPUs	Sets a limit on processing capacity within the private cloud that is equivalent to the capacity that can be provided by a specified number of CPUs. Applied against running virtual machines. Setting a CPU quota doesn't guarantee

Quota Type	Description
	contiguous capacity; it only guarantees total CPU capacity available among hosts in the private cloud.
Memory	Sets a quota on memory (in gigabytes) that is available for virtual machines that are deployed on the private cloud. Applied against running virtual machines only. Setting a memory quota doesn't guarantee contiguous capacity. For example, the private cloud might have 2 GB of memory available on one host and 2 GB of memory on the other.
Storage	Sets a quota on storage capacity (in gigabytes) that is available to virtual machines that are deployed on the private cloud. For dynamic virtual hard disks, quota calculations are based on maximum size.
Custom quota (points)	Sets a quota on virtual machines that are deployed on the private cloud based on total quota points that are assigned to the virtual machines through their virtual machine templates. Quota points are an arbitrary value that can be assigned to a virtual machine template based on the anticipated size of the virtual machines. Custom quotas are provided for backward compatibility with self-service user roles that were created in VMM.
Virtual machines	Limits the total number of virtual machines that can be deployed on the private cloud.

11. In **Capability Profiles**, select **ESX Server**, and then select **Next**. The built-in capability profiles represent the minimum and maximum values that can be configured for a virtual machine for each supported hypervisor platform.

12. In **Summary** page, confirm the settings, and then select **Finish**.

View status in **Jobs** and ensure the job is complete.

To verify that the private cloud was created, check **VMs and Services** > **Clouds**. You can also verify in **Library** > **Cloud Libraries** to view the read-only library shares.

Assign storage QoS policies to a private cloud

System Center - Virtual Machine Manager (SCVMM) supports storage QoS policies on a private cloud.

The VMM fabric admin can now offer the storage QoS policies in the cloud. Tenant admins and self-service users can consume these while deploying the VMs and services. This will enable the cloud providers to guarantee and/or limit the amount of storage performance as per the subscription opted by the tenants.

The fabric admin can now offer storage QoS policies while authoring the VMM private clouds. After which the authorized users (admin and self-service users) with access to this cloud can consume the available QoS policies for provisioning VMs and Services on the cloud.

> ⓘ Note
>
> A cloud with at least one QoS policy offered won't allow the deployment of disks without a policy. This helps in preventing the cloud consumers to pick infinite resources with a null policy. Also, the change in IOPS by self-service users won't be allowed after this release to avoid the same scenario of selecting unauthorized performance.

Storage QoS Policies option in the **Create cloud** wizard helps the fabric admin to select the list of policies that should be made available for the cloud consumers.

follow these steps:

1. Follow the create a private cloud from a host group procedure until step 14.
2. In **Storage QoS Policies**, select the policies that you want to assign to this cloud.
3. Proceed to step 15; complete the remaining steps.
4. Review the summary and select **Finish**.

> ⓘ Note
>
> This list contains only those policies that are available in scope of all the clusters selected in the Resources section of the cloud wizard. This helps the self-service user to choose between the available plans even after the VM is placed.

On Upgrade

1. After the upgrade, the existing clouds won't have any QoS policy in their offering. Admin needs to update the cloud with the policy offerings.
2. The existing VMs on the cloud, which have disks with a QoS policy already assigned, will go to inconsistent state. Their policy stays intact, but the VMM UI displays it as blank. Admins can either remove those policies or offer these in the affected clouds.
3. Proceed with the rest of the steps and complete the wizard.

Assign private clouds to user roles

After you create a private cloud, you can assign the private cloud to one or more user roles.

1. In **VMs and Services**, select the private cloud that you want to assign.
2. Right-click the selected cloud, and select **Assign Cloud**.
3. Select an existing user role, or select **Create a user role and assign this cloud** to create a new one.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage a VMM private cloud

Article • 07/10/2024

This article describes how to manage System Center - Virtual Machine Manager (VMM) cloud settings.

Manage cloud capacity

You place virtual machines in a VMM cloud if they fit within your capacity settings for the cloud.

- By default, VMM assumes that all the resources allocated to a replica VM are in use and uses this assumption when figuring out whether placing a VM in a cloud or host group will fit within the cloud or host group limits.
- If you want to override this default behavior, you can configure a registry key that allows you to overcommit cloud and host groups in the VMM fabric. In other words, you can place a VM in a cloud or host group even if that placement will bring a cloud or group above its capacity limits. This is useful if you know that you don't need all your replica VMs to be running simultaneously.

Example with the default settings

You have a cloud with a maximum setting of 32 GB of memory. That cloud has two VMs with 4 GB of memory each. If you don't want to place a third VM with 26 GB of memory, the action will fail with **Not enough memory available**.

Example with the registry setting

You have a cloud with a maximum setting of 32 GB of memory. That cloud has two VMs with 4 GB of memory each. To place a third VM with 26 GB of memory, do the following:

1. Update the capacity in the cloud properties to accommodate the increased memory size to, say 64 GB.
2. Navigate to registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings\Placement\IgnoreMemoryForStoppedReplicaVM**.
3. Set the DWORD value to 1. If the value **IgnoreMemoryForStoppedReplicaVM** doesn't exist, create it.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Scenario - Deploy guarded hosts and shielded virtual machines in VMM

Article • 07/17/2024

This article provides an overview of deploying Hyper-V guarded hosts and shielded virtual machines in a System Center Virtual Machine Manager (VMM) compute fabric.

Guarded fabrics provide additional protections for VMs to prevent tampering and theft by malicious administrators and malware. As a cloud service provider or private cloud administrator, you can deploy a guarded fabric that typically consists of a server running the Host Guardian Service (HGS), one or more guarded Hyper-V host servers, and one or more shielded VMs running on those hosts. Learn more about guarded fabrics.

Why do I need to protect VMs?

Virtual machines contain sensitive data and configuration that the VM owner would not want a fabric administrator to see. However, since all the data for VMs are stored in files, the data can easily be copied off and inspected by malware or a malicious administrator.

Shielded VMs in Windows Server help prevent such attacks by rigorously attesting to the health of a Hyper-V host before booting up a VM, ensuring the VM can only be started in datacenters authorized by the VM owner, and enabling the guest OS to encrypt its own data by using a new, virtual TPM. The VM owner can select from the following two types of protection when creating a security-sensitive VM:

- **Encryption Supported**: Ideal for enterprise private cloud scenarios where encryption of data at rest and in-flight is necessary, but the fabric administrators are still trusted. The VM console and other management conveniences remain available to fabric administrators.
- **Shielded**: The most secure deployment option, shielding prevents fabric administrators from connecting to the VM console or modifying security aspects of the VM configuration. VM owners can only access the VM through remote management tools they choose to enable. This is recommended for tenants running sensitive workloads on public or shared infrastructure.

Manage a guarded fabric with VMM

The core guarded fabric infrastructure (consisting of one or more guarded Hyper-V hosts, the Host Guardian Service, and the artifacts needed to create shielded VMs) is included with applicable Windows Server version and must be configured according to the guarded fabric documentation. Once set up, you can optionally use System Center Virtual Machine Manager to simplify management of the guarded fabric.

VMM can be used to:

- **Provision and manage guarded hosts in the VMM fabric**: You can add and manage guarded hosts to the VMM fabric. A guarded host is a Hyper-V server that:
  - Meets the guarded host prerequisites.
  - Is authorized by the Host Guardian Service for the fabric to run shielded VMs. The HGS admin determines the requirements for hosts to successfully attest and become **guarded**.
  - Is marked as guarded in VMM by configuring it to use the same HGS URLs as those specified in the global VMM settings.
- **Configure a shielded virtual hard disk and optionally a VM template**: Signed template disks (VHDX) used to deploy new shielded VMs can be stored in the VMM library for easy deployment. You can then use this VHDX in a VM template.
- **Provision and manage shielded VMs**: VMM supports the full lifecycle of shielded VMs. This includes:
  - Creating new shielded VMs from a signed template disk (VHDX), and optionally using a VM template.
  - Converting the existing VMs to shielded VMs.

Next steps

Provision guarded hosts in the VMM fabric

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Provision guarded hosts in VMM

Article • 07/17/2024

This article describes how to deploy guarded Hyper-V hosts in a System Center Virtual Machine Manager (VMM) compute fabric. Learn more about guarded fabric.

There are a couple of ways to set up guarded Hyper-V hosts in a VMM fabric.

- **Configure an existing host to be a guarded host**: You can configure an existing host to run shielded VMs.
- **Add or provision a new guarded host**: This host could be:
  - An existing Windows Server computer (with or without the Hyper-V role)
  - A bare-metal computer

You set up guarded hosts in the VMM fabric as follows:

1. **Configure global HGS settings**: VMM connects all the guarded hosts to the same Host Guardian Service (HGS) server so that you can successfully migrate shielded VMs between the hosts. You specify the global HGS settings that apply to all the guarded hosts, and you can specify the host-specific settings that override the global settings. Settings include:

   - **Attestation URL**: The URL that the host uses to connect to the HGS attestation service. This service authorizes a host to run shielded VMs.
   - **Key protection server URL**: The URL that the host uses to retrieve the key needed to decrypt VMs. The host must pass attestation to retrieve keys.
   - **Code integrity policies**: A code integrity policy restricts the software that can run on a guarded host. When HGS is configured to use TPM attestation, guarded hosts must be configured to use a code integrity policy authorized by the HGS server. You can specify the location of code integrity policies in VMM and deploy them to your hosts. This is optional and isn't required to manage a guarded fabric.
   - **VM shielding helper VHD**: A specially prepared virtual hard disk that is used to convert the existing VMs to shielded VMs. You must configure this setting if you wish to shield the existing VMs.

2. **Configure the cloud**: If the guarded host will be included in a VMM cloud, you need to enable the cloud to support shielded VMs.

Before you start

Ensure that you've deployed and configured the Host Guardian Service before proceeding. Learn more about configuring HGS in the Windows Server documentation.

Additionally, ensure any hosts that will become guarded hosts meet the guarded host prerequisites:

- **Operating system**: Host servers must run Windows Server Datacenter. It's recommended to use Server Core for guarded hosts.
- **Role and features**: Host servers should be running the Hyper-V role and the Host Guardian Hyper-V Support feature. Host Guardian Hyper-V Support lets the host communicate with HGS to attest to its health and request keys for shielded VMs. If your host is running Nano Server, it should have the Compute, SCVMM-Package, SCVMM-Compute, SecureStartup, and ShieldedVM packages installed.
- **TPM-attestation**: If your HGS is configured to use TPM attestation, the host servers must:
  - Use UEFI 2.3.1c and a TPM 2.0 module
  - Boot in UEFI mode (not BIOS or **legacy** mode)
  - Enable Secure Boot
- **HGS registration**: Hyper-V hosts must be registered with HGS. How they're registered depends on whether HGS is using AD or TPM attestation. Learn more
- **Live migration**: If you want to live migrate shielded VMs, you need to deploy two or more guarded hosts.
- **Domain**: Guarded hosts and the VMM server must be in the same domain or in domains with a two-way trust.

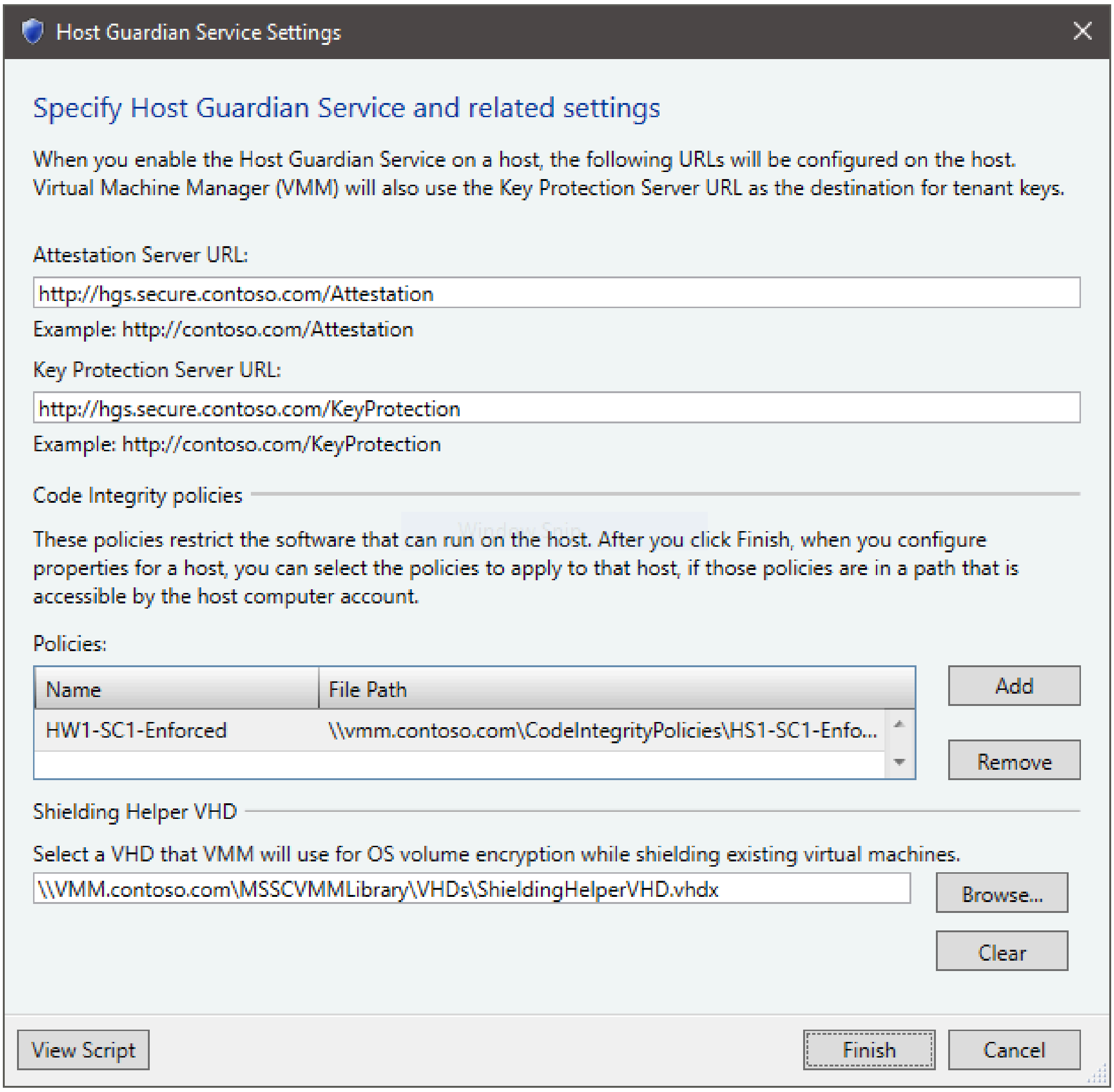
Configure global HGS settings

Before you can add guarded hosts to your VMM compute fabric, you must configure VMM with information about the HGS for the fabric. The same HGS will be used for all guarded hosts managed by VMM.

1. Obtain the attestation and key protection URLs for your fabric from your HGS administrator.

2. In the VMM console, select **Settings** > **Host Guardian Service Settings**.

3. Enter the attestation and key protection URLs in the respective fields. You don't need to configure the code integrity policies and VM shielding helper VHD sections at this time.



Host Guardian Service Settings

Specify Host Guardian Service and related settings

When you enable the Host Guardian Service on a host, the following URLs will be configured on the host. Virtual Machine Manager (VMM) will also use the Key Protection Server URL as the destination for tenant keys.

Attestation Server URL: http://hgs.secure.contoso.com/Attestation

Example: http://contoso.com/Attestation

Key Protection Server URL: http://hgs.secure.contoso.com/KeyProtection

Example: http://contoso.com/KeyProtection

Code Integrity policies

These policies restrict the software that can run on the host. After you click Finish, when you configure properties for a host, you can select the policies to apply to that host, if those policies are in a path that is accessible by the host computer account.

Policies:

Name	File Path
HW1-SC1-Enforced	\\vmm.contoso.com\CodeIntegrityPolicies\HS1-SC1-Enfo...

Shielding Helper VHD

Select a VHD that VMM will use for OS volume encryption while shielding existing virtual machines.

\\VMM.contoso.com\MSSCVMMLibrary\VHDs\ShieldingHelperVHD.vhdx

4. Select **Finish** to save the configuration.

Add or provision a new guarded host

1. Add the host:

   - If you want to add an existing server running Windows Server as a guarded Hyper-V host, add it to the fabric.
   - If you want to provision a Hyper-V host from a bare-metal computer, follow these prerequisites and instructions.

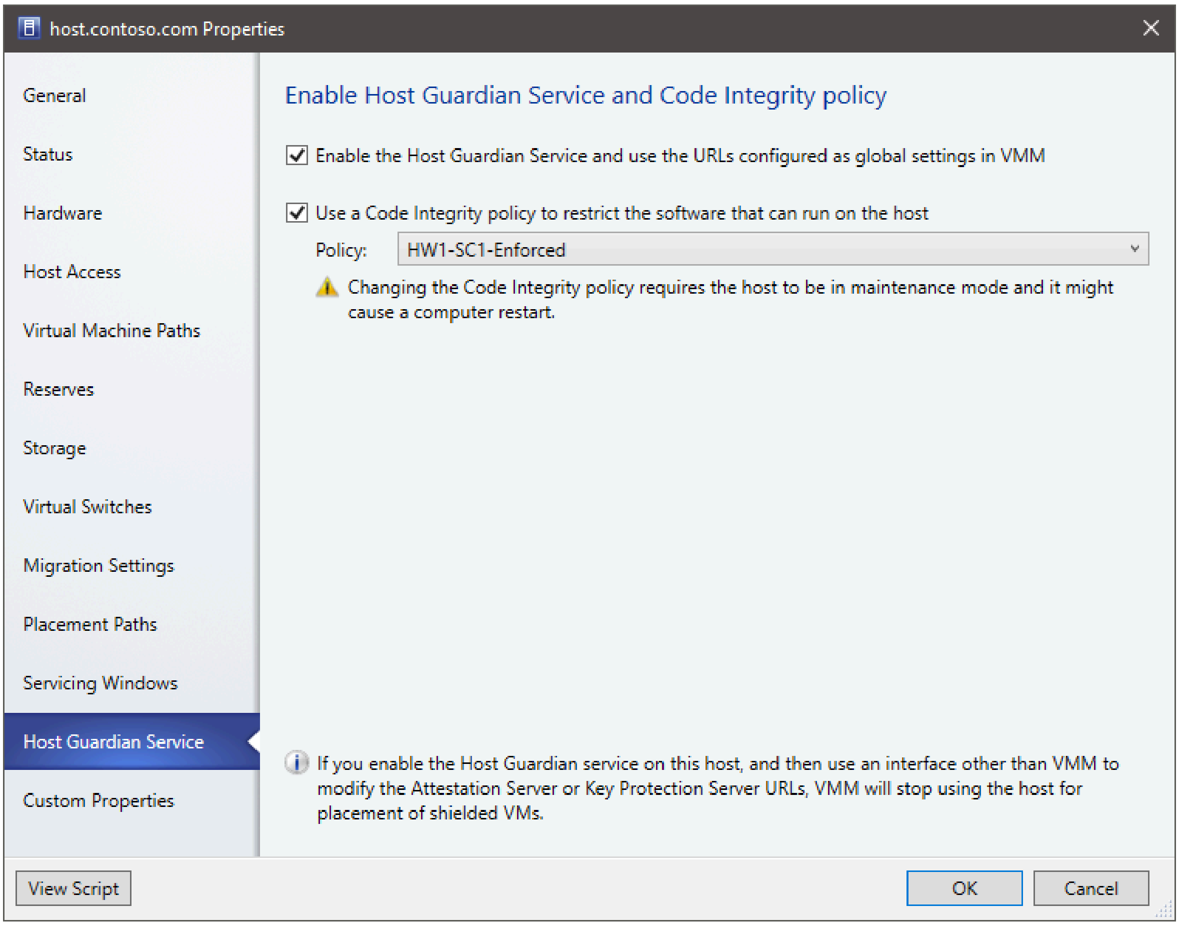
   > ⓘ **Note**
   >
   > You can deploy the host as guarded when you provision it (Add Resource Wizard > **OS Settings** > **Configure as guarded host**).

2. Continue to the next section to configure the host as a guarded host.

Configure an existing host to be a guarded host

To configure an existing Hyper-V host managed by VMM to be a guarded host, complete the following steps:

1. Place the host in maintenance mode.
2. In **All Hosts**, right-click the host > **Properties** > **Host Guardian Service**.



host.contoso.com Properties

Enable Host Guardian Service and Code Integrity policy

☑ Enable the Host Guardian Service and use the URLs configured as global settings in VMM

☑ Use a Code Integrity policy to restrict the software that can run on the host

Policy: HW1-SC1-Enforced

Changing the Code Integrity policy requires the host to be in maintenance mode and it might cause a computer restart.

If you enable the Host Guardian service on this host, and then use an interface other than VMM to modify the Attestation Server or Key Protection Server URLs, VMM will stop using the host for placement of shielded VMs.

3. Select to enable the Host Guardian Hyper-V Support feature and configure the host.

> ⓘ **Note**
>
> - The global attestation and key protection server URLs will be set on the host.
> - If you modify these URLs outside the VMM console, you need to update them in VMM too. If you don't, VMM won't place shielded VMs on the

> host until the URLs match again. You can also uncheck and re-check the **Enable** box to reconfigure the host with the URLs configured in VMM.

4. If you're using VMM to manage code integrity policies, you can enable the second checkbox and select the appropriate policy for the system.

5. Select **OK** to update the host's configuration.

6. Take the host out of the maintenance mode.

VMM checks that the host passes attestation when you add it and every time the host status is refreshed. VMM only deploys and migrates shielded VMs on hosts that have passed attestation. You can check the attestation status of a host in **Properties** > **Status** > **HGS Client Overall**.

Enable guarded hosts on a VMM cloud

Enable a cloud to support guarded hosts:

1. In the VMM console, select **VMs and Services** > **Clouds**. Right-click the cloud name > **Properties**.
2. In **General** > **Shielded VM support**, select **Supported on this private cloud**.

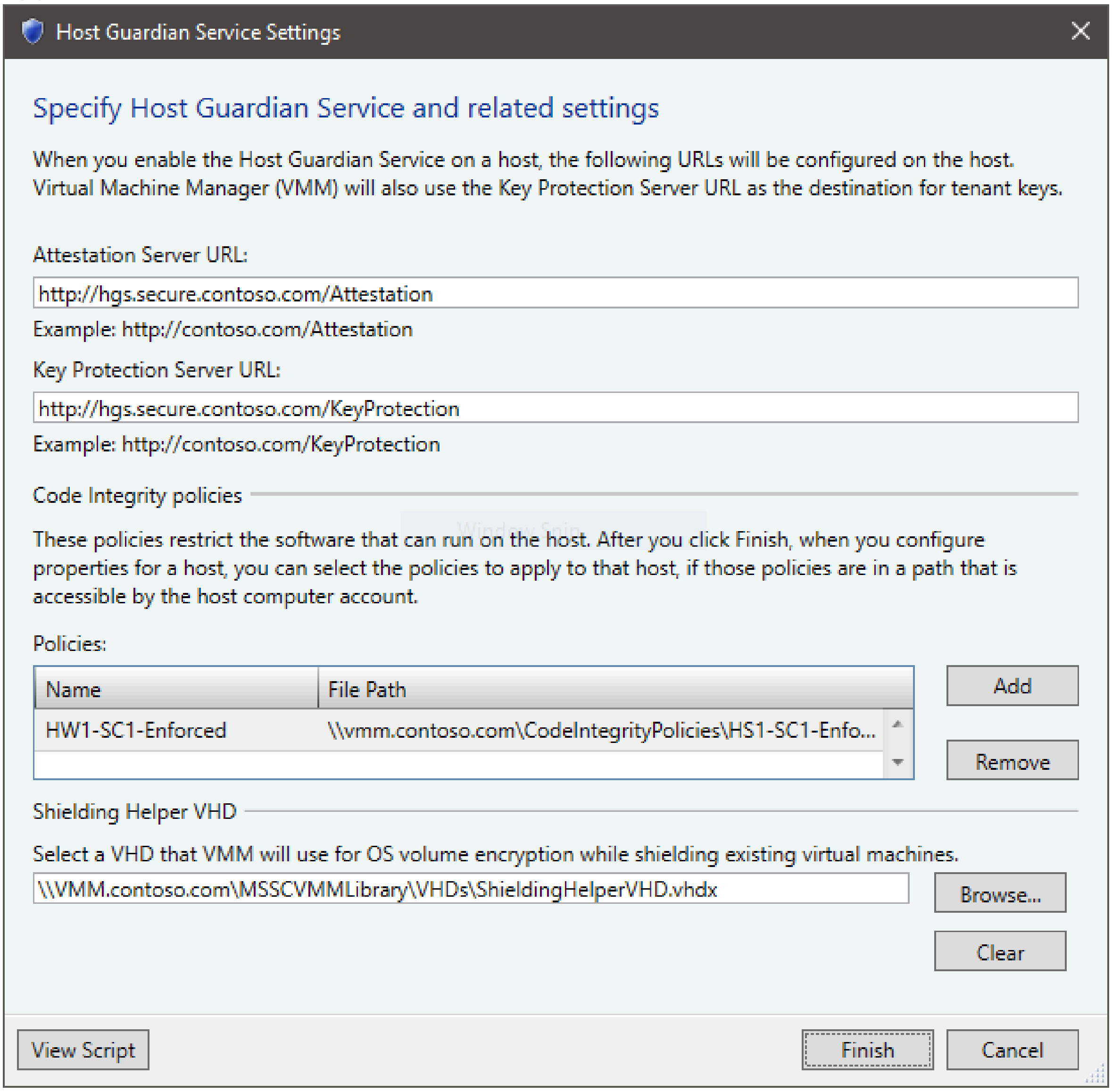
Manage and deploy code integrity policies with VMM

In guarded fabrics configured to use TPM attestation, each host must be configured with a code integrity policy that is trusted by the Host Guardian Service. To ease the management of code integrity policies, you can optionally use VMM to deploy new or updated policies to your guarded hosts.

To deploy a code integrity policy to a guarded host managed by VMM, complete the following steps:

1. Create a code integrity policy for each reference host in your environment. You need a different CI policy for each unique hardware and software configuration of your guarded hosts.
2. Store the CI policies in a secure file share. The computer accounts for each guarded host require **read access** to the share. Only trusted administrators should have write access.
3. In the VMM console, select **Settings** > **Host Guardian Service Settings**.

4. Under the Code Integrity Policies section, select **Add** and specify a friendly name and the path to a CI policy. Repeat this step for each unique CI policy. Ensure to name your policies in a manner that will help you identify which policy should be applied to which hosts.



Host Guardian Service Settings

Specify Host Guardian Service and related settings

When you enable the Host Guardian Service on a host, the following URLs will be configured on the host. Virtual Machine Manager (VMM) will also use the Key Protection Server URL as the destination for tenant keys.

Attestation Server URL: http://hgs.secure.contoso.com/Attestation

Example: http://contoso.com/Attestation

Key Protection Server URL: http://hgs.secure.contoso.com/KeyProtection

Example: http://contoso.com/KeyProtection

Code Integrity policies

These policies restrict the software that can run on the host. After you click Finish, when you configure properties for a host, you can select the policies to apply to that host, if those policies are in a path that is accessible by the host computer account.

Policies:

Name	File Path
HW1-SC1-Enforced	\\vmm.contoso.com\CodeIntegrityPolicies\HS1-SC1-Enfo...

Shielding Helper VHD

Select a VHD that VMM will use for OS volume encryption while shielding existing virtual machines.

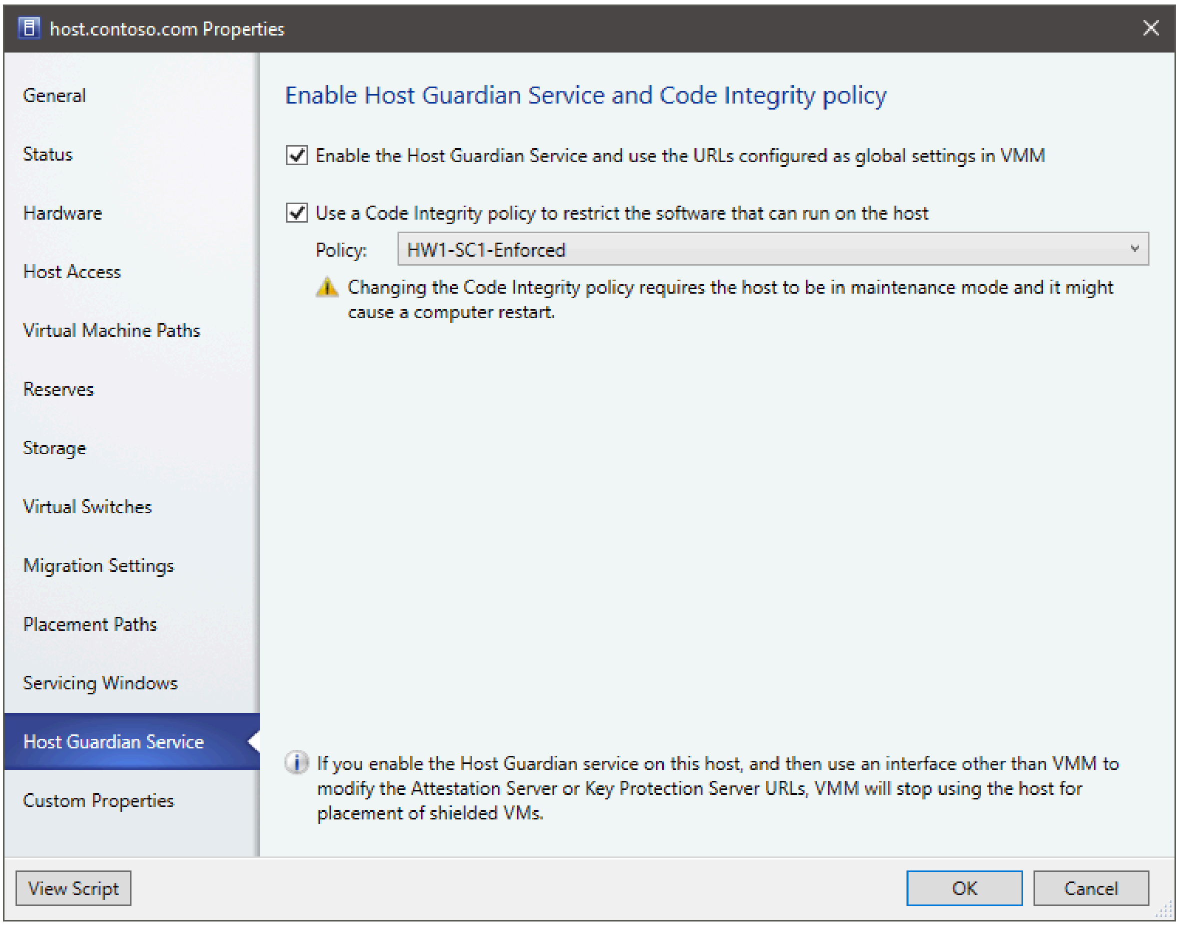
\\VMM.contoso.com\MSSCVMMLibrary\VHDs\ShieldingHelperVHD.vhdx

5. Select **Finish** to save the configuration.

Now, for each guarded host, complete the following steps to apply a code integrity policy:

1. Place the host in maintenance mode.

2. In **All Hosts**, right-click the host > **Properties** > **Host Guardian Service**.



host.contoso.com Properties

Enable Host Guardian Service and Code Integrity policy

☑ Enable the Host Guardian Service and use the URLs configured as global settings in VMM

☑ Use a Code Integrity policy to restrict the software that can run on the host

Policy: HW1-SC1-Enforced

⚠ Changing the Code Integrity policy requires the host to be in maintenance mode and it might cause a computer restart.

ⓘ If you enable the Host Guardian service on this host, and then use an interface other than VMM to modify the Attestation Server or Key Protection Server URLs, VMM will stop using the host for placement of shielded VMs.

3. Select to enable the option to configure the host with a code integrity policy. Then select the appropriate policy for the system.

4. Select **OK** to apply the configuration change. The host can restart to apply the new policy.

5. Take the host out of maintenance mode.

> ⚠ **Warning**
>
> Ensure that you select the correct code integrity policy for the host. If an incompatible policy is applied to the host, some applications, drivers, or operating system components may no longer work.

If you update the code integrity policy in the file share and wish to also update the guarded hosts, you can do so by completing the following steps:

1. Place the host in maintenance mode.
2. In **All Hosts**, right-click the host > **Apply Latest Code Integrity Policy**.
3. Take the host out of maintenance mode.

Next steps

- Set up a shielded template disk, utility disk, and VM template.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Configure HGS fallback URLs in VMM

Article • 07/17/2024

This article describes how to define the fallback Host Guardian Service (HGS) URLs in System Center Virtual Machine Manager (VMM) global settings. For information about guarded fabrics, see this article.

Being at the heart of providing attestation and key protection services to run shielded VMs on Hyper-V hosts, the host guardian service (HGS) must operate even in situations of disaster.

With fallback HGS configuration feature in VMM, a guarded host can be configured with a primary and secondary pair of HGS URLS (an attestation and key protection URI). This capability enables scenarios, such as guarded fabric deployments spanning two data centers for disaster recovery purposes, HGS running as shielded VMs, and so on.

The primary HGS URLs will always be used in favor of the secondary. If the primary HGS fails to respond after the appropriate timeout and retry count, the operation will be reattempted against the secondary. Subsequent operations will always favor the primary; the secondary will only be used when the primary fails.

Before you start

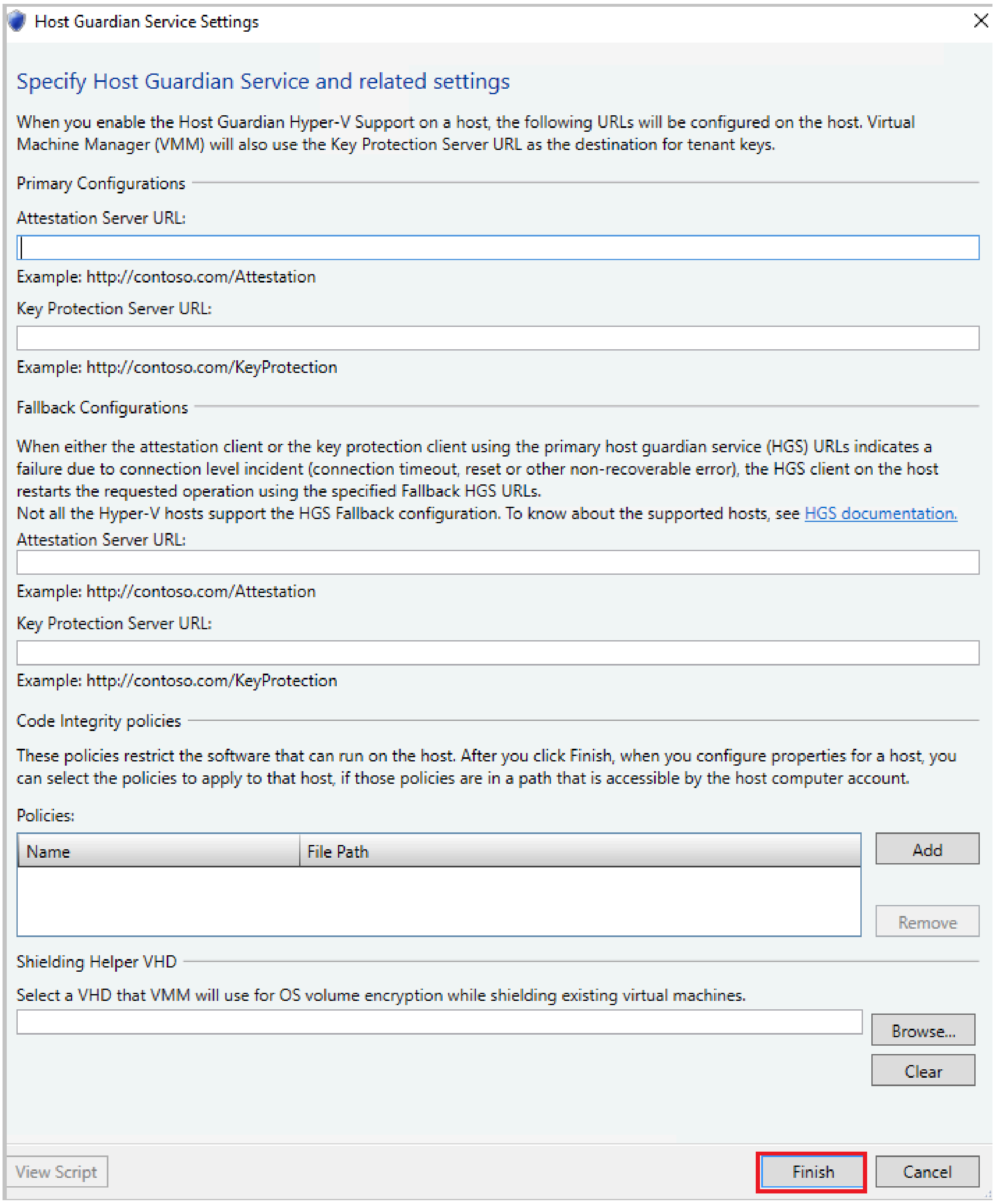
Ensure that you've deployed and configured the Host Guardian Service before proceeding. Learn more about configuring HGS.

Configure fallback HGS

Use the following steps:

1. Navigate to **VMM Settings** > **General Settings** > **Host Guardian Service Settings**. On the **Host Guardian Service Settings** page, you see a section for Fallback Configurations.

2. Define the **primary and fallback HGS URLs** and select **Finish**.



Host Guardian Service Settings

Specify Host Guardian Service and related settings

When you enable the Host Guardian Hyper-V Support on a host, the following URLs will be configured on the host. Virtual Machine Manager (VMM) will also use the Key Protection Server URL as the destination for tenant keys.

Primary Configurations

Attestation Server URL:

Example: http://contoso.com/Attestation

Key Protection Server URL:

Example: http://contoso.com/KeyProtection

Fallback Configurations

When either the attestation client or the key protection client using the primary host guardian service (HGS) URLs indicates a failure due to connection level incident (connection timeout, reset or other non-recoverable error), the HGS client on the host restarts the requested operation using the specified Fallback HGS URLs.
Not all the Hyper-V hosts support the HGS Fallback configuration. To know about the supported hosts, see HGS documentation.

Attestation Server URL:

Example: http://contoso.com/Attestation

Key Protection Server URL:

Example: http://contoso.com/KeyProtection

Code Integrity policies

These policies restrict the software that can run on the host. After you click Finish, when you configure properties for a host, you can select the policies to apply to that host, if those policies are in a path that is accessible by the host computer account.

Policies:

Name	File Path

Shielding Helper VHD

Select a VHD that VMM will use for OS volume encryption while shielding existing virtual machines.

3. Enable the fallback URLs on the host by navigating to **Host Properties** > **Host Guardian Service**. Select Enable host Guardian Hyper-V support and use the URLs as configured as global settings in VMM and select **OK**.

> ⓘ Note
>
> After this step, the VMM service configures the supported hosts with primary and fallback HGS URLs. Only hosts on and above Windows Server 1709 support fallback HGS URLs.

PowerShell command updates

1. The following two parameters are added to the existing **Set-SCVMHost** PowerShell command:

   - **AttestationFallbackServerUrl**
   - **KeyProtectionFallbackServerUrl**

   Here's the sample syntax.

   PowerShell

```
Set-SCVMHost [-VMHost] <Host> [-ApplyLatestCodeIntegrityPolicy] [-
AttestationServerUrl <String>]        [-AttestationFallbackServerUrl
<String>]
[-AvailableForPlacement <Boolean>] [-BMCAddress <String>]
[-BMCCustomConfigurationProvider <ConfigurationProvider>] [-BMCPort
<UInt32>]
[-BMCProtocol <OutOfBandManagementType>] [-BMCRunAsAccount
<RunAsAccount>] [-BaseDiskPaths <String>]
[-BypassMaintenanceModeCheck] [-CPUPercentageReserve <UInt16>] [-
CodeIntegrityPolicy <CodeIntegrityPolicy>]
[-Custom1 <String>] [-Custom10 <String>] [-Custom2 <String>] [-Custom3
<String>] [-Custom4 <String>]
[-Custom5 <String>] [-Custom6 <String>] [-Custom7 <String>] [-Custom8
<String>] [-Custom9 <String>]
[-Description <String>] [-DiskSpaceReserveMB <UInt64>] [-
EnableLiveMigration <Boolean>]
[-FibreChannelWorldWideNodeName <String>] [-
FibreChannelWorldWidePortNameMaximum <String>]
[-FibreChannelWorldWidePortNameMinimum <String>] [-
IsDedicatedToNetworkVirtualizationGateway <Boolean>]
[-JobGroup <Guid>] [-JobVariable <String>] [-KeyProtectionServerUrl
<String>] [-KeyProtectionFallbackServerUrl <String>] [-
LiveMigrationMaximum <UInt32>]
[-LiveStorageMigrationMaximum <UInt32>] [-MaintenanceHost <Boolean>] [-
ManagementAdapterMACAddress <String>]
[-MaxDiskIOReservation <UInt64>] [-MemoryReserveMB <UInt64>]
[-MigrationAuthProtocol <MigrationAuthProtocolType>]
[-MigrationPerformanceOption <MigrationPerformanceOptionType>] [-
MigrationSubnet <String[]>]
[-NetworkPercentageReserve <UInt16>] [-NumaSpanningEnabled <Boolean>]
[-OverrideHostGroupReserves <Boolean>]
[-PROTipID <Guid>] [-RemoteConnectCertificatePath <String>] [-
RemoteConnectEnabled <Boolean>]
[-RemoteConnectPort <UInt32>] [-RemoveRemoteConnectCertificate] [-
RunAsynchronously] [-SMBiosGuid <Guid>]
[-SecureRemoteConnectEnabled <Boolean>] [-UseAnyMigrationSubnet
<Boolean >]
[-VMHostManagementCredential <VMMCredential>] [-VMPaths <String>]
[<CommonParameters>]
```

2. The following parameter is added to **Get-SCGuardianConfiguration** to let the user specify from which HGS the metadata must be fetched.

   [-Guardian {Primary | Fallback}]

   Syntax

   PowerShell

   ```PowerShell
   Get-SCGuardianConfiguration [-Guardian {Primary | Fallback}] [-
   OnBehalfOfUser <String>] [-OnBehalfOfUserRole <UserRole>] [-VMMServer
   <ServerConnection>] [<CommonParameters>]
   ```

Next steps

- Deploy the Host Guardian Service (HGS)
- Manage HGS
- Set up a fallback HGS for a branch office

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up a disk and a VM template to deploy shielded VMs

Article • 07/17/2024

You deploy shielded virtual machines in the System Center Virtual Machine Manager (VMM) compute fabric using a signed virtual machine hard disk (VHDX) and optionally with a VM template. This article describes how to add signed template disks to VMM, configure a shielding utility disk, deploy new shielded VMs, and convert the existing VMs to shielded VMs in VMM.

Before you start

- The signed template disk used to create the shielded VM template must have the family and version marked.
- The VMM library to which you add the signed template disk must be accessible to clouds from which shielded VMs will be provisioned.
- The library shared should be added to clouds from which shielded VMs will be provisioned (not in read-only mode).

Add signed template disks for shielded VMs to the VMM library

Shielded VMs can be deployed in two ways: by deploying directly from a signed template disk or by converting an existing VM to a shielded VM.

Signed template disks assure tenants that the disk contents haven't been modified and enable tenants to securely transfer deployment secrets like administrator passwords and certificates to the VM in an encrypted manner. For this reason, it's preferred to deploy shielded VMs from signed template disks.

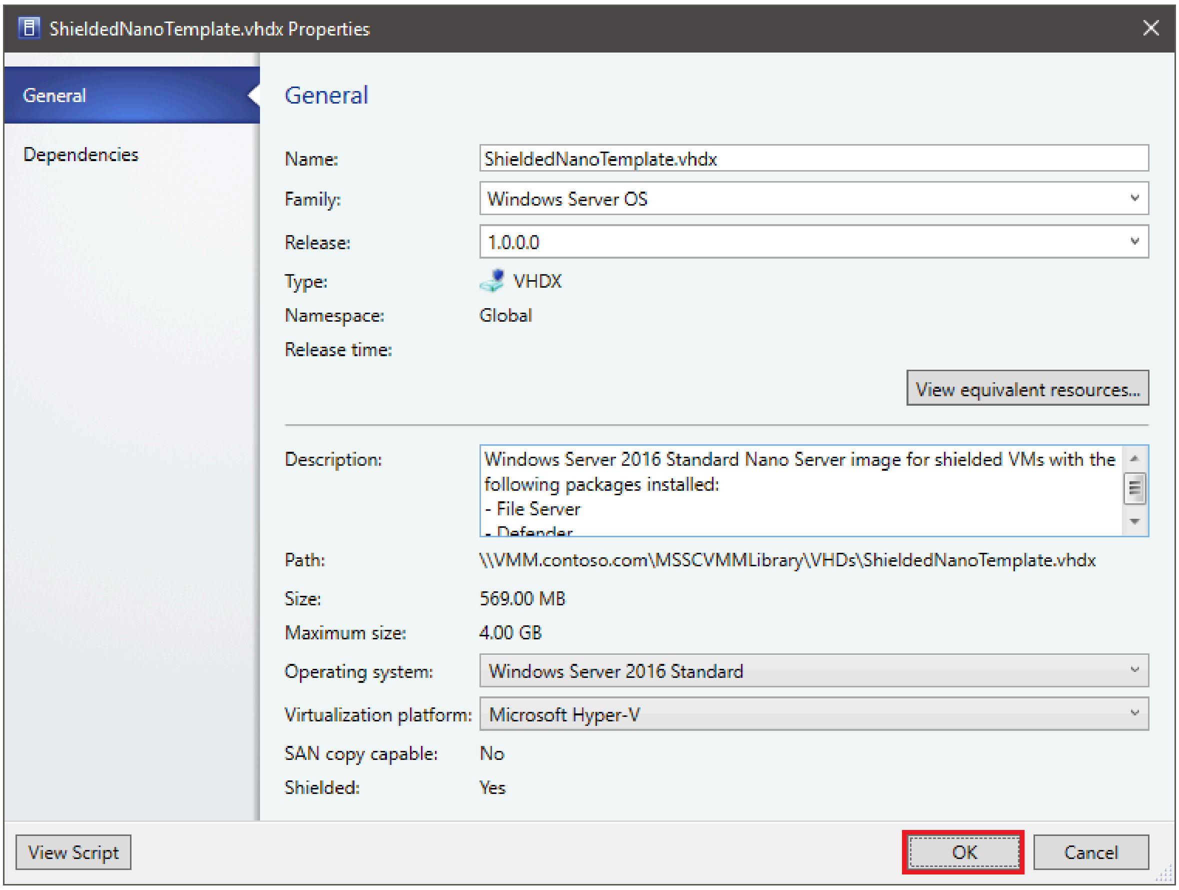
To prepare and add a signed template disk to the VMM library, complete the following steps:

1. Prepare a signed template disk on a machine running Windows Server 2016 or 2019 with Desktop Experience or later, or Windows 10 or Windows 11 with the Remote Server Administration Tools installed.

2. Copy the template disk to a library share (\\<vmmserver>\MSSCVMMLibrary\VHDs by default), and refresh the library server.

3. To provide VMM with information about the operating system on the template disk, in **Library**, right-click the disk > **Properties**.

4. In **Operating system**, select the operating system installed on the disk. This indicates to VMM that the VHDX isn't blank. The shield icon next to the disk name denotes it as a signed template disk for shielded VMs. Supply the information about the **Family** and **Release** of the disk as well to make the resources available in the tenant Azure Pack self-service portal (optional).


ShieldedNanoTemplate.vhdx Properties
General
Dependencies
View equivalent resources...
View Script
OK
Cancel

General

Name: ShieldedNanoTemplate.vhdx
Family: Windows Server OS
Release: 1.0.0.0
Type: VHDX
Namespace: Global
Release time:
Description: Windows Server 2016 Standard Nano Server image for shielded VMs with the following packages installed:
- File Server
- Defender
Path: \\VMM.contoso.com\MSSCVMMLibrary\VHDs\ShieldedNanoTemplate.vhdx
Size: 569.00 MB
Maximum size: 4.00 GB
Operating system: Windows Server 2016 Standard
Virtualization platform: Microsoft Hyper-V
SAN copy capable: No
Shielded: Yes

5. Select **OK** to save the properties of the signed template disk.

Create a shielded VM template

You can optionally create a shielded VM template using a signed template disk. VM templates define virtual machine resources such as CPU count, RAM, and networking for an OS disk.

Templates for shielded VMs vary slightly from a regular VM template. Some settings are fixed; for example, the VM must be a Generation 2 VM with Secure Boot enabled. Create the VM template as follows:

1. Select **Library** > **Create VM Template**. In **Select Source**, select Use an existing VM template or a virtual hard disk stored in the library > **Browse**.

2. Select the signed template disk, specify a template name and optional description, and select **OK**.
3. In **Configure Hardware**, specify the hardware properties for the VMs you create from the template. Ensure there's at least one NIC configured and available. Tenants connect to shielded VMs over Remote Desktop Connection, Windows Remote Management, or other remote management tools that require networking.
4. If you want to use static IP addressing in the tenant pool, you need to let your tenants know. Tenants need to provide an answer file with values, which specializes a shielded VM for them. There are special, well-known placeholder values required to support static IP pools.
5. In **Configure Operating System**, specify the OS version, computer name, product key, and time zone. The tenant provides secure information, such as the administrator password in a shielding data file (.PDK), that they'll provide when provisioning a new VM. If you specify a product key, ensure it's valid for the operating system on the template disk. If it isn't, the VM won't provision successfully. After the VM template is created, ensure that it's available to the Tenant Administrator user role. Tenants can then use it to provision new VMs.

Configure the shielding helper VHD

The existing Windows VMs can also be converted to shielded VMs with the use of a shielding helper VHD. The helper VHD is a special disk prepared with tools to encrypt another VM's operating system drive. VMM must be configured with a helper VHD before you can shield the existing VMs.

1. Prepare a helper VHD on a computer running Windows Server 2016 or later or Windows 10 or Windows 11 with the Remote Server Administration Tools installed.
2. Copy the helper VHD to a library share, and refresh the library server.
3. In the VMM console, select **Settings** > **Host Guardian Service Settings**.
4. In the Shielding Helper VHD section, select **Browse** and select the helper VHD from the list of files in the library shares.
5. Select **Finish** to save the configuration.

With the shielding helper VHD configured, you can proceed to shield an existing VM.

Next steps

Review Provision shielded VMs to understand how to deploy shielded virtual machines in a VMM compute fabric.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Provision shielded virtual machines in the VMM fabric

Article • 07/17/2024

This article describes how to deploy shielded virtual machines in the System Center Virtual Machine Manager (VMM) compute fabric.

You can deploy shielded VMs in VMM in a couple of ways:

- Convert an existing VM into a shielded VM.
- Create a new shielded VM using a signed virtual machine hard disk (VHDX) and optionally a VM template.

> ⓘ **Note**
>
> You may experience issues deploying a shielded virtual machine over a network with a load balancer or WAN optimization device. It's required for the packet to not be modified during transit for Shielded VMs to successfully deploy.

Before you start

Watch a video that provides a quick, two-minute overview of provisioning shielded VMs in VMM. Then, ensure that you've done the following:

1. **Prepare an HGS server**: You should have an HGS server deployed. Learn more.

2. **Set up VMM**: You need to configure global HGS settings in VMM, and set up at least one guarded host. If guarded hosts belong to a cloud, the cloud should be enabled to support shielded VMs. Learn more.

3. **Prepare a shielded VHDX and VM template**: You should deploy shielded VMs from a shielded virtual hard disk (VHDX), and optionally using a VM template. Learn more about preparing these.

   > ⓘ **Note**
   >
   > You cannot use a service template to create a shielded VM. Use a script instead.

4. **Prepare shielding data files**: To use the signed template disks in the VMM library, tenants must prepare one or more shielding data files. This file contains all the secrets that a tenant needs to deploy a VM, including the unattend file used to specialize the VM, certificates, and administrator account passwords. The file also specifies which guarded fabric a tenant trusts to host their VM and information about the signed template disks. The file is encrypted and can only be read by a host in a guarded fabric trusted by the tenant. Learn more.

5. **Set up host group**: For easy management, we recommend that guarded hosts be placed in a dedicated VMM host group.

6. **Verify existing VM requirements**: If you want to convert an existing VM to shielded, note the following:

    - The VM must be Generation 2 and have the Microsoft Windows Secure Boot template enabled
    - The operating system on the disk must be one of:
        - Windows Server 2022, Windows Server 2019, Windows Server 2016
        - Windows 11, Windows 10
    - The OS disk for the VM must use the GUID Partition Table. This is required for Generation 2 VMs to support UEFI.

7. **Set up helper VHD**: The hosting service provider will need to create a VM that acts as a helper VHD for converting the existing machines. Learn more.

Add shielding data files to VMM

Before you can convert an existing VM to a shielded VM or provision a new shielded VM from a template, the VM owner must generate a shielding data file and add it to VMM.

If you don't already have a shielding data file imported, complete the following steps:

1. Create a shielding data file if you don't have one already. Ensure that the shielding data file authorizes the hosting fabric VMM manages to run your shielded VMs.
2. In the VMM console, select **Library** > **Import Shielding Data** > **Browse** and select your shielding data file.
3. Specify a friendly name for the shielding data file in **Name** and optionally add a description. We recommend that you indicate whether the shielding data file is intended for use with the existing or new VMs in its name to make it easier to find again.
4. Select **Import** to save the shielding data in VMM.

To manage your imported shielding data files, go to **Library** > **VM Shielding Data** (under **Profiles**).

Provision a new shielded VM

1. Ensure that you have all the prerequisites in place before you start.
2. In **VMs and Services**, select **Create Virtual Machine** to open the Create Virtual Machine Wizard.
3. In **Select Source**, select **Use an existing virtual machine, VM template, or virtual hard disk** > **Browse**.
4. Select a shielded VM template or signed template disk. Both are identified by the shield icon 🛡.
5. In **Select Shielding Data File**, select **Browse**, and select a shielding data file. Only shielding data files that can be used to create a new shielded VM will be shown. Select **OK** > **Next** to continue.
6. Follow these instructions to complete the wizard, and to deploy the VM on a host/cloud.

When you complete the wizard, VMM creates a new shielded VM from the disk or template:

1. The template disk (VHDX) file is copied from the VMM library.
2. VM provisioning decrypts the data in the shielding data file, completes any substitution strings in the unattend.xml file, and copies additional files from the shielding data file to the operating system drive (for example, the RDP certificate).
3. The VM restarts, is customized, and re-encrypted with BitLocker. The BitLocker full volume encryption key is stored in the virtual TPM of the new VM.
4. VM customization is complete when the shutdown command in the unattend.xml file runs; the VM remains switched off. If customization gets stuck, check the unattend.xml file by running it on an unshielded VM, or using an encryption-supported shielding data file that allows console access.
5. After VMM detects that specialization has finished, it will update its status to indicate the VM is created and, if selected, start up the VM.

Shield an existing VM

You can enable shielding for a VM currently running on a host in the VMM fabric that isn't guarded.

1. Ensure that you've all the prerequisites in place before you start.
2. Take the VM offline.

3. We recommend that you enable BitLocker on all disks attached to the VM before moving it to the guarded host.
4. Select the VM > **Properties** > **Shield** and select a shielding data file.
5. Shut down the VM, export from nonguarded host, and import it to a guarded host. Only a guarded host can access the VM data.

Next steps

Review Manage virtual machine settings to learn how to configure performance and availability settings for VMs.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Provision a shielded Linux virtual machine in the VMM fabric

Article • 07/17/2024

This article describes how to deploy Linux shielded virtual machines (VMs) in System Center Virtual Machine Manager (VMM).

Procedure to shield a Linux VM

Windows Server 2016 introduced the concept of a shielded VM for Windows OS-based virtual machines. Shielded VMs provide protection against malicious administrator actions when the VM's data is at rest or when untrusted software is running on Hyper-V hosts. Learn more.

With Windows Server version 1709, Hyper-V introduced support for provisioning Linux shielded VMs.

Shield a Linux VM

1. Create a signed template disk.
2. Create a Linux shielded VM template in VMM.
3. Generate a shielding data file (PDK).
4. Create a Linux shielded VM by using the VM template and the PDK.

> ⓘ **Note**
>
> If you use Wireless Application Protocol (WAP), you can provision Linux shielded VMs in the same way you provision Windows shielded VMs.

Prepare a template disk

1. Follow these steps to create the template disk.

2. In the **Preparing a Linux Image** section of the directions, before you install lsvmtools, install the VMM specialization agent.

Sign the template disk

1. Generate a certificate. You can use a self-signed certificate for testing.

   Use the following sample cmdlet:

   PowerShell

   ```
       $cert = New-SelfSignedCertificate -DnsName
   '<<signing.contoso.com>>'
   ```

2. Sign the disk by using a Windows Server 1709 or later machine. Use the following sample cmdlet:

   PowerShell

   ```
   Protect-TemplateDisk -Path "<<Path to the VHDX>>" -TemplateName "
   <<Template Name>>" -Version <<x.x.x.x>> -Certificate $cert -
   ProtectedTemplateTargetDiskType PreprocessedLinux
   ```

3. Copy the template disk and the signed image to the VMM library.

Create a Linux shielded VM template in VMM

1. In the VMM console library, select **Create VM Template**.

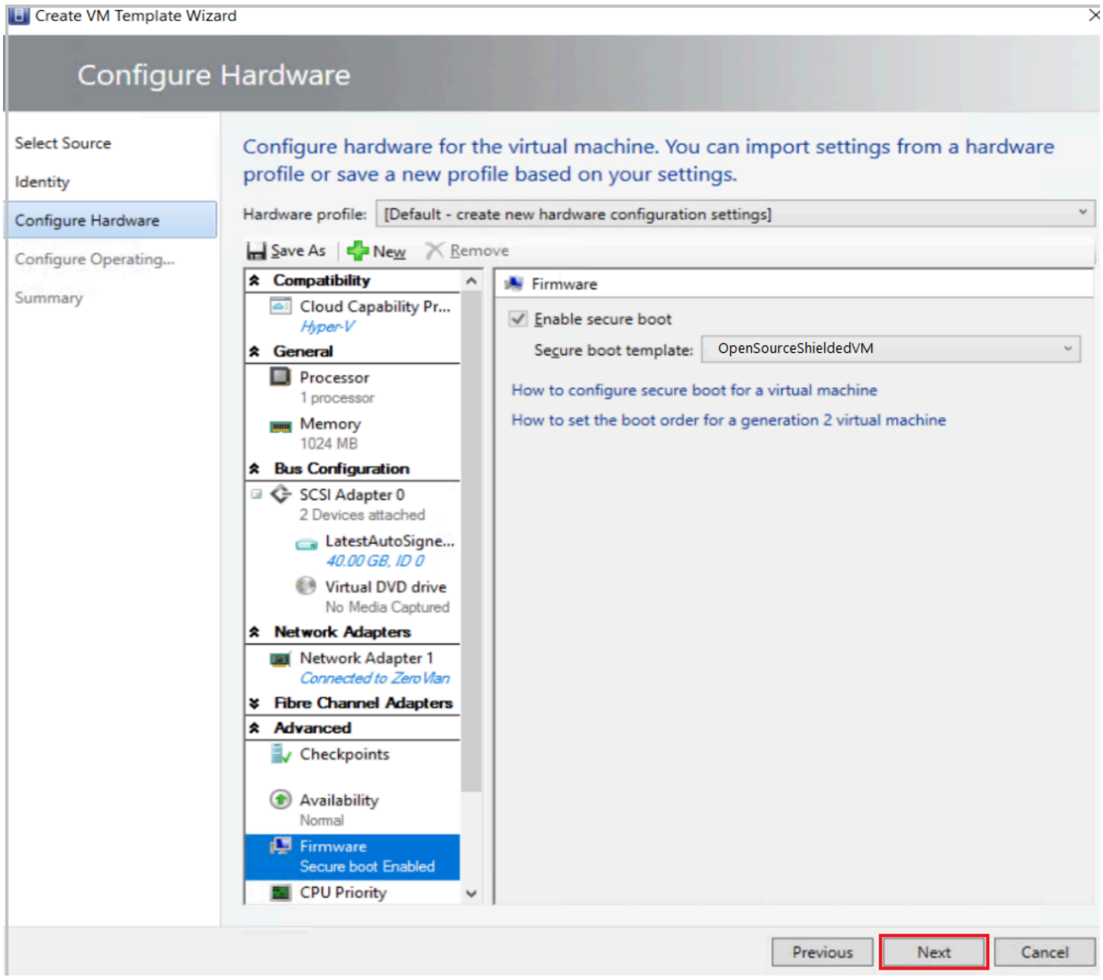
2. In **Select Source**, select **Use an existing VM template**. Browse to select the signed template disk that you added to the VMM library. Then, select **Next**.

3. In **Configure Hardware**:

   - Under **Firmware**, select **Enable secure boot**. From the **Secure boot template** dropdown menu, select **OpenSourceShieldedVM**.

     > ⓘ Note
     >
     > This boot template is a new addition to RS3 hosts. If no RS3 hosts are in VMM, this option won't show up on the **Secure boot template** menu.

   - Select the required configuration for other hardware properties, such as processors, memory, and the VM network.



Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings.

Hardware profile: [Default - create new hardware configuration settings]

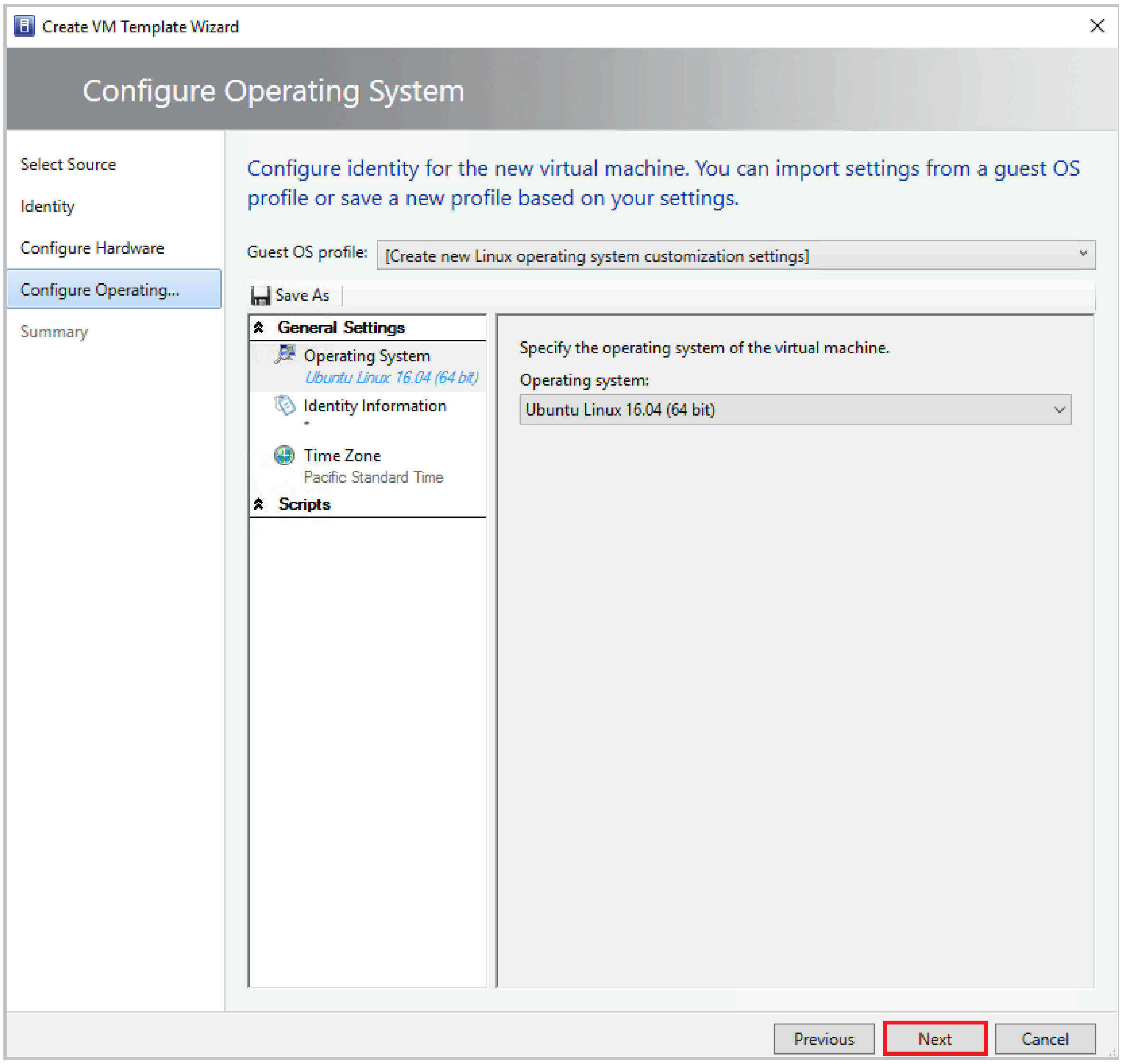
☑ Enable secure boot

Secure boot template: OpenSourceShieldedVM

4. In **Configure Operating System**:

- Select the Guest OS profile as **[Create new Linux operating system customization settings]**.
- Select the OS on the template disk that you created earlier (**Ubuntu Linux**).

5. Select **Next**.



Create VM Template Wizard

Configure Operating System

Configure identity for the new virtual machine. You can import settings from a guest OS profile or save a new profile based on your settings.

Guest OS profile: [Create new Linux operating system customization settings]

Specify the operating system of the virtual machine.

Operating system: Ubuntu Linux 16.04 (64 bit)

6. In **Summary**, review the details and select **Create to finish generation of Linux shielded VM template in VMM**.

Generate the shielding data file

Before you generate the shielding data file (PDK):

1. Get the guardian metadata from the Host Guardian Service (HGS).
2. Extract the volume signature catalog (VSC) file.

To generate the PDK, run the following sample script on a server that's running Windows Server version 1709 or later:

```PowerShell
# Create a VolumeSignatureCatalog file for the template disk to ensure that
no one tampers with the template disk at the deployment time
# Create an owner certificate
```

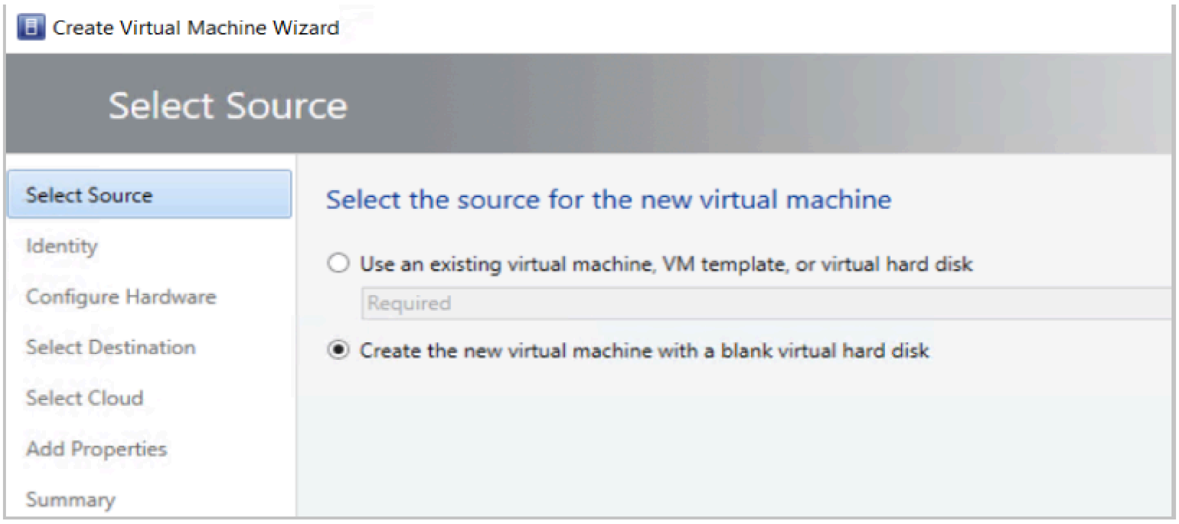
```
$Owner = New-HgsGuardian -Name '<<Owner>>' -GenerateCertificates

# Import the HGS guardian
$Guardian = Import-HgsGuardian -Path <<Import the xml from pre-step 1>> -
Name '<<Name of the guardian>>' -AllowUntrustedRoot

# Create the PDK file on a server running Windows Server version 1709

New-ShieldingDataFile -ShieldingDataFilePath '<<Shielding Data file path>>'
-Owner $Owner -Guardian $guardian -VolumeIDQualifier (New-VolumeIDQualifier
-VolumeSignatureCatalogFilePath '<<Path to the .vsc file generated in pre-
step 2>>' -VersionRule Equals) -AnswerFile '<<Path to
LinuxOsConfiguration.xml>>' -policy Shielded
```

Create a Linux shielded VM by using the VM template and the PDK

1. In the VMM console, select **Create Virtual Machine**.

2. Select **Use an existing virtual machine, VM template, or virtual hard disk**.

3. Select **Linux shielded VM template** > **Next**.


Create Virtual Machine Wizard

Select Source

Select the source for the new virtual machine

○ Use an existing virtual machine, VM template, or virtual hard disk

Required

● Create the new virtual machine with a blank virtual hard disk

4. Name the VM and select **Next**.

5. In **Configure Hardware**, ensure that the details match your template settings. Then select **Next**.

6. In **Configure Operating System** settings, ensure the details conform to the settings you made when you created the template. Then select **Next**.

7. Select the shielding data file (PDK) that you created.

8. Select the destination host group, and then select **Next**.

9. Select the host by the rating that the VMM placement engine gave. Then select **Next**.

10. In **Configure Settings**, review the virtual machine settings and select **Next**.

11. Review the actions in **Add properties** and select **Next**.

12. To create the Linux shielded VM, select **Create**.

While provisioning the VM, the VMM specialization agent reads the Linux configuration file PDK and customizes the VM.

Next steps

- Get an overview of Guarded fabric and shielded VMs.
- Find out more about Linux shielded VM tools ↗.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Deploy and manage a Software Defined Network (SDN) infrastructure in the VMM fabric

Article • 07/24/2024

System Center Virtual Machine Manager (VMM) can be used to deploy and manage a Software Defined Network (SDN) infrastructure.

Software Defined Network overview

SDN virtualizes your network to abstract physical hardware network elements, such as switches and routers. Using SDN, you can dynamically manage your datacenter networking to meet workload and app requirements. Network policies can be implemented consistently, at scale, even as you deploy new workloads or move workloads across virtual or physical networks.

If you deploy SDN in the VMM fabric, you can:

- Provision and manage virtual networks at scale.
- Deploy and manage the SDN infrastructure, including network controllers, software load balancers, and gateways.
- Define and control virtual network policies centrally and link them to your applications or workloads. When your workload is deployed or moved, the network configuration adjusts itself automatically. This is important because it removes the need for manual reconfiguration of network hardware, thereby reducing operational complexity while saving your valuable resources for higher-impact work.
- Control traffic flow between virtual networks, including the ability to define guaranteed bandwidth for your critical applications and workloads.

SDN combines many technologies, among them:

- **Network Controller**: The network controller allows you to automate the configuration of your network infrastructure instead of manually configuring network devices and services.

- **RAS Gateway for SDN**: RAS Gateway is a software-based, multitenant BGP capable router that is designed for CSPs and enterprises that host multiple tenant virtual networks using HNV.

- **Software Load Balancing (SLB) for SDN**: SDN can use Software Load Balancing (SLB) to evenly distribute tenant and tenant customer network traffic among virtual network resources. The Windows Server SLB enables multiple servers to host the same workload, providing high availability and scalability.

Read more about technologies in the SDN stack.

Next steps

- Deploy SDN components using PowerShell
- Alternatively, deploy SDN components manually in the VMM console:
  - Set up a network controller
  - Set up a software load balancer
  - Set up a RAS gateway

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up an SDN network controller in the VMM fabric

Article • 07/24/2024

This article describes how to set up a Software Defined Networking (SDN) network controller in the System Center Virtual Machine Manager (VMM) fabric.

The SDN network controller is a scalable and highly available server role that enables you to automate network infrastructure configuration instead of performing manual network device configuration. Learn more.

VMM 2022 provides dual stack support for SDN network controller.

For a great introduction, watch a video (~ five minutes) that provides an overview of network controller deployment.

> ⓘ **Note**
>
> - VMM 2022 supports dual stack (Ipv4 + Ipv6) for SDN components.
> - See System Requirements for the full list of supported server Operating System.

Prerequisites

• Plan for a Software Defined Network (SDN). Learn more.

• Plan for an SDN Network Controller Installation and deployment. Learn more.

Before you start

To set up SDN in the VMM fabric, you need the following:

- **A service template**: VMM uses a service template to automate network controller deployment. Service templates for the network controller support multi-node deployment on Generation 1 and Generation 2 VMs.
- **A virtual hard disk**: The service template needs a prepared virtual hard disk that's imported into the VMM library. This virtual hard disk is used for network controller VMs.

- The virtual hard disk must be running the applicable Windows Server version with the latest patches installed.
- It can be in VHD or VHDX format.

- **A management logical network**: That models your physical management network's connectivity for the VMM hosts, network controller hosts, and tenant VM hosts.
- **A logical switch**: To provide the management logical network with connectivity to the network controller VMs.
- **An SSL certificate**: To authenticate communications between the VMM server and the network controller.
- **An HNV provider logical network and tenant VM networks**: To validate the network controller deployment.
- **Other prerequisites**: Verify other requirements.

Deployment steps

Here's what you need to do to set up an SDN network controller:

1. **Configure hosts and physical network infrastructure**: You need access to your physical network devices to configure VLANs, routing, and others. You also need Hyper-V hosts to host the SDN infrastructure and tenant VMs. Learn more.

2. **Prepare a virtual hard disk**: You can prepare a virtual hard disk for the network controller service template in VHD or VHDX format, as appropriate, for the service template generation you choose.

3. **Download the service templates**: Download the network controller service templates and import them to the VMM library.

4. **Set up Active Directory security groups**: You'll need an Active Directory security group for network controller management, and another security group for network controller clients. Each group will need at least one user account in it.

5. **Set up a VMM library share**. You can have an optional library file share for keeping diagnostic logs. This library share will be accessed by the network controller to store diagnostics information throughout its lifetime.

6. **Set up a VMM host group**: Set up a dedicated host group for all the SDN Hyper-V hosts.

   ⓘ Note

Hosts must be running applicable Windows Server with latest patches installed and have the Hyper-V role enabled.

7. **Create the management logical network**: Create a logical network to mirror management network connectivity for the VMM host, network controller hosts, and tenant VM hosts. If you want to allocate static IP addresses from a pool, create a pool on this logical network.

8. **Create and deploy a management logical switch**: You create the logical switch and deploy it on network controller hosts to provide connectivity to the management network for network controller VMs.

9. **Set up a certificate**: You need an SSL certificate for secure/HTTPS communication with the network controller.

10. **Import the template**: Import and customize the network controller service template.

11. **Deploy the service**: Deploy the network controller service using the service template. Then add it as a VMM service.

Prepare a virtual hard disk

1. Prepare the VHD or VHDX based on the type of template you would like to use.
2. After you prepare the hard disk, install the latest applicable Windows Server updates, and any language packs you need if you've a non-English environment.
3. Import the VHD/VHDX files to the VMM library. Learn more.

Download the network controller service template

1. Download the SDN folder from the Microsoft SDN GitHub repository and copy the templates from **VMM** >**Templates** > **NC** to a local path on the VMM server.

2. Extract the contents to a folder on a local computer.

3. Refresh the library, you'll import the service templates, later.

ⓘ **Note**

The custom resource files are used when setting up the network controller and other SDN components (software load balancer, RAS gateway).

The NC folder contains four service templates and five custom resource folders. These are summarized in the following table:

Templates and resource files

⛶ Expand table

Name	Type	Details
Network Controller Production Generation 1 VM.xml	Template	Three-node network controller for Generation 1 VMs
Network Controller Production Generation 2 VM.xml	Template	Three-node network controller for Generation 2 VMs
Network Controller Standalone Generation 1 VM.xml	Template	Single-node network controller for Generation 1 VMs
Network Controller Standalone Generation 2 VM.xml	Template	Single-node network controller for Generation 2 VMs
NcSetup.cr	Custom resource file	A library resource containing scripts used to set up the network.
ServerCertificate.cr	Custom resource file	Library resource containing the private key for the network controller in .pfx format.
NcCertificate.cr	Custom resource file	Library resource containing the trusted root certificate (.CER) for the network controller. This is used for secure communications between the network controller and other subservices (For example, SLB MUXes).
TrustedRootCertificate.cr	Custom resource file	Library resource containing the CA public key (.cer) imported as the trusted root certificate to validate the SSL certificate.
EdgeDeployment.cr	Template	Used for installing SLB MUX roles and gateway roles (for example, VPN).

Set up Active Directory groups

Create security groups for network controller management and clients.

1. In **Active Directory Users and Computers**, create a security group for network controller management.

   - In the group, add all the users who have permissions to configure the network controller. For example, create a group named Network Controller Admins.
   - All the users that you add to this group must also be members of the Domain Users group in Active Directory.
   - The group for network controller management must be a domain local group. Members of this group will be able to create, delete, and update the deployed network controller configuration.
   - Create at least one user account that is a member of this group and have access to its credentials. After the network controller is deployed, VMM can be configured to use the user account credentials to establish communication with the network controller.

2. Create another security group for network controller clients.

   - Add users with permissions to configure and manage networks using network controller. For example, create a group named Network Controller Users.
   - All the users that you add to the new group must also be members of the Domain Users group in Active Directory.
   - All Network Controller configuration and management is performed using Representational State Transfer (DNS).
   - The group must be a Domain Local group. After the network controller is deployed, any members of this group will have permissions to communicate with the network controller via the REST-based interface.
   - Create at least one user account that is a member of this group. After the network controller is deployed, VMM can be configured to use the user account credentials to establish communication with the network controller.

Create a library share for logging

1. Optionally create a file share in the VMM library to keep diagnostic logs.
2. Ensure that the share can be accessed by the network controller. The network controller accesses the share to store diagnostic information. Note the credentials for the account that will have write access to the share.

Set up host groups

1. Create a dedicated host group for Hyper-V hosts that will be managed by SDN.
2. Ensure that Hyper-V hosts are running Windows Server 2016 with the latest patches installed.

Create the management logical network

You can create a management logical network in VMM to mirror your physical management network.

- The logical network provides network connectivity settings for the VMM host, network controller hosts, and tenant VM hosts.
- We recommend that you create this logical network specifically to provide connectivity for infrastructure VMs that are managed by the network controller.
- If you already have a VMM logical network that's configured with **Create a VM Network with the same name to allow virtual machines to access this logical network directly**, then you can reuse this logical network to provide management connectivity to network controller.

Use the following procedure to create management logical network:

1. Select **Fabric** > **Networking**. Right-click **Logical Networks** > **Create Logical Network**.
2. Specify a **Name** and optional **Description**.
3. In **Settings**, select **One Connected Network**. All management networks need to have routing and connectivity between all hosts in that network. Select **Create a VM network with the same name to allow virtual machines to access this logical network directly** to automatically create a VM network for your management network.
4. Select **Network Site** > **Add**. Select the host group for the hosts that will be managed by the network controller. Insert your management network IP subnet details. This network must already exist and be configured in your physical switch.
5. Review the **Summary** information and select **Finish** to complete.

Create an IP address pool

ⓘ Note

You can create IP address pool using **Create Logical Network** wizard.

If you want to allocate static IP addresses to network controller VMs, create an IP address pool in the management logical network. If you're using DHCP, you can skip this step.

1. In the VMM console, right-click the management logical network and select **Create IP Pool**.
2. Provide a **Name** and optional description for the pool, and ensure that the management network is selected for the logical network.
3. In **Network Site** panel, select the subnet that this IP address pool will service.
4. In **IP Address range** panel, enter the starting and ending IP addresses.
5. To use an IP as REST IP, enter one of the IP addresses from the specified range in the **IP addresses to be reserved for other uses** box. In case you want to use the REST End Point, skip this step.
   - Don't use the first three IP addresses of your available subnet. For example, if your available subnet is from .1 to .254, start your range at .4 or greater.
   - If the nodes are in the same subnet, you must provide REST IP address. If the nodes are in different subnets, you must provide a REST DNS name.
6. Specify the default gateway address and optionally configure DNS and WINS settings.
7. In the **Summary** page, review the settings and select **Finish** to complete the wizard.

Create and deploy a management logical switch

You need to deploy a logical switch on the management logical network. The switch provides connectivity between the management logical network and the network controller VMs.

1. In the VMM console, select **Fabric** > **Networking** > **Create Logical Switch**. Review the Getting Started information and select **Next**.
2. Provide a **Name** and optional description. Select **No Uplink Team**. If you need teaming, select **Embedded Team**.

> ⓘ Note
>
> Don't use **Team**.

3. For minimum bandwidth mode, choose the **Weight** option.

4. In **Extensions**, clear all the switch extensions. This is important. If you select any of the switch extensions at this stage, it could block the network controller onboarding later.

5. You can optionally add a virtual port profile and choose a port classification for host management.

6. Select an existing uplink port profile, or select **Add** > **New Uplink Port Profile**. Provide a **Name** and optional description. Use the defaults for load balancing algorithm and teaming mode. Select all the network sites in the management logical network.

7. Select **New Network Adapter**. This adds a host virtual network adapter (vNIC) to your logical switch and uplink port profile, so that when you add the logical switch to your hosts, the vNICs get added automatically.

8. Provide a **Name** for the vNIC. Verify that the management VM network is listed in **Connectivity**.

9. Select **This network adapter will be used for host management** > **Inherit connection settings from the host adapter**. This allows you to take the vNIC adapter settings from the adapter that already exists on the host. If you created a port classification and virtual port profile earlier, you can select it now.

10. In **Summary**, review the information and select **Finish** to complete the wizard.

Deploy the logical switch

You must deploy the management logical switch on all the hosts where you intend to deploy the NC. These hosts must be a part of VMM host group that you created earlier. Learn more.

Set up the security certificates

You need an SSL certificate that will be used for secure/HTTPS communication with the network controller. You can use the following methods:

- **Self-signed certificate**: You can generate a self-signed certificate, and export it with the private key protected with a password.
- **Certificate Authority (CA) certificate**: You can use a certificate signed by a CA.

Use a self-signed certificate

The following example creates a new self-signed certificate and must be run on the VMM server.

> Note
>
> - You can use an IP address as the DNS name, but this isn't recommended as it restricts the network controller to a single subnet.
> - You can use any friendly name for the network controller.
> - For multi-node deployment, The DNS name must be the REST name you want to use.
> - For single-node deployment, the DNS name must be the network controller name followed by the full domain name.

Expand table

Deployment	Syntax	Example
Multi-node	`New-SelfSignedCertificate -KeyUsageProperty All -Provider "Microsoft Strong Cryptographic Provider" -FriendlyName "<YourNCComputerName>" -DnsName @("<NCRESTName>")`	`New-SelfSignedCertificate -KeyUsageProperty All -Provider "Microsoft Strong Cryptographic Provider" -FriendlyName "MultiNodeNC" -DnsName @("NCCluster.Contoso.com")`
Single-node	`New-SelfSignedCertificate -KeyUsageProperty All -Provider "Microsoft Strong Cryptographic Provider" -FriendlyName "<YourNCComputerName>" -DnsName @("<NCFQDN>")`	`New-SelfSignedCertificate -KeyUsageProperty All -Provider "Microsoft Strong Cryptographic Provider" -FriendlyName "SingleNodeNC" -DnsName @("SingleNodeNC.Contoso.com")`

Export the self-signed certificate

Export the certificate and its private key in .pfx format.

1. Open the **Certificates** snap-in (certlm.msc) and locate the certificate in Personal/Certificates.

2. Select the certificate > **All Tasks** > **Export**.

3. Select **Yes, export the private key** option, and select **Next**.

4. Choose **Personal Information Exchange - PKCS #12 (.PFX)** and accept the default to **Include all certificates in the certification path if possible**.

5. Assign the **Users/Groups** and a password for the certificate you're exporting; select **Next**.

6. On the **File to export** page, browse the location where you want to place the exported file, and give it a name.

7. Similarly, export the certificate in .CER format

   > ⓘ **Note**
   >
   > To export to .CER format, uncheck the **Yes, export the private key** option.

8. Copy the .PFX to the ServerCertificate.cr folder.

9. Copy the .CER file to the NCCertificate.cr folder.

When you're done, refresh these folders, and ensure that you've these certificates copied.

Use a CA

1. Request a CA-signed certificate. For a Windows-based enterprise CA, request certificates using the certificate request Wizard.

2. Ensure that the certificate includes the serverAuth EKU, specified by the OID 1.3.6.1.5.5.7.3.1. In addition, the certificate subject name must match the DNS name of the network controller.

3. Copy the .PFX to the ServerCertificate.cr folder.

4. Copy the .CER file to the NCCertificate.cr folder.

5. Copy the public key of the CA in .CER format to TrustedRootCertificate.cr.

> ⓘ **Note**
>
> Ensure that the enterprise CA is configured for certificate auto enrollment.

Enhanced key usage

1. If the Personal (My – cert:\localmachine\my) certificate store on the Hyper-V host has more than one X.509 certificate with Subject Name (CN) as the host Fully Qualified Domain Name (FQDN), ensure that the certificate that is used by SDN has an additional custom Enhanced Key Usage property with the OID 1.3.6.1.4.1.311.95.1.1.1. Otherwise, the communication between Network Controller and the host might not work.

2. Ensure that certificate issued by CA for south bound communication has an additional custom Enhanced Key Usage property with the OID 1.3.6.1.4.1.311.95.1.1.1.

Set up the service template

Import the template and update the parameters for your environment.

Import the template

Import the service template into the VMM library. For this example, we'll import the Generation 2 template.

1. Select **Library** > **Import Template**.

2. Browse to your service template folder, select the **Network Controller Production Generation 2 VM.xml** file.

3. Update the parameters for your environment as you import the service template. Review the details and then select **Import**.

   - **WinServer.vhdx** Select the base virtual hard drive image that you prepared earlier.
   - **NCSetup.cr**: Map to the NCSetup.cr library resource in the VMM library.
   - **ServerCertificate.cr**: Map to the ServerCertificate.cr resource in the VMM library. In addition, put the .pfx SSL certificate that you prepared earlier inside this folder. Ensure that you only have one certificate in the ServerCertificate.cr folder.

- **TrustedRootCertificate.cr**: Map to the TrustedRootCertificate.cr folder in your VMM library. If you don't need a trusted root certificate, this resource still needs to be mapped to a CR folder. However, the folder must be left empty.

4. Once done, ensure that the Job is complete.

Customize the template

You can customize the service template to meet any specific requirements related to your organization, such as product key, IP assignment, DHCP, MAC Spoofing, and High availability. You can also customize properties for objects such as host groups, host clusters, and service instances.

As an example, here are the steps to enter the product key, enable DHCP and high availability:

1. In the VMM library, select the service template, and open it in designer mode.

2. Double-click the computer tier to open the Windows Server Network Controller Properties page.

3. To specify a product key, select **OS Configuration** > **Product Key**, and specify the key shared by CCEP.

4. To enable high availability, select **Hardware configuration** > **Availability**, select the **Make the Virtual machine highly available** checkbox.

5. To enable dynamic IP configuration and use DHCP for network controller management, select network adapter on the designer, and change the IPV4 address type to **Dynamic**.

   > ⓘ **Note**
   >
   > - If you customize the template for high availability, ensure that you deploy this on clustered nodes.
   > - While configuring your Network Controller and specifying FQDN as the REST name, don’t pre-create Host A record for your primary NC node in your DNS. This may impact Network Controller connectivity once primary NC node changes. This is applicable even if you're deploying the NC by using the SDN Express or VMM Express script.

Deploy the network controller

1. Select the network controller service template > **Configure Deployment**. Enter a service name, and select a destination for the service instance. The destination must map to the dedicated host group containing hosts that will be managed by the network controller.

2. Configure the deployment settings as described in the table below.

3. It's normal for the virtual machine instances to be initially red. Select **Refresh Preview** to have the deployment service automatically find suitable hosts for the virtual machines to be created.

4. After you configure these settings, select **Deploy Service** to begin the service deployment job.

   > ⓘ **Note**
   >
   > Deployment times will vary depending on your hardware but are typically between 30 and 60 minutes. If you're not using a volume licensed VHD\VHDX, or if the VHD\VHDX doesn't supply the product key using an answer file, then the deployment stops at the **Product Key** page during network controller VM provisioning. You need to manually access the VM desktop and either skip or enter the product key.

5. If the network controller deployment fails, delete the failed service instance before you retry the network controller deployment. Select **VMs and Services** > **All Hosts** > **Services**, and delete the instance.

Deployment settings

Expand table

Setting	Requirement	Description
ClientSecurityGroup	Required	Name of the security group that you created, containing network controller client accounts.
DiagnosticLogShare	Optional	File share location where the diagnostic logs will be periodically uploaded. If this isn't provided, the logs are stored locally on each node.

Setting	Requirement	Description
DiagnosticLogShareUsername	Optional	Full username (including domain name) for an account that has access permissions to the diagnostic log share. In the format: [domain]\[username].
DiagnosticLogSharePassword	Optional	The password for the account specified in the DiagnosticLogShareUsername parameter.
LocalAdmin	Required	Select a Run As account in your environment, which will be used as the local administrator on the network controller virtual machines. **Note**: While creating Run As accounts, uncheck the **validate domain credentials option** if you're creating a local account. Username must be .\Administrator (create it if it doesn't exist).
Management	Required	Select the management logical network you created earlier.
MgmtDomainAccount	Required	Select a Run As account in your environment, which will be used to prepare the network controller. This user must be a member of the management security group, specified below, which has privileges to manage the network controller.
MgmtDomainAccountName	Required	This must be the full username (including domain name) of the Run As account mapped to MgmtDomainAccount. The domain username will be added to the Administrators group during deployment.
MgmtDomainAccountPassword	Required	Password for the management Run As account mapped to MgmtDomainAccount.
MgmtDomainFQDN	Required	FQDN for the Active directory domain that the network controller virtual machines will join.
MgmtSecurityGroup	Required	Name of the security group you created previously containing network controller management accounts.
RestEndPoint	Required	Enter the RESTName you used when preparing the certificates. This parameter isn't used for standalone templates.

Setting	Requirement	Description
		If the nodes are in the same subnet, you must provide the REST IP address. If the nodes are in different subnets, provide the REST DNS name.
ServerCertificatePassword	Required	Password to import the certificate into the machine store.

> ⓘ **Note**
>
> Windows Server 2019 onwards, the Network Controller machines must be provided permission to register and modify the SPN in the Active Directory. For more information, see Kerberos with Service Principal Name.

Add the network controller service to VMM

After the network controller service is successfully deployed, the next step is to add it to VMM as a network service.

1. In **Fabric**, right-click **Networking** > **Network Service**, and select **Add Network Service.**
2. The **Add Network Service Wizard** starts. Specify a name and optional description.
3. Select **Microsoft** for the manufacturer and for model select **Microsoft network controller**.
4. In **Credentials**, provide the Run As account you want to use to configure the network service. This must be the same account that you included in the network controller clients group.
5. For the **Connection String**:
   - In multi-node deployment, **ServerURL** must use the REST endpoint, and **servicename** must be the name of the network controller instance.
   - In single node deployment, **ServerURL** must be the network controller FQDN and, **servicename** must be the network controller service instance name. Example: `serverurl=https://NCCluster.contoso.com;servicename=NC_VMM_RTM`
6. In **Review Certificates**, a connection is made to the network controller virtual machine to retrieve the certificate. Verify that the certificate shown is the one you

expect. Ensure that you select **These certificates have been reviewed and can be imported to the trusted certificate store box**.

7. On the next screen, select **Scan Provider** to connect to your service and list the properties and their status. This is also a good test of whether the service was created correctly, and that you're using the right connect string to connect to it. Examine the results, and check that isNetworkController = true. When it completes successfully, select **Next**.

8. Configure the host group that your network controller will manage.

9. Select **Finish** to complete the wizard. When the service has been added to VMM, it will appear in the **Network Services** list in the VMM console. If the network service isn't added, check **Jobs** in the VMM console to troubleshoot.

Validate the deployment

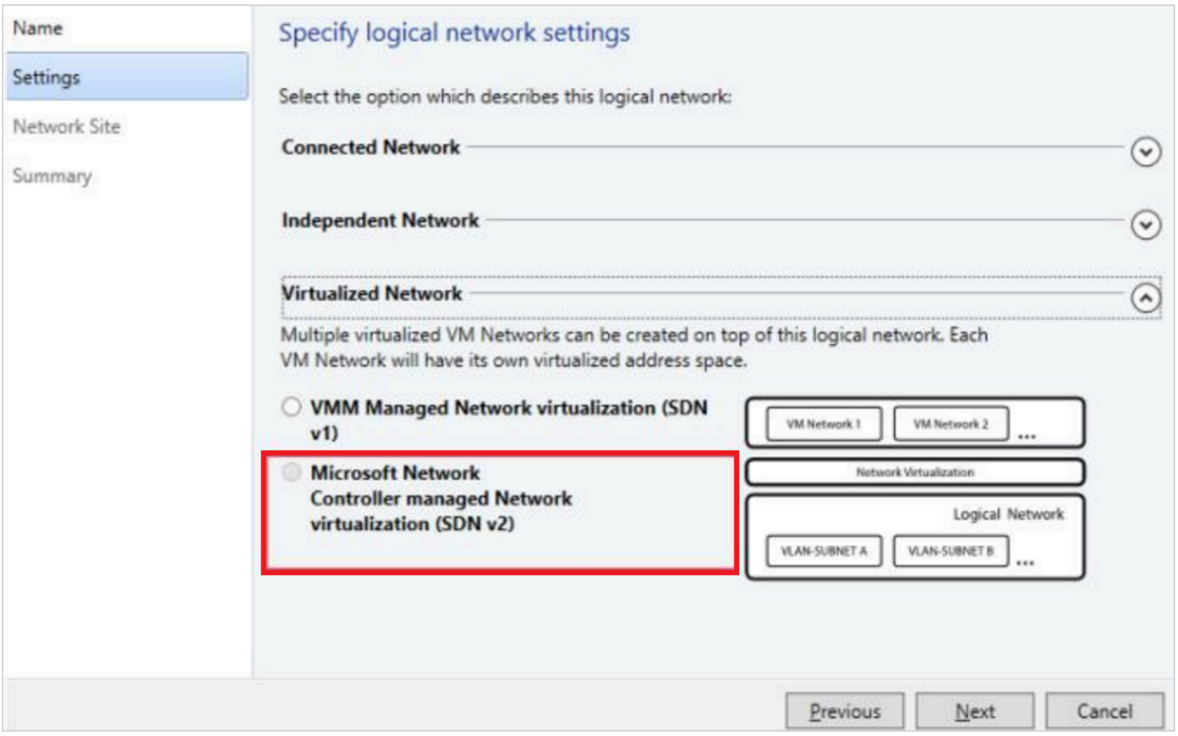
You can optionally validate the network controller deployment. To do this:

1. Create **HNV provider** network (the backend network), managed by the network controller for tenant VM connectivity. This network is used to validate that the network controller has been deployed successfully and that tenant VMs within the same virtual network can ping each other. This network must exist in your physical network infrastructure, and all SDN fabric hosts must have physical connectivity to it.
2. After creating the HNV provide network, you configure two tenant VM networks on top of it. Create VM networks and IP address pools, and then deploy the tenant VMs. You can also test connectivity between two tenant VMs deployed on different hosts to ensure the network controller is deployed correctly.

Create the HNV provider network

1. Start the **Create Logical Network Wizard**. Enter a name and optional description for this network.

2. In **Settings**, verify that **Connected Network** is selected, since all HNV Provider networks need to have routing and connectivity between all hosts in that network. Ensure that you check **Allow new VM networks created on this logical network to use network virtualization**. In addition, check **Managed by the network controller**.



Specify logical network settings

Select the option which describes this logical network:

Connected Network

Independent Network

Virtualized Network

Multiple virtualized VM Networks can be created on top of this logical network. Each VM Network will have its own virtualized address space.

○ VMM Managed Network virtualization (SDN v1)

○ Microsoft Network Controller managed Network virtualization (SDN v2)

3. In **Network Site**, add the network site information for your HNV provider network. This must include the host group, subnet, and VLAN information for the network.
4. Review the **Summary** information and complete the wizard.

Create the IP address pool

> ⓘ Note
>
> You can create IP address pool using **Create Logical Network** wizard.

The configure HNV logical network needs an IP address pool, even if DHCP is available on this network. If you've more than one subnet on the configure HNV network, create a pool for each subnet.

1. Right-click the configure HNV logical network > **Create IP Pool**.
2. Provide a name and optional description, and ensure that the HNV Provider logical network is selected for the logical network.

3. In **Network Site**, you need to select the subnet that this IP address pool will service. If you've more than one subnet as part of your HNV provider network, you need to create a static IP address pool for each subnet. If you've only one site (for example, like the sample topology), then you can just select **Next**.

> ⓘ Note
>
> - To enable IPv6 support, add an IPv6 subnet and create an IPv6 address pool.

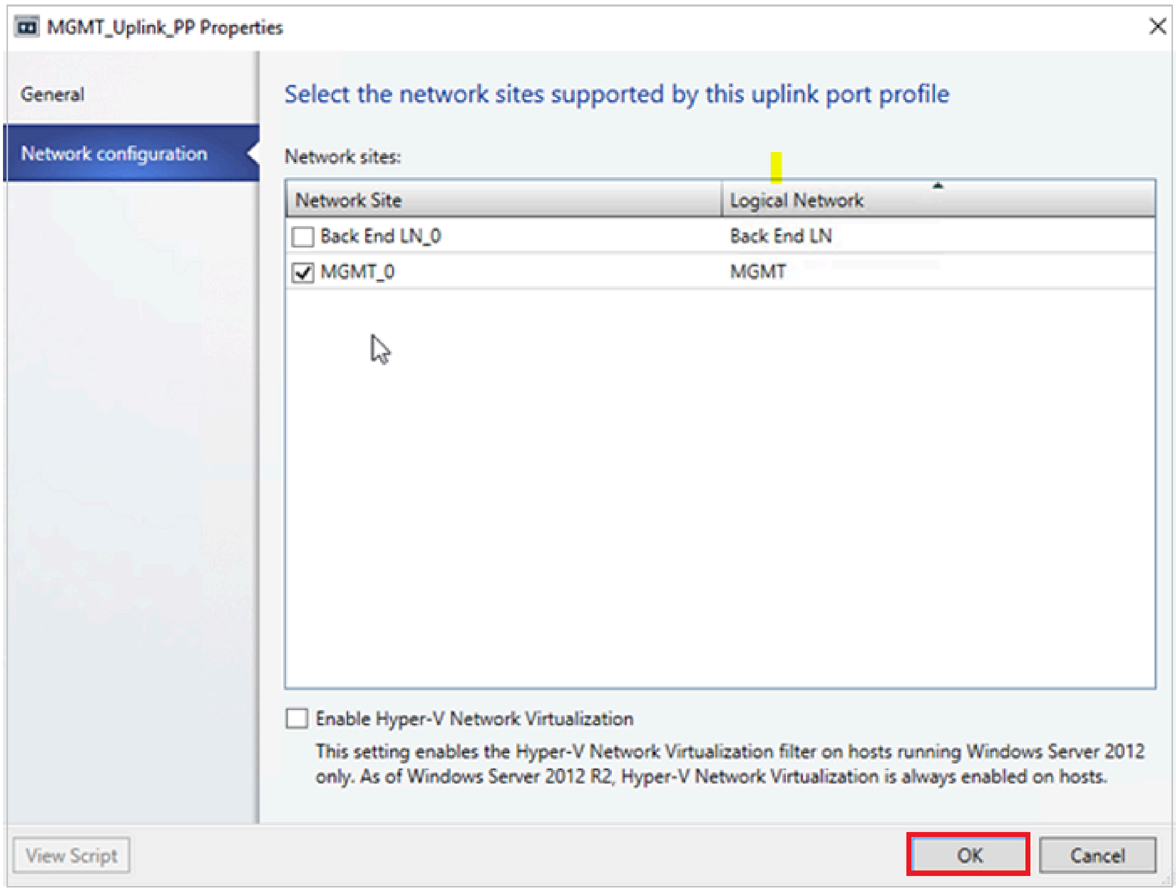
- To enable IPv4 support, add an IPv4 subnet and create an IPv4 address pool.
- To use IPv6 address space, add both IPv4 and IPv6 subnets to the network site.
- To enable dual stack support, create IP pools with both IPv4 and IPv6 address space.

4. In **IP Address range**, configure the starting and ending IP address. Don't use the first IP address of your available subnet. For example, if your available subnet is from .1 to .254, start your range at .2 or greater.

5. Next, configure the default gateway address. Select **Insert** next to the **Default gateways** box, enter the address, and use the default metric. Optionally configure DNS and WINS.

6. Review the summary information and select **Finish** to complete the wizard.

7. As part of network controller onboarding, the switch that you deployed on the hosts for the Management logical network connectivity was converted to an SDN switch. This switch can now be used to deploy a network controller managed network, including the HNV provider logical network. Ensure that you select the network site corresponding to the HNV provider logical network in the uplink port profile settings for the Management logical switch.



MGMT_Uplink_PP Properties

Select the network sites supported by this uplink port profile

Network sites:

Network Site	Logical Network
□ Back End LN_0	Back End LN
☑ MGMT_0	MGMT

□ Enable Hyper-V Network Virtualization

This setting enables the Hyper-V Network Virtualization filter on hosts running Windows Server 2012 only. As of Windows Server 2012 R2, Hyper-V Network Virtualization is always enabled on hosts.

The HNV provider logical network is now accessible to all the hosts in the network controller managed host group.

Create tenant VM networks and IP pools

Now, create two VM networks and IP pools for two tenants in your SDN infrastructure to test connectivity.

ⓘ Note

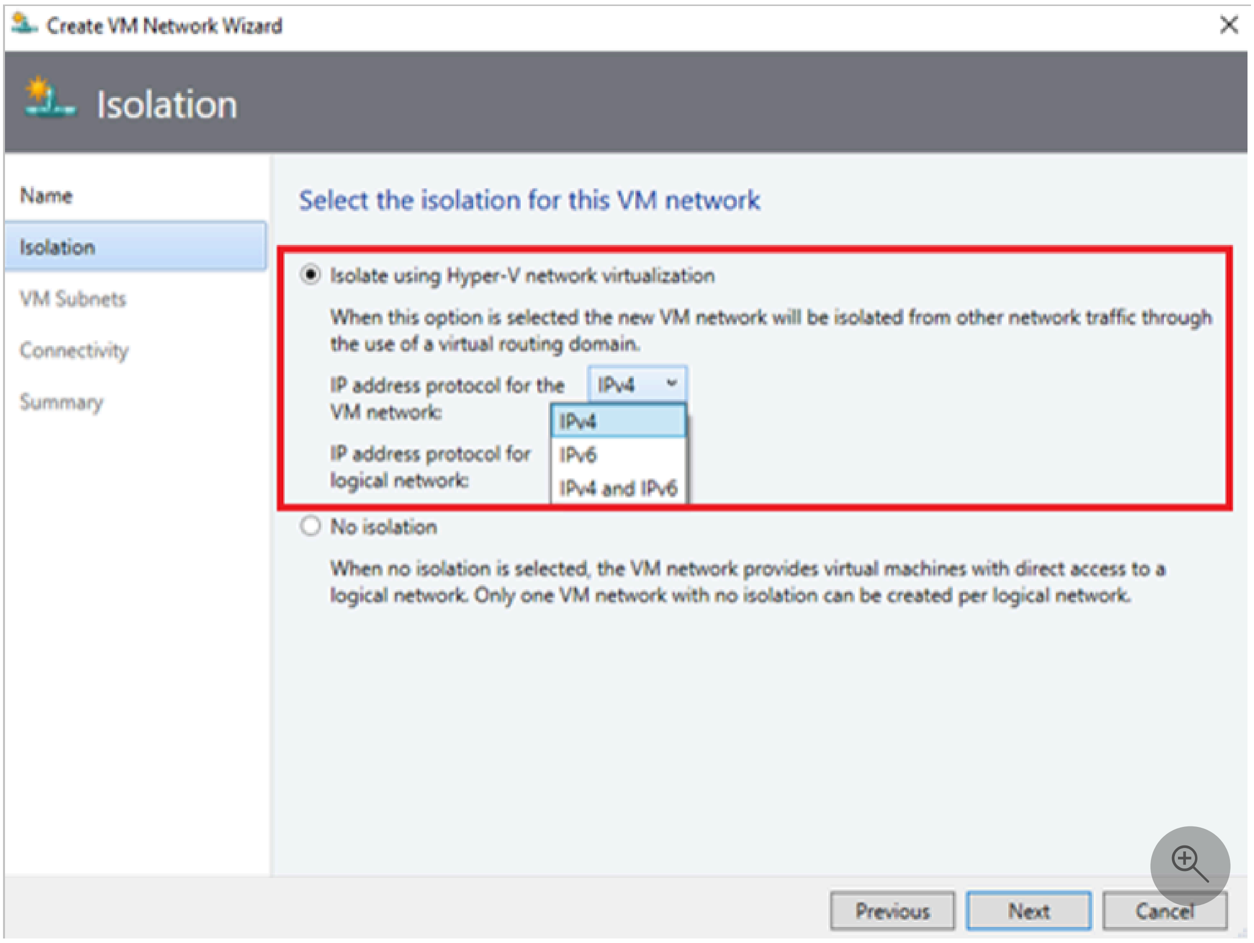
- Do not use the first IP address of your available subnet. For example, if your available subnet is from .1 to .254, start your range at .2 or greater.
- Currently you can’t create a VM network with **No Isolation** for logical networks that are managed by the network controller. You must choose the **Isolate using Hyper-V Network Virtualization** isolation option when creating VM Networks associated with HNV Provider logical networks.

1. Create a VM network for each tenant.

2. Create an IP address pool for each VM network.

ⓘ Note

When you create a VM network, to enable IPv6 support, select IPv6 from the **IP address protocol for the VM network** dropdown menu. When you create a VM network, to enable dual stack support, select IPv4 and IPv6 from the **IP address protocol for the VM network** dropdown menu (applicable to 2022 and later).



Select the isolation for this VM network

● Isolate using Hyper-V network virtualization

When this option is selected the new VM network will be isolated from other network traffic through the use of a virtual routing domain.

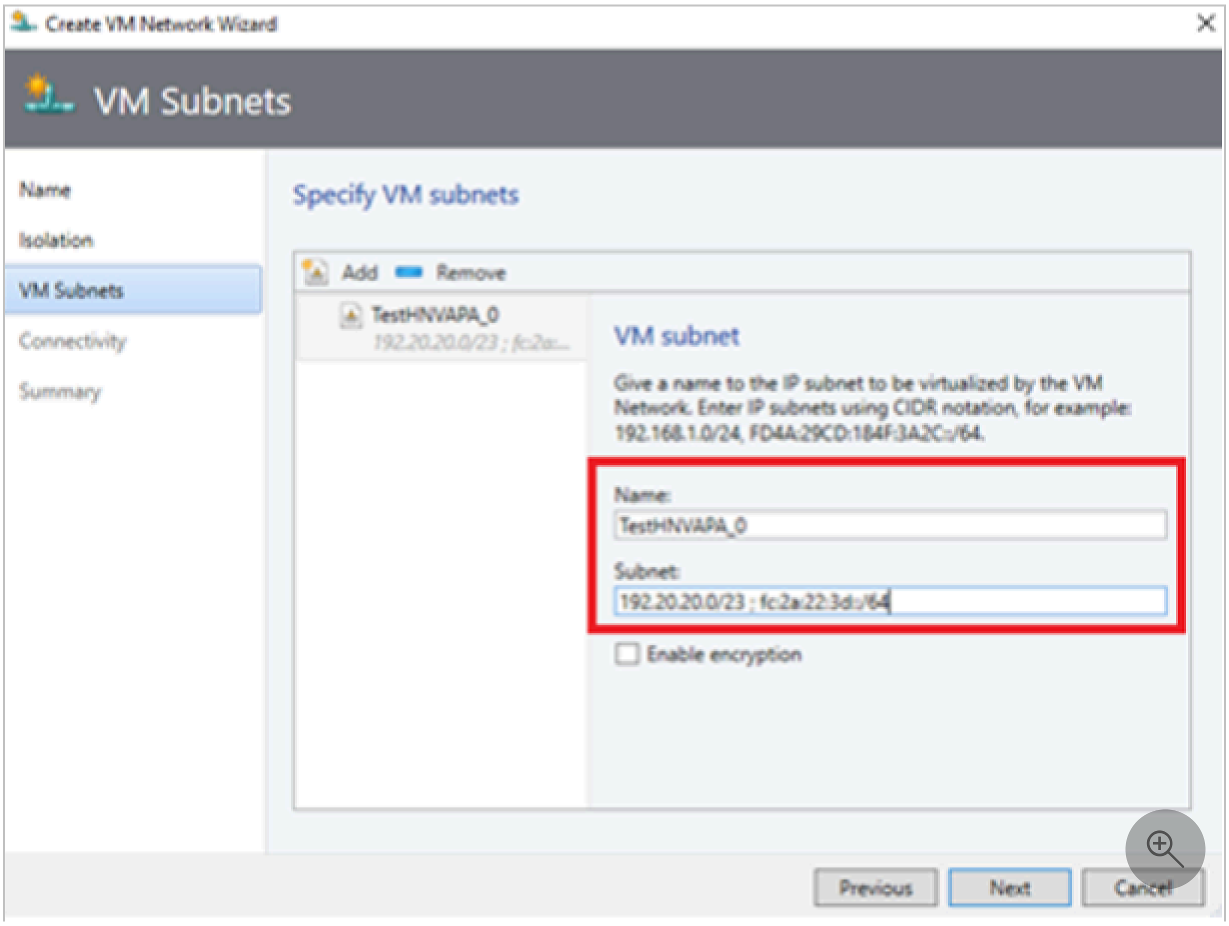
IP address protocol for the VM network: IPv4

IP address protocol for logical network:

○ No isolation

When no isolation is selected, the VM network provides virtual machines with direct access to a logical network. Only one VM network with no isolation can be created per logical network.

When you create VM Subnets, to enable dual stack support, provide both IPv4 subnet and IPv6 subnet, separated by a semicolon (;). (applicable to 2022 and later)



Specify VM subnets

VM subnet

Give a name to the IP subnet to be virtualized by the VM Network. Enter IP subnets using CIDR notation, for example: 192.168.1.0/24, FD4A:29CD:184F:3A2C::/64.

Name: TestHNVAPA_0

Subnet: 192.20.20.0/23 ; fc2a:22:3d::/64

□ Enable encryption

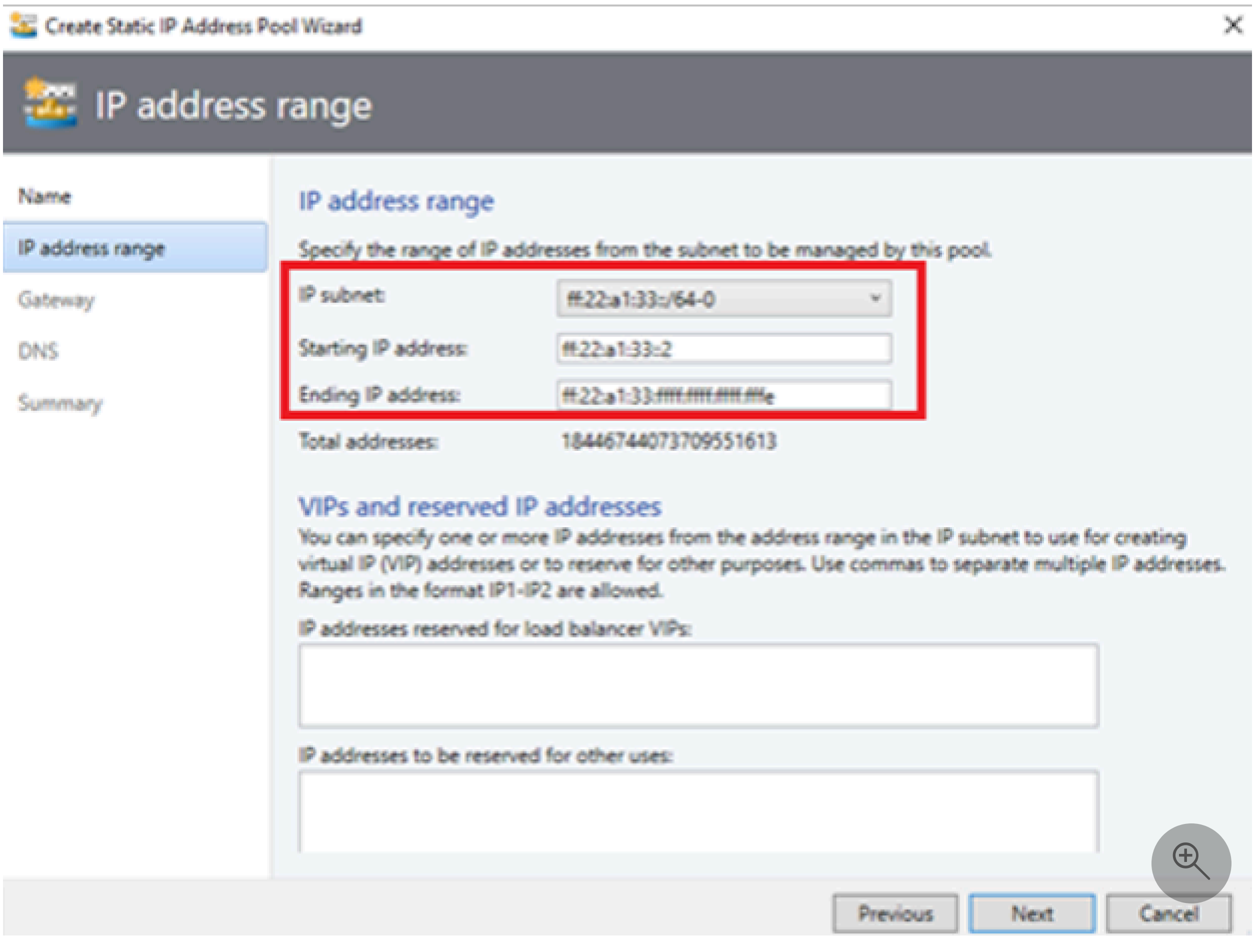
Create tenant virtual machines

Now, you can create tenant virtual machines connected to the tenant virtual network.

- Ensure that your tenant virtual machines allow IPv4/IPv6 ICMP through their firewall. By default, Windows Server blocks this.
  - To allow IPv4 ICMP through the firewall, run the command **New-NetFirewallRule –DisplayName “Allow ICMPv4-In” –Protocol ICMPv4**.
  - To allow IPv6 ICMP through the firewall, run the command **New-NetFirewallRule –DisplayName “Allow ICMPv6-In” –Protocol ICMPv6**

1. If you want to create a VM from an existing hard disk, follow these instructions.
2. After you deploy at least two VMs connected to the network, you can ping one tenant virtual machine from the other tenant virtual machine to validate that the network controller has been deployed as a network service successfully, and that it can manage the HNV Provider network so that tenant virtual machines can ping each other.

> ⓘ **Note**
>
> To enable dual stack support, for the VM networks, create two IP pools by selecting the two IP subnets from the dropdown menu.



IP address range

Specify the range of IP addresses from the subnet to be managed by this pool.

IP subnet: ff:22:a1:33::/64-0

Starting IP address: ff:22:a1:33::2

Ending IP address: ff:22:a1:33:ffff:ffff:ffff:fffe

Total addresses: 18446744073709551613

VIPs and reserved IP addresses

You can specify one or more IP addresses from the address range in the IP subnet to use for creating virtual IP (VIP) addresses or to reserve for other purposes. Use commas to separate multiple IP addresses. Ranges in the format IP1-IP2 are allowed.

IP addresses reserved for load balancer VIPs:

IP addresses to be reserved for other uses:

Create a new VM and deploy the dual stack VM network to assign both IPv4 and IPv6 address to the virtual machine.

Remove the network controller from the SDN fabric

Use these steps to remove the network controller from the SDN fabric.

Next steps

Create a software load balancer

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Set up an SDN software load balancer in the VMM fabric

Article • 07/24/2024

This article provides information on how to deploy a software load balancer (SLB) in a Software Defined Network (SDN).

The SLB enables even distribution of tenant and tenant customer network traffic among virtual network resources so that multiple servers can host the same workload to provide high availability and scalability. Learn more.

You can use VMM to deploy a network controller and a software load balancer. After you set up the SLB, you can use the multiplexing and NAT capabilities in your SDN infrastructure.

VMM 2022 provides dual stack support for SLB.

Before you start

Ensure the following:

- **Planning**: Read about planning a software defined network, and review the planning topology in this document. The diagram shows a sample 4-node setup. The setup is highly available with Three network controller nodes (VM) and Three SLB/MUX nodes. It shows Two tenants with One virtual network broken into Two virtual subnets to simulate a web tier and a database tier. Both the infrastructure and tenant virtual machines can be redistributed across any physical host.
- **Network controller**: You must have an SDN network controller deployed in the VMM fabric so that you've the compute and network infrastructure running before you set up the load balancing.
- **SSL certificate**: To import the SLB service template, you'll need to prepare an SSL certificate. You made the certificate available during network controller deployment. To use the certificate you prepared in network controller deployment for SLB, right-click the certificate and export it without a password in .CER format. Place it in the library in the NCCertificate.cr folder you created when you set up the network controller.
- **Service template**: VMM uses a service template to automate SLB deployment. Service templates support multi-node deployment on Generation 1 and Generation 2 VMs.

- **SLB VMs**: All the SLB virtual machines must be running Windows Server 2016 or later with the latest patches installed.
- **HNV Network**: Ensure that you created the Provider HNV network as part of NC validation. Learn more.

Deployment steps

1. **Prepare the SSL certificate**: Put the certificate in the VMM library.
2. **Download the service template**: Download the service template that you need to deploy the SLB/MUX.
3. **Create the transit logical networks**: You need to create logical networks:

    - A logical network to mirror the transit (Frontend) physical network.
    - Private virtual IP (VIP) and public VIP networks to assign VIPs to the SLB service.

4. **Create private and public VIP logical networks**: Private virtual IP (VIP) and public VIP networks to assign VIPs to the SLB service.
5. **Import the service template**: Import and customize the SLB service template.
6. **Deploy SLB**: Deploy SLB as a VMM service and configure the service properties.
7. **Validate the deployment**: Configure BGP peering between the SLB/MUX instance and a BGP router, assign a public IP address to a tenant VM or service, and access the VM or service from outside the network.

Prepare the certificate

Ensure that the SSL certificate that you created during the NC deployment is copied to NCCertificate.cr folder.

Download the service template

1. Download the SDN folder from the Microsoft SDN GitHub repository, and copy the templates from **VMM** >**Templates** > **SLB** to a local path on the VMM server.
2. Extract the contents to a folder on a local computer. You'll import them to the library later.

The download contains two templates:

- The SLB Production Generation 1 VM.xml template is for deploying the SLB Service on Generation 1 virtual machines.

- The SLB Production Generation 2 VM.xml template is for deploying the SLB Service on Generation 2 virtual machines.

Both the templates have a default count of three virtual machines, which can be changed in the service template designer.

We recommend you use simplified SDN topology (two physical network) for SLB deployments. Skip creating transit logical network when simplified SDN topology template is used.

Create the transit logical network

1. Open the **Create logical network Wizard**, and enter a **Name** and optional description.

2. In **Settings**, select **Connected Network**, and then select **Managed by the network controller**.

3. In **Network Site**, add the network site information for your subnet.
4. Review the **Summary** information and complete the logical network wizard.

Create an IP address pool for the transit logical network

This is the IP address pool where DIPs are assigned to the SLB/MUX virtual machines and BGP Peer virtual machine (if deployed).

You can create IP address pool using the **Create Logical Network** wizard.

> ⓘ **Note**
>
> - Ensure that you use the IP address range that corresponds to your transit network IP address space. Don't include the first IP address of your subnet in the IP pool you're about to create. For example, if your available subnet is from .1 to .254, start your range at .2.
> - After you create the Transit logical network, ensure that you associate this logical network with the Management switch uplink port profile you created during the network controller deployment.

Create the IP address pool:

1. Right-click the logical network > **Create IP Pool**.

2. Provide a **Name** and optional description for the IP Pool and ensure that the correct logical network is selected.

3. In **Network Site**, select the subnet that this IP address pool will service. If you've more than one subnet as part of your HNV provider network, you need to create a static IP address pool for each subnet. If you've only one site (for example, like the sample topology), then you can just select **Next**.

4. In **IP Address range**, configure the starting and ending IP address. Don't use the first three IP addresses of your available subnet. For example, if your available subnet is from .1 to .254, start your range at .4 or greater.

5. Next, configure the default gateway address. Select **Insert** next to the **Default gateways** box, enter the address, and use the default metric. Optionally configure DNS and WINS.

6. Review the summary information, and select **Finish** to complete the wizard.

   > ⓘ **Note**
   >
   > Ensure that you associate the logical network with the management switch uplink port profile.

Create private and public VIP logical networks

You need a private VIP address pool to assign a VIP, and a public VIP, to the SLB Manager service.

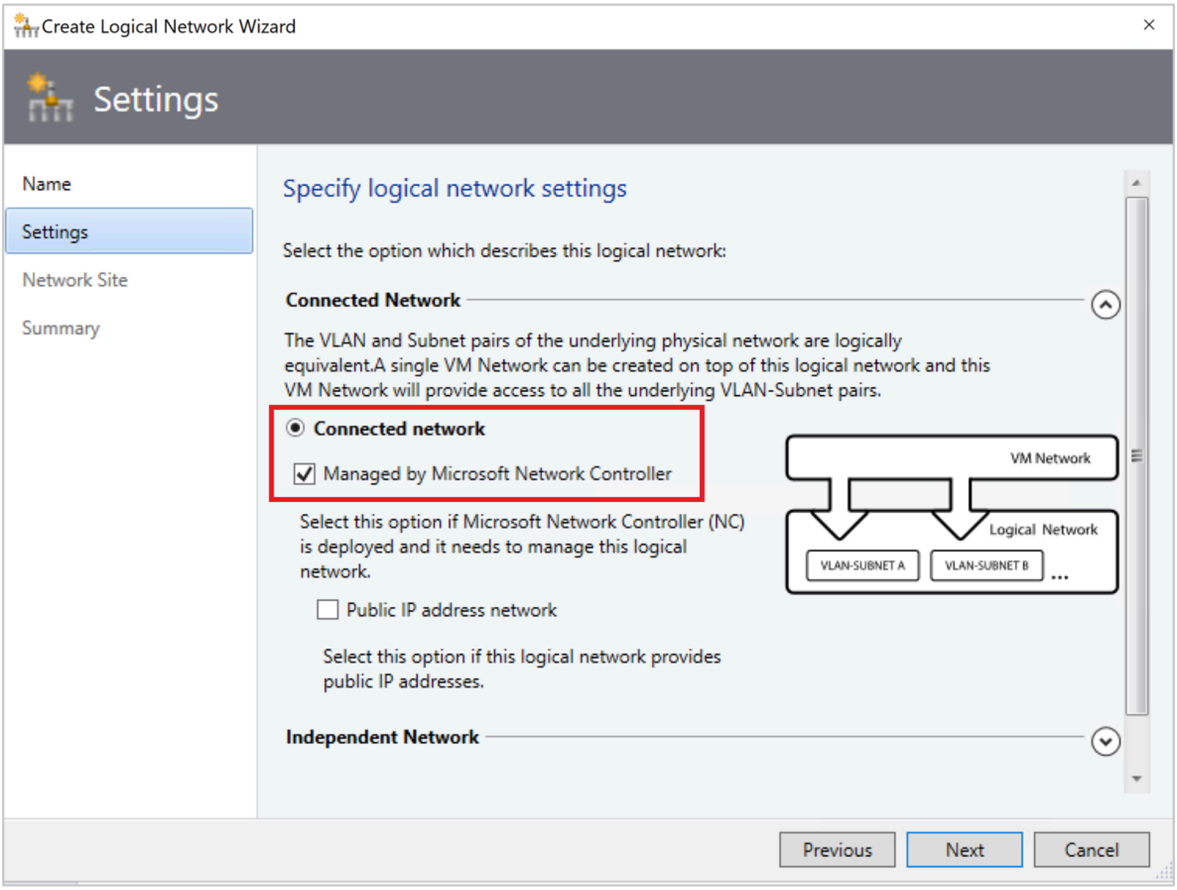
> ⓘ **Note**
>
> The procedure for creating both is similar, but there are some differences.

Create a private VIP:

1. Start the **Create logical network Wizard**. Enter a **Name** and optional description for this network.

2. In **Settings**, select **One Connected Network**. Select **Create a VM network with the same name to allow virtual machines to access this logical network directly**. Select **Managed by the network controller**. For UR1 and later, in **Settings**, select

connected Network and select **Managed by the network controller**.



Specify logical network settings

Select the option which describes this logical network:

Connected Network

The VLAN and Subnet pairs of the underlying physical network are logically equivalent.A single VM Network can be created on top of this logical network and this VM Network will provide access to all the underlying VLAN-Subnet pairs.

● **Connected network**

☑ Managed by Microsoft Network Controller

Select this option if Microsoft Network Controller (NC) is deployed and it needs to manage this logical network.

□ Public IP address network

Select this option if this logical network provides public IP addresses.

Independent Network

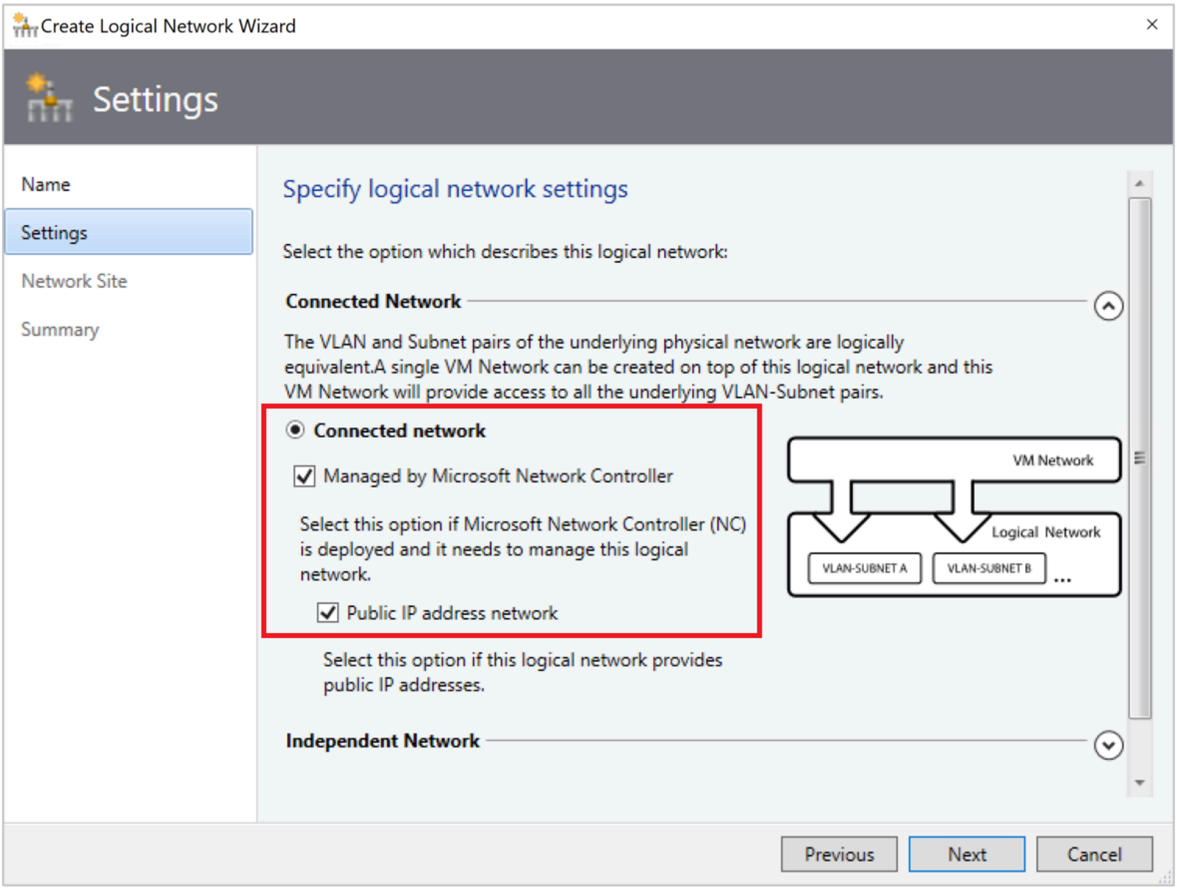
3. In **Network Site**, add the network site information for your private VIP logical network.
4. Review the **Summary** information, and complete the wizard.

Create a public VIP:

1. Start the **Create logical network Wizard**. Enter a **Name** and optional description for this network.

2. In **Settings**, select **One Connected Network**. Select **Create a VM network with the same name to allow virtual machines to access this logical network directly**. Select **Managed by the network controller**.

   For UR1 and later, in **Settings**, select **connected Network** and select both **Managed by the network controller** and **Public IP address network**.



Specify logical network settings

Select the option which describes this logical network:

Connected Network

The VLAN and Subnet pairs of the underlying physical network are logically equivalent.A single VM Network can be created on top of this logical network and this VM Network will provide access to all the underlying VLAN-Subnet pairs.

● **Connected network**

☑ Managed by Microsoft Network Controller

Select this option if Microsoft Network Controller (NC) is deployed and it needs to manage this logical network.

☑ Public IP address network

Select this option if this logical network provides public IP addresses.

Independent Network

3. In **Network Site**, add the network site information for your public VIP logical network.
4. Review the **Summary** information and complete the wizard.

Create IP address pools for the private and public VIP networks

1. Right-click the private VIP logical network > **Create IP Pool**.
2. Provide a **Name** and optional description for the IP Pool and ensure that the correct logical network is selected.
3. Accept the default network site and select **Next**.

4. In **IP Address range**, configure the starting and ending IP address. Add IPv6 subnet to network site and create IPv6 address pools if you're using the IPv6 address space.

   ⓘ Note

   - Add IPv6 address pools when you onboard an SLB.
   - Don't use the first IP address of your available subnet. For example, if your available subnet is from .1 to .254, start your range at .2 or greater.

- The maximum number of addresses allowed in a single VIP range is 1024.

5. In **IP addresses reserved for load balancer VIPs**, enter the IP address range in the subnet. It must match the start and end addresses you specified.
6. You don't need to provide gateway, DNS, or WINS information because this pool is used to allocate IP addresses for VIPs through the network controller only. Select **Next** to skip these screens. Enter the address and use the default metric. Optionally configure DNS and WINS.
7. Review the summary information, and select **Finish** to complete the wizard.
8. Repeat the procedure for the public VIP logical network; this time enter the IP address range for the public network.

Import the service template

Import the service template into the VMM library. For this example, we'll import the Generation 2 template.

1. Select **Library** > **Import Template**.

2. Browse to your service template folder, select the **SLB Production Generation 2 VM.xml** file.

3. Update the parameters for your environment as you import the service template.

> ⓘ **Note**
>
> The library resources were imported during network controller deployment.

   - **WinServer.vhdx**: Select the virtual hard drive image that you prepared and imported earlier during the network controller deployment.
   - **NCCertificate.cr**: This library resource contains scripts used to set up the network controller. Map to the NCCertificate.cr library resource in the VMM library.
   - **EdgeDeployment.cr**: Map to the EdgeDeployment.cr library resource in the VMM library.

4. Remember that you must have copied the .CER certificate that you previously created to the **NCCertificate.cr** folder.

5. On the **Summary** page, review the details and select **Import**.

> ⓘ Note
>
> You can customize the service template. Learn more.

Deploy the SLB service

Now deploy an SLB/MUX service instance.

1. Select the **SLB Production Generation 2 VM.xml** service template > **Configure Deployment**. Enter a **Name** and optional destination for the service instance. The destination must map to a host group that contains the hosts you've configured.

2. In the **Network Settings** section, map **TransitNetwork** to your transit VM network and **ManagementNetwork** to your management VM network.

   > ⓘ Note
   >
   > - Transit network isn't applicable when you're using simplified topology templates.
   > - The **Deploy Service** screen appears after the mapping is complete. It is normal for the virtual machine instances to be initially Red. Select **Refresh Preview** to automatically find suitable hosts for the virtual machine.

3. On the left of the **Configure Deployment** window, configure the settings as detailed in the following table:

   Expand table

Setting	Requirement	Description
Transit network	Required	Your transit VM network.
LocalAdmin	Required	Select a Run As Account in your environment, which will be used as the local Administrator on the virtual machines. The username must be Administrator.
Management network	Required	Choose the management VM network that you created for host management.

Setting	Requirement	Description
MgmtDomainAccount	Required	Select a Run As Account with permissions to add the SLB/MUX virtual machines to the Active Directory domain associated with the network controller. This can be the same account you used in MgmtDomainAccount while deploying the network controller.
MgmtDomainFQDN	Required	FQDN for the Active directory domain that the SLB/MUX virtual machines will join.
SelfSignedConfiguration	Required	Specify **True** if the certificate you're using is self-signed.

4. After you configure these settings, select **Deploy Service** to begin the service deployment job. Deployment times will vary depending on your hardware but are typically between 30 and 60 minutes.

5. If you're not using a volume licensed VHDX, or if the VHDX doesn't have the product key from an answer file, then deployment will stop at the **Product Key** page during SLB/MUX VM provisioning. You need to manually access the VM desktop, and either skip or enter the product key.

6. When the service deployment job is complete, verify that your service appears in **VMs and Services** > **Services** > **VM Network Information for Services**. Right-click the service and verify that the state is **Deployed** in **Properties**.

After deployment, verify that the service appears in **All Hosts** > **Services** > **VM Network Information for Services**. Right-click the SLB MUX service > **Properties**, and verify that the state is **Deployed**. If the SLB/MUX deployment fails, ensure that you delete the failed service instance before you try to deploy the SLB once again.

If you want to scale in or scale out a deployed software load balancer service instance, read this blog .

ⓘ **Note**

After the SLB service is deployed, disable DNS registration on the virtual network adapter connected to the transit VM network on all the SLB MUX VMs.

Configure the SLB role and SLB/MUX properties

ⓘ Note

Before you proceed, ensure that you create the HNV PA Logical Network.

Now that the service is deployed, you can configure its properties. You'll need to associate the SLB service instance that you deployed with network controller, and then configuring BGP peering between the SLB/MUX instance and a TOR switch or a BGP router peer.

1. Select **Fabric** > **Network Service**. Right-click the **network controller** service > **Properties**.
2. Select the **Services** tab > **Load Balancer Role** > **Associated Service** > **Browse**.
3. Select the SLB/MUX service instance you created earlier. Select a Run As Account.
4. For the **Management IP address**, use an IP address from the private VIP pool you created earlier. Optionally specify the IP address ranges to be excluded from the outbound NAT. Under **SLBM VIP Pools**, select both the private and public VIP pools for publishing to NC.
5. Select the SLB/MUX instance listed under **Load Balancer Role** in the wizard. Enter the local ASN for your datacenter and the details for the devices or BGP peers the SLB/MUX can peer with.
6. Select **OK**.

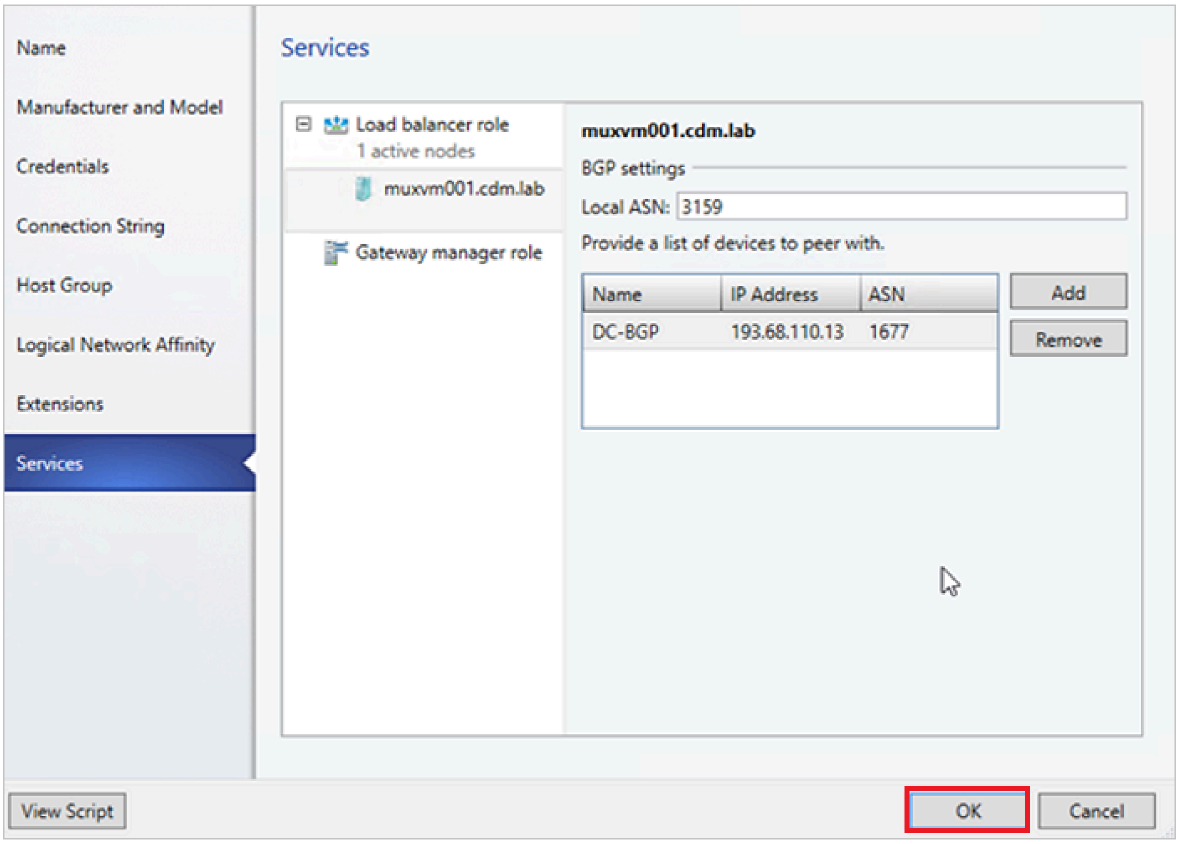
The SLB service instance is now associated with the SLBM service, and you must see the SLB/MUX virtual machine instance with all the settings listed under the **Load Balancer role**.

Validate the deployment

After you deploy the SLB/MUX, you can validate the deployment by configuring BGP peering between the SLB/MUX instance and a BGP router, assigning a public IP address to a tenant virtual machine or Service, and accessing the tenant virtual machine or service from outside the network.

Use the following procedure to validate:

1. Enter your external router details in the wizard. For example:



muxvm001.cdm.lab

BGP settings

Local ASN: 3159

Provide a list of devices to peer with.

Name	IP Address	ASN
DC-BGP	193.68.110.13	1677

2. Select **OK** to complete the SLB/MUX service instance configuration.

3. Check the **Jobs** window to verify that the **Update Fabric Role with required configuration** and **Associate service instance with fabric role** jobs have completed successfully.

4. To complete the BGP peering operation, you need to configure BGP to peer with your SLB/MUX instance on the router. If you use a hardware router, you need to consult your vendor's documentation regarding how to set up BGP peering for that device.

   You also need to know the IP address of the SLB/MUX instance that you deployed earlier. To do this, you can either sign in to the SLB MUX virtual machine and run **ipconfig /all** from the command prompt, or you can get the IP address from the VMM console.

   > ⓘ **Note**
   >
   > Enter an IP from the transit network.

5. If you create a new VIP pool after peering is complete, you need to advertise all the VIP address pools using the VMM console.

After you validate, you can start using the SLB for load balancing. For related information, see load balance network traffic and configure NAT rules.

Remove the software load balancer from the SDN fabric

Use these steps to remove the SLB from the SDN fabric.

Next steps

Create a RAS gateway

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Set up an SDN RAS gateway in the VMM fabric

Article • 09/04/2024

This article describes how to set up a Software Defined Networking (SDN) RAS gateway in the System Center Virtual Machine Manager (VMM) fabric.

An SDN RAS gateway is a data path element in SDN that enables site-to-site connectivity between two autonomous systems. Specifically, a RAS gateway enables site-to-site connectivity between remote tenant networks and your datacenter using IPSec, Generic Routing Encapsulation (GRE), or Layer 3 Forwarding. Learn more.

ⓘ Note

VMM 2022 provides dual stack support for RAS gateway.

Before you start

Ensure the following before you start:

- **Planning**: Read about planning a software defined network, and review the planning topology in this document. The diagram shows a sample 4-node setup. The setup is highly available with Three network controller nodes (VM) and Three SLB/MUX nodes. It shows Two tenants with One virtual network broken into Two virtual subnets to simulate a web tier and a database tier. Both the infrastructure and tenant virtual machines can be redistributed across any physical host.
- **Network controller**: You must deploy the network controller before you deploy the RAS gateway.
- **SLB**: To ensure that dependencies are handled correctly, you must also deploy the SLB before setting up the gateway. If an SLB and a gateway are configured, you can use and validate an IPsec connection.
- **Service template**: VMM uses a service template to automate GW deployment. Service templates support multi-node deployment on Generation 1 and Generation 2 VMs.

Deployment steps

To set up a RAS gateway, do the following:

1. **Download the service template**: Download the service template that you need to deploy the GW.
2. **Create the VIP logical network**: Create a GRE VIP logical network. It needs an IP address pool for private VIPs and to assign VIPs to GRE endpoints. The network exists to define VIPs that are assigned to gateway VMs running on the SDN fabric for a site-to-site GRE connection.

   > ⓘ Note
   >
   > To enable dual stack support, while creating GRE VIP logical network, add IPv6 subnet to the network site and create IPv6 address pool. (applicable for 2022 and later)

3. **Import the service template**: Import the RAS gateway service template.
4. **Deploy the gateway**: Deploy a gateway service instance, and configure its properties.
5. **Validate the deployment**: Configure site-to-site GRE, IPSec, or L3, and validate the deployment.

Download the service template

1. Download the SDN folder from the Microsoft SDN GitHub repository and copy the templates from **VMM** >**Templates** > **GW** to a local path on the VMM server.
2. Extract the contents to a folder on a local computer. You'll import them to the library later.

The download contains Two templates:

- The EdgeServiceTemplate_Generation 1 VM.xml template is for deploying the GW Service on Generation 1 virtual machines.
- The EdgeServiceTemplate_Generation 2 VM.xml is for deploying the GW Service on Generation 2 virtual machines.

Both the templates have a default count of three virtual machines, which can be changed in the service template designer.

Create the GRE VIP logical network

1. In the VMM console, run the Create Logical Network Wizard. Enter a **Name**, optionally provide a description, and select **Next**.

2. In **Settings**, select **Connected Network**, select **Managed by the Network Controller**, and then select **Next**.

3. In **Network Site**, specify the settings:

   Here are the sample values:

   - Network name: GRE VIP
   - Subnet: 31.30.30.0
   - Mask: 24
   - VLAN ID on trunk: NA
   - Gateway: 31.30.30.1

4. To use IPv4, add IPv4 subnet to the network site and create IPv4 address pool. Here are the sample values:

   - Network name: GRE VIP
   - Subnet:
   - Mask:
   - VLAN ID on trunk: NA
   - Gateway:

5. To use IPv6, add both IPv4 and IPV6 subnets to the network site and create IPv6 address pool. Here are the sample values:

   - Network name: GRE VIP
   - Subnet: FD4A:293D:184F:382C::
   - Mask: 64
   - VLAN ID on trunk: NA
   - Gateway: FD4A:293D:184F:382C::1

6. In **Summary**, review the settings and finish the wizard.

Create an IP address pool for GRE VIP addresses

> ⓘ **Note**
>
> You can create an IP address pool using the **Create Logical Network** wizard.

1. Right-click the GRE VIP logical network > **Create IP Pool**.

2. Enter a **Name** and optional description for the pool, and check that the VIP network is selected. Select **Next**.
3. Accept the default network site and select **Next**.

4. If you had created IPv6 subnet, create a separate IPv6 GRE VIP address pool.
5. Choose a starting and ending IP address for your range. Start the range on the second address of your available subnet. For example, if your available subnet is from .1 to .254, start the range at .2. For specifying VIP range, don't use the shortened form of IPv6 address; Use the *2001:db8:0:200:0:0:0:7* format instead of *2001:db8:0:200::7*.
6. In the **IP addresses reserved for load balancer VIPs** box, enter the IP addresses range in the subnet. This must match the range you used for starting and ending IP addresses.
7. You don't need to provide gateway, DNS, or WINS information as this pool is used to allocate IP addresses for VIPs through the network controller only. Select **Next** to skip these screens.
8. In **Summary**, review the settings and finish the wizard.

Import the service template

1. Select **Library** > **Import Template**.
2. Browse to your service template folder. As an example, select the **EdgeServiceTemplate Generation 2.xml** file.
3. Update the parameters for your environment as you import the service template.

> ⓘ **Note**
>
> The library resources were imported during the network controller deployment.

- **WinServer.vhdx**: Select the virtual hard drive image that you prepared and imported earlier during the network controller deployment.
- **EdgeDeployment.CR**: Map to the EdgeDeployment.cr library resource in the VMM library.

4. On the **Summary** page, review the details and select **Import**.

> ⓘ **Note**
>
> You can customize the service template. Learn more.

Deploy the gateway service

To enable IPv6, while onboarding Gateway service, select the **Enable IPv6** checkbox and select the IPv6 GRE VIP subnet that you created previously. Also, select public IPv6 pool and provide the public IPv6 address.

This example uses the Generation 2 template.

1. Select the **EdgeServiceTemplate Generation2.xml** service template, and select **Configure Deployment**.

2. Enter a **Name**, and choose a destination for the service instance. The destination must map to a host group that contains the hosts configured previously for gateway deployment.

3. In **Network Settings**, map the management network to the management VM network.

   > ⓘ **Note**
   >
   > The **Deploy Service** dialog appears after the mapping is complete. It's normal for the VM instances to be initially Red. Select **Refresh Preview** to automatically find suitable hosts for the VM.

4. On the left of the **Configure Deployment** window, configure the following settings:

   - **AdminAccount**. Required. Select a RunAs account that will be used as the local administrator on the gateway VMs.
   - **Management Network**. Required. Choose the Management VM network that you created for host management.
   - **Management Account**. Required. Select a Run As account with permissions to add the gateway to the Active Directory domain associated with the network controller. This can be the same account used for MgmtDomainAccount while deploying the network controller.
   - **FQDN**. Required. FQDN for the Active directory domain for the gateway.

5. Select **Deploy Service** to begin the service deployment job.

   > ⓘ **Note**
   >
   > - Deployment times will vary depending on your hardware but are typically between 30 and 60 minutes. If gateway deployment fails, delete

the failed service instance in **All Hosts** > **Services** before you retry the deployment.

- If you aren't using a volume licensed VHDX (or the product key isn't supplied using an answer file), then deployment will stop at the **Product Key** page during VM provisioning. You need to manually access the VM desktop, and either enter the key or skip it.

- If you want to scale in or scale out a deployed SLB instance, read this blog.

Gateway limits

The following are the default limits for NC managed gateway:

- **MaxVMNetworksSupported**= 50
- **MaxVPNConnectionsPerVMNetwork**= 10
- **MaxVMSubnetsSupported**= 550
- **MaxVPNConnectionsSupported**= 250

> **Note**
>
> For an SDNv2 virtualized network, an internal routing subnet is created for every VM network. The **MaxVMSubnetsSupported** limit includes the internal subnets created for VM networks.
>
> You can override the default limits set for the network controller managed gateway. However, overriding the limit to a higher number could impact the performance of the network controller.

Override the gateway limits

To override the default limits, append the override string to the network controller service connection string and update in VMM.

- **MaxVMNetworksSupported**= followed by the number of VM networks that can be used with this gateway.
- **MaxVPNConnectionsPerVMNetwork**= followed by the number of VPN Connections that can be created per VM network with this gateway.

- **MaxVMSubnetsSupported**= followed by the number of VM network subnets that can be used with this gateway.
- **MaxVPNConnectionsSupported**= followed by the number of VPN Connections that can be used with this gateway.

Example:

To override the maximum number of VM networks that can be used with the gateway to 100, update the connection string as follows:

`serverurl=https://NCCluster.contoso.com;servicename=NC_VMM_RTM; MaxVMNetworksSupported==100`

Configure the gateway manager role

Now that the gateway service is deployed, you can configure the properties and associate it with the network controller service.

1. Select **Fabric** > **Network Service** to display the list of network services installed. Right-click the network controller service > **Properties**.

2. Select the **Services** tab, and select the **Gateway Manager Role**.

3. Find the **Associated Service** field under **Service information**, and select **Browse**. Select the gateway service instance you created earlier, and select **OK**.

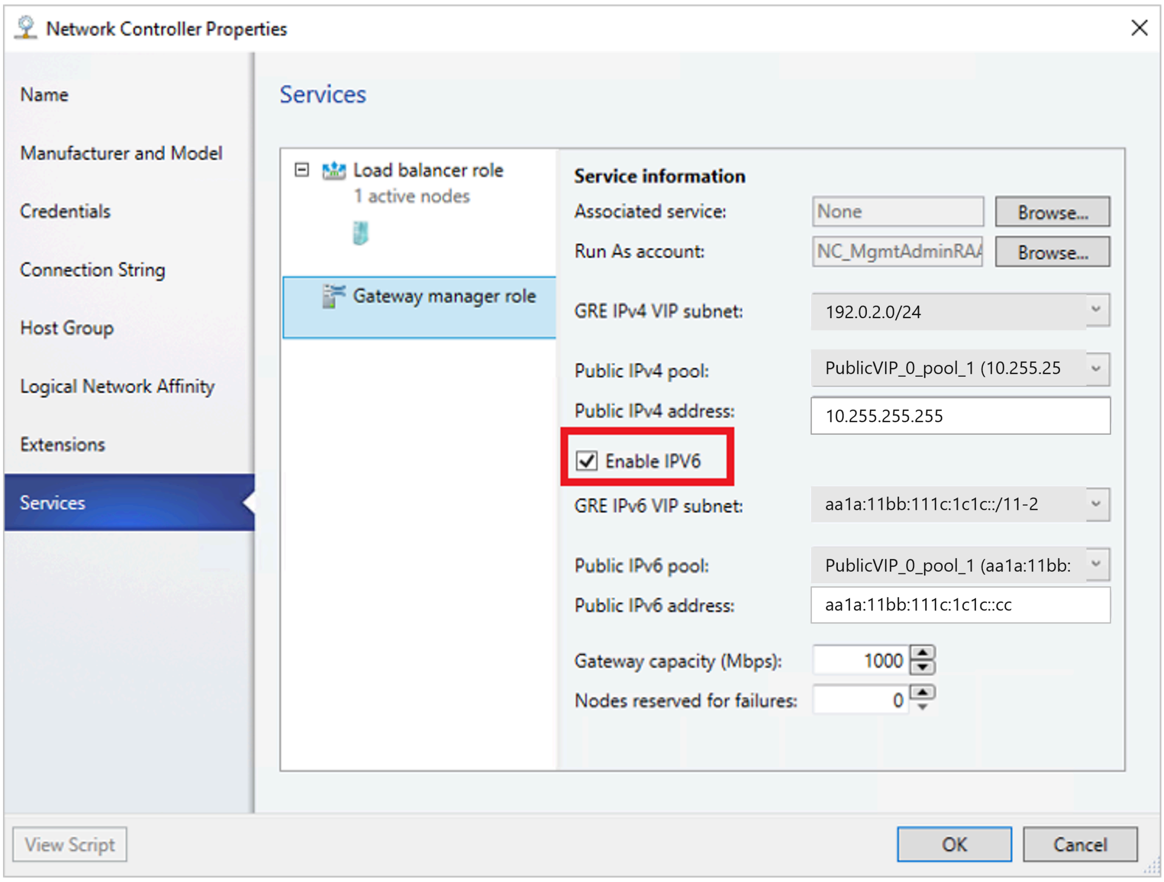
4. Select the **Run As account** that will be used by network controller to access the gateway virtual machines.

   > ⓘ **Note**
   >
   > The Run As account must have Administrator privileges on the gateway VMs.

5. In **GRE VIP subnet**, select the VIP subnet that you created previously.

6. To enable IPv4 support, in **Public IPv4 pool**, select the pool you configured during SLB deployment. In **Public IPv4 address**, provide an IP address from the previous pool, and ensure you don't select the initial three IP addresses from the range.

7. To enable IPv6 support, from **Network Controller Properties** > **Services**, select **Enable IPv6** checkbox, select the IPv6 GRE VIP subnet that you've created previously, and input the public IPv6 pool and public IPv6 address, respectively. Also, select IPv6 frontend subnet that will be assigned to Gateway VMs.



Services

Service information

Associated service: None

Run As account: NC_MgmtAdminRAA

GRE IPv4 VIP subnet: 192.0.2.0/24

Public IPv4 pool: PublicVIP_0_pool_1 (10.255.25

Public IPv4 address: 10.255.255.255

☑ Enable IPV6

GRE IPv6 VIP subnet: aa1a:11bb:111c:1c1c::/11-2

Public IPv6 pool: PublicVIP_0_pool_1 (aa1a:11bb:

Public IPv6 address: aa1a:11bb:111c:1c1c::cc

Gateway capacity (Mbps): 1000

Nodes reserved for failures: 0

8. In **Gateway Capacity**, configure the capacity settings.

   The gateway capacity (Mbps) denotes the normal TCP bandwidth that is expected out of the gateway VM. You must set this parameter based on the underlying network speed you use.

   IPsec tunnel bandwidth is limited to (3/20) of the gateway capacity. Which means, if the gateway capacity is set to 1000 Mbps, the equivalent IPsec tunnel capacity would be limited to 150 Mbps.

   > ⓘ Note
   >
   > The bandwidth limit is the total value of inbound bandwidth and outbound bandwidth.

   The equivalent ratios for GRE, and L3 tunnels are 1/5 and 1/2, respectively.

9. Configure the number of reserved nodes for backup in **Nodes for reserved for failures field**.

10. To configure individual gateway VMs, select each VM and select the IPv4 frontend subnet, specify the local ASN, and optionally add the peering device information for the BGP peer.

> **Note**
>
> You must configure the gateway BGP peers if you plan to use GRE connections.

The service instance you deployed is now associated with the gateway Manager role. You must see the gateway VM instance listed under it.

> **Note**
>
> You must configure the gateway BGP peers if you plan to use GRE connections.

The service instance you deployed is now associated with the gateway Manager role. You must see the gateway VM instance listed under it.

Validate the deployment

After you deploy the gateway, you can configure S2S GRE, S2S IPSec, or L3 connection types, and validate them. For more information, see the following contents:

- Create and validate site-to-site IPSec connections
- Create and validate site-to-site GRE connections
- Create and validate L3 connections

For more information on connection types, see this.

Set up the traffic selector from PowerShell

Here's the procedure to set up the traffic selector by using the VMM PowerShell.

1. Create the traffic selector by using the following parameters.

   > **Note**
   >
   > Values used are examples only.

   PowerShell

   ```
   $t= new-object Microsoft.VirtualManager.Remoting.TrafficSelector

   $t.Type=7 // IPV4=7, IPV6=8
   ```

```
$t.ProtocolId=6 // TCP =6, reference:
https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers

$t.PortEnd=5090

$t.PortStart=5080

$t.IpAddressStart=10.100.101.10

$t.IpAddressEnd=10.100.101.100
```

2. Configure the above traffic selector by using **-LocalTrafficSelectors** parameter of **Add-SCVPNConnection** or **Set-SCVPNConnection**.

Remove the gateway from the SDN fabric

Use these steps to remove the gateway from the SDN fabric.

Set up Software Defined Network (SDN) components in the VMM fabric using PowerShell

Article • 07/24/2024

System Center Virtual Machine Manager (VMM) can be used to deploy and manage a Software Defined Network (SDN) infrastructure.

You can deploy SDN components in the VMM fabric, including:

- **Network Controller**: The network controller allows you to automate the configuration of your network infrastructure instead of manually configuring network devices and services.
- **RAS Gateway for SDN**: RAS Gateway is a software-based, multi-tenant, BGP capable router in Windows Server 2016 that is designed for CSPs and enterprises that host multiple tenant virtual networks using HNV.
- **Software Load Balancing (SLB) for SDN**: SDN in Windows Server 2016 can use Software Load Balancing (SLB) to evenly distribute tenant and tenant customer network traffic among virtual network resources. The Windows Server SLB enables multiple servers to host the same workload, providing high availability and scalability.

There are a couple of ways to deploy these components:

- **VMM console**: Deploy the network controller, SLB, and RAS gateway manually in the VMM console.
- **PowerShell**: Deploy all components using PowerShell scripts.

Advantages of PowerShell deployment

- Deploy all SDN components with PowerShell scripts.
- The use of a script reduces the introduction of manual errors and save significant deployment time.
- If you deploy using the script, you can modify settings in the VMM console afterwards just as you would if you deploy the SDN components manually.
- Like the manual deployment, you have the option of setting up a new management logical network and switch or to reuse an existing network and switch.

- If the script deployment fails, all the changed settings are rolled back so that you can start again.
- You can turn off deployment for specific components. For example, if you already have network controller deployed, you can deploy SLB and RAS gateway only.

Before you start

- SET-enabled switch deployment isn't currently supported in a PowerShell deployment. You need to deploy the SET-enabled switch out-of-band, and then specify the name of the switch during deployment.
- Check if you have the prerequisites for SDN component deployment in place:
  - Network controller prerequisites
  - SLB prerequisites
  - RAS gateway prerequisites

Deployment steps

Here's what you need to do to set up SDN components in VMM with PowerShell.

1. **Configure hosts and physical network infrastructure**: You need access to your physical network devices to configure VLANs, routing, and others. You also need Hyper-V hosts to host the SDN infrastructure and tenant VMs. Learn more.

2. Prepared virtual hard disk for the service templates in VHD or VHDX format.

3. Download the network controller service template, the SLB service template, and the RAS gateway service template.

4. Import the network controller, SLB, and RAS gateway templates into the VMM library.

5. Set up Active Directory security groups. One for network controller management, and another for network controller clients. Each group will need at least one user account in it.

6. Set up a VMM library share. You can have an optional library file share for keeping diagnostics logs. This library share will be accessed by the network controller to store diagnostics information throughout its lifetime.

7. Set up a dedicated VMM host group for all SDN Hyper-V hosts.

   ⓘ Note

Hosts must be running the latest version of applicable Windows Server version and have the Hyper-V role enabled.

8. Set up a certificate. You need an SSL certificate for HTTPS communications between VMM and the network controller.

9. Download and run the SDN scripts. There are three scripts:

   - **VMMExpress.ps1**: This script deploys the SDN stack. After you download it, you can add your own customizations.
   - **Fabricconfig.psd1**: This file accepts all the inputs for setting up SDN.
   - **Fabricconfig_Example.psd1**: A sample file that contains dummy parameters. You can replace those with your own parameters.

Next steps

Configure hosts and physical network infrastructure for SDN .

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up VM networks in SDN using VMM

Article • 07/24/2024

This article provides information about how to create VM networks in an SDN using System Center Virtual Machine Manager (VMM).

VM networks are abstract objects that act as an interface to logical networks. In a virtualized network environment, by using the VM networks, you can abstract virtual machines from the underlying logical network.

VMM 2022 provides dual stack support for VM networks.

A logical network can have one or more VM networks associated with it based on its isolation settings.

The following two types of isolation settings are supported in SDN fabric:

- **Network virtualization**: If a logical network is isolated using network virtualization, you can create multiple VM networks for this logical network. Within a VM network, tenants can use any IP addresses regardless of the IP addresses used on other VM networks. As a service provider, you can host workloads from multiple tenants on a single logical network. Tenants can also configure network connections on these VM networks.
- **No Isolation**: If a logical network has no isolation, then only a single VM network can be associated with it. As a service provider, you can host infrastructure workloads using this type of isolation settings.

> ⓘ **Note**
>
> VLAN isolation is not supported in SDN fabric.

Before you start

Ensure the following:

- Network controller is deployed in the SDN fabric. Learn more.
- A logical network with appropriate isolation settings is created and is set to be managed by the Microsoft network controller. Also, create the IP pools for this logical network.

ⓘ Note

If you want to deploy the VMs with dynamic IP on **no isolation** network, then IP pools are not required.

- By default, VMs connected to a VM network with network virtualization isolation setting can't connect to other networks. If you want your VM network to connect to other networks, you need to first deploy SDN SLB and SDN gateway.

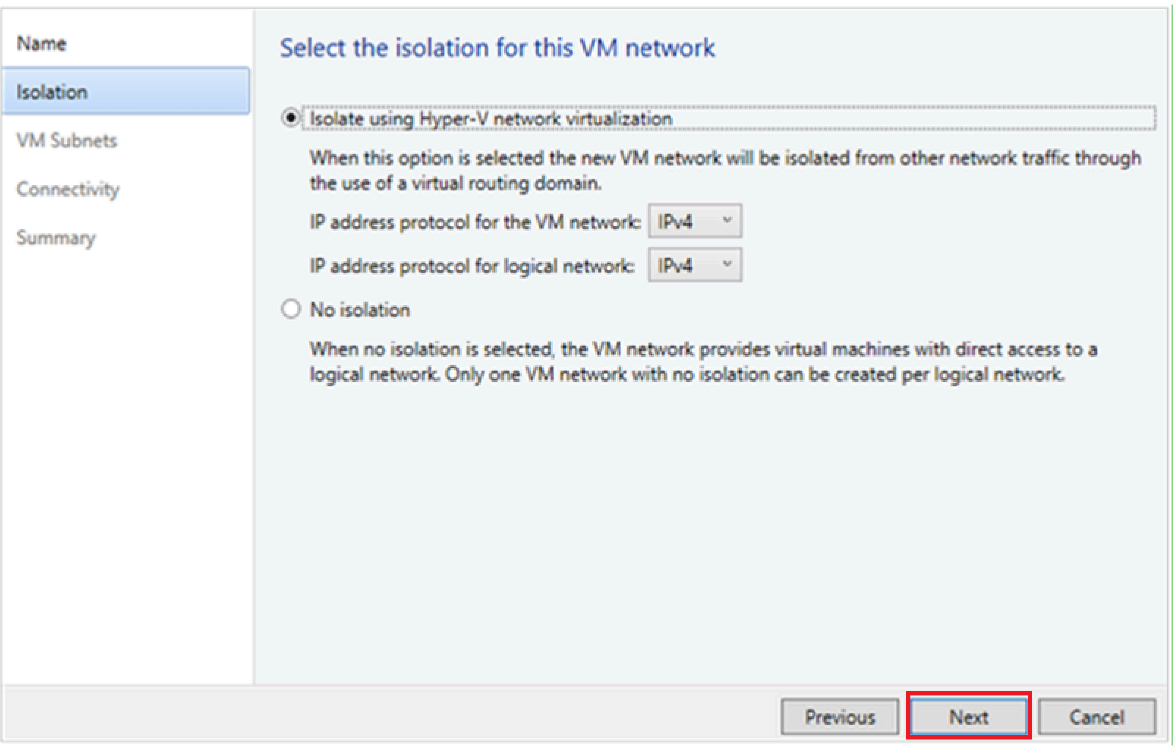
Create a VM network (network virtualization)

1. In the VMM fabric, select **VMs and Services** > **VM Networks** > **Create VM Network**.

2. In **Create VM Network Wizard** > **Name**, enter a name and optional description, and select a logical network that was created with network virtualization isolation settings.

3. In **Isolation**, select **Isolate using Hyper-V network virtualization**, and then select IPv4 for IP address protocols for the VM network. Select **Next**.

4. To enable dual stack support in Isolation, select **Isolate using Hyper-V network virtualization**, and then select **IPv4 and IPv6** for **IP address protocols for the VM network**. Select **Next**.



Select the isolation for this VM network

● Isolate using Hyper-V network virtualization

When this option is selected the new VM network will be isolated from other network traffic through the use of a virtual routing domain.

IP address protocol for the VM network: IPv4

IP address protocol for logical network: IPv4

○ No isolation

When no isolation is selected, the VM network provides virtual machines with direct access to a logical network. Only one VM network with no isolation can be created per logical network.

5. In **VM Subnets**, select **Add**, specify the name and subnets for VM network, and then select **Next**.

   > ⓘ **Note**
   >
   > - You can add multiple subnets.
   > - To enable dual stack support, provide both IPv4 subnet and IPv6 subnet separated by a semicolon (;).
   > - For VM network with dual stack support, create two static IP pools with both IPv4 and IPv6 address space.

6. In **Connectivity** panel, select the type of connectivity you want to use for this VM network.

   > ⓘ **Note**
   >
   > By default, all virtual machines in a VM network communicate with each other. If you want virtual machines on this VM network to communicate with other networks, configure the following settings in the **Connectivity** page:

   - **Connect to another network through a VPN tunnel**: Select this option if you want the virtual machines on this VM network to communicate with other networks over a VPN. To automatically learn routes between the sites connected through the VPN tunnel, select the **Enable the border gateway protocol** option. Select the **VPN gateway device** that you want to use and confirm the settings.

     Based on your selection, the **VPN Connections** and **Border Gateway Protocol** pages appear. Complete the settings based on the information provided by the VPN admin.

   - **Connect directly to an additional logical network**: Select this option if you want the virtual machines on this VM network to connect directly to an additional logical network. To enable access to internet resources, select **Network Address Translation (NAT)** or select **Direct Routing** to bridge a virtualized IP address space with a physical IP address space.

7. In **Summary**, verify the settings and select **Finish**.

Once the job is completed successfully, you can view the newly created VM network under **VMs and Services** > **VM Networks**.

ⓘ Note

After you create a VM network with network virtualization, ensure that you create an IP Pool for this VM network.

Create a VM network (no isolation)

ⓘ Note

While creating the logical network, if you have chosen the option **Create VM network with same name to allow virtual machines to access this logical network directly**, then you can skip the following steps.

1. Select **VMs and Services** > **VM Networks** . **Create VM Network**.
2. In **Create VM Network Wizard** > **Name**, enter a name and optional description. Select a **One connected logical network** for this VM network. Select **Next**.
3. In **Summary**, verify the settings and select **Finish**.

Once the job is successfully completed, you can view the newly created VM network under **VMs and Services** > **VM Networks**.

ⓘ Note

If you had created an IP pool on the logical network, the same will be directly available for the VM network.

Next steps

Create an IP pool for a VM network

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Configure encrypted networks in SDN using VMM

Article • 07/24/2024

This article explains how to encrypt the VM networks in software defined network (SDN) using System Center Virtual Machine Manager (VMM).

Network traffic can be encrypted by the guest OS or an application using technologies like IPSec and TLS. However, these technologies are difficult to implement because of their inherent complexity and challenges related to interoperability between systems because of the nature of implementation.

Using the encrypted networks feature in VMM, end-to-end encryption can be easily configured on the VM networks by using the Network Controller (NC). This encryption prevents traffic between two VMs on the same VM network and same subnet from being read and manipulated.

The control of encryption is at the subnet level, and encryption can be enabled/disabled for each subnet of the VM network.

This feature is managed through the SDN Network Controller (NC). If you don't already have a Software Defined Network (SDN) infrastructure with an NC, for more information, see deploy SDN.

> ⓘ **Note**
>
> This feature currently provides protection from non-Microsoft and network admins and doesn’t offer any protection against fabric admins.

Before you start

Ensure the following prerequisites are met:

- At least two hosts for tenant VMs to validate the encryption.
- HNV-based VM network with encryption enabled and a certificate, which can be created and distributed by fabric administrator.

  > ⓘ **Note**

The certificate, along with its private key, must be stored in the local certificate store of all the hosts where the VMs (of that network) reside.

Procedure - configure encrypted networks

Follow these steps to configure encrypted networks:

1. Create a certificate and then place the certificate in the local certificate store of all the hosts where you plan to place the tenant VMs for this validation.

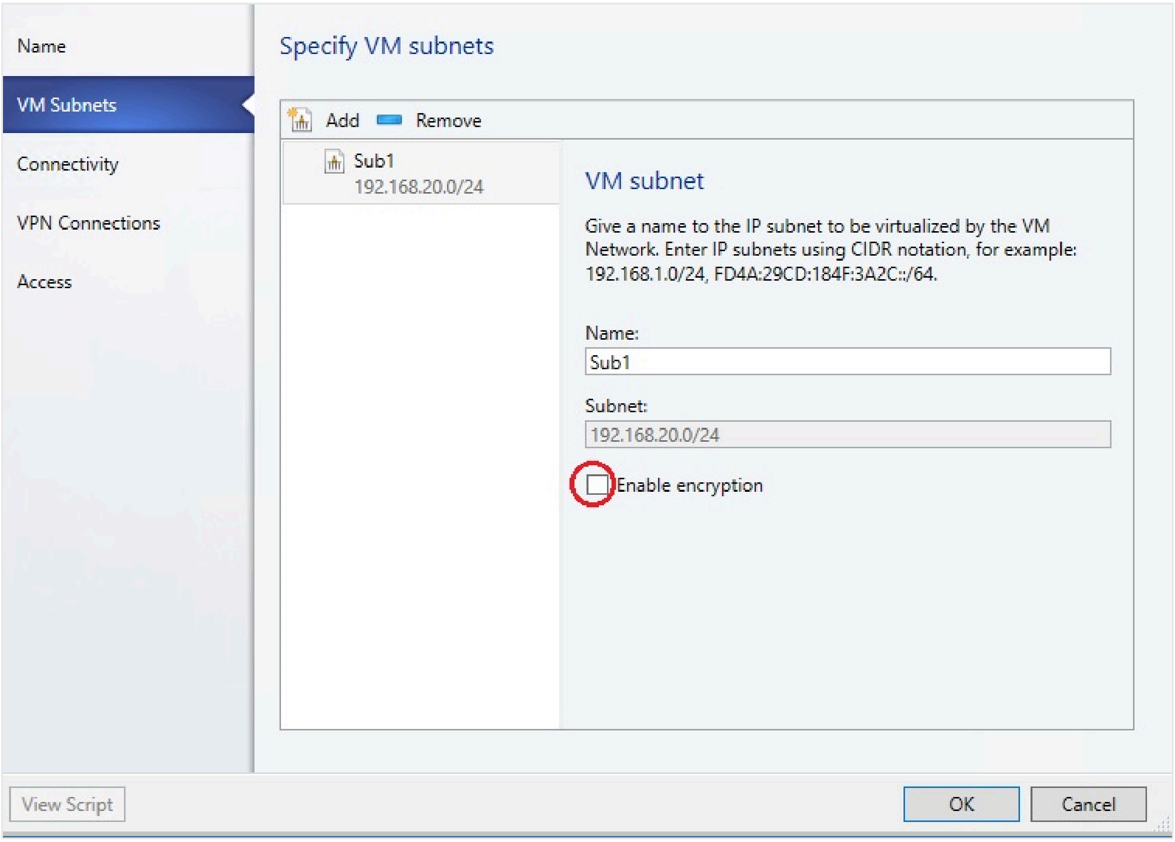
2. You can either create a self-signed certificate or get a certificate from a CA. For information on how to generate self-signed certificates and place them in the appropriate locations of each host you'll be using, see Configure Encryption for a Virtual Subnet.

   > ⓘ **Note**
   >
   > Make a note of the **Thumbprint** of the certificate that you generate. In the article above in step 2, you don't have to perform the actions detailed in **Creating a Certificate Credential** and **Configuring a Virtual Network for Encryption**. You will configure those settings using VMM in the following steps.

3. Set up an HNV provider network for tenant VM connectivity, which will be managed by the NC. Learn more.

4. Create a tenant VM Network and a subnet. While creating the subnet, select **Enable Encryption** under **VM Subnets**. Learn more.

   In the next step, paste the thumbprint of the certificate that you created.



Specify VM subnets

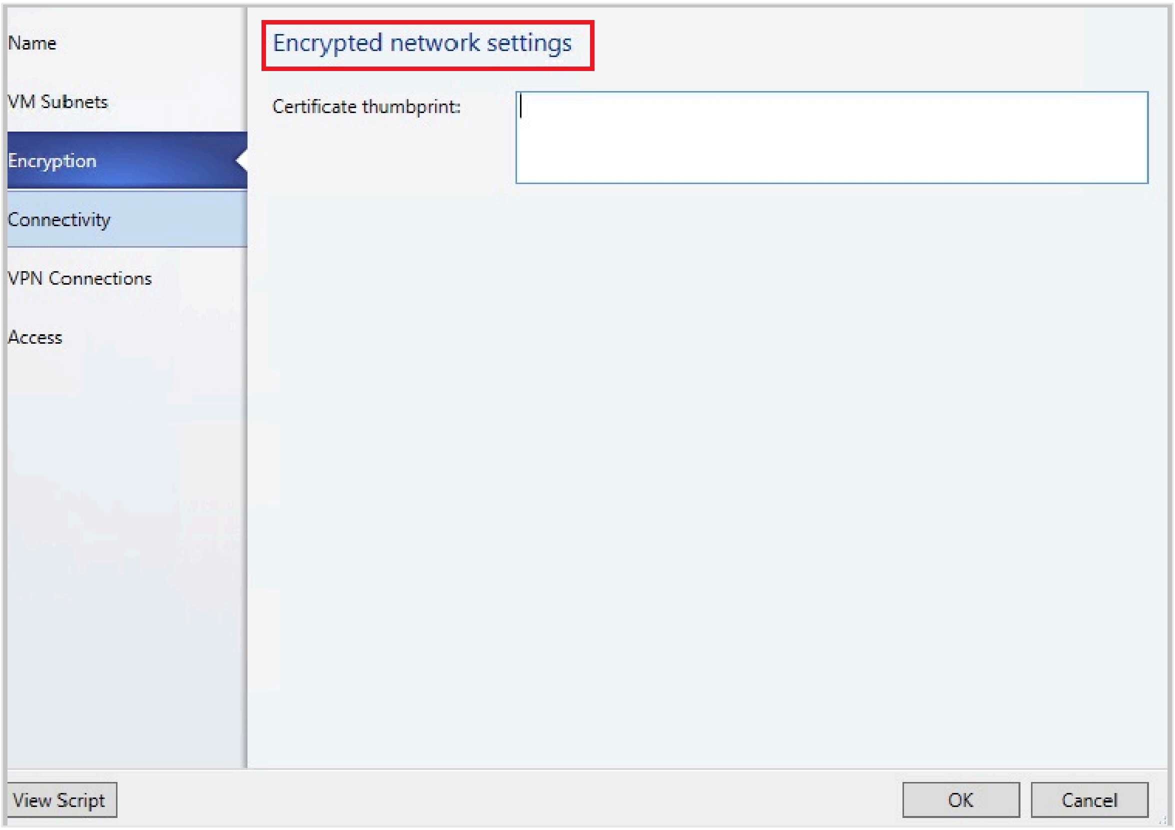
VM subnet

Give a name to the IP subnet to be virtualized by the VM Network. Enter IP subnets using CIDR notation, for example: 192.168.1.0/24, FD4A:29CD:184F:3A2C::/64.

Name: Sub1

Subnet: 192.168.20.0/24

□ Enable encryption



Encrypted network settings

Certificate thumbprint:

5. Create two VMs on two separate physical hosts and connect them to the above subnet. Learn more.

6. Attach any packet sniffing application on the two network interfaces of the two hosts where the tenant VMs are placed.

7. Send traffic, ping, HTTP, or any other packets between the two hosts, and check the packets in the packet sniffing application. The packets must not have any discernible plain text like the parameters of an HTTP request.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Allow and block VM traffic using SDN port ACLs

Article • 07/24/2024

In System Center Virtual Machine Manager (VMM), you can centrally configure and manage software defined network (SDN) port access control lists (ACLs).

- A port ACL is a set of port ACL rules that filter the traffic at layer 2 port level.
- A port ACL in VMM filters access to a specific VMM network object.
- Each VMM network object can have only one port ACL attached.
- An ACL contains rules and can be attached to any number of VMM network objects. You can create an ACL without rules and add the rules later.
- If an ACL has multiple rules, they're applied based on the priority. After a rule matches the criteria and is applied, no other rules are processed.
- SDN Port ACLs can be applied to virtual subnets and virtual network adapters.

> ⓘ **Note**
>
> Port ACL settings are exposed only through PowerShell cmdlets in VMM and can't be configured in the VMM console.

Using VMM PowerShell, you can also configure Hyper-V port ACLs. For more information, see Hyper-V port ACLs.

This article provides information on how to create and manage SDN port ACLs by using the VMM PowerShell cmdlets.

Before you start

Ensure that SDN network controller is deployed.

Create a port ACL

1. Open PowerShell in VMM.

2. Create a port ACL.

   PowerShell

```
PS C:\> New-SCPortACL -Name "RDPAccess" -Description "PortACL to
control RDP access" -ManagedByNC
```

> ⓘ **Note**
>
> The parameter **-ManagedByNC** ensures that the port ACL is managed by Network Controller (NC) and can only be attached to NC managed objects. The cmdlets provided here use example values.

Create a port ACL rule

1. Get an existing port ACL.

PowerShell

```
PS C:\> $portACL = Get-SCPortACL -Name "RDPAccess"
```

2. Create a port ACL rule.

PowerShell

```
PS C:\> New-SCPortACLRule -Name "AllowRDPAccess" -PortACL $portACL -
Description "Allow RDP Rule from a subnet" -Action Allow -Type Inbound
-Priority 110 -Protocol Tcp -LocalPortRange 3389 -RemoteAddressPrefix
10.184.20.0/24
```

> ⓘ **Note**
>
> - Priority range for SDN port ACL rules: 1 – 64500.
> - Only TCP/UDP/Any protocol parameters are supported for creating ACL rules.

Attach an ACL to a virtual network adapter

1. Get the virtual network adapter.

PowerShell

```
PS C:\> $vm = Get-SCVirtualMachine -Name “TenantVM”
PS C:\> $adapter = Get-SCvirtualNetworkAdapter -VM $vm"
```

2. Attach an existing port ACL to the virtual network adapter.

PowerShell

```
PS C:\> $portACL = Get-SCPortACL -Name "RDPAccess"
PS C:\> Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter $adapter -
PortACL $portACL
```

> ⓘ Note
>
> You can also attach a port ACL while creating the virtual network adapter through **New-SCVirtualNetworkAdapter** cmdlet. Learn more.

Detach a port ACL from a virtual network adapter

1. Get the virtual network adapter that you want to detach the port ACL from.

PowerShell

```
PS C:\> $vm = Get-SCVirtualMachine -Name “TenantVM”
PS C:\> $adapter = Get-SCvirtualNetworkAdapter -VM $vm
```

2. Detach the port ACL from the virtual network adapter.

PowerShell

```
PS C:\> Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter $adapter -
RemovePortACL
```

Attach an ACL to a VM subnet

1. Get the VM subnet to attach the ACL.

PowerShell

```
PS C:\> $vmSubnet = Get-SCVMSubnet -Name “Tenant Subnet”
```

2. Attach an existing port ACL to the VM subnet.

PowerShell

```
PS C:\> Set-SCVMSubnet -VMSubnet $vmSubnet -PortACL $portACL
```

ⓘ Note

You can also attach a port ACL while creating VM subnet through **New-SCVMSubnet cmdlet**. Learn more.

Detach a port ACL from a VM subnet

1. Get the VM subnet that you want to detach the port ACL from.

PowerShell

```
PS C:\> $vmSubnet = Get-SCVMSubnet -Name “Tenant Subnet”
```

2. Detach the port ACL from the VM subnet.

PowerShell

```
PS C:\> Set-SCVMSubnet –VMSubnet $vmSubnet -RemovePortACL
```

Remove a port ACL rule

1. Get the port ACL rule that you want to remove.

PowerShell

```
PS C:\> $portACLRule = Get-SCPortACLRule –Name “AllowRDPAccess”
```

2. Remove the port ACL rule.

PowerShell

```
PS C:\> Remove-SCPortACLRule -PortACLRule $portACLRule
```

Remove a port ACL

1. Get the port ACL that you want to remove.

PowerShell

```
PS C:\> $portACL = Get-SCPortACL -Name “RDPAccess”
```

2. Remove the port ACL.

PowerShell

```
PS C:\> Remove-SCPortACL -PortACL $portACL
```

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Control SDN virtual network bandwidth with QoS

Article • 07/24/2024

This article provides information about how to configure the Quality of Service (QoS) settings for SDN virtual networks in System Center Virtual Machine Manager (VMM). Through this configuration, you can limit the bandwidth of the traffic flowing in or out of a virtual network adapter (vNIC) by specifying the minimum reserved bandwidth or maximum bandwidth for the adapter.

- Service providers can prevent a high-traffic VM from blocking other VMs.
- Tenants can get the minimum reserved bandwidth regardless of the network traffic.

For detailed information on the SDN QoS settings available in Network Controller, see Configure Quality of Service (QoS) for a Tenant VM Network Adapter.

QoS settings are managed in VMM through virtual network adapter port profiles associated with a port classification. Port profile settings enable uniformity and ease of application across multiple adapters.

Before you start

Ensure that you have the network controller deployed in the SDN fabric. Learn more.

Create virtual network adapter port profiles

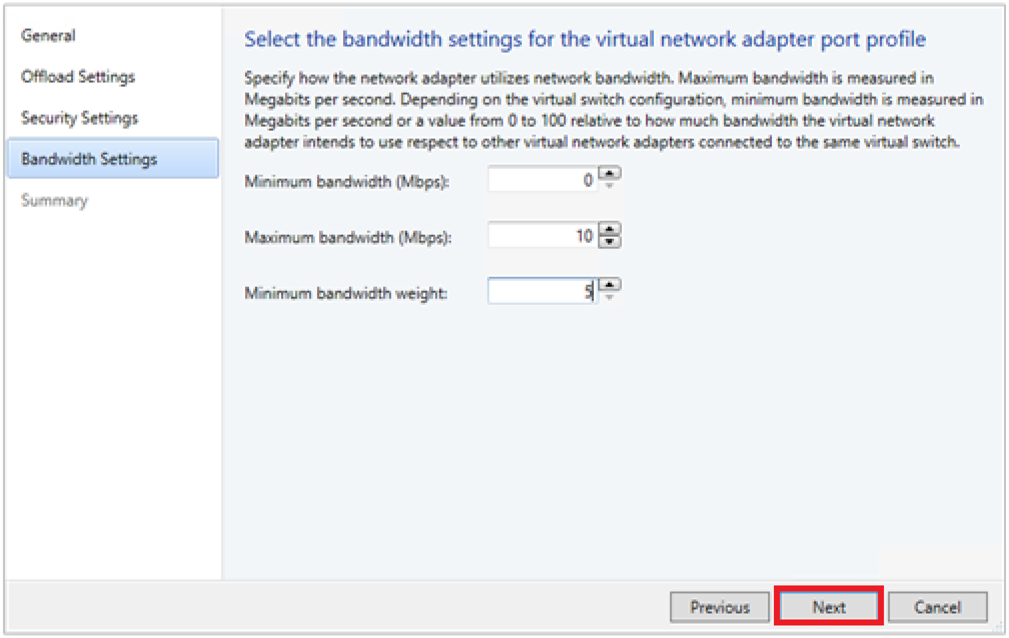
To create virtual network adapter port profile, use the following procedure:

1. Go to **Fabric** > **Port Profiles**.

2. Right-click **Port Profile** and select **Create Hyper -V Port Profile**. Provide a name and optional description. For example, name can be **TenantA**.

3. In **General**, select **Virtual Network Adapter Port Profile**.

4. Go to **Bandwidth Settings**.



Select the bandwidth settings for the virtual network adapter port profile

Specify how the network adapter utilizes network bandwidth. Maximum bandwidth is measured in Megabits per second. Depending on the virtual switch configuration, minimum bandwidth is measured in Megabits per second or a value from 0 to 100 relative to how much bandwidth the virtual network adapter intends to use respect to other virtual network adapters connected to the same virtual switch.

Minimum bandwidth (Mbps): 0

Maximum bandwidth (Mbps): 10

Minimum bandwidth weight: 5

.

5. In **Bandwidth Settings**, enter the minimum and maximum bandwidth values that you want to apply to the selected vNIC. Maximum bandwidth (Mbps) and Minimum bandwidth (Weight) are used to reserve a portion of the outbound bandwidth for the vNICs.

   - **Maximum bandwidth (Mbps)**: Specify the maximum outbound bandwidth that can be used by this vNIC. This is irrespective of the bandwidth mode configured on the switch. A value of 0 implies that the maximum isn't configured.

   - **Minimum bandwidth (Weight)**: Specify a weighted portion of the outbound bandwidth that you want to reserve for this vNIC. This will reserve a weighted portion of the total physical NIC(s) bandwidth based on the total weights reserved by all other vNICs for a particular switch.

6. In **Summary**, view the settings and select **Finish**.

> ⓘ Note
>
> - Minimum bandwidth (Mbps) is not supported by VMM for SDN.
> - Limiting the inbound bandwidth of the vNIC is not supported by VMM.
> - Minimum bandwidth (Weight) sets the **outboundReservedValue** setting on the network controller, and maximum bandwidth (Mbps) sets the **outboundMaximumMbps** setting.
> - Ensure that the minimum and maximum values for bandwidth are within the bandwidth range of the physical NIC(s) that the logical switch is deployed on. Otherwise, the bandwidth allocation request will be rejected.

Create port classification

To create a port classification:

1. Go to **Fabric** > **Networking**.
2. Right-click **Port Classifications** > **Create Port Classification**.
3. In the **Create Port Classification** wizard, in **General**, give a name to the classification and select **Finish**.

As an example, we created a port classification with the name **TenantA workload**, which we use later.

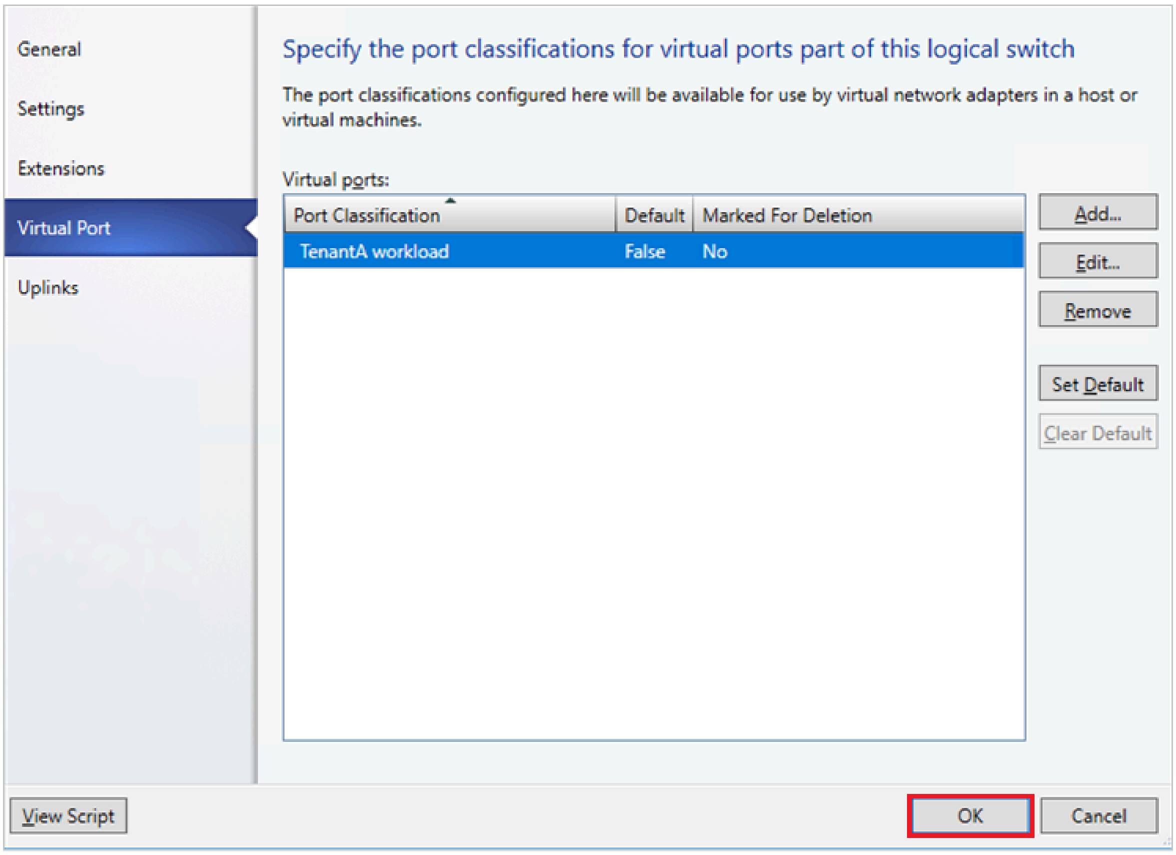
Associate port classifications to logical switch

To associate a port classification to the logical switch, use the following procedure:

1. Go to **Fabric** > **Networking** > **Logical Switches**.

2. Right-click the selected logical switch to view its **Properties**.

3. Select Virtual Ports, select **Add** to open the **Add Virtual Port** page.



Specify the port classifications for virtual ports part of this logical switch

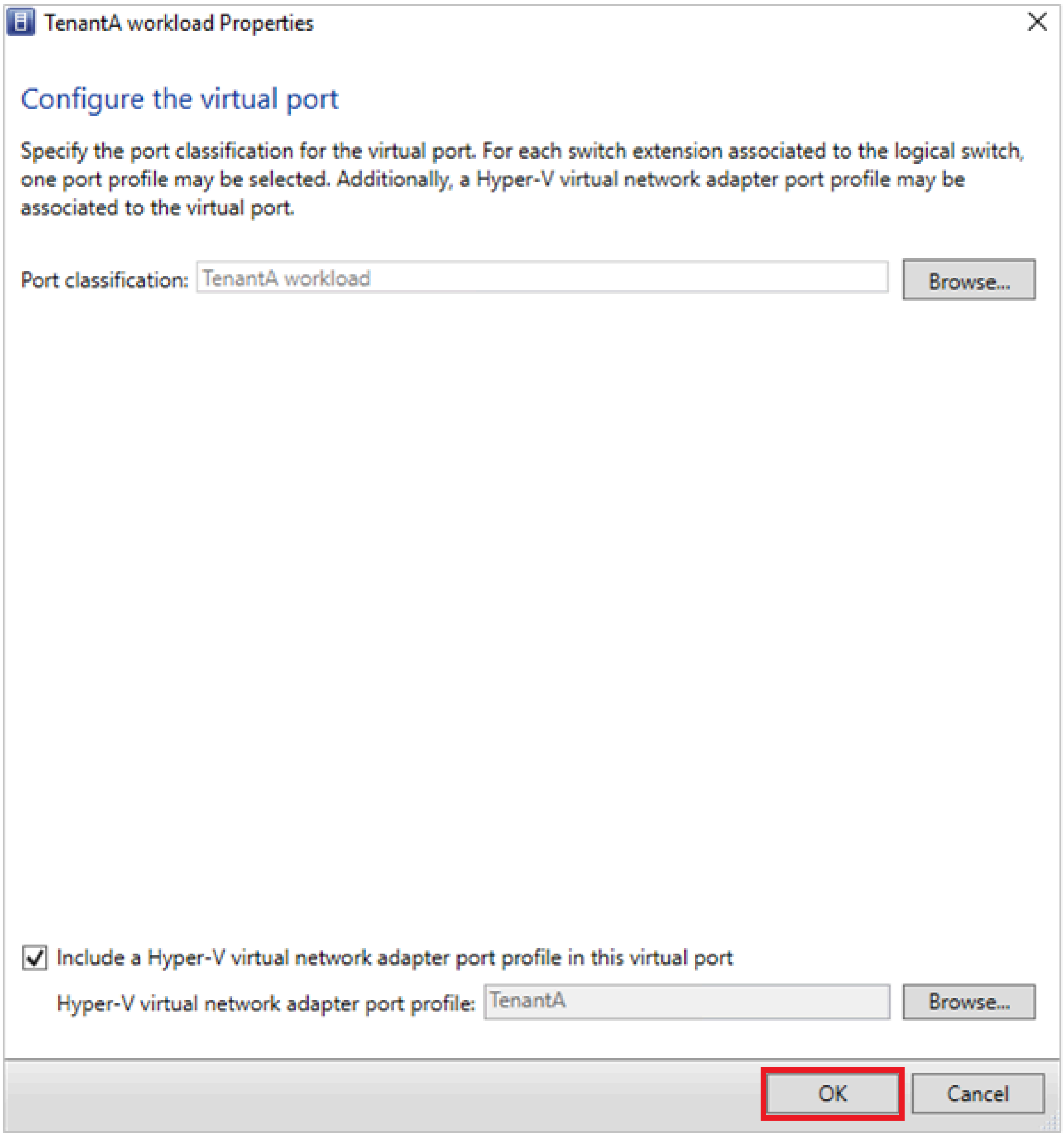
The port classifications configured here will be available for use by virtual network adapters in a host or virtual machines.

Virtual ports:

Port Classification	Default	Marked For Deletion
TenantA workload	False	No

4. **Browse** to select the port classification (as an example, **TenantA Workload**) and select **OK**.

5. Select the **Include the Hyper-V virtual network adapter port profile** option and select **Browse**. Select the vNIC port profile (as an example, **TenantA** that you created in the previous procedure). Select **OK**.



TenantA workload Properties

Configure the virtual port

Specify the port classification for the virtual port. For each switch extension associated to the logical switch, one port profile may be selected. Additionally, a Hyper-V virtual network adapter port profile may be associated to the virtual port.

Port classification: TenantA workload

☑ Include a Hyper-V virtual network adapter port profile in this virtual port

Hyper-V virtual network adapter port profile: TenantA

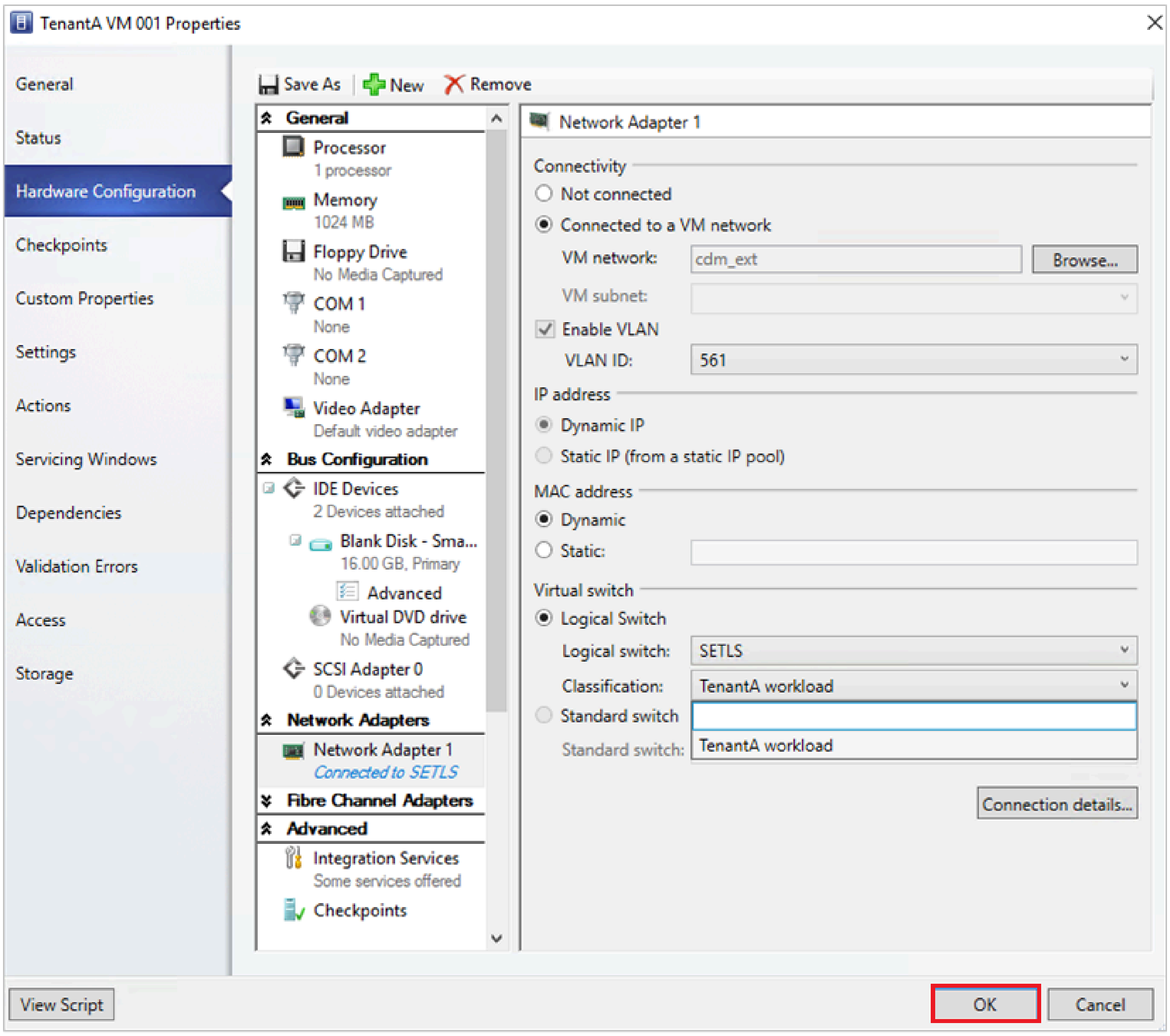
6. Repeat the above steps to add the port classifications required for this logical switch.

Apply port classification to virtual network adapter

To apply a port classification (and hence the QoS settings) to a virtual network adapter, use the following procedure:

1. Go to **VMs and Services**, right-click the selected VM and open its **Properties**.
2. Go to the **Hardware Configuration** page and select the virtual network adapter.

3. Select the desired port classification from the **Classification** dropdown list.



TenantA VM 001 Properties

Network Adapter 1

Connectivity

○ Not connected

● Connected to a VM network

VM network: cdm_ext

VM subnet:

☑ Enable VLAN

VLAN ID: 561

IP address

● Dynamic IP

○ Static IP (from a static IP pool)

MAC address

● Dynamic

○ Static:

Virtual switch

● Logical Switch

Logical switch: SETLS

Classification: TenantA workload

○ Standard switch

Standard switch: TenantA workload

ⓘ **Note**

- Only the classifications available for the logical switch are displayed here. You can also apply a port classification while creating a VM.
- You can also apply a port classification to the host virtual network adapter via the host properties Virtual Switches page.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Load balance network traffic in an SDN fabric using VMM

Article • 07/30/2024

You can use the Software Load Balancer (SLB) to distribute the network traffic evenly among the workloads in Software Define Networking (SDN) managed by the Cloud Service Providers (CSPs) and the tenants. For more information, see Software Load Balancer (SLB).

System Center Virtual Machine Manager (VMM) supports the following two scenarios of load balancing:

- **Load balancing the external network traffic**: This scenario includes load balancing the network traffic coming from an external network. Load balancing is done through a public Virtual IP (VIP). The workload VMs can be connected to a **no isolation** VM network or to a **network virtualization** enabled VM network.
- **Load balancing the internal network traffic** (Internal load balancing): This scenario includes load balancing the network traffic of workloads in the VM network that is enabled for **network virtualization**. Load balancing is done through a VIP.

> ⓘ **Note**
>
> VMM supports configuration of load balancing by using PowerShell. Configuration through Service templates is currently not supported.

This article provides information about how to configure the load balancing of workload VMs by using PowerShell.

Before you start

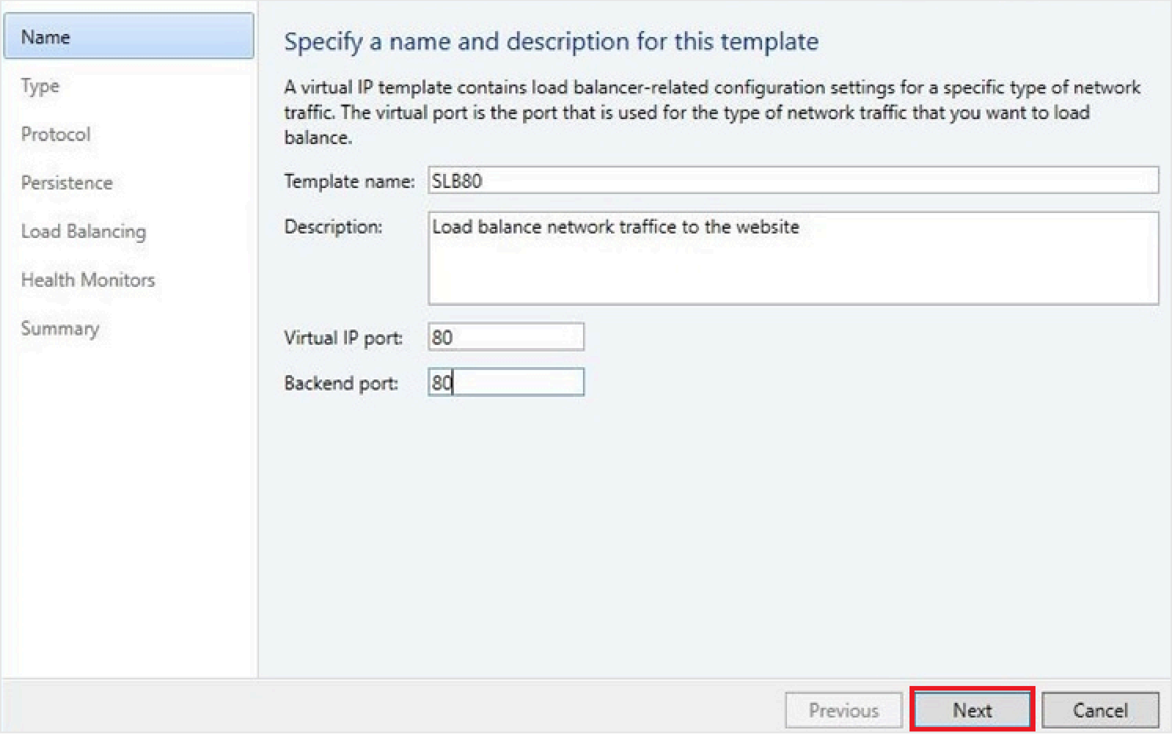
Ensure the following:

- SDN network controller and the SDN software load balancer are deployed.
- Required VMs are created on appropriate networks and are identified for load balancing.

Create a VIP template

Use the following procedures to configure the VIPs to load balance the workload VMs (DIPs).

1. In the VMM console, select **Fabric** > **VIP Templates**. Right-click and select **Create VIP Template**.



Specify a name and description for this template

A virtual IP template contains load balancer-related configuration settings for a specific type of network traffic. The virtual port is the port that is used for the type of network traffic that you want to load balance.

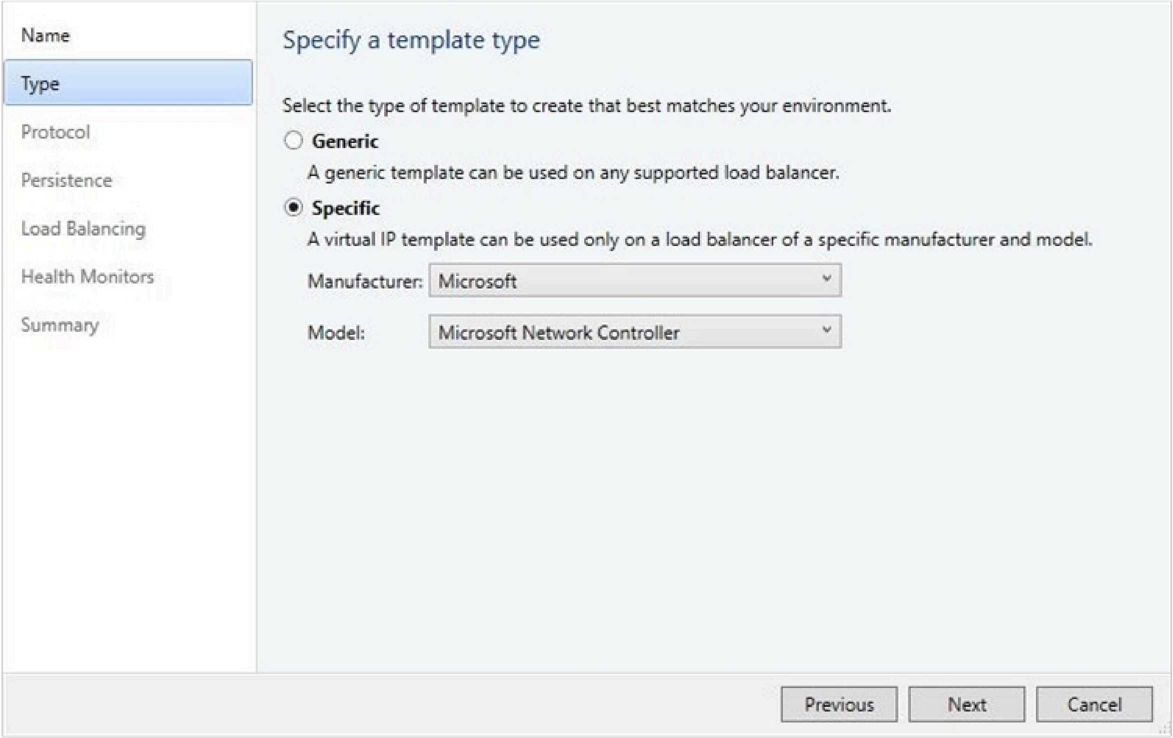
Template name: SLB80

Description: Load balance network traffice to the website

Virtual IP port: 80

Backend port: 80

2. In the **Name** page, provide the name and optional description. Specify the **Virtual IP Port** that will be used as front-end port for the network traffic. In the **Backend port**, specify the port on which the back-end workloads are hosted. Select **Next**.



Specify a template type

Select the type of template to create that best matches your environment.

○ **Generic**

A generic template can be used on any supported load balancer.

● **Specific**

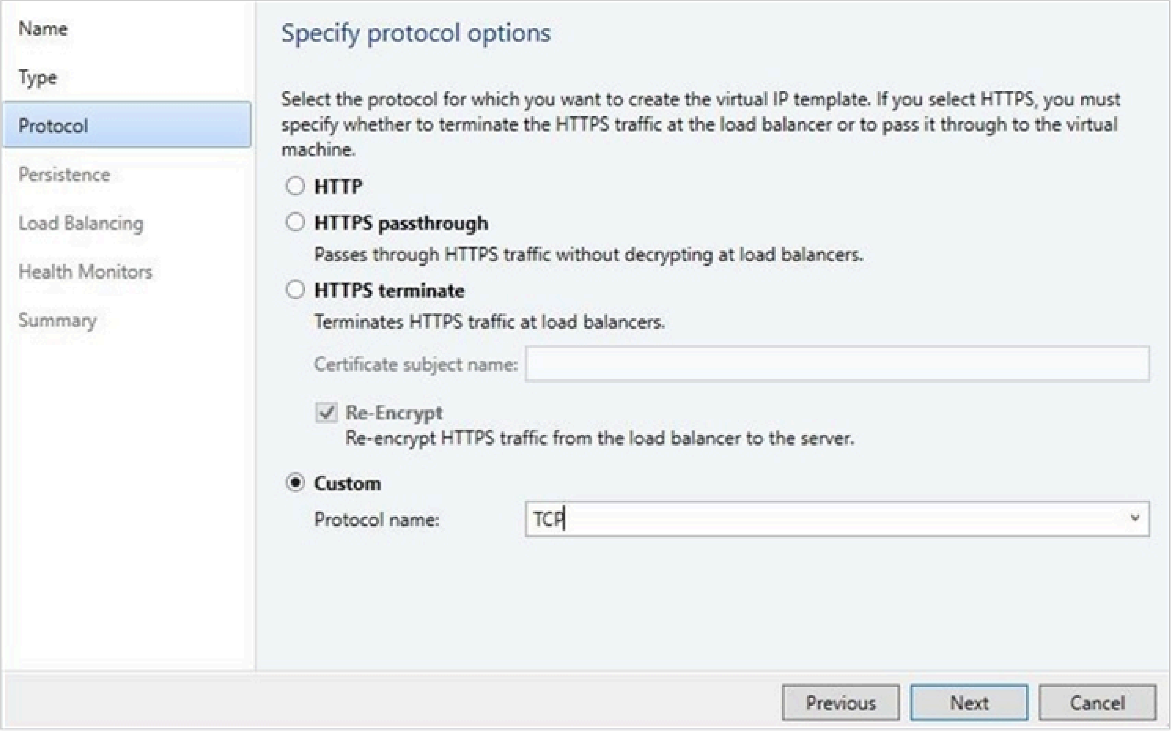
A virtual IP template can be used only on a load balancer of a specific manufacturer and model.

Manufacturer: Microsoft

Model: Microsoft Network Controller

3. In **Type**, under **Specify a template type**, select **Specific**. Select **Microsoft** from the Manufacturer dropdown and **Microsoft Network Controller** from the Model dropdown.

4. Select **Next**.



Specify protocol options

Select the protocol for which you want to create the virtual IP template. If you select HTTPS, you must specify whether to terminate the HTTPS traffic at the load balancer or to pass it through to the virtual machine.

○ **HTTP**

○ **HTTPS passthrough**
Passes through HTTPS traffic without decrypting at load balancers.

○ **HTTPS terminate**
Terminates HTTPS traffic at load balancers.

Certificate subject name:

☑ Re-Encrypt
Re-encrypt HTTPS traffic from the load balancer to the server.

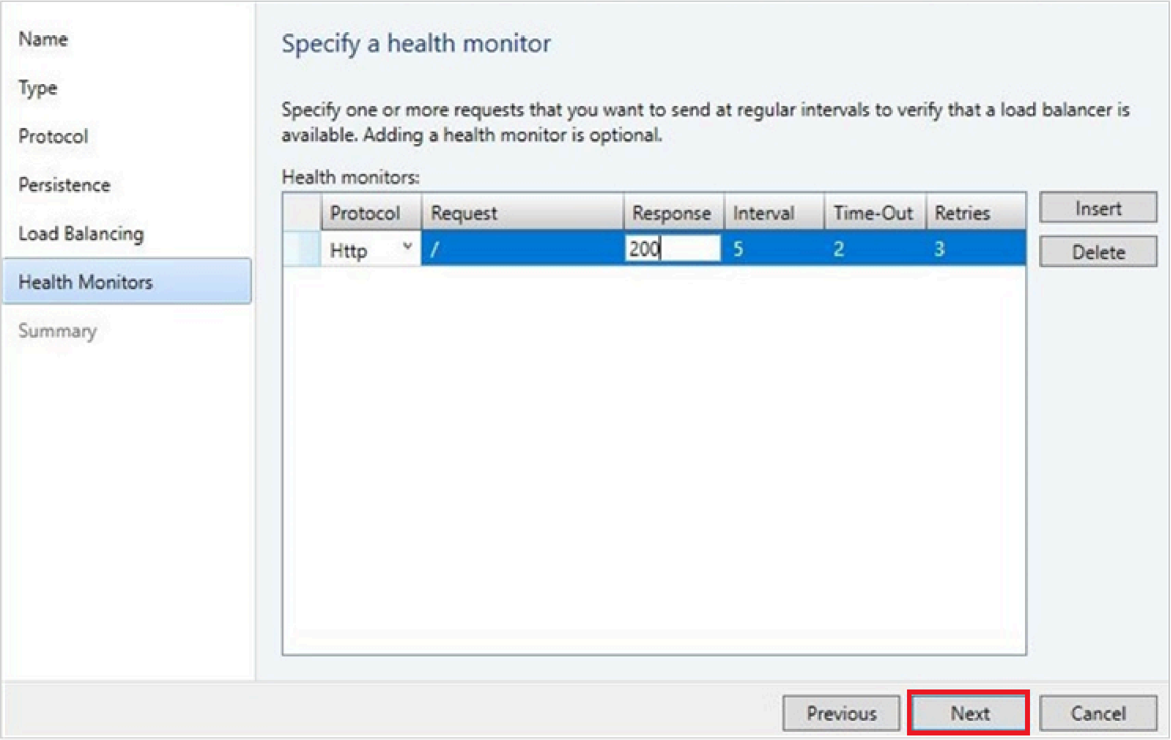
● **Custom**

Protocol name: TCP

5. In **Specify Protocol options**, select the Custom option and TCP/UDP in Protocol name. Select **Next**.

> ⓘ Note
>
> SLB supports only layer 4 load balancing of TCP/UDP traffic. HTTP/HTTPS protocols are not supported.

6. For **Persistence** and **Load Balancing**, use the defaults. Select **Next**.



Specify a health monitor

Specify one or more requests that you want to send at regular intervals to verify that a load balancer is available. Adding a health monitor is optional.

Health monitors:

Protocol	Request	Response	Interval	Time-Out	Retries
Http	/	200	5	2	3

ⓘ Note

SLB doesn't support persistence and different load balancing methods. By default, SLB uses Round Robin algorithm for load balancing.

7. In **Health Monitors**, optionally, insert appropriate values. Select **Next**.

   Options: TCP and HTTP are supported as health monitor protocols if SLB is used.

8. Verify the settings, and select **Finish**.

Once the template is created, you can find this under **Fabric** > **VIP Templates**.

Create a VIP using PowerShell

Create a VIP by using the following example scripts. Select the script based on the type of network traffic that you want to load balance:

- Script for creating a VIP to load balance external network traffic
- Script for creating a VIP to load balance internal network traffic

Script for creating VIP to load balance external network traffic

The following example script creates the VIP from a public IP network to load balance the workload VMs WGB-001 & WGB-002 on port 80.

This script can be used to create load balancing VIP by passing IPv6 VIP address as well.

The workload VMs can be connected to a **no isolation** network or **network virtualization** enabled VM networks.

> ⓘ **Note**
>
> - In the script parameters section, substitute the actual values that match your test environment for the samples used in this script.
> - Ensure that you run the script on a VMM server or on a computer running the VMM console.

PowerShell

```powershell
param(

[Parameter(Mandatory=$false)]
# Name of the Network Controller Network Service
# This value should be the name you gave the Network Controller service
# when you on-boarded the Network Controller to VMM
$LBServiceName = "NC",

[Parameter(Mandatory=$false)]
# Name of the workload VMs you want to load balance.
$VipMemberVMNames =  @("WGB-001","WGB-002"),

[Parameter(Mandatory=$false)]
# Name of the VIP VM Network
$VipNetworkName = "PublicVIP",


[Parameter(Mandatory=$false)]
# VIP address you want to assign from the VIP VM Network IP pool.
# Pick any VIP that falls within your VIP IP Pool range.
$VipAddress = "44.15.10.253",


[Parameter(Mandatory=$false)]
# The name of the VIP template you created via the VMM Console.
$VipTemplateName = "WebsiteHTTP",

[Parameter(Mandatory=$false)]
# Arbitrary but good to match the VIP you're using.
$VipName = "scvmm_44_15_10_253_80"

)
```

```
Import-Module virtualmachinemanager

$lb = Get-scLoadBalancer | where { $_.Service.Name -like $LBServiceName};
$vipNetwork = get-scvmnetwork -Name $VipNetworkName;

$vipMemberNics = @();
foreach ($vmName in $VipMemberVMNames)
{
$vm = get-scvirtualmachine -Name $vmName;
#    if ($vm.VirtualNetworkAdapters[0].VMNetwork.ID -ne $vipNetwork.ID)
#    {
#        $vm.VirtualNetworkAdapters[0] | set-scvirtualnetworkadapter -
VMNetwork $vipNetwork;
#    }

$vipMemberNics += $vm.VirtualNetworkAdapters[0];
}

$existingVip = get-scloadbalancervip -Name $VipName
    if ($existingVip -ne $null)
{
#    foreach ($mem in $existingVip.VipMembers)
#    {
#        $mem | remove-scloadbalancervipmember;
#    }

    $existingVip | remove-scloadbalancervip;
}

$vipt = get-scloadbalancerviptemplate -Name $VipTemplateName;

$vip = New-SCLoadBalancerVIP -Name $VipName -LoadBalancer $lb
-IPAddress $VipAddress -LoadBalancerVIPTemplate $vipt
-FrontEndVMNetwork $vipNetwork
-BackEndVirtualNetworkAdapters $vipMemberNics;
Write-Output "Created VIP " $vip;

$vip = get-scloadbalancervip -Name $VipName;
Write-Output "VIP created successfully " $vip;
```

Script for creating VIP to load balance internal network traffic

For the following example script, we created a new VIP template by name ILB-VIP-Template for load balancing the port 443 using the procedure detailed in the previous section. The script creates a VIP from tenant VM network to load balance the VMs ILB-001 & ILB-002, which are part of the same tenant VM network.

This script can be used to create load balancing VIP by passing IPv6 VIP address as well.

Note

- In the internal load balancing scenario, the VIP comes from the tenant VM network. So, the **$VipNetworkName** is the same tenant VM network name where the VMs are connected. Ensure that the tenant VM network IP pool has the IPs reserved for VIPs. The **$VipAddress** is one of the IP addresses from the reserved VIPs.
- In the script parameters section, substitute the actual values that match your test environment for the samples used in this script.
- Ensure that you run the script on a VMM server or on a computer running the VMM console.

PowerShell

```powershell
param(

[Parameter(Mandatory=$false)]
# Name of the Network Controller Network Service
# This value should be the name you gave the Network Controller service
# when you on-boarded the Network Controller to VMM
$LBServiceName = "NC",

[Parameter(Mandatory=$false)]
# Name of the workload VMs you want to load balance.
$VipMemberVMNames =  @("ILB-001","ILB-002"),

[Parameter(Mandatory=$false)]
# Name of the VIP VM Network
$VipNetworkName = "TenantNetwork",

[Parameter(Mandatory=$false)]
# VIP address you want to assign from the VIP VM Network IP pool.
# Pick any VIP that falls within your VIP IP Pool range.
$VipAddress = "192.168.100.75",

[Parameter(Mandatory=$false)]
# The name of the VIP template you created via the VMM Console.
$VipTemplateName = "ILB-VIP-Template",

[Parameter(Mandatory=$false)]
# Arbitrary but good to match the VIP you're using.
$VipName = "scvmm_192_168_100_75_443"

)

Import-Module virtualmachinemanager

$lb = Get-scLoadBalancer | where { $_.Service.Name -like $LBServiceName};
```

```
$vipNetwork = get-scvmnetwork -Name $VipNetworkName;

$vipMemberNics = @();
foreach ($vmName in $VipMemberVMNames)
{
$vm = get-scvirtualmachine -Name $vmName;
#    if ($vm.VirtualNetworkAdapters[0].VMNetwork.ID -ne $vipNetwork.ID)
#    {
#        $vm.VirtualNetworkAdapters[0] | set-scvirtualnetworkadapter -
VMNetwork $vipNetwork;
#    }

$vipMemberNics += $vm.VirtualNetworkAdapters[0];
}

$existingVip = get-scloadbalancervip -Name $VipName
if ($existingVip -ne $null)
{
#    foreach ($mem in $existingVip.VipMembers)
#    {
#        $mem | remove-scloadbalancervipmember;
#    }

$existingVip | remove-scloadbalancervip;
}

$vipt = get-scloadbalancerviptemplate -Name $VipTemplateName;

$vip = New-SCLoadBalancerVIP -Name $VipName -LoadBalancer $lb
-IPAddress $VipAddress -LoadBalancerVIPTemplate $vipt
-FrontEndVMNetwork $vipNetwork
-BackEndVirtualNetworkAdapters $vipMemberNics;
Write-Output "Created VIP " $vip;

$vip = get-scloadbalancervip -Name $VipName;
Write-Output " VIP created successfully " $vip;
```

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up NAT for traffic forwarding in the SDN infrastructure

Article • 07/25/2024

This article describes how to set up Network Address Translation (NAT) for traffic forwarding in a software-defined network (SDN) infrastructure set up in the System Center Virtual Machine Manager (VMM) fabric.

NAT allows virtual machines (VMs) in an isolated SDN virtual network to obtain external connectivity. VMM configures a Virtual IP (VIP) to forward the traffic to and from an external network.

The following two NAT types are supported by VMM.

- **Outbound NAT** - Forwards the VM network traffic from a virtual network to external destinations.
- **Inbound NAT** - Forwards the external traffic to a specific VM in a virtual network.

This article provides information about how to configure a NAT connection for SDN virtual networks using VMM.

VMM 2022 supports dual stack. NAT rules to Dual stack VM networks isn't supported at VMM console. NAT rules can be specified using PowerShell cmdlets. For more information, see Add rules to a NAT connection.

Before you start

Ensure the following:

- SDN network controller and the SDN software load balancer are deployed.
- An SDN VM network with network virtualization is created.

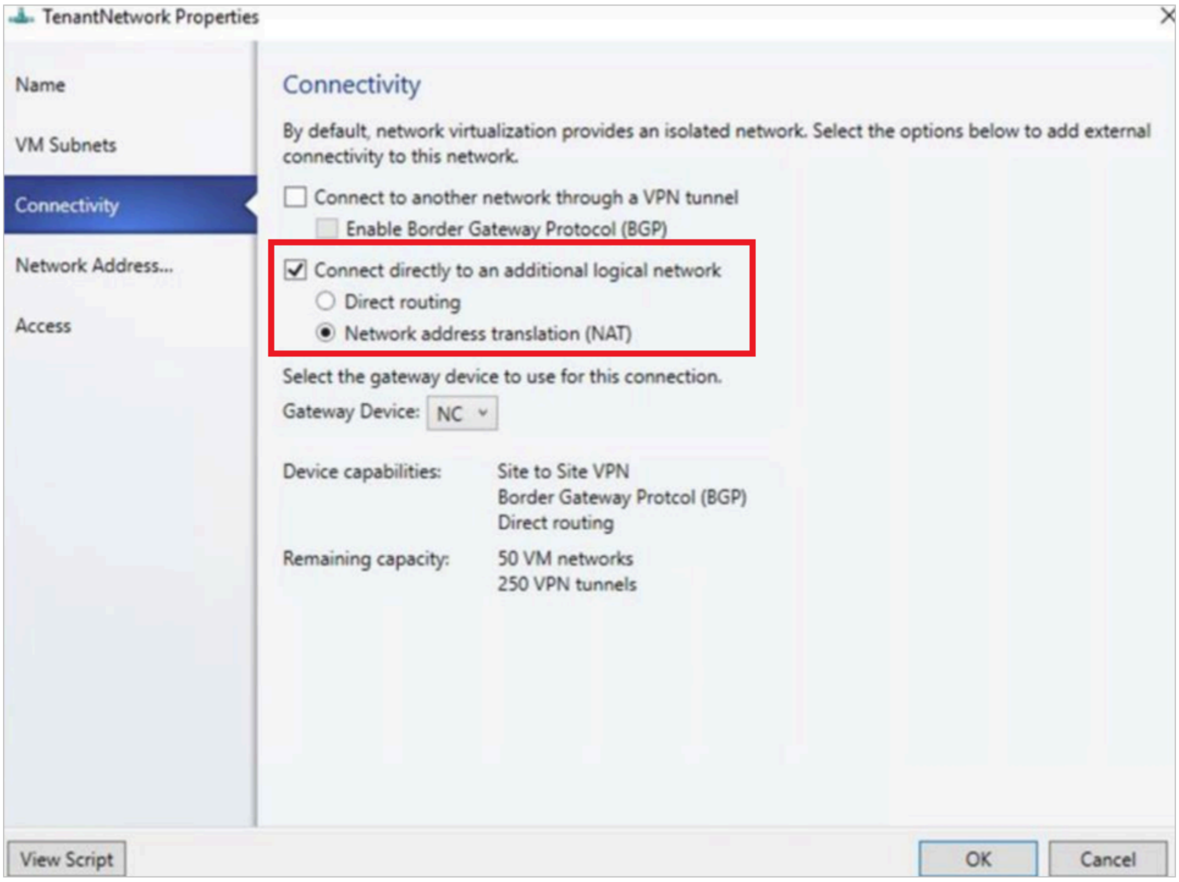
Create a NAT connection

Use the following procedure:

1. In the VMM console, select **VMs and Services** > **VM Networks**. Right-click the selected VM network for which you want to create the NAT connection and select **Properties**.

2. Select **Connectivity** on the wizard page displayed.

3. In **Connectivity**, select **Connect directly to an additional logical network** and select **Network address translation (NAT)** under this option.



Connectivity

By default, network virtualization provides an isolated network. Select the options below to add external connectivity to this network.

☐ Connect to another network through a VPN tunnel

☐ Enable Border Gateway Protocol (BGP)

☑ Connect directly to an additional logical network

○ Direct routing

● Network address translation (NAT)

Select the gateway device to use for this connection.

Gateway Device: NC

Device capabilities: Site to Site VPN
Border Gateway Protcol (BGP)
Direct routing

Remaining capacity: 50 VM networks
250 VPN tunnels

4. In the **IP address pool**, choose the IP pool from which the VIP must come from. In IP address, choose an IP address from the pool selected. Select **OK**.

5. To enable IPv6, select an IPv6 address pool and provide an IPv6 address.

A NAT connection will be created for this VM network.

ⓘ Note

- Along with the NAT connection, this procedure also creates a default Outbound NAT rule that enables the outbound connectivity for the VM network.
- To enable inbound connectivity and forward an external traffic to a specific VM, you must add NAT rules to the NAT connection.

Add rules to a NAT connection

VMM 2022 supports dual stack. NAT rules to dual stack VM networks isn't supported at the VMM console. NAT rules can be specified using PowerShell cmdlets.

```
$vmNetwork = Get-SCVMNetwork -ID <VMNetwork ID>

$vmSubnet = Get-SCVMSubnet -Name <VMSubnet Name> | where { $_.ID -eq
<VMSubnet ID> }
$gatewayDevice = Get-SCNetworkGateway -ID <Gateway Device ID>
$VmNetworkGateway = Add-SCVMNetworkGateway -Name "TenantDS_Gateway" -
EnableBGP $false -NetworkGateway $gatewayDevice -VMNetwork $vmNetwork
```

For IPv6 NAT Connection

```
$externalIpPoolVar = Get-SCStaticIPAddressPool -ID <VIP Pool Id>
$natConnectionIPv6 = Add-SCNATConnection -VMNetwork $vmNetwork -Name
"TenantDS_NatConnection_IPv6" -ExternalIPPool $externalIpPoolVar -
ExternalIPAddress <IP From IPv6 VIP Pool>
Add-SCNATRule -Name "NATIPv6" -Protocol "TCP" -InternalIPAddress <IP From
IPv6 subnet> -ExternalPort <External Port> -NATConnection $natConnectionIPv6
-InternalPort <Internal Port>
```

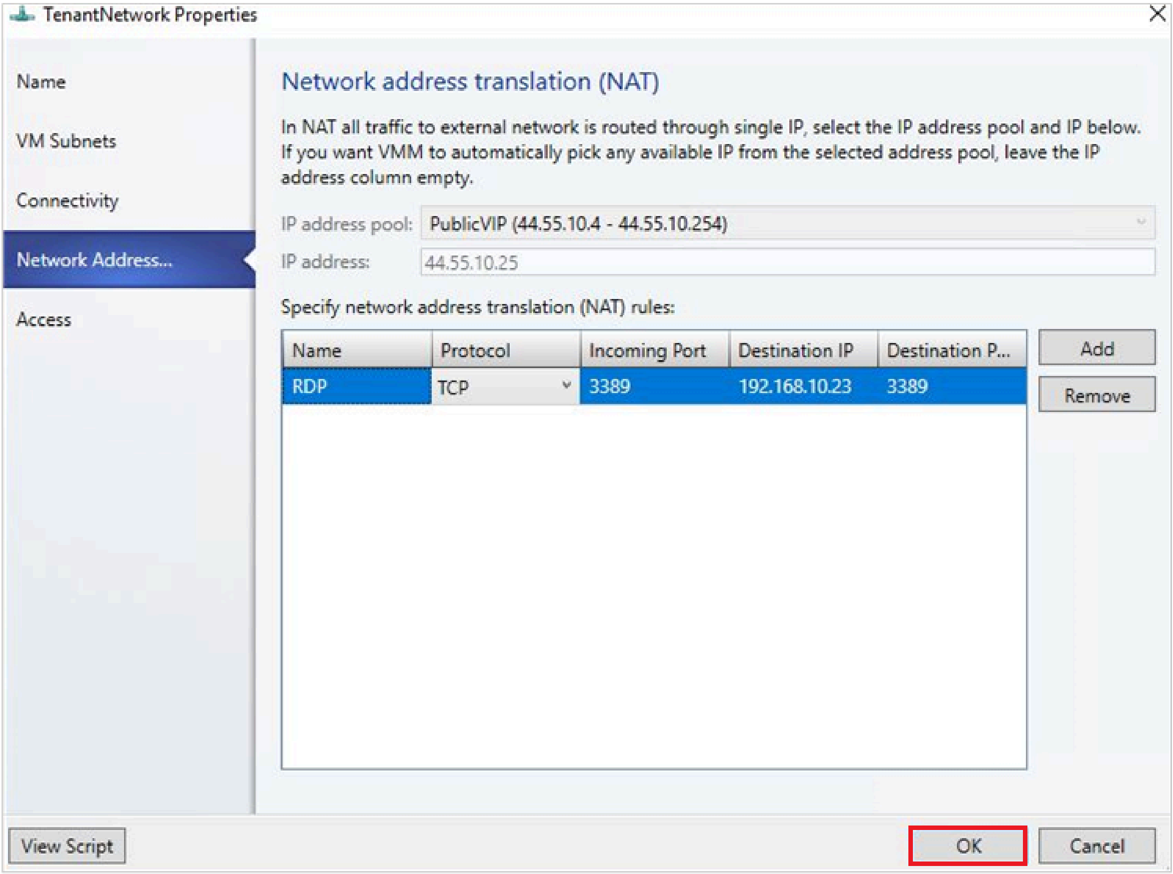
For IPv4 NAT Connection

```
$externalIpPoolVar1 = Get-SCStaticIPAddressPool -Name
"PublicVIP_IPAddressPool_0"
$natConnectionIPv4 = Add-SCNATConnection -VMNetwork $vmNetwork -Name
"TenantDS_NatConnection_IPv4" -ExternalIPPool $externalIpPoolVar1 -
ExternalIPAddress <IP From IPv4 VIP Pool>
Add-SCNATRule -Name "NATIPv4" -Protocol "TCP" -InternalIPAddress <IP From
IPv4 subnet>" -ExternalPort <External Port> -NATConnection
$natConnectionIPv4 -InternalPort <Internal Port>
```

Use the following procedure to add rules to a NAT connection:

1. In the VMM console, select **VMs and Services** > **VM Networks**. Right-click the selected VM network and select **Properties**.

2. Select **Network Address Translation** on the wizard.



Network address translation (NAT)

In NAT all traffic to external network is routed through single IP, select the IP address pool and IP below. If you want VMM to automatically pick any available IP from the selected address pool, leave the IP address column empty.

IP address pool: PublicVIP (44.55.10.4 - 44.55.10.254)

IP address: 44.55.10.25

Specify network address translation (NAT) rules:

Name	Protocol	Incoming Port	Destination IP	Destination P...
RDP	TCP	3389	192.168.10.23	3389

3. Under **Specify network address translation (NAT) rules**, select **Add**. Type the following details as appropriate:

- **Name** – Name for the inbound NAT rule.
- **Protocol** – Inbound network traffic protocol. TCP/UDP are supported.
- **Incoming Port** – Port number that you want to use along with the VIP to access the VM.
- **Destination IP** – IP address of the VM to which you want to direct the external traffic.
- **Destination Port** – Port number on the VM, the external traffic must be forwarded to.

4. Select **OK**.

> ⓘ Note
>
> Multiple NAT rules can be created to forward the traffic to multiple VMs that are part of the VM network.

Remove a NAT rule

Use the following procedure:

1. In the VMM console, select **VMs and Services** > **VM Networks**. Right-click the selected VM network and select **Properties**.
2. Select **Network Address Translation** on the wizard.
3. Select the NAT rule that you want to remove, select **Remove**, and then select **OK**.

Remove a NAT connection

1. In the VMM console, select **VMs and Services** > **VM Networks**. Right-click the selected VM network and select **Properties**.
2. Select **Connectivity** on the wizard.
3. Clear the option **Connect directly to an additional logical network** and select **OK**.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Route traffic across networks in the SDN infrastructure

Article • 07/24/2024

This article describes how to route traffic across networks in a software-defined network (SDN) infrastructure set up in the System Center Virtual Machine Manager (VMM) fabric.

An SDN RAS gateway enables you to route network traffic between physical and virtual networks, regardless of where the resources are located. SDN RAS gateway is multitenant, Boarder Gateway Protocol (BGP) capable and supports connectivity using Site-to-Site virtual private network (VPN) using IPsec or Generic Routing Encapsulation (GRE) or Layer 3 Forwarding. Learn more.

ⓘ **Note**

- IPv6 is supported for IPSec tunnel, GRE tunnel, and L3 layer tunnel.

Before you start

Ensure the following:

- SDN Network Controller, SDN Software Load Balancer, and SDN RAS gateway are deployed.
- An SDN VM network with network virtualization is created.

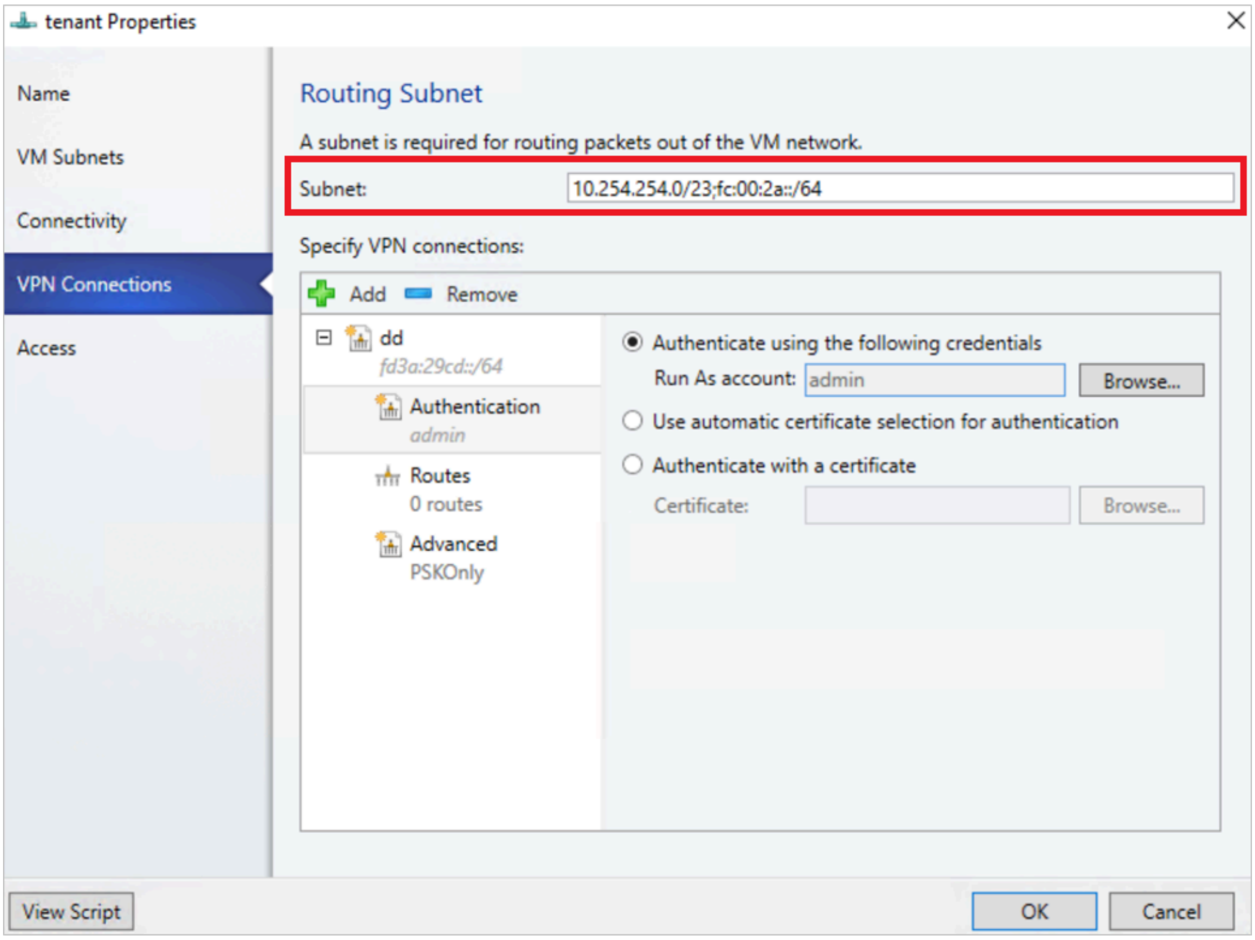
Configure Site-to-Site VPN connections using VMM

A Site-to-Site VPN connection allows you to securely connect two networks at different physical locations by using the Internet.

For Cloud Service Providers (CSPs) that host many tenants in their datacenter, SDN RAS gateway provides a multi-tenant gateway solution that allows your tenants to access and manage their resources over Site-to-Site VPN connections from remote sites, which in turn allows network traffic between virtual resources in your datacenter and their physical network.

VMM 2022 supports dual stack (Ipv4 + Ipv6) for SDN components.

To enable IPv6 for site-to-site VPN connection, routing subnet must be both IPv4 and IPv6. For gateway to work in IPv6, provide IPv4 and IPv6 addresses separated by semicolon (;) and provide IPv6 address in the remote endpoint. For example, *192.0.2.1/23;2001:0db8:85a3:0000:0000:8a2e:0370::/64*. For specifying VIP range, don't use the shortened form of the IPv6 address; use '2001:db8:0:200:0:0:0:7' format instead of '2001:db8:0:200::7'.



Routing Subnet

A subnet is required for routing packets out of the VM network.

Subnet: 10.254.254.0/23;fc:00:2a::/64

Specify VPN connections:

dd
fd3a:29cd::/64
Authentication
admin
Routes
0 routes
Advanced
PSKOnly

● Authenticate using the following credentials

Run As account: admin

○ Use automatic certificate selection for authentication

○ Authenticate with a certificate

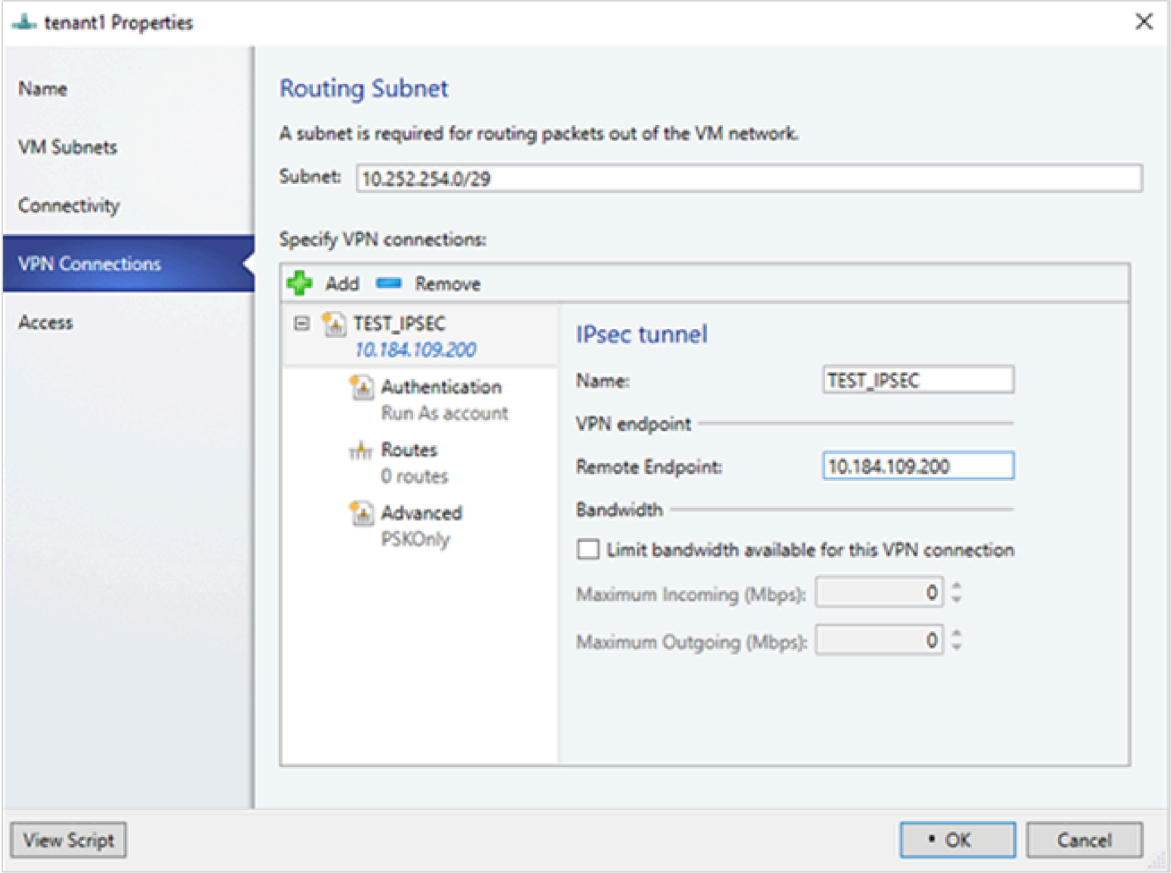
Certificate:

Configure IPSec connection

Use the following procedure:

1. Select the VM Network that you want to configure a Site-to-Site IPSec connection and select **Connectivity**.
2. Select **Connect to another network through a VPN tunnel**. Optionally, to enable BGP peering in your datacenter, select **Enable Border Gateway Protocol (BGP)**.
3. Select the network controller service for the gateway device.
4. Select the **VPN Connections** > **Add** > **Add IPSec Tunnel**.
5. Enter a subnet as shown in the following diagram. This subnet is used to route packets out of the VM Network. You don't need to pre-configure this subnet in

your datacenter.


tenant1 Properties

Routing Subnet

A subnet is required for routing packets out of the VM network.

Subnet: 10.252.254.0/29

Specify VPN connections:

TEST_IPSEC 10.184.109.200

Authentication: Run As account

Routes: 0 routes

Advanced: PSKOnly

IPsec tunnel

Name: TEST_IPSEC

VPN endpoint

Remote Endpoint: 10.184.109.200

Bandwidth

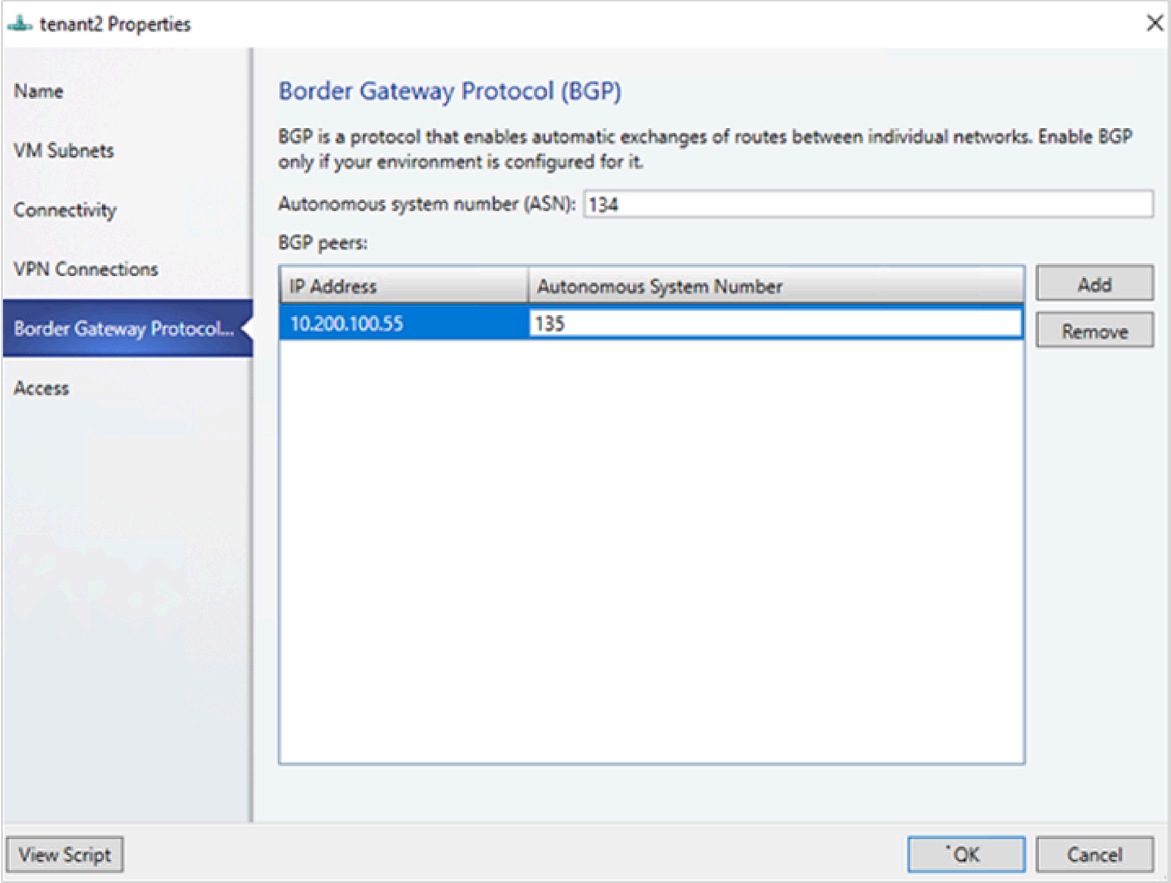
□ Limit bandwidth available for this VPN connection

Maximum Incoming (Mbps): 0

Maximum Outgoing (Mbps): 0

6. Enter a name for the connection, and the IP address of the remote endpoint. Optionally, configure the bandwidth.
7. In **Authentication**, select the type of authentication you want to use. If you choose to authenticate by using a Run as account, create a user account with a username, and the IPSec key as the password for the account.
8. In **Routes**, enter all the remote subnets that you want to connect to. If you've selected **Enable Border Gateway Protocol (BGP)** in the **Connectivity** page, routes aren't required.
9. On the **Advanced** tab, accept the default settings.
10. If you've selected **Enable Border Gateway Protocol (BGP)** in the Connectivity page, then you can fill out your ASN, peer BGP IP, and its ASN on the **Border Gateway**

Protocol wizard page as shown below.



tenant2 Properties

Border Gateway Protocol (BGP)

BGP is a protocol that enables automatic exchanges of routes between individual networks. Enable BGP only if your environment is configured for it.

Autonomous system number (ASN): 134

BGP peers:

IP Address	Autonomous System Number
10.200.100.55	135

11. To validate the connection, try to ping the remote endpoint IP address from one of the virtual machines on your VM network.

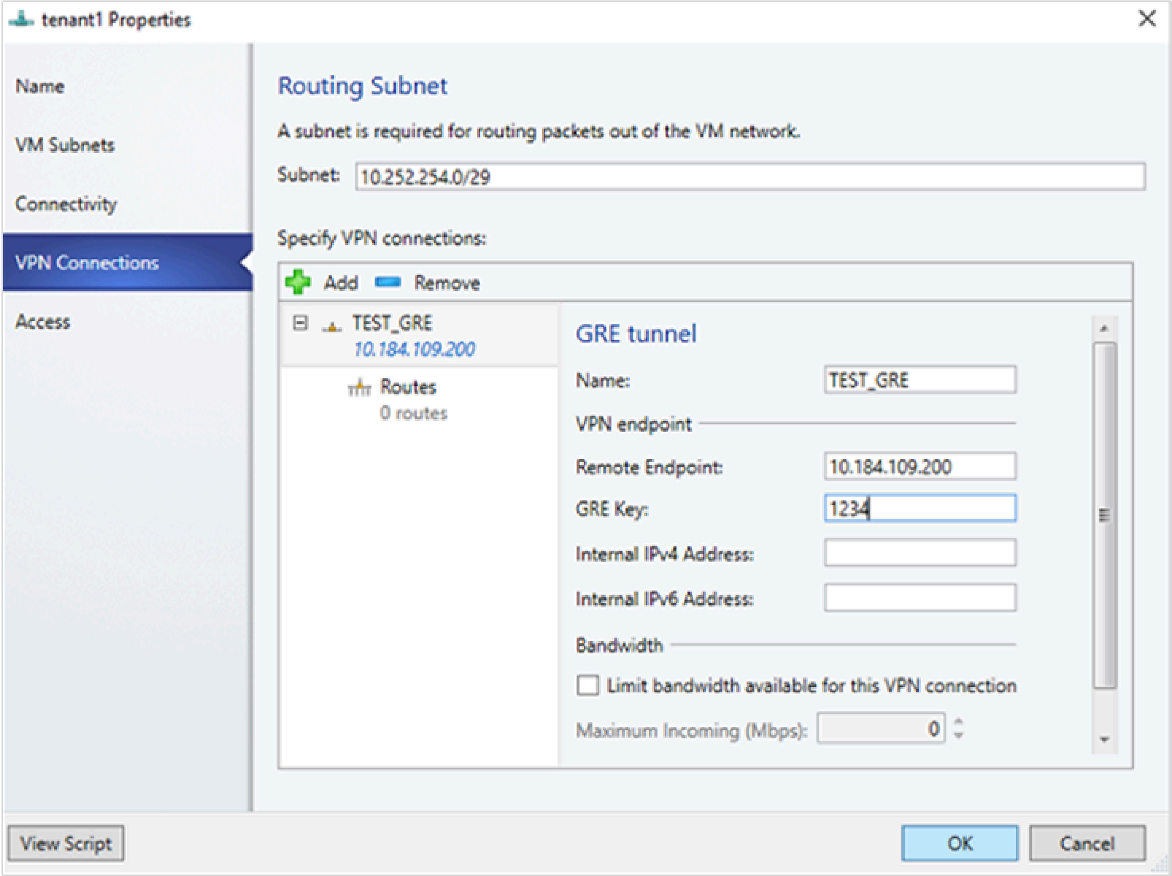
Configure GRE tunneling

GRE tunnels enable connectivity between tenant virtual networks and external networks. Since the GRE protocol is lightweight and support for GRE is available on most of the network devices, it becomes an ideal choice for tunneling where encryption of data isn't required. GRE support in Site-to-Site (S2S) tunnels facilitates traffic forwarding between tenant virtual networks and tenant external networks.

Use the following procedure:

1. Select the VM network where you want to configure a S2S GRE connection, and select **Connectivity**.
2. Select **Connect to another network through a VPN tunnel**. Optionally, to enable BGP peering in your datacenter, select **Enable Border Gateway Protocol (BGP)**.
3. Select the Network Controller Service for the Gateway Device.
4. Select **VPN Connections** > **Add** > **Add GRE Tunnel**.
5. Enter a subnet as shown in the following diagram. This subnet is used to route packets out of the VM network. This subnet doesn't need to be preconfigured in

your datacenter.



tenant1 Properties

Routing Subnet

A subnet is required for routing packets out of the VM network.

Subnet: 10.252.254.0/29

Specify VPN connections:

GRE tunnel

Name: TEST_GRE

VPN endpoint

Remote Endpoint: 10.184.109.200

GRE Key: 1234

Internal IPv4 Address:

Internal IPv6 Address:

Bandwidth

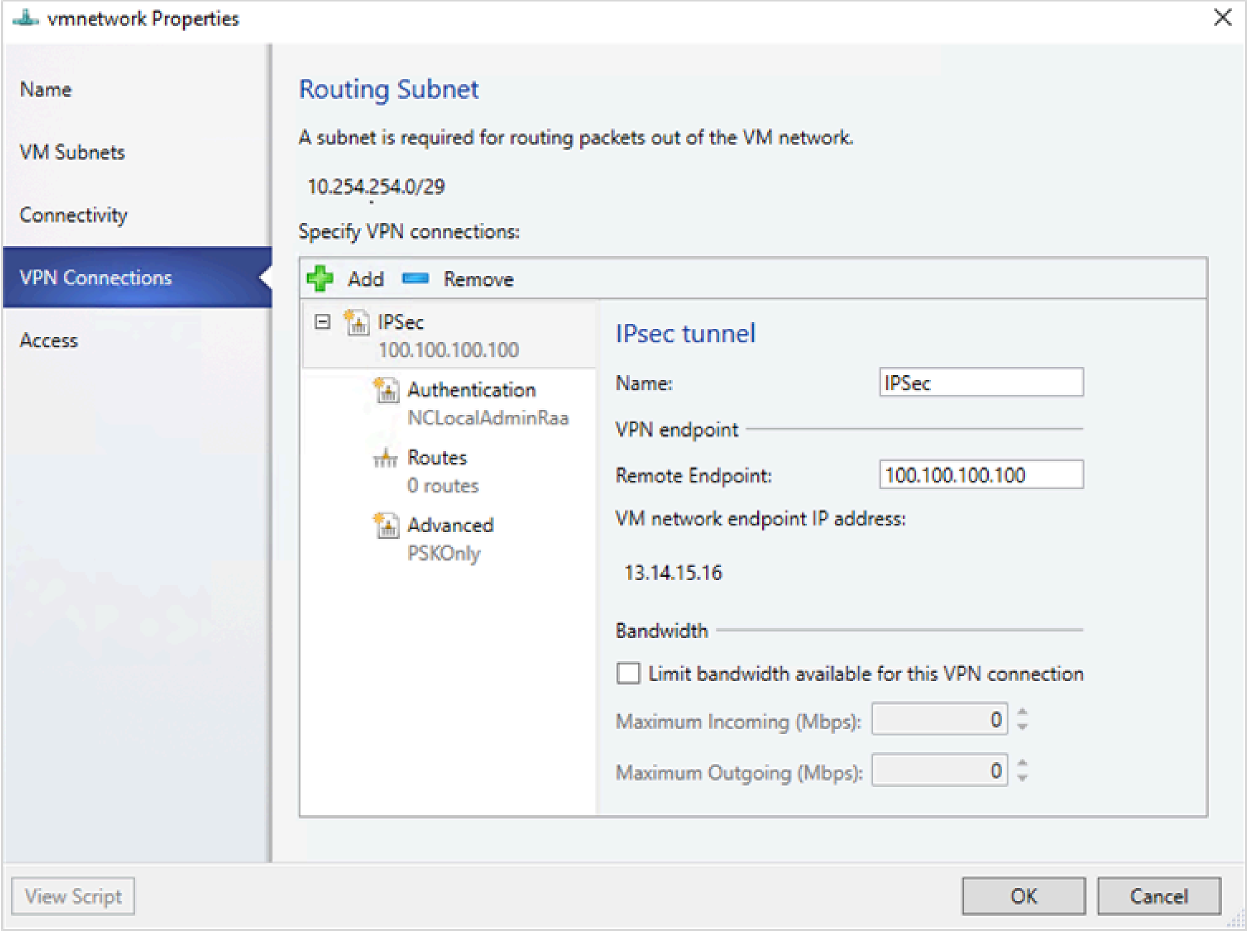
□ Limit bandwidth available for this VPN connection

Maximum Incoming (Mbps): 0

6. Enter a connection name, and specify the IP address of the remote endpoint.
7. Enter the **GRE key**.
8. Optionally, you can complete the other fields on this screen; these values aren't needed to set up a connection.
9. In **Routes**, add all the remote subnets that you want to connect to. If you selected **Enable Border Gateway Protocol (BGP)** in **Connectivity**, you can leave this screen blank and instead complete your ASN, peer BGP IP, and ASN fields on the **Border Gateway Protocol** tab.
10. You can use the defaults for the remaining settings.
11. To validate the connection, try to ping the remote endpoint IP address from one of the virtual machines on the VM network.

Configure IPsec and GRE connections on the remote site

On the remote peer device, use the **VM network endpoint IP address** from the VMM UI as destination Address while setting up the IPSec\GRE connection.



Routing Subnet

A subnet is required for routing packets out of the VM network.

10.254.254.0/29

Specify VPN connections:

- IPSec 100.100.100.100
  - Authentication NCLocalAdminRaa
  - Routes 0 routes
  - Advanced PSKOnly

IPsec tunnel

Name: IPSec

VPN endpoint

Remote Endpoint: 100.100.100.100

VM network endpoint IP address:

13.14.15.16

Bandwidth

☐ Limit bandwidth available for this VPN connection

Maximum Incoming (Mbps): 0

Maximum Outgoing (Mbps): 0

Configure L3 forwarding

L3 forwarding enables connectivity between the physical infrastructure in the datacenter and the virtualized infrastructure in the Hyper-V network virtualization cloud.

Using L3 forwarding connection, tenant network virtual machines can connect to a physical network through the Windows Server 2016/2019/2022 SDN Gateway, which is already configured in an SDN environment. In this case, the SDN gateway acts as a router between the virtualized network and the physical network.

To learn more, check these articles: Windows server gateway as a forwarding gateway and RAS gateway high availability.

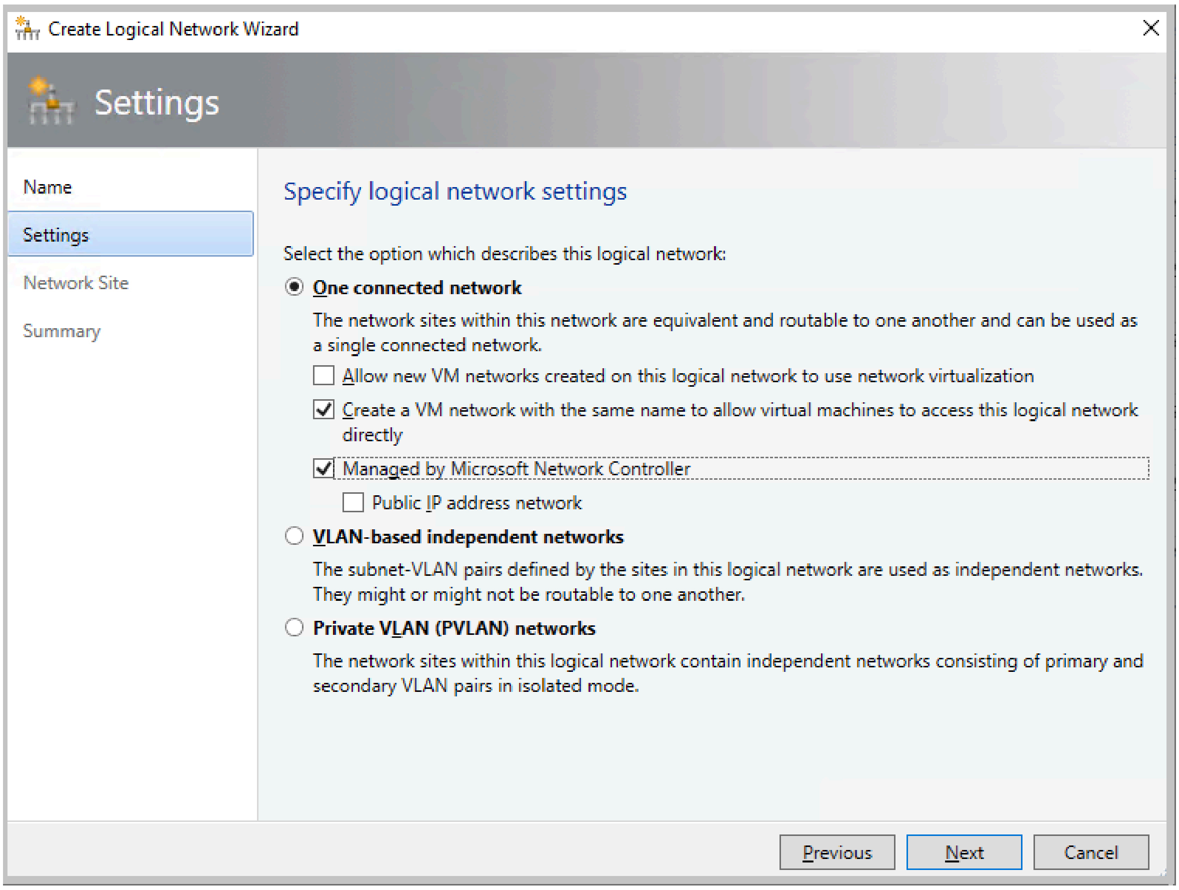
Ensure the following before you attempt to configure L3 connection:

- Ensure you're logged on as an administrator on the VMM server.
- You must configure a unique next-hop logical network, with unique VLAN ID, for each Tenant VM network for which L3 forwarding needs to be set up. There must be 1:1 mapping between a tenant network and corresponding physical network (with unique VLAN ID).

Use the following steps to create the next-hop logical network in VMM:

1. On the VMM console, select **Logical Networks**, right-click and select **Create Logical Network**.

2. In the **Settings** page, choose **One connected network** and select **Create a VM network with the same name to allow virtual machines to access this logical network directly** and **Managed by Microsoft Network Controller**.



Specify logical network settings

Select the option which describes this logical network:

● **One connected network**

The network sites within this network are equivalent and routable to one another and can be used as a single connected network.

□ Allow new VM networks created on this logical network to use network virtualization

☑ Create a VM network with the same name to allow virtual machines to access this logical network directly

☑ Managed by Microsoft Network Controller

□ Public IP address network

○ **VLAN-based independent networks**

The subnet-VLAN pairs defined by the sites in this logical network are used as independent networks. They might or might not be routable to one another.

○ **Private VLAN (PVLAN) networks**

The network sites within this logical network contain independent networks consisting of primary and secondary VLAN pairs in isolated mode.

3. Create an IP Pool for this new logical network. IP address from this pool is required for setting up L3 forwarding.

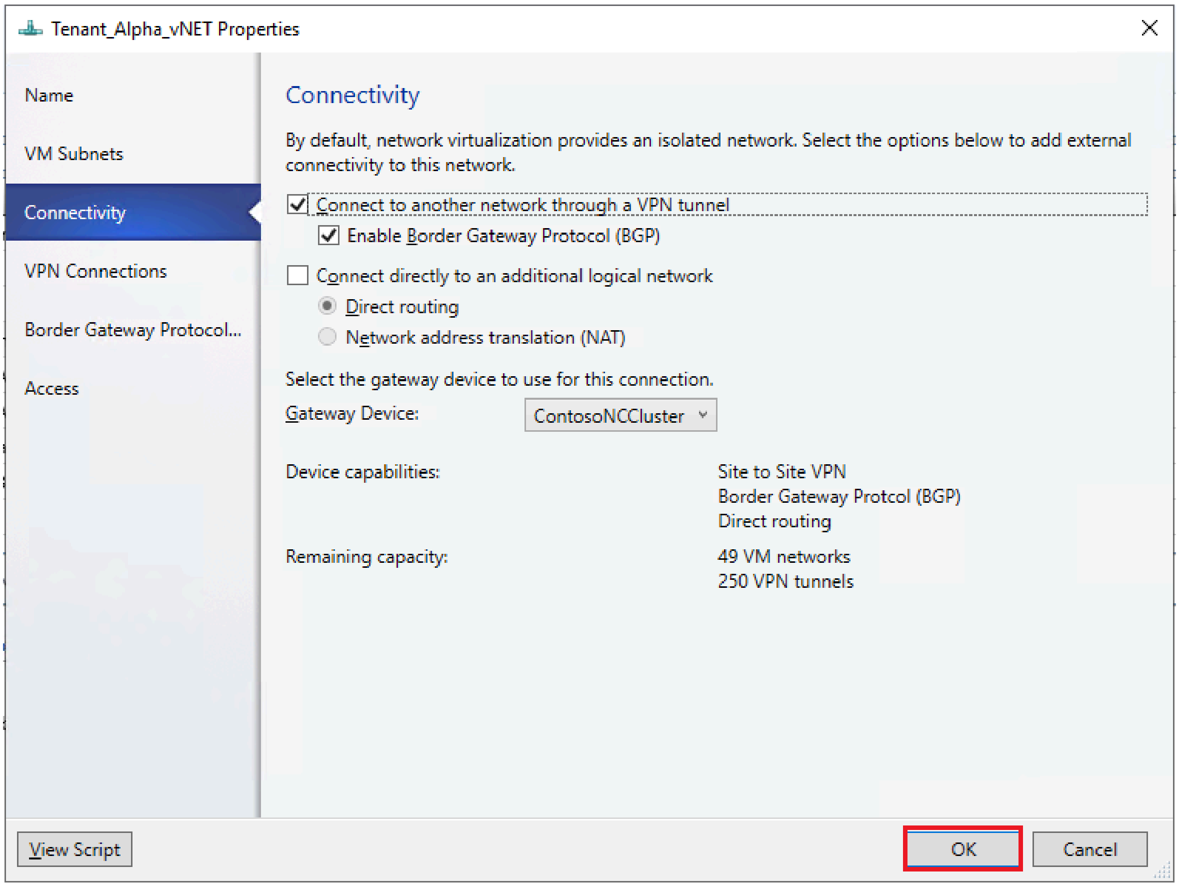
Use the following steps to configure L3 forwarding:

> ⓘ **Note**
>
> You can't limit bandwidth in L3 VPN connection.

1. In the VMM console, select the tenant virtual network that you want to connect to the physical network through L3 gateway.

2. Right-click the selected tenant virtual network, select **Properties** > **Connectivity**.

3. Select **Connect to another network through a VPN tunnel**. Optionally, to enable BGP peering in your datacenter, select **Enable Border Gateway Protocol (BGP)**.



Tenant_Alpha_vNET Properties

Name
VM Subnets
Connectivity
VPN Connections
Border Gateway Protocol...
Access

Connectivity

By default, network virtualization provides an isolated network. Select the options below to add external connectivity to this network.

☑ Connect to another network through a VPN tunnel

☑ Enable Border Gateway Protocol (BGP)

□ Connect directly to an additional logical network

● Direct routing

○ Network address translation (NAT)

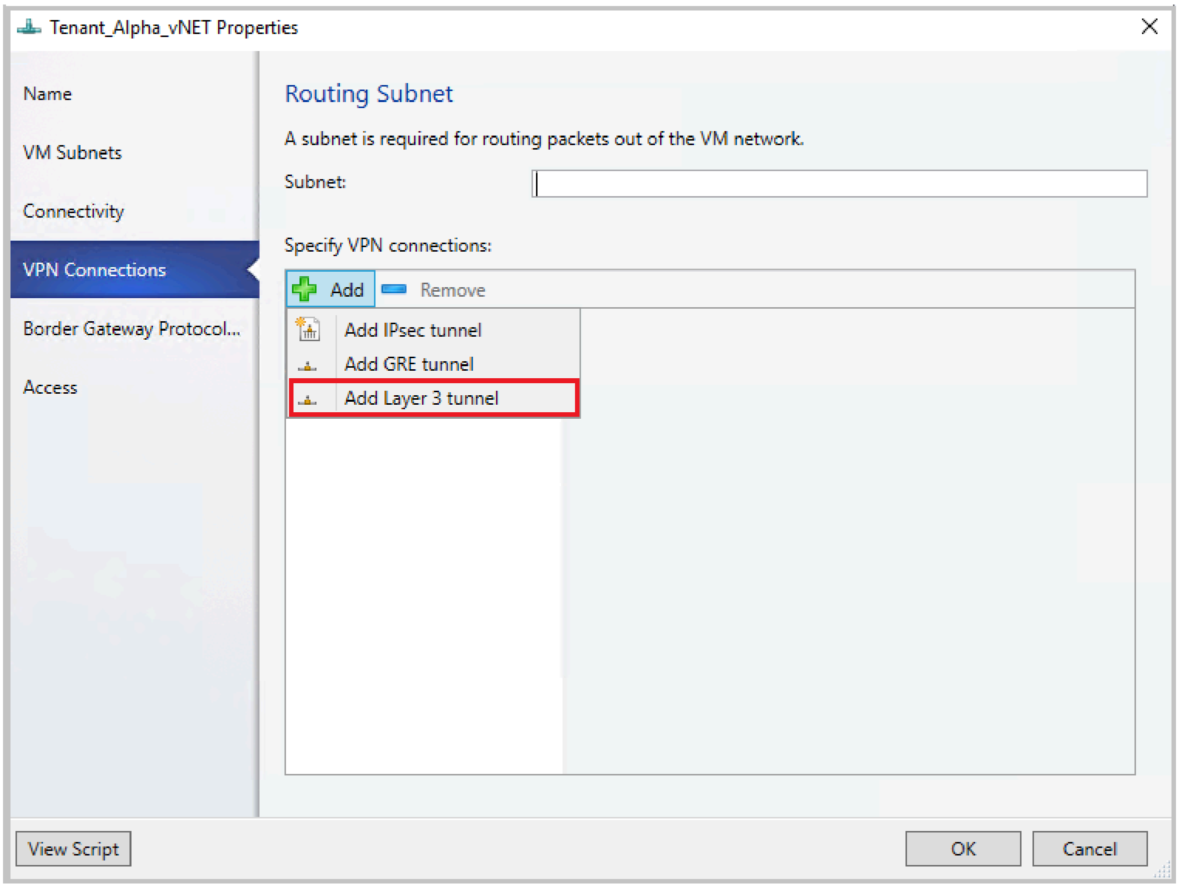
Select the gateway device to use for this connection.

Gateway Device: ContosoNCCluster

Device capabilities:	Site to Site VPN Border Gateway Protcol (BGP) Direct routing
Remaining capacity:	49 VM networks 250 VPN tunnels

4. Select the network controller service for the gateway device.

5. In the **VPN Connections** page, select **Add**> **Add Layer 3 tunnel**.



Tenant_Alpha_vNET Properties

Name
VM Subnets
Connectivity
VPN Connections
Border Gateway Protocol...
Access

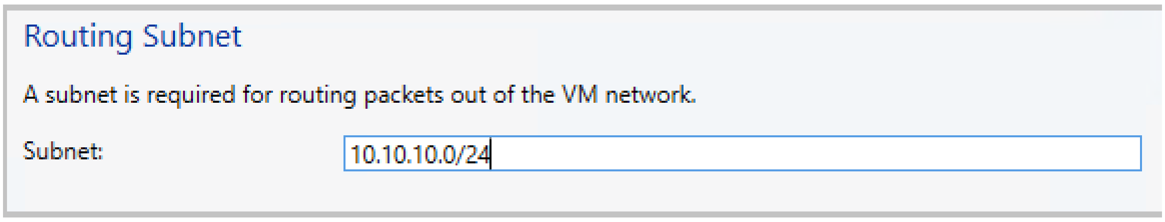
Routing Subnet

A subnet is required for routing packets out of the VM network.

Subnet:

Specify VPN connections:

6. Provide a subnet in the CIDR notation format for **Routing Subnet**. This subnet is used to route packets out of the VM network. You don't need to pre-configure this subnet in your datacenter.



Routing Subnet

A subnet is required for routing packets out of the VM network.

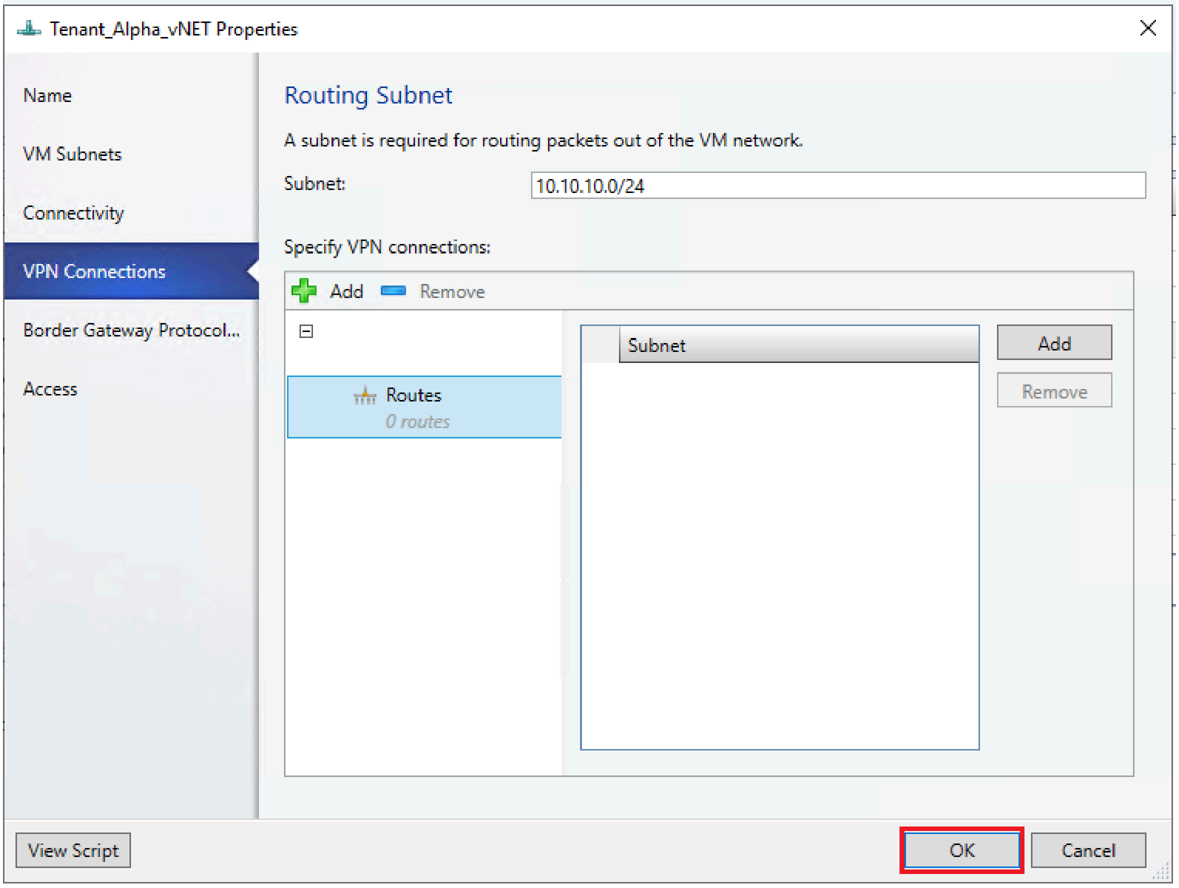
Subnet: 10.10.10.0/24

7. Use the following information and configure the L3 connection:

Expand table

Parameter	Details
Name	User-defined name for the L3 forwarding network connection.
VM Network (NextHop)	User-defined name for the next hop VM network, which was created as a prerequisite. This represents the physical network that wants to communicate with the tenant VM network. When you select *Browse*, only the *One Connected VM Networks* managed by Network service will be available for selection.
Peer IP Address	IP address of the physical network gateway, reachable over L3 logical network. This IP address must belong to the next hop logical network that you created as the prerequisite. This IP will serve as the next hop, once the traffic destined to the physical network from the tenant VM network reaches the SDN gateway. This must be an IPv4 address. There can be multiple peer IP addresses, and they must be separated by commas.
Local IP Addresses	IP addresses to be configured on the SDN gateway L3 network interface. These IP addresses must belong to the next hop logical network that you created as prerequisite. You must also provide the subnet mask. Example: 10.127.134.55/25. This must be an IPv4 address and must be in CIDR notation format. Peer IP address and Local IP addresses must be from the same Pool. These IP addresses must belong to the subnet defined in Logical Network Definition of VM Network.

- If you're using static routes, enter all the remote subnets that you want to connect to, in **Routes**.



A subnet is required for routing packets out of the VM network.

Subnet: 10.10.10.0/24

Specify VPN connections:

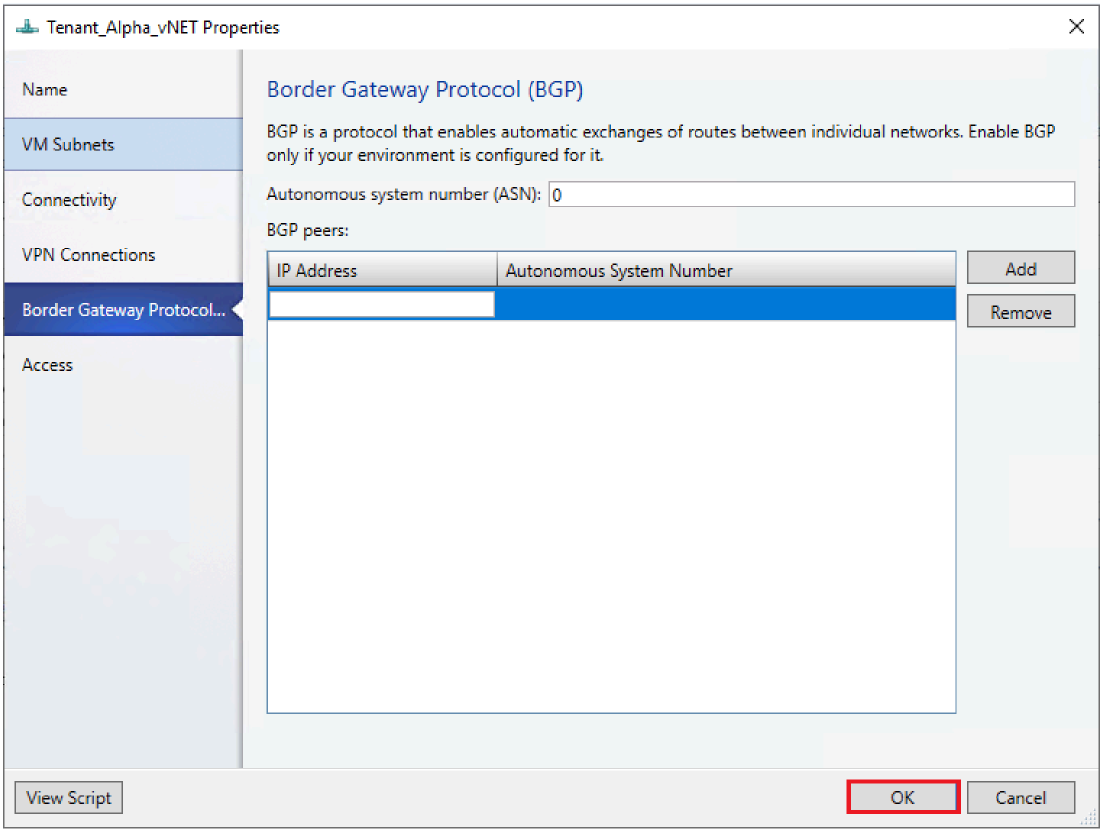
ⓘ Note

You must configure routes in your physical network, for the tenant virtual network subnets, with the next hop as the IP address of the L3 interface on the SDN gateway (Local IP address used in the creation of L3 connection). This is to ensure that the return traffic to the tenant virtual network is routed correctly through the SDN gateway.

- If you're using BGP, ensure that BGP peering is established between the SDN gateway internal interface IP address, which is present in a different compartment on the gateway VM (not the default compartment) and the peer device on the physical network.

  For BGP to work, you must do the following steps:

  1. Add BGP peer for the L3 connection. Enter your ASN, peer BGP IP, and its ASN on the **Border Gateway Protocol** page.



Tenant_Alpha_vNET Properties

Border Gateway Protocol (BGP)

BGP is a protocol that enables automatic exchanges of routes between individual networks. Enable BGP only if your environment is configured for it.

Autonomous system number (ASN): 0

BGP peers:

IP Address	Autonomous System Number

2. Determine the SDN gateway internal address as detailed in the following section.

3. Create BGP peer on the remote end (physical network gateway). While creating the BGP peer, use the SDN gateway internal address (as determined in the previous step) as the peer IP address.

4. Configure a route on the physical network with the destination as the SDN gateway internal address and the next hop as the L3 interface IP address (Local IP address value used when creating L3 connection).

Determine the SDN gateway internal address

Use the following procedure:

Run the following PowerShell cmdlets on a network controller installed computer or a computer that was configured as a network controller client:

```PowerShell
$gateway = Get-NetworkControllerVirtualGateway -ConnectionUri <REST uri of
your deployment>
$gateway.Properties.NetworkConnections.Properties.IPAddresses
```

The results of this command can display multiple virtual gateways depending on how many tenants have configured gateway connections. Each virtual gateway can have multiple connections (IPSec, GRE, L3).

As you already know the L3 interface IP address (LocalIPAddresses) of the connection, you can identify the correct connection based on that IP address. After you've the correct network connection, run the following command (on the corresponding virtual gateway) to get the BGP router IP address of the virtual gateway.

PowerShell

```
$gateway.Properties.BgpRouters.Properties.RouterIp
```

The result of this command provides the IP address that you must configure on the remote router as the peer IP Address.

Set up the traffic selector from VMM PowerShell

Use the following procedure:

> ⓘ **Note**
>
> Values used are examples only.

1. Create the traffic selector by using the following parameters.

   PowerShell

   ```
   $t= new-object Microsoft.VirtualManager.Remoting.TrafficSelector

   $t.Type=7 // IPV4=7, IPV6=8

   $t.ProtocolId=6 // TCP =6, reference:
   https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers

   $t.PortEnd=5090

   $t.PortStart=5080

   $t.IpAddressStart=10.100.101.10

   $t.IpAddressEnd=10.100.101.100
   ```

2. Configure the above traffic selector by using **-LocalTrafficSelectors** parameter of **Add-SCVPNConnection** or **Set-SCVPNConnection**.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Configure guest clusters in SDN through VMM

Article • 07/24/2024

This article explains how to configure guest clusters in SDN using System Center Virtual machine Manager (VMM).

With the introduction of the network controller, VMs that are connected to the virtual network are only permitted to use the IP address that network controller (NC) assigns for communication. NC doesn't support floating IP addresses, which are essential for technologies such as Microsoft Failover Clustering to work.

You can enable this feature by emulating the floating IP functionality through the Software Load Balancer (SLB) in SDN.

VMM supports guest clustering in SDN through an Internal Load Balancer (ILB) Virtual IP (VIP). The ILB uses probe ports, which are created on the guest cluster VMs to identify the active node. At any given time, the probe port of only the active node responds to the ILB and all the traffic directed to the VIP is routed to the active node.

Before you start

Ensure the following prerequisite:

Guesting clustering is managed through the SDN NC. Ensure you have set up SDN and deployed NC and SLB.

Procedure - configure guest clusters

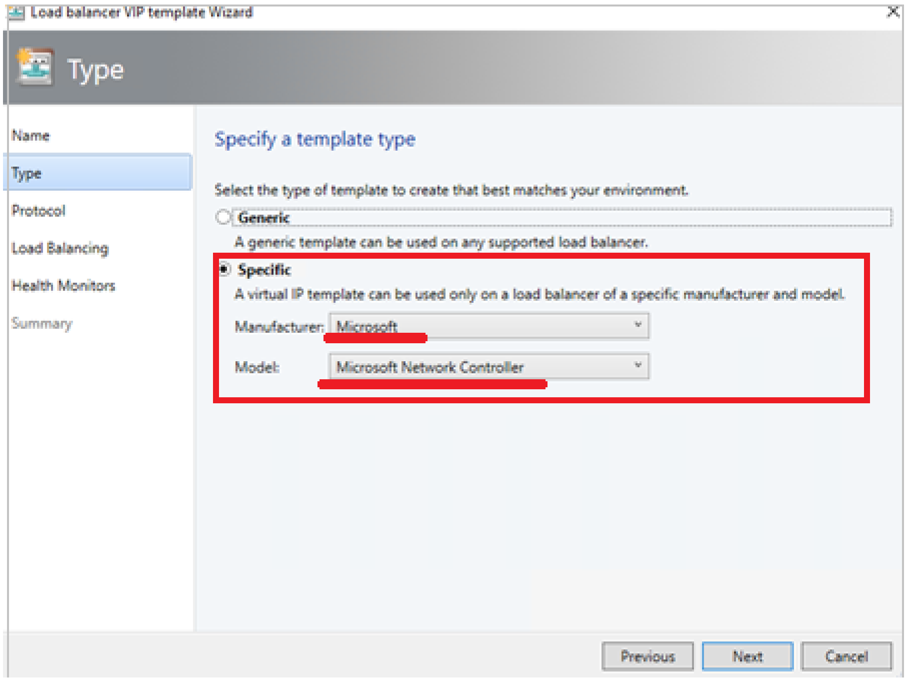
Use the following steps:

1. Create a cluster for your VMs using the information provided in this article.

   > ⓘ **Note**
   >
   > Cluster must have a ProbePort parameter set to a port of your choice. This port is required while configuring the VIP template in the next step. Note the reserved IP address you're using for this cluster. This IP will be required later while creating a VIP using the VIP template.

2. Create a VIP template. In the VMM console > **Fabric** > **Networking** > **VIP Templates**, right-click and select **Add VIP Template**.

   - In **Type**, under **Specify a template type**, select **Specific**. Select **Microsoft** from the Manufacturer dropdown and **Microsoft Network Controller** from the Model dropdown.


Load balancer VIP template Wizard

Type

Specify a template type

Select the type of template to create that best matches your environment.

○ Generic

A generic template can be used on any supported load balancer.

● Specific

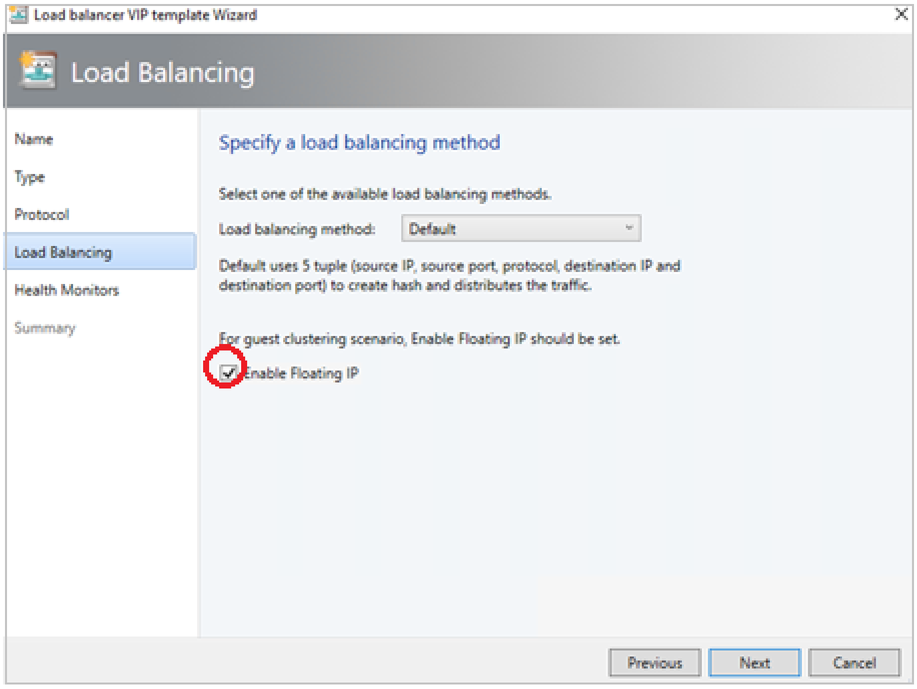
A virtual IP template can be used only on a load balancer of a specific manufacturer and model.

Manufacturer: Microsoft

Model: Microsoft Network Controller

   - Select **Next**.

   - In **Load Balancing**, select the **Enable Floating IP** checkbox.


Load balancer VIP template Wizard

Load Balancing

Specify a load balancing method

Select one of the available load balancing methods.

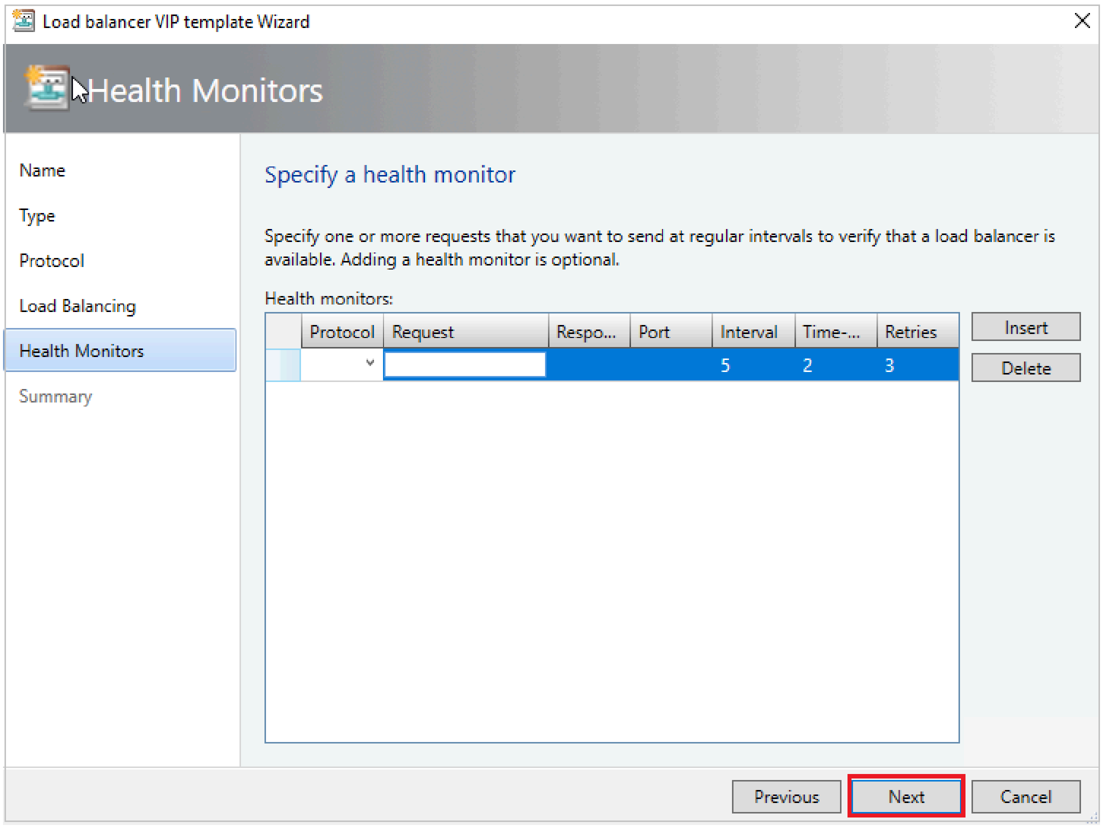
Load balancing method: Default

Default uses 5 tuple (source IP, source port, protocol, destination IP and destination port) to create hash and distributes the traffic.

For guest clustering scenario, Enable Floating IP should be set.

☑ Enable Floating IP

   - In **Health Monitor**, add the probe that would be used on the guest cluster VMs. Here, you must add the same port that was configured while clustering the hosts in the previous step.



Specify a health monitor

Specify one or more requests that you want to send at regular intervals to verify that a load balancer is available. Adding a health monitor is optional.

Health monitors:

	Protocol	Request	Respo...	Port	Interval	Time-...	Retries
					5	2	3

3. Using PowerShell, create a VIP using the VIP template.

ⓘ Note

As explained at the beginning of this article, an Internal Load Balancer VIP is being implemented to support Guest Clustering. The PowerShell script for creating a VIP from the VIP template to Load Balance Internal Network traffic is provided below.

Use the sample script here to create a VIP and load balance the internal network. Modify the parameters as required, based on the following details:

- LBServiceName – Name of the Network Controller service.
- VipMemberNames – Names of the VMs in the cluster.
- VipNetworkName – Name of the tenant network.
- VipAddress – The reserved IP address from the tenant network, which was used in step 2 as the IP address for the VM cluster.
- VipTemplateName – Name of the VIP template created in step 3 above.
- VipName – Any friendly name you want to refer to the VIP by.

Feedback

Update the network controller server certificate

Article • 07/24/2024

Network controller (NC) uses a certificate for Northbound communication with REST clients, such as VMM, and Southbound communication with Hyper-V hosts and software load balancers.

You can change or update this certificate in the following scenarios after you deploy the NC.

- The certificate has expired
- You want to move from a self-signed certificate to a certificate that is issued by a certificate authority (CA).

  > ⓘ **Note**
  >
  > If you renew the existing certificate with the same key, these steps are not required.

Before you start

Ensure that you create a new SSL certificate with the existing network controller's REST name. Learn more.

Update the server certificate

1. If the certificate is self-signed, do the following:
   - Certificate with private key - Export the certificate and import it on all the NC nodes' **My** store.
   - Certificate without a private key - Export the certificate and import it on all the NC nodes' **Root** store.
2. If the certificate is a CA issued certificate, import it on all network controller nodes' **My** store.

   > ⓘ **Note**

> DO NOT remove the current certificate from the NC nodes. You should validate the updated certificate before you remove the existing one. Proceed with the rest of the steps to update the certificate.

3. Update the server certificate by executing the following PowerShell command on one of the NC nodes.

   PowerShell

   ```
   $certificate = Get-ChildItem -Path Cert:\LocalMachine\My | Where
   {$_.Thumbprint -eq “Thumbprint of new certificate”}
   Set-NetworkController -ServerCertificate $certificate
   ```

4. Update the certificate used for encrypting the credentials stored in the NC by executing the following command on one of the NC nodes.

   PowerShell

   ```
   $certificate = Get-ChildItem -Path Cert:\LocalMachine\My | Where
   {$_.Thumbprint -eq “Thumbprint of new certificate”}
   Set-NetworkControllerCluster -CredentialEncryptionCertificate
   $certificate
   ```

5. Retrieve a server REST resource by executing the following PowerShell command on one of the NC nodes.

   PowerShell

   ```
   Get-NetworkControllerServer -ConnectionUri <REST uri of your
   deployment>
   ```

6. In the Server REST resource, navigate to the **Credentials** object and check the credential of type **X509Certificate** with a value matching your certificate's thumbprint. Note the credential resource ID.

   PowerShell

   ```
   "Connections":
   {
      {
         "ManagementAddresses":[ “contoso.com" ],
         "CredentialType":  "X509Certificate",
   ```

```
        "Protocol":  null,
        "Port":  null,
        "Credential": {
                          "Tags":  null,
                          "ResourceRef":  "/credentials/<credential
resource Id>,
                          "InstanceId":  "00000000-0000-0000-0000-
000000000000",
                          …
                          …
                      }
    }
}
```

7. Update the credential REST resource of type **X509Certificate** retrieved above with the thumbprint of the new certificate.

   Execute this PowerShell cmdlet on any of the NC nodes.

   PowerShell

   ```
   $cred=New-Object
   Microsoft.Windows.Networkcontroller.credentialproperties
   $cred.type="X509Certificate"
   $cred.username=""
   $cred.value="<thumbprint of the new certificate>"
   New-NetworkControllerCredential -ConnectionUri <REST uri of the
   deployment> -ResourceId <credential resource Id> -Properties
   $cred
   ```

8. If the new certificate is a self-signed certificate, provision the certificate (without the private key) in the trusted root certificate store of all the Hyper-V hosts and software load balancer MUX virtual machines.

9. Provision the NC certificate (without the private key) in the trusted root certificate store of the VMM machine using the following PowerShell cmdlet:

   PowerShell

   ```
   $certificate = Get-SCCertificate -ComputerName "NCRestName"
   $networkservice = Get-SCNetworkService | Where {$_.IsNetworkController
   -eq $true}
   Set-SCNetworkService -ProvisionSelfSignedCertificatesforNetworkService
   $true -Certificate
   $certificate -NetworkService $networkservice
   ```

- **NetworkService** is the network controller service, **Certificate** is the new NC server certificate.
- **ProvisionSelfSignedCertificatesforNetworkService** is **$true** if you're updating to a self-signed certificate.

10. Verify that the connectivity is working fine with the updated certificate.

    You can now remove the previous certificate from the NC nodes.

Next steps

Validate the NC deployment to ensure that the deployment is successful.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Configure SLB VIPs through VMM service templates

Article • 07/24/2024

Software Defined Networking (SDN) can use Software Load Balancing (SLB) to evenly distribute network traffic among workloads managed by service provider and tenants.

System Center Virtual Machine Manager (VMM) supports configuration of SLB VIPs while deploying multi-tier application by using service templates and also supports both public and internal load balancing.

Before you begin

Ensure the following prerequisites are met:

- Deployed SDN Network Controller.
- Deployed SDN Software load balancer.

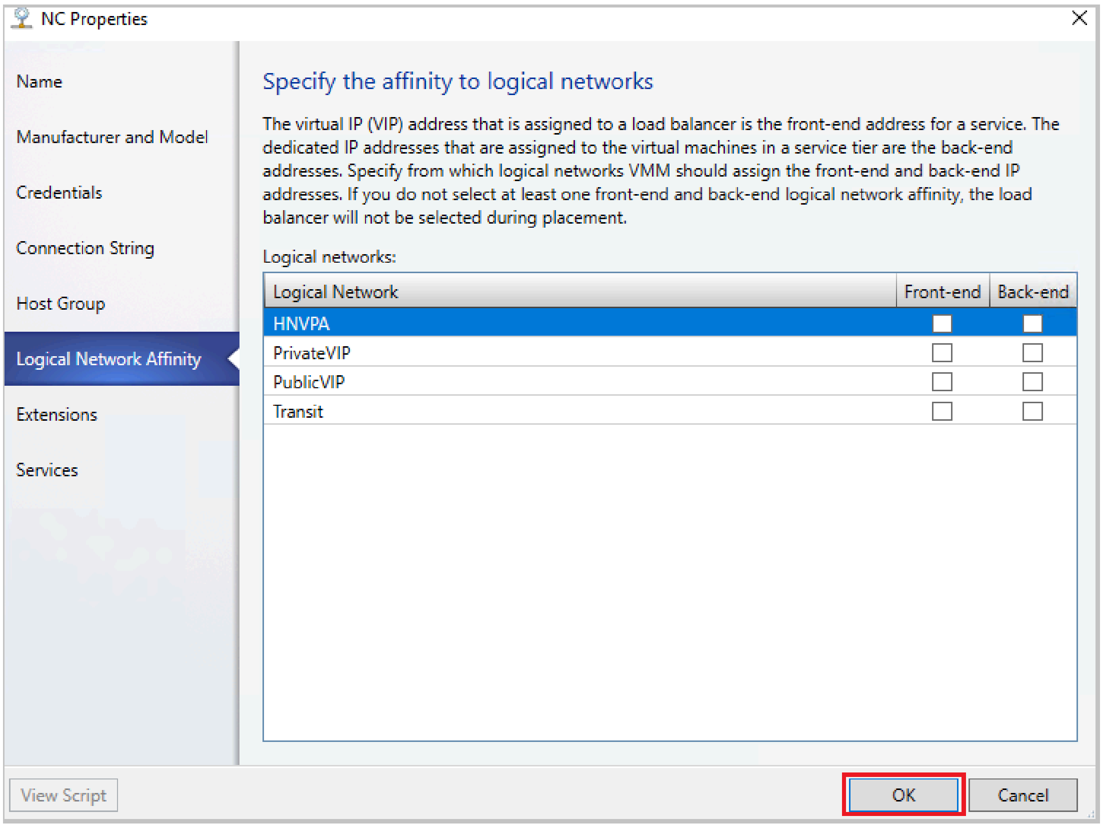
Procedure to create SLB VIPs

Use the following steps:

1. Specify the affinity to logical networks.

    - In the VMM console, select **Fabric** > **Network Service** > **Network Controller** > **Properties** > **Logical Network Affinity** page.

    - Specify the Front-end and Back-end networks available for load balancing and select **OK**.



Specify the affinity to logical networks

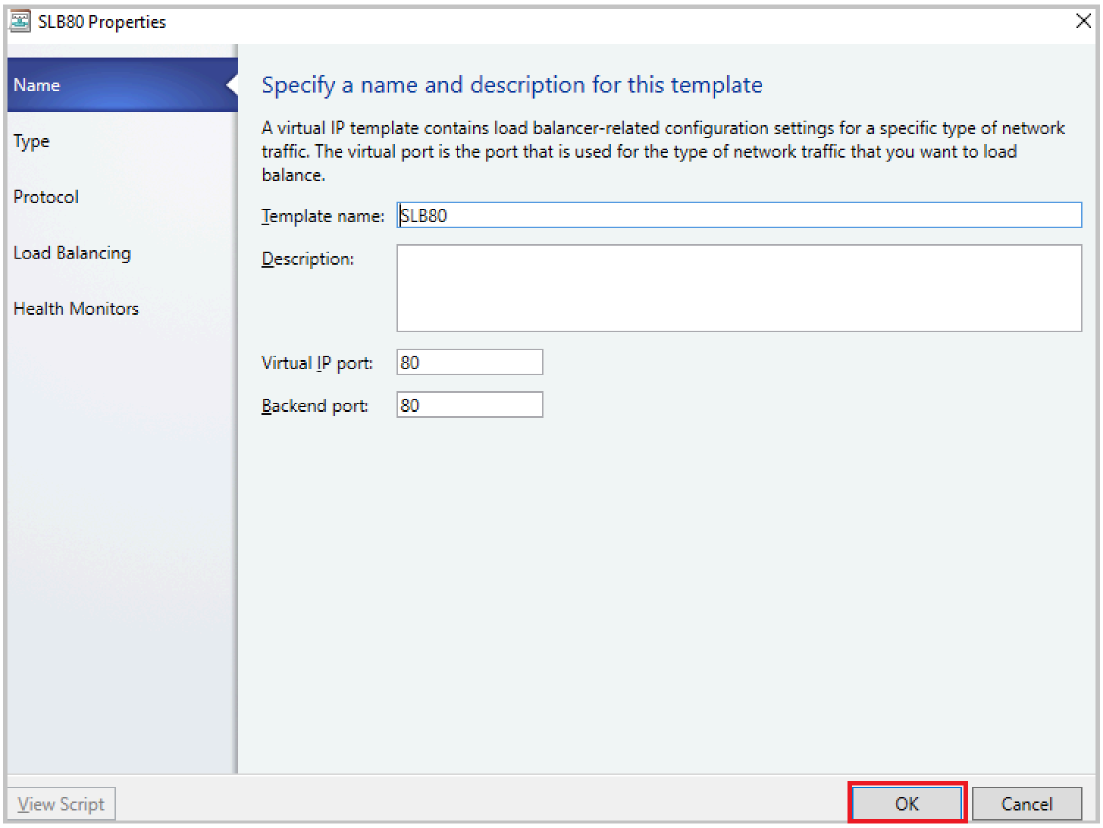
The virtual IP (VIP) address that is assigned to a load balancer is the front-end address for a service. The dedicated IP addresses that are assigned to the virtual machines in a service tier are the back-end addresses. Specify from which logical networks VMM should assign the front-end and back-end IP addresses. If you do not select at least one front-end and back-end logical network affinity, the load balancer will not be selected during placement.

Logical networks:

Logical Network	Front-end	Back-end
HNVPA	□	□
PrivateVIP	□	□
PublicVIP	□	□
Transit	□	□

2. Create a VIP template.

- In the VMM console, select **Fabric** > **Create VIP Template**.
- In the **Load Balancer VIP Template Wizard** > **Name**, specify the template name and description.
- In the **Virtual IP port**, specify the port that will be used for the type of network traffic you want to balance.
- In the **Backend port**, specify the port on which the backend server is listening for requests.



SLB80 Properties

Specify a name and description for this template

A virtual IP template contains load balancer-related configuration settings for a specific type of network traffic. The virtual port is the port that is used for the type of network traffic that you want to load balance.

Template name: SLB80

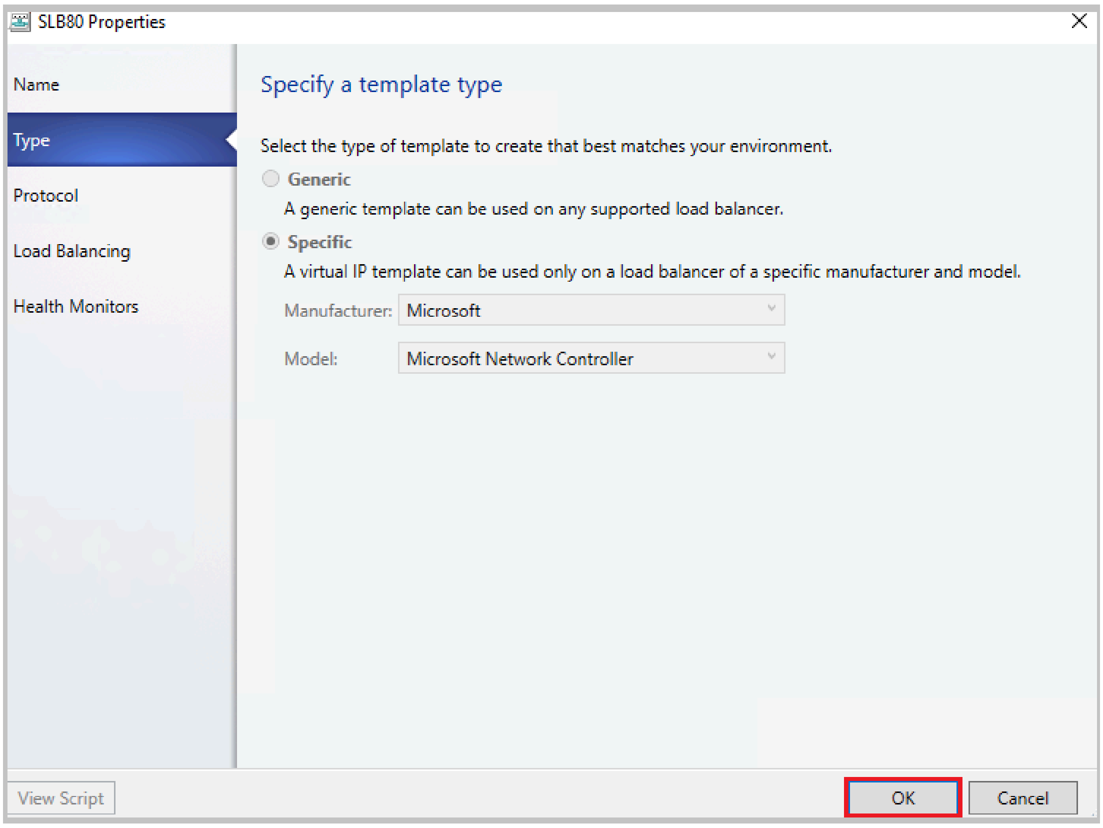
Description:

Virtual IP port: 80

Backend port: 80

- In **Type**, under **Specify a template type**, select **Specific**. Select **Microsoft** from the Manufacturer dropdown and **Microsoft Network Controller** from the Model dropdown.

- Select **Next**.



SLB80 Properties

Specify a template type

Select the type of template to create that best matches your environment.

○ Generic

A generic template can be used on any supported load balancer.

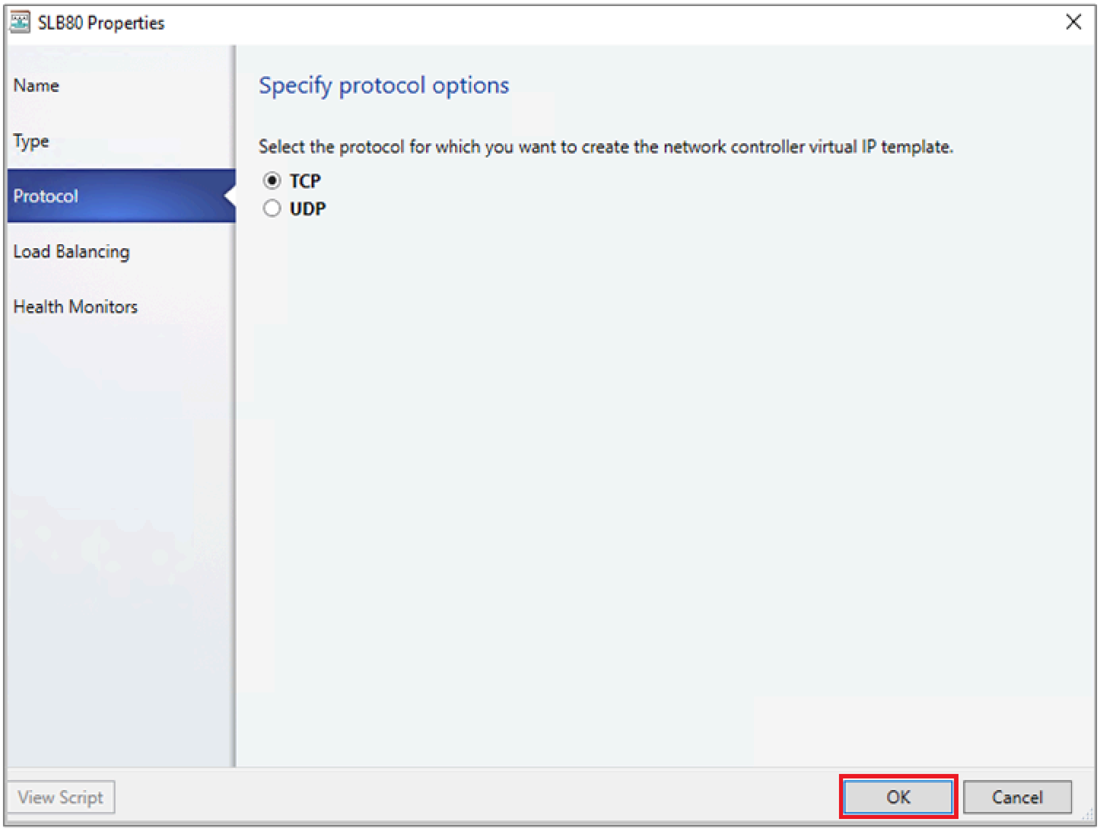
● Specific

A virtual IP template can be used only on a load balancer of a specific manufacturer and model.

Manufacturer: Microsoft

Model: Microsoft Network Controller

- In **Protocol**, specify protocol options. Select **OK**.

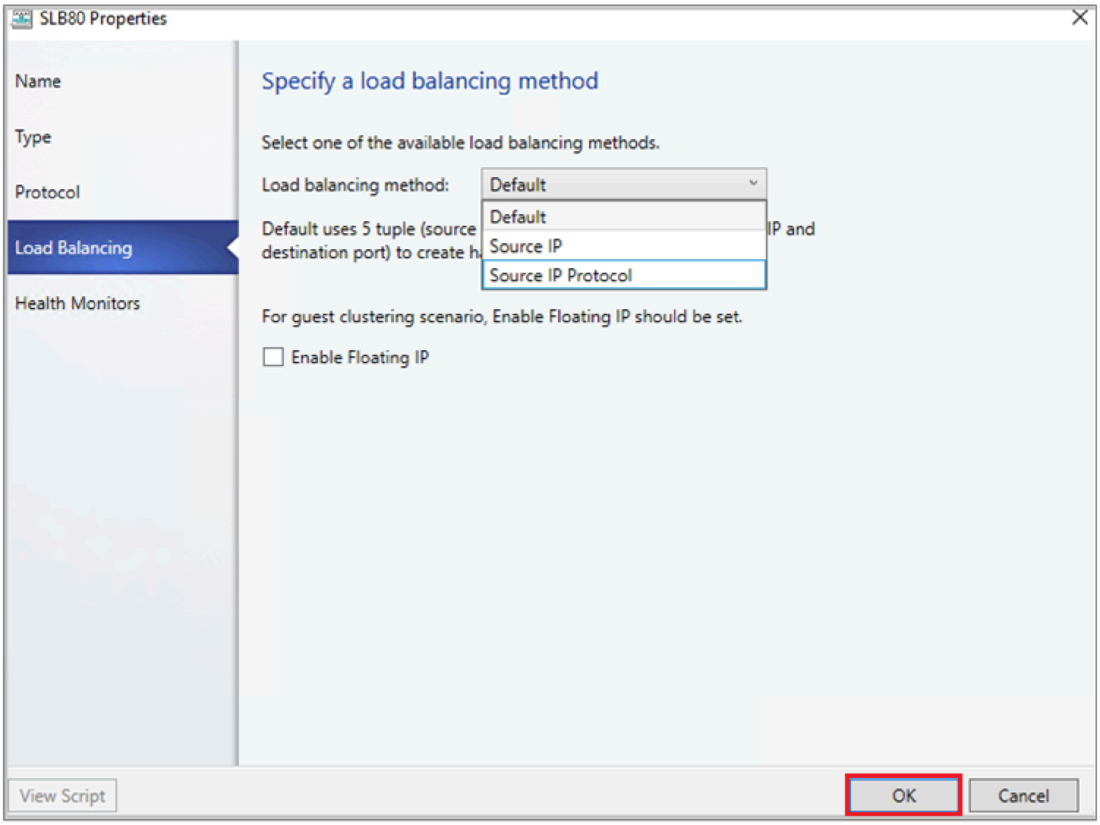


Specify protocol options

Select the protocol for which you want to create the network controller virtual IP template.

● TCP
○ UDP

- In **Load Balancing method**, select the method and select **OK**.



Specify a load balancing method

Select one of the available load balancing methods.

Load balancing method: Default

Default
Source IP
Source IP Protocol

Default uses 5 tuple (source … IP and destination port) to create h…

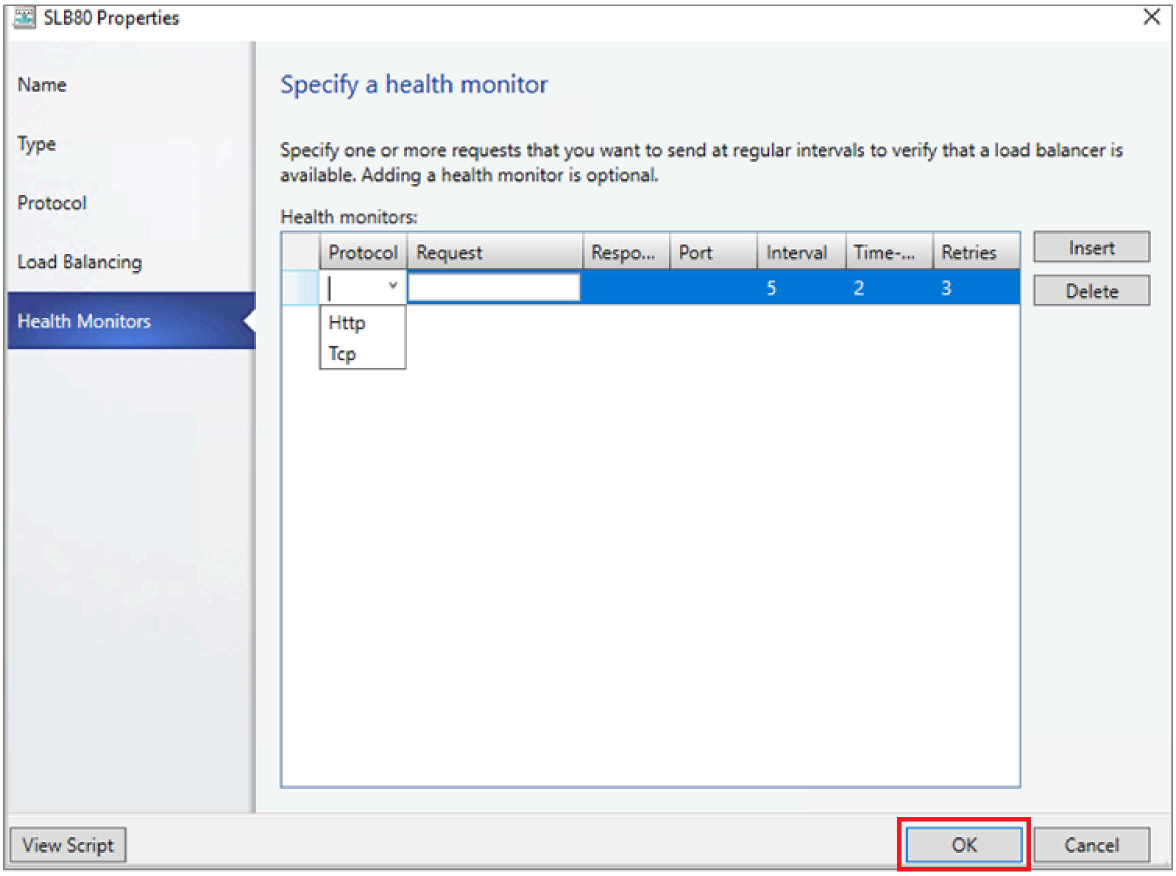
For guest clustering scenario, Enable Floating IP should be set.

□ Enable Floating IP

- In **Health Monitors**, you can optionally specify that a verification must run against the load balancer at regular intervals. To add a health monitor, specify the protocol and the request. For example, entering the command GET makes an HTTP GET request for the home page of the load balancer and checks for a header response. You can also modify the response type, monitoring interval, timeout, and retries.

ⓘ **Note**

The timeout must be less than the interval.



Specify a health monitor

Specify one or more requests that you want to send at regular intervals to verify that a load balancer is available. Adding a health monitor is optional.

Health monitors:

Protocol	Request	Respo...	Port	Interval	Time-...	Retries
				5	2	3

- In **Summary**, confirm the settings and select **Finish** to create the VIP template.

3. Configure SLB VIP while deploying Service

- If the service template isn't open, select **Library** > **Templates** > **Service Templates** and open it.
- Select **Actions** > **Open Designer**.
- In the **Service Template Designer**, select the **Service Template Components group** > **Add Load Balancer**.
- Select the load balancer object. You'll identify it with the VIP template name.
- Select **Tool** > **Connector**. Select the Server connection associated with the template and then select a NIC object to connect the load balancer to the adapter. In the **NIC properties**, check the address types and ensure that the MAC address is static.

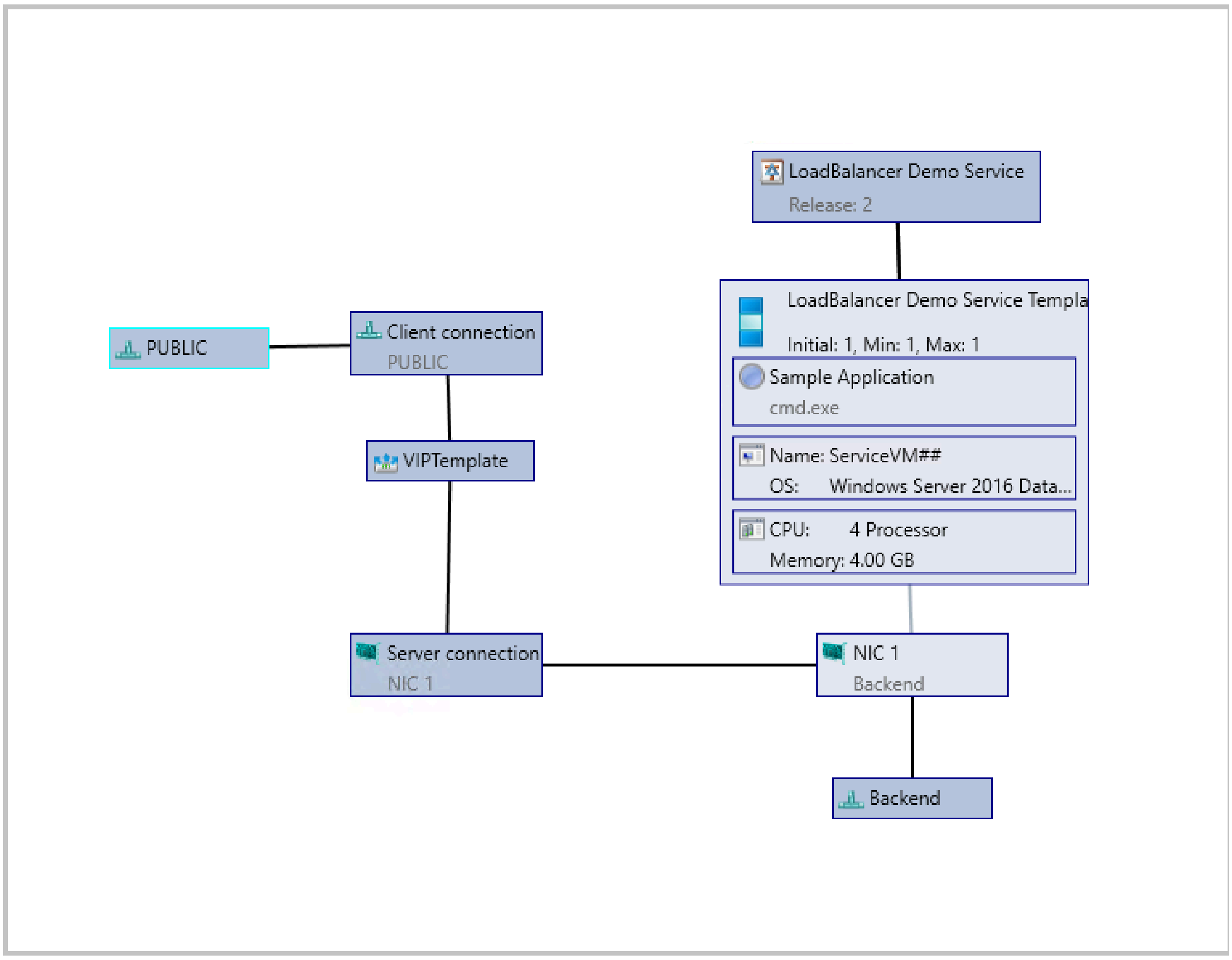
> ⓘ Note
>
> The server connection must be connected to the back-end network interface of the service. The back-end network interface can be connected to either a One Connected VM Network or a network virtualized VM Network.

- With the Connector enabled, select the client connection associated with the load balancer and then select a logical network object.

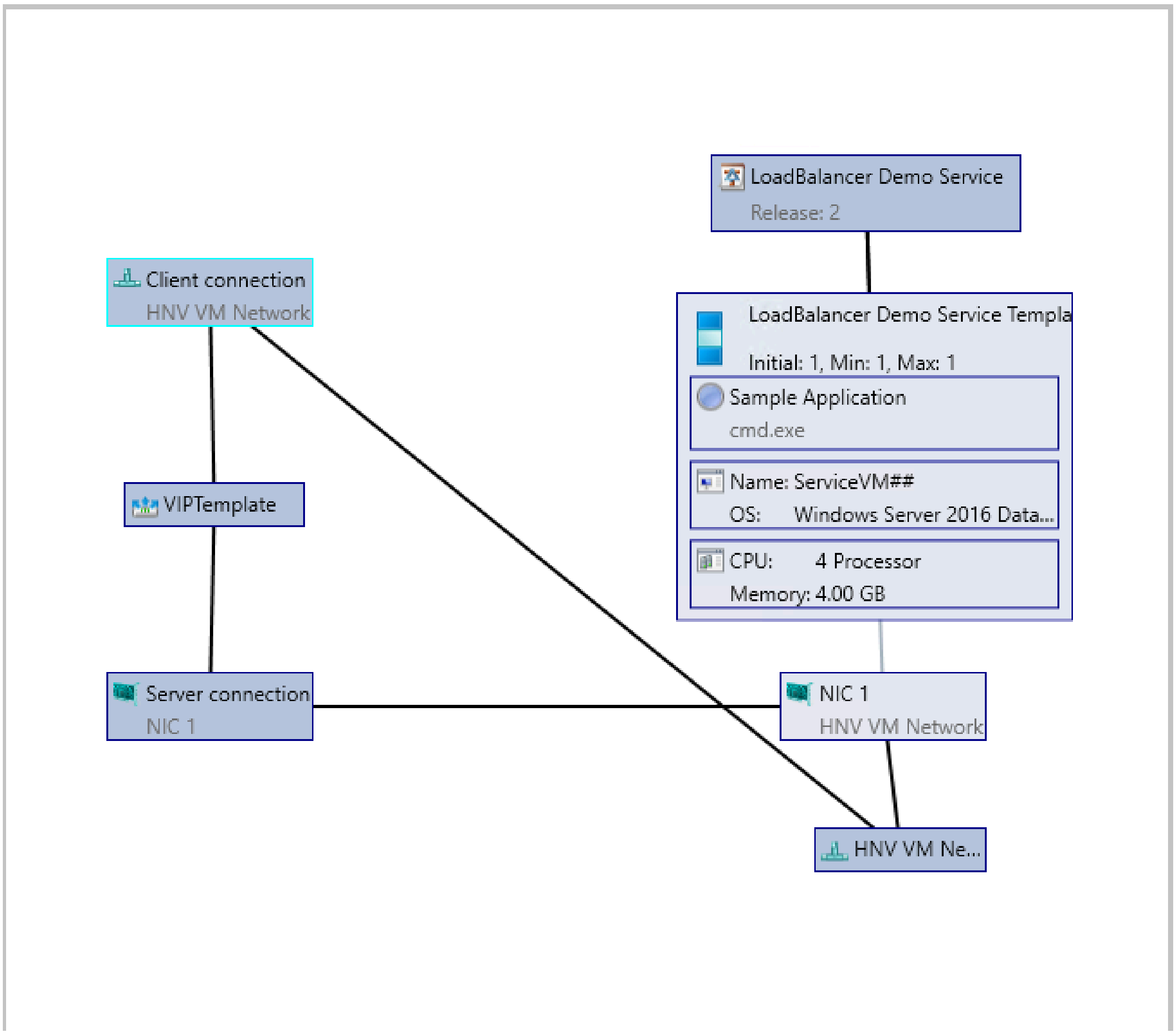
  > ⓘ Note
  >
  > Client connection must be connected to a front-end network of the load balancer. This can be a Public VM network or a network virtualized VM network. A network virtualized VM Network is used for internal load balancing scenarios.

- Save the service template in **Service Template** > **Save and Validate**.

Example 1: Configuring Service with *Public* VM Network as front-end. Here the *Backend* network can be One connected or network virtualized VM network.



Example 2: Configuring Service with front-end and back-end connected to network virtualized VM Network *HNV VM Network*. This scenario is used for internal load balancing.



Set up the VIP for user access

When the service is deployed, VMM automatically selects a VIP from the reserved range in the static IP address pool and assigns it to the load-balanced service tier. To enable users to connect to the service, after the service is deployed, you need to determine the VIP and configure a DNS entry for it.

1. After the service is deployed, select **Fabric** > **Networking** > **Load Balancers**.
2. Select **Show** > **Service** > **Load Balancer Information for Services** and expand the service to see which VIP is assigned.
3. If users use the DNS name to access the service, request the DNS administrator to manually create a DNS entry for the VIP. The entry must be the name that users will specify to connect to the service. For example, servicename.contosol.com.

Back up and restore the SDN infrastructure

Article • 07/24/2024

This article describes the backup and recovery process of a software defined network (SDN) infrastructure in the System Center Virtual Machine Manager (VMM) fabric and provides any applicable recommendations for the process completion.

To back up and restore an SDN, you must back up and restore the network controller (NC) that is deployed in the SDN. Use the following procedures in the sequence explained.

Back up the network controller

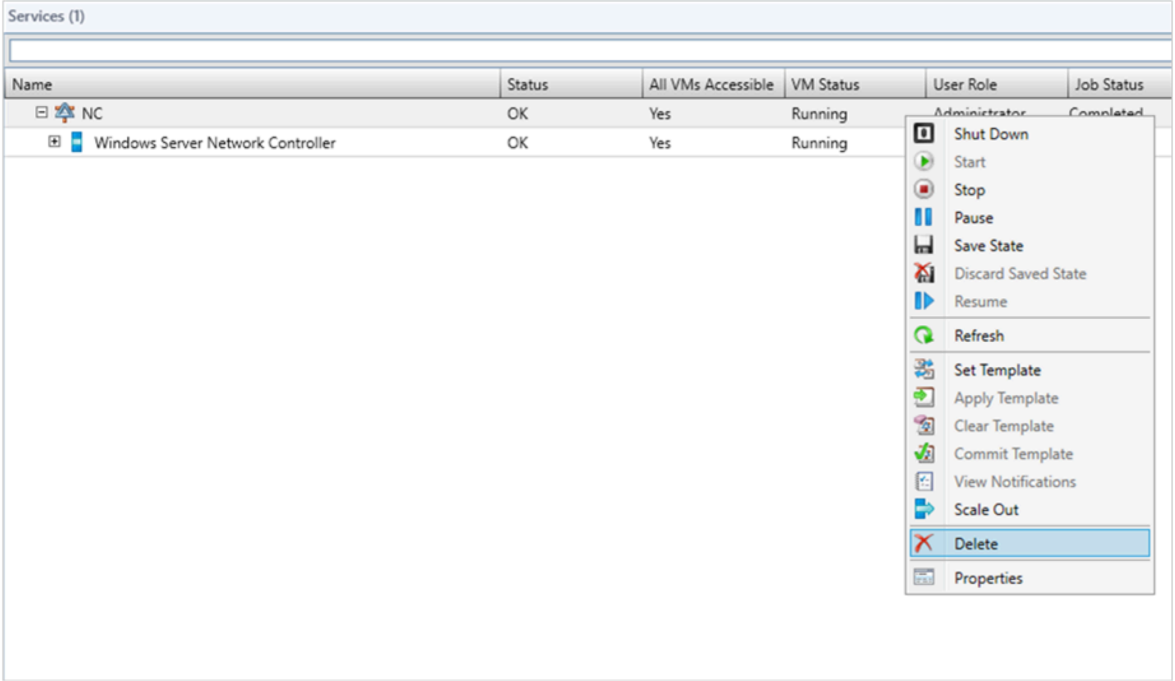
Back up the network controller database by using the network controller Rest API. Learn more.

Bring up the new network controller

Use the following procedures to bring up a new network controller:

1. In the VMM console, **VMs and Services** > **Services**, select the network controller service instance and select **Delete**.

   > ⓘ **Note**
   >
   > Remove the network controller service instance only. Do not remove the network controller from **Fabric** > **Network Services.**



Services (1)

Name	Status	All VMs Accessible	VM Status	User Role	Job Status
NC	OK	Yes	Running	Administrator	Completed
Windows Server Network Controller	OK	Yes	Running		

2. Ensure that the DNS record for the network controller is removed from the DNS.

3. Deploy a new network controller service instance from the VMM by using the same service deployment settings that were used for the original service instance deployment. Learn more.

4. Verify that the deployment job is successful.

Restore the network controller from a backup

Restore the network controller from a network controller backup by using the network controller Rest API. Learn more.

Refresh the network controller and synchronize VMM and NC

Depending on the SDN state captured in the network controller backup and the current VMM state, some of the resources in VMM and network controller can be out of sync.

Use the following refresh procedures to find any such differences between VMM and NC and resolve them accordingly.

> ⓘ Note
>
> - Refresh cmdlets for refreshing network controller objects.

- If the network controller contains any objects that are not present in the VMM DB, then the VMM will not refresh (even if those objects are created by using VMM earlier). Delete those objects from NC and recreate the objects from VMM to manage these objects from VMM again.

Refresh port ACLs

1. Get all the NC-managed port ACLs from the VMM server by using the following cmdlet:

   PowerShell

   ```
   $portACLs = Get-SCPortACL | Where-Object {$_.ManagedByNC -eq $True}
   ```

2. Run the **Read-SCPortACL** cmdlet on all the NC-managed port ACLs to refresh.

   PowerShell

   ```
   foreach($portACL in $portACLs)
   {
      Read-SCPortACL -PortACL $portACL
   }
   ```

3. Verify the VMM jobs' log for the result status and follow the recommendations from the log if there're any failures.

Refresh logical networks

1. Get all the NC-managed logical networks from the VMM server by using the following cmdlet:

   PowerShell

   ```
   $logicalNetworks = Get-SCLogicalNetwork | Where-Object
   {$_.IsManagedByNetworkController -eq $True}
   ```

2. Run the **Read-SCLogicalNetwork** cmdlet on all the NC-managed logical networks to refresh.

PowerShell

```
foreach($logicalNetwork in $logicalNetworks)
{
    Read-SCLogicalNetwork -LogicalNetwork $logicalNetwork
}
```

3. Verify the VMM jobs' log for the result status and follow the recommendations from the log if there're any failures.

Refresh gateways and load balancer muxes

1. Get all the gateways and load balancer muxes by using the following cmdlet:

PowerShell

```
$networkService =  Get-SCNetworkService  | Where-Object {$_.Model -eq
'Microsoft Network Controller'}
$fabricRoles = Get-SCFabricRole -NetworkService $networkService
$fabricRoleResources = @()
foreach($fabricRole in $fabricRoles)
{
    $fabricRoleResources += $fabricRole.ServiceVMs
}
$fabricRoleResources
```

2. Run the **Read-SCFabricRoleResource** cmdlet to refresh.

PowerShell

```
foreach($fabricRoleResource in $fabricRoleResources)
{
    Read-SCFabricRoleResource -FabricResource $fabricRoleResource
}
```

3. Verify the VMM jobs' log for the result status and follow the recommendations from the log if there're any failures.

Refresh NAT connections and NAT rules

1. Get all the NAT connections by using the following cmdlet:

PowerShell

```
$vmNetworks = Get-SCVMNetwork | Where-Object {$_.NetworkManager.Model -
eq 'Microsoft Network Controller' -and $_.IsolationType -eq
'WindowsNetworkVirtualization'}

$natConnections = @()
foreach($vmNetwork in $vmNetworks)
{
     $natConnections += $vmNetwork.NATConnections
}
$natConnections
```

2. Run the **Read-SCNATConnection** cmdlet to refresh NAT connections and NAT rules.

PowerShell

```
foreach($natConnection in $natConnections)
{
     Read-SCNATConnection -NATConnection $natConnection
}
```

3. Verify the VMM jobs' log for the result status and follow the recommendations from the log if there're any failures.

Refresh all load balancer VIPs

1. Get all the load balancer VIPs configured on NC by using the following cmdlet:

PowerShell

```
$loadBalancerVIPs = Get-SCLoadBalancerVIP |  Where-Object
{$_.LoadBalancer.Model -eq 'Microsoft Network Controller'}
```

2. Run the **Read-SCLoadBalancerVIP** cmdlet to refresh all the load balancer VIPs.

PowerShell

```
foreach($loadBalancerVIP in $loadBalancerVIPs)
{
    Read-SCLoadBalancerVIP -LoadBalancerVIP $loadBalancerVIP
}
```

3. Verify the VMM jobs' log for the result status and follow the recommendations from the log if there're any failures.

Refresh VM Networks

1. Get all the NC-managed HNV VM networks from the VMM server by using the following cmdlet:

PowerShell

```
$VMNetworks = Get-SCVMNetwork | Where-Object {$_.NetworkManager.Model -
eq 'Microsoft Network Controller' -and $_.IsolationType -eq
'WindowsNetworkVirtualization'}
```

2. Run the **Read-SCVMNetwork** cmdlet on all the VM networks to refresh.

PowerShell

```
foreach($VMNetwork in $VMNetworks)
{
    Read-SCVMNetwork -VMNetwork $VMNetwork
}
```

3. Verify the VMM jobs' log for the result status and follow the recommendations from the log if there're any failures.

Refresh gateway pools

1. Get the gateway fabric role from the VMM server by using the following cmdlet:

PowerShell

```
$networkService =  Get-SCNetworkService  | Where-Object {$_.Model -eq
'Microsoft Network Controller'}
$gatewayFabricRole = Get-SCFabricRole -NetworkService $networkService |
Where-Object {$_. RoleType -eq ‘Gateway ’}
```

2. Run the **Read-SCFabricRole** cmdlet to refresh the fabric role.

PowerShell

```
foreach($fabricRole in $gatewayFabricRole )
{
    Read-SCFabricRole -FabricRole $fabricRole
}
```

3. Verify the VMM jobs' log for the result status and follow the recommendations from the log if there're any failures.

Refresh VM network gateways

1. Get all the VM network gateways that are configured for the VM networks by using the following cmdlet:

PowerShell

```
$vmNetworks = Get-SCVMNetwork | Where-Object {$_.NetworkManager.Model -eq 'Microsoft Network  Controller' -and $_.IsolationType -eq 'WindowsNetworkVirtualization'  -and $_.VMNetworkGateways.Count -gt 0}}
$VMNetworkGateways = @()
foreach($vmNetwork in $vmNetworks)
{
     $VMNetworkGateways += $vmNetwork.$VMNetworkGateways
}
```

2. Run the **Read-SCVMNetworkGateway** cmdlet to refresh the gateways.

PowerShell

```
foreach($VMNetworkGateway in $VMNetworkGateways)
{
    Read-SCVMNetworkGateway -VMNetworkGateway $VMNetworkGateway
}
```

3. Verify the VMM jobs' log for the result status and follow the recommendations from the log if there're any failures.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Remove a Software Defined Network (SDN) from VMM fabric

Article • 07/24/2024

To remove an SDN from the System Center Virtual Machine Manager (VMM) fabric, you must remove the following objects in the specified order:

- VM networks (associated with the NC managed logical networks).
- Logical networks (managed by NC).
- Software load balancer (if deployed or deployed and configured).
- Gateway (if deployed or deployed and configured).
- Network controller (if deployed or deployed and configured).

Remove the VM networks

ⓘ **Note**

Ensure that no VMs or NICs are connected to the VM networks that you want to remove.

1. Select **VMs and Services** > **VM Networks**, and select the VM network to remove.
2. Right-click the VM network and select **Delete**.
3. Repeat steps 1 and 2 for each VM network that you need to remove.

Remove the logical networks

ⓘ **Note**

Ensure that no port profiles are associated with the logical networks that you want to remove. You can only remove HNV logical network. Do not remove transient network.

1. Select **Fabric** > **Logical networks** and select the logical network to remove.
2. Right-click the logical network and select **Remove**.
3. Repeat steps 1 and 2 for each logical network that you need to remove.

ⓘ **Note**

> Logical networks associated with the SLB cannot be removed from the console. Use force delete to remove these (by using **-Force** flag).

Remove the software load balancer

1. Select **Fabric** > **Network Services** and select the software load balancer role.

2. Under **Services** > **Associated Services**, select **Browse**, and then select **Clear Selection**.

   This action removes the software load balancer service. Ensure the job is complete. If the job fails, restart the job after making the required changes that the error message details you.

3. Uncheck the pools that are associated with the SLB, except for the private VIP pool that is associated with the SLB Manager VIP.

4. To complete the removal of the SLB, force delete the private VIP pool, the corresponding logical network definition, and the logical networks (by using **-Force** flag).

Remove the gateway

1. Select **Fabric** > **Network Services** and select the Gateway manager role.

2. Under **Services** > **Associated Services**, select **Browse**, and then select **Clear Selection**.

   This action removes the gateway service. Ensure the job is complete. If the job fails, restart the job after making the required changes that the error message details you.

3. To complete the removal of the gateway, remove the gateway pool by using the following PowerShell scripts:

   ```PowerShell
   $nc=get-scnetworkservice | Where {$_.Model -eq "Microsoft Network Controller"}
   $gwrole=get-scfabricrole -NetworkService $nc | Where {$_.RoleType -eq "Gateway"}
   Set-SCFabricRole -FabricRole  $gwrole  -GatewayConfiguration $null
   ```

Remove the network controller

> ⓘ Note
>
> Ensure that SLB/GW and associated logical networks are successfully removed.

1. Select **Fabric** > **Network Services** and select the network controller.

2. Right-click the NC and select **Remove**.

   This action removes the NC service. Ensure that the job is complete. If the job fails, restart the job after making the required changes that the error message details you.

Manage SDN resources in the VMM fabric

Article • 07/24/2024

This article summarizes the software-defined network (SDN) operations that you can manage in the System Center Virtual Machine Manager (VMM) fabric. For operations that can't be managed in the fabric, you need to use REST APIs or Windows Server PowerShell.

A software-defined network (SDN) abstracts physical hardware network infrastructure into virtual networks. In the VMM fabric, you can deploy and manage an SDN infrastructure, including network controller, software load balancers, and gateways, to provision and manage virtual networks at scale. Learn more.

What can I manage in VMM?

SDN resources fall into two broad categories in VMM:

- **Known resources**: Resources that can be created and managed with VMM.
- **Unknown resources**: Resources that must be created and managed outside of VMM.

Known resources

These resources can be created and managed with or without VMM. If you make changes to these resources outside VMM, VMM overwrites the out-of-box changes, when a VMM operation is performed on the object. This could cause configuration and connectivity issues and should be avoided whenever possible. There's no way to revert an overwrite unless you detect the issue and reconfigure manually.

We strongly recommend that you configure resources that are known to VMM in the VMM fabric only.

Expand table

Known object	Details	Modify
AccessControlList	An AccessControlList contains a list of ACL rules and can be assigned to virtual subnets or IP configurations.	Overwritten by VMM if you enable out-of-box

Known object	Details	Modify
AclRule	Summarizes the network traffic that is allowed or denied for a VM network interface.	Overwritten by VMM if you enable out-of-box
Gateway	Provides gateway services to one or more virtualNetworks.	Overwritten by VMM if you enable out-of-box
GatewayPool	GatewayPools aggregate a set of gateways resources into a single pool.	Overwritten by VMM if you enable out-of-box
Host		Overwritten by VMM if you enable out-of-box
HostProperties		Overwritten by VMM if you enable out-of-box
IpConfigurations	IP addresses of the load balancer.	Overwritten by VMM if you enable out-of-box
IpPool	Create an IP address pool on the network controller.	Overwritten by VMM if you enable out-of-box
LoadBalancerManager	Configures the load balancing service of the Network Controller.	Overwritten by VMM if you enable out-of-box
LoadBalancerMux	Represents a MUX VM deployed in the network controller fabric.	Overwritten by VMM if you enable out-of-box
LogicalSubnets	A subnet/VLAN pair.	Overwritten by VMM if you enable out-of-box
MACPool	Creates a MAC address pool on the network controller.	Overwritten by VMM if you enable out-of-box
NatRules	Configures the load balancer to apply NAT to traffic.	Overwritten by VMM if you enable out-of-box
NetworkInterface	Specifies the configuration of either a host virtual interface (host vNIC) or a virtual server NIC	Overwritten by VMM if you

Known object	Details	Modify
	(VMNIC).	enable out-of-box
PortSettings		Overwritten by VMM if you enable out-of-box
PublicIPAddress	Specifies an IP address, which is publicly available. It's used by virtualGateways and loadBalancers to indicate the IP address that can be used to communicate with the virtual network from outside.	Overwritten by VMM if you enable out-of-box
QualityOfService		Overwritten by VMM if you enable out-of-box
Servers	Represents a physical server that is being controlled by the Network Controller.	Overwritten by VMM if you enable out-of-box
VirtualGateway	Describes the gateway used for cross-premises connectivity from the virtual network.	Overwritten by VMM if you enable out-of-box
VirtualGatewayBgpPeer	Configures BGP peers of the virtualGateways resource.	Overwritten by VMM if you enable out-of-box
VirtualNetwork	Used to create a virtual network using HNV for tenant overlays.	Overwritten by VMM if you enable out-of-box
VirtualServer	Corresponds to a virtual machine. Must be created for VMs that correspond to gateway and MUX resources.	Overwritten by VMM if you enable out-of-box
VirtualSubnet	Used to create virtual subnets (VSIDs) under a tenant's virtual network (RDID).	Overwritten by VMM if you enable out-of-box
VirtualSwitchManager	Configures the virtual switch properties on every server managed by the Network Controller.	Overwritten by VMM if you enable out-of-box
VM	Corresponds to a virtual machine.	Overwritten by VMM if you enable out-of-box

Unknown resources

These resources are to be created and managed outside the VMM fabric. VMM has no knowledge of them, and obviously doesn't overwrite them when they're configured outside the VMM console.

Unknown objects are any Network Controller resources that aren't listed in the table above. Get the latest list of SDN resources.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage Storage Spaces Direct in VMM

Article • 08/02/2024

This article provides an overview of Storage Spaces Direct (S2D), and how it's deployed in the System Center Virtual Machine Manager (VMM) fabric.

Storage Spaces Direct (S2D) was introduced in Windows Server 2016. It groups physical storage drives into virtual storage pools to provide virtualized storage. With virtualized storage, you can:

- Manage multiple physical storage sources as a single virtual entity.
- Get inexpensive storage, with and without external storage devices.
- Gather different types of storage into a single virtual storage pool.
- Easily provision storage, and expand virtualized storage on demand by adding new drives.

> ⓘ **Note**
>
> VMM 2022 supports Azure Stack Hyper Converged Infrastructure (HCI, version 20H2 and 21H2).

How does it work?

S2D creates pools of storage from storage that's attached to specific nodes in a Windows Server cluster. The storage can be internal on the node or disk devices that are directly attached to a single node. Supported storage drives include NVMe, SSD connected via SATA or SAS, and HDD. Learn more.

- When you enable S2D on a Windows Server cluster, S2D automatically discovers eligible storage and adds it to a storage pool for the cluster.
- S2D also creates a built-in server-side storage cache to maximize performance. The fastest drives are used for caching and the remaining drives for capacity. Learn more about the cache.
- You create volumes from a storage pool. Creating a volume creates the virtual disk (storage space), partitions and formats it, adds it to the cluster, and converts it to a cluster shared volume (CSV).
- You configure different levels of fault tolerance for a volume, to specify how virtual disks are spread across physical disks in the pool, using SMB 3.0. You can configure a volume with no resiliency or with mirror or parity resilience. Learn more.

Converged and non-converged deployment

A cluster running S2D can be deployed in a couple of ways:

- **Hyper-converged deployment**: Hyper-V compute and S2D storage run within the same cluster, with no separation between them. This provides simultaneous scaling of compute and storage resources.
- **Disaggregated deployment**: Compute resources run on one Hyper-V cluster. S2D storage runs on a different cluster. You scale the clusters separately for finely tuned management.

Hyper-converged deployment

Here's an illustration for hyper-converged deployment

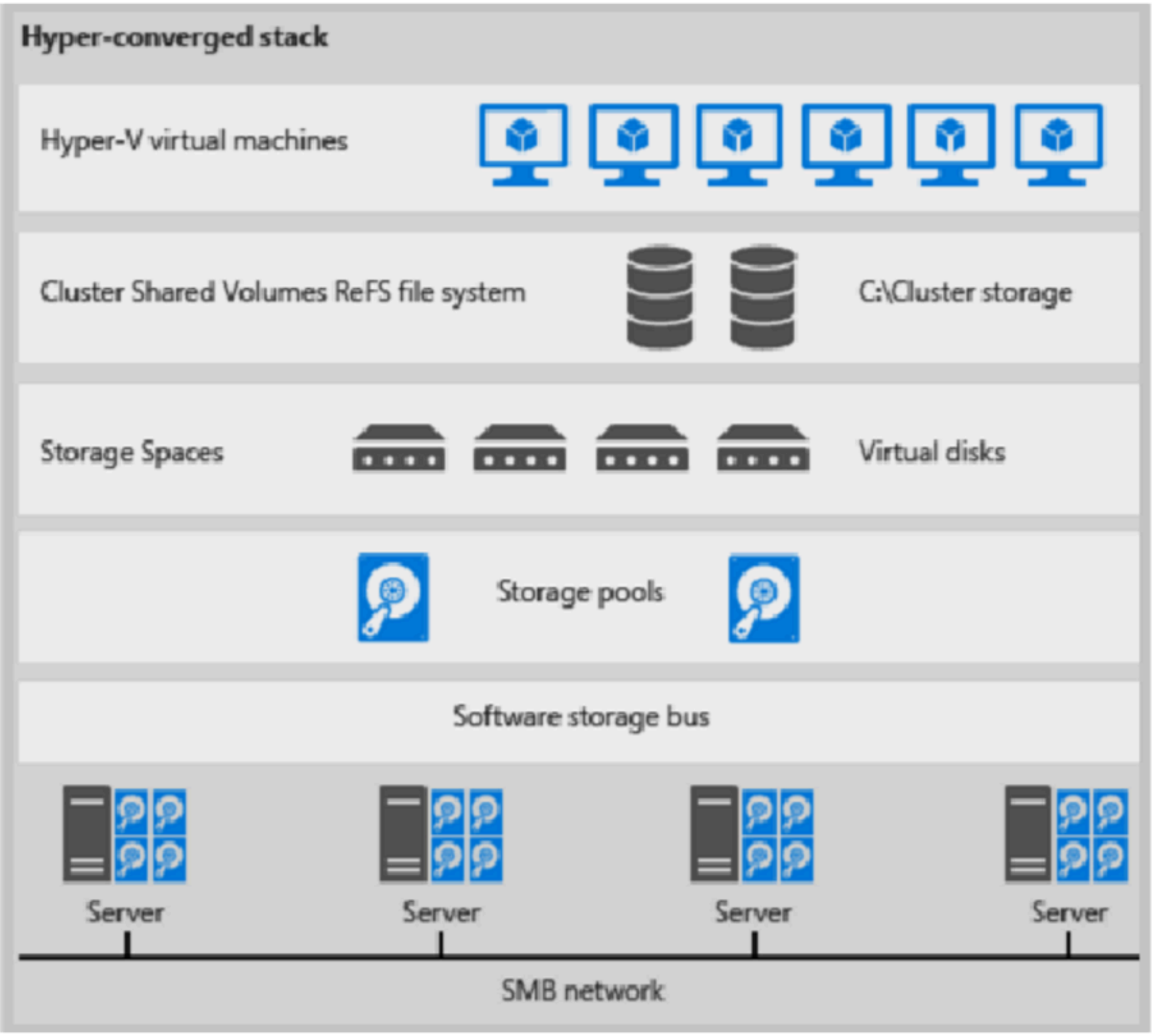


Figure 1: Hyper-converged deployment

- VM files are stored on local CSVs.
- File shares and SMB aren't used.

- After S2D CSV volumes are available, you provision them as you would any other Hyper-V deployment.
- You scale the Hyper-V compute cluster together with its S2D storage.

Disaggregated deployment

Here's an illustration for disaggregated deployment

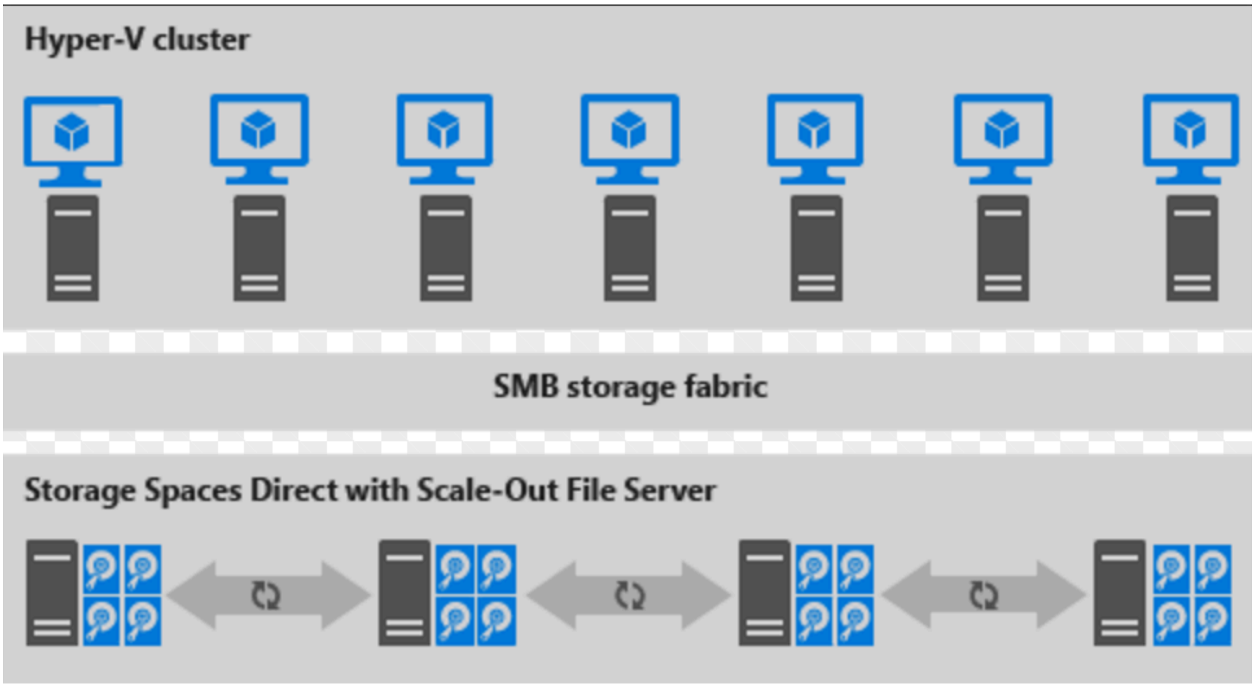


Figure 2: Disaggregated deployment

- File shares are created on the S2D CSVs.
- Hyper-V VMs are configured to store their files on the scaled-out file server (SOFS) and accessed using SMB 3.0.
- You scale the Hyper-V and SOFS clusters separately for finely tuned management. For example, compute nodes might be near full capacity for many VMs, but storage nodes might have excess disk and IOPS capacity; so you add only additional compute nodes.

Next steps

Deploy a hyper-converged S2D cluster

Feedback

Was this page helpful? Yes No

Provide product feedback ↗ | Get help at Microsoft Q&A

Deploy a Storage Spaces Direct hyper-converged cluster in VMM

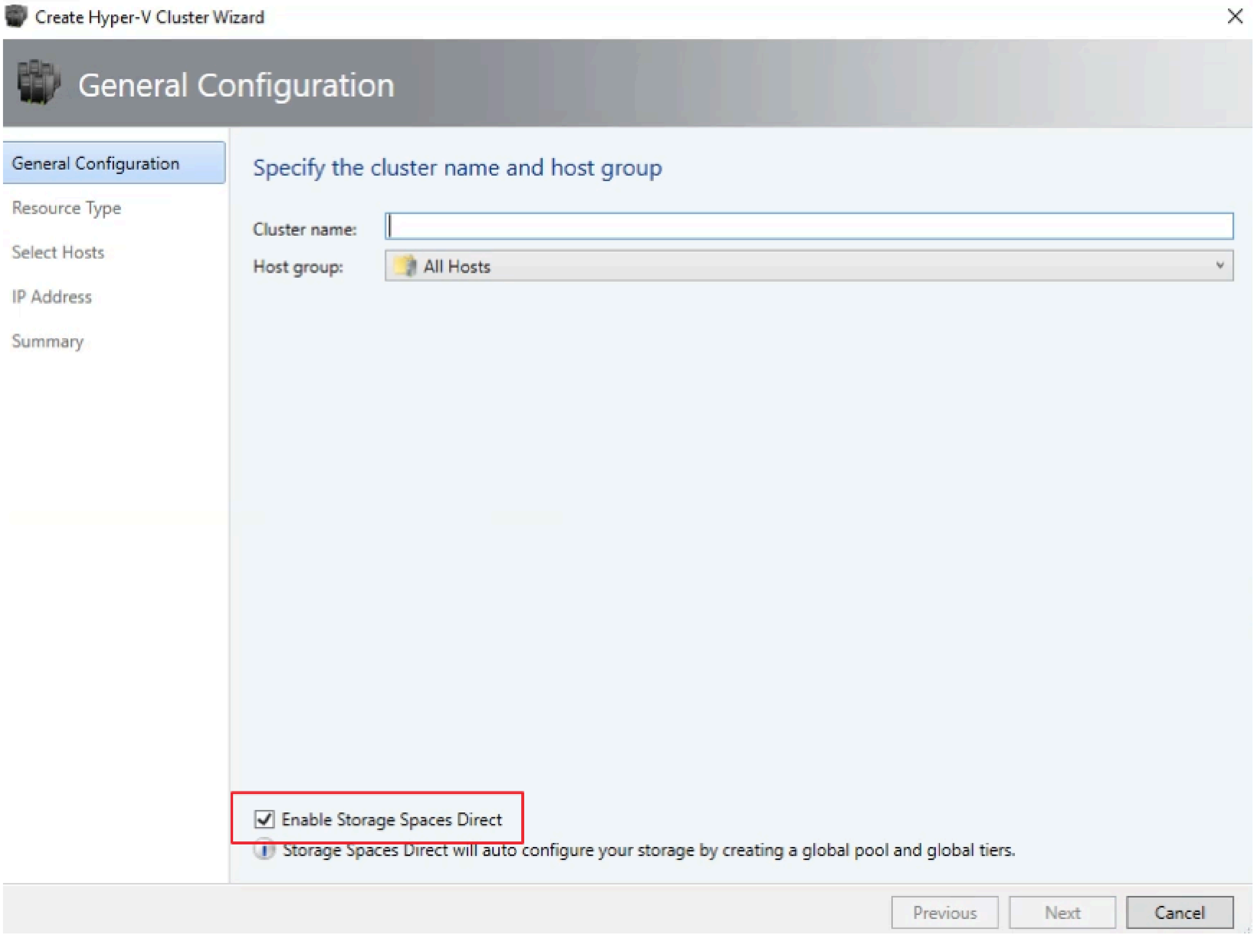
Article • 08/21/2024

This article describes how to set up a hyper-converged cluster running Storage Spaces Direct (S2D) in System Center Virtual Machine Manager (VMM). Learn more about S2D.

You can deploy a hyper-converged S2D cluster by provisioning a Hyper-V cluster and enable S2D from existing Hyper-V hosts or by provisioning from bare-metal servers.

> ⓘ **Note**
>
> You must enable S2D before adding the storage provider to VMM.

To enable S2D, go to **General Configuration** > **Specify the cluster name and host group**, and select the **Enable Storage Spaces Direct** option as shown below:


Create Hyper-V Cluster Wizard

General Configuration

Specify the cluster name and host group

Cluster name:

Host group: All Hosts

☑ Enable Storage Spaces Direct

Storage Spaces Direct will auto configure your storage by creating a global pool and global tiers.

After you enable a cluster with S2D, VMM does the following:

1. The File Server role and the Failover Clustering feature are enabled.
2. Storage replica and data deduplication are enabled.

3. The cluster is optionally validated and created.
4. S2D is enabled, and a storage array is created with the same name you provide in the wizard.

If you use PowerShell to create a hyper-converged cluster, the pool and the storage tier are automatically created with the **Enable-ClusterS2D autoconfig=true** option.

Before you start

- Ensure that you're running VMM 2016 or later.
- Hyper-V hosts in a cluster must be running Windows Server 2016 or later with the Hyper-V Role installed and be configured to host VMs.

> ⓘ **Note**
>
> VMM 2022 supports Azure Stack Hyper Converged Infrastructure (HCI, version 20H2 and 21H2).

After these prerequisites are in place, you provision a cluster, and set up storage resources on it. You can then deploy VMs on the cluster or export the storage to other resources using SOFS.

Step 1: Provision the cluster

You can provision a cluster in the following ways:

1. From Hyper-V hosts
2. From bare metal machines

Select the required tab for the steps to provision a cluster:

From Hyper-V hosts

Follow these steps to provision a cluster from Hyper-V hosts:

1. If you need to add the Hyper-V hosts to the VMM fabric, follow these steps. If they’re already in the VMM fabric, skip to the next step.
2. Follow the instructions for provisioning a cluster from standalone Hyper-V hosts managed in the VMM fabric.

> ⓘ **Note**

- When you set up the cluster, ensure to select the **Enable Storage Spaces Direct** option on the **General Configuration** page of the Create Hyper-V Cluster wizard. In **Resource Type**, select **Existing servers running a Windows Server operating system**, and select the Hyper-V hosts to add to the cluster.
- If S2D is enabled, you must validate the cluster. Skipping this step isn't supported.

Step 2: Set up networking for the cluster

After the cluster is provisioned and managed in the VMM fabric, you need to set up networking for cluster nodes.

1. Start by creating a logical network to mirror your physical management network.
2. You need to set up a logical switch with Switch Embedded Teaming (SET) enabled so that the switch is aware of virtualization. This switch is connected to the management logical network and has all the host virtual adapters that are required to provide access to the management network or configure storage networking. S2D relies on a network to communicate between hosts. RDMA-capable adapters are recommended.
3. Create VM networks.

Step 3: Configure DCB settings on the S2D cluster

ⓘ Note

Configuration of DCB settings is an optional step to achieve high performance during S2D cluster creation workflow. Skip to step 4 if you don't wish to configure DCB settings.

Recommendations

- If you have vNICs deployed, for optimal performance, we recommend you to map all your vNICs with the corresponding pNICs. Affinities between vNIC and pNIC are set randomly by the operating system, and there could be scenarios where multiple vNICs are mapped to the same pNIC. To avoid such scenarios, we recommend you to manually set affinity between vNIC and pNIC by following the steps listed here.

- When you create a network adapter port profile, we recommend you to allow **IEEE priority**. Learn more. You can also set the IEEE Priority using the following PowerShell commands:

```
PS> Set-VMNetworkAdapterVlan -VMNetworkAdapterName SMB2 -VlanId "101" -
Access -ManagementOS
PS> Set-VMNetworkAdapter -ManagementOS -Name SMB2 -IeeePriorityTag on
```

Before you begin

Ensure the following:

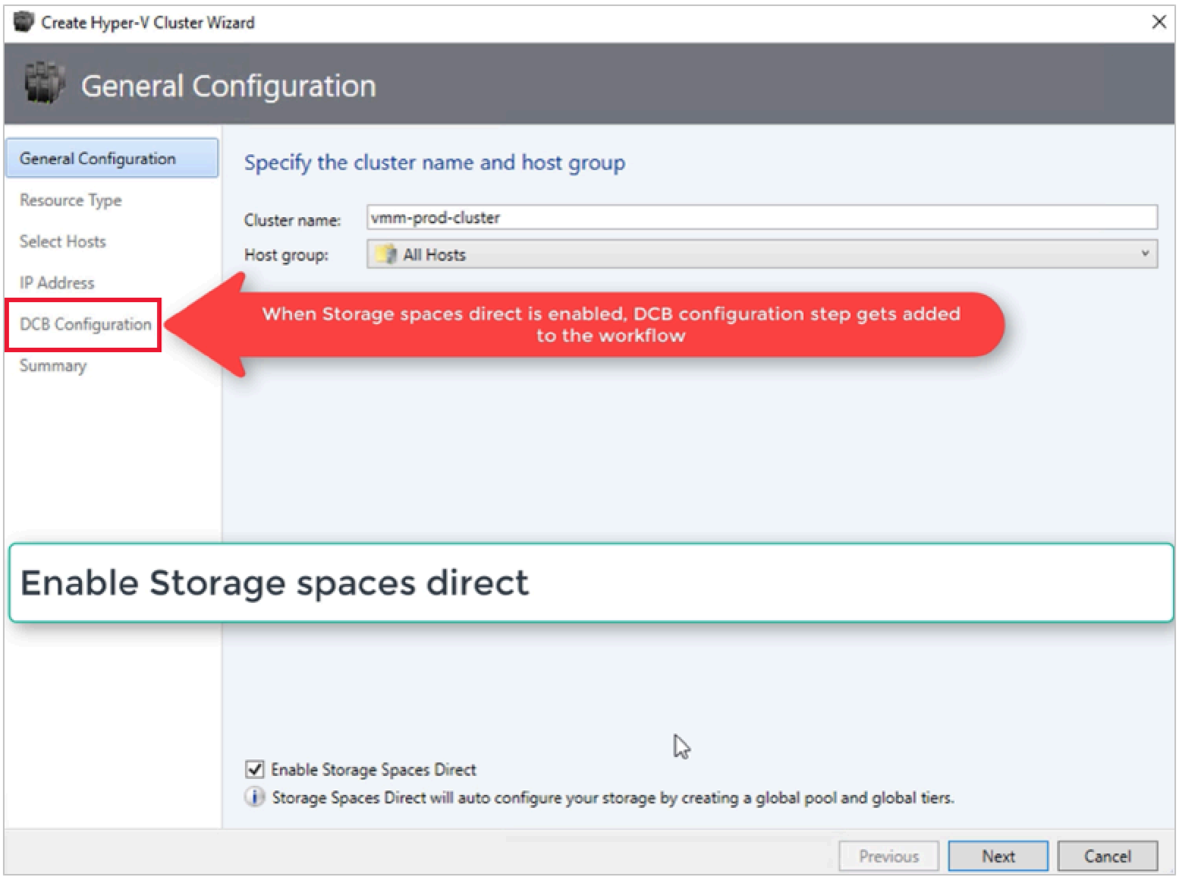
1. You're running VMM 2016 or later.

2. Hyper-V hosts in the cluster are running Windows Server 2016 or later with the Hyper-V role installed and configured to host VMs.

> ⓘ Note
>
> - You can configure DCB settings on both Hyper-V S2D cluster (Hyper-converged) and SOFS S2D cluster (disaggregated).
> - You can configure the DCB settings during cluster creation workflow or on an existing cluster.
> - You can't configure DCB settings during SOFS cluster creation; you can only configure on an existing SOFS cluster. All the nodes of the SOFS cluster must be managed by VMM.
> - Configuration of DCB settings during cluster creation is supported only when the cluster is created with an existing Windows server. It isn't supported with bare metal/operating system deployment workflow.

Use the following steps to configure DCB settings:

1. Create a new Hyper-V cluster, and select **Enable Storage Spaces Direct**. *DCB Configuration* option gets added to the Hyper-V cluster creation workflow.


Create Hyper-V Cluster Wizard

General Configuration

Specify the cluster name and host group

Cluster name: vmm-prod-cluster

Host group: All Hosts

When Storage spaces direct is enabled, DCB configuration step gets added to the workflow

Enable Storage spaces direct

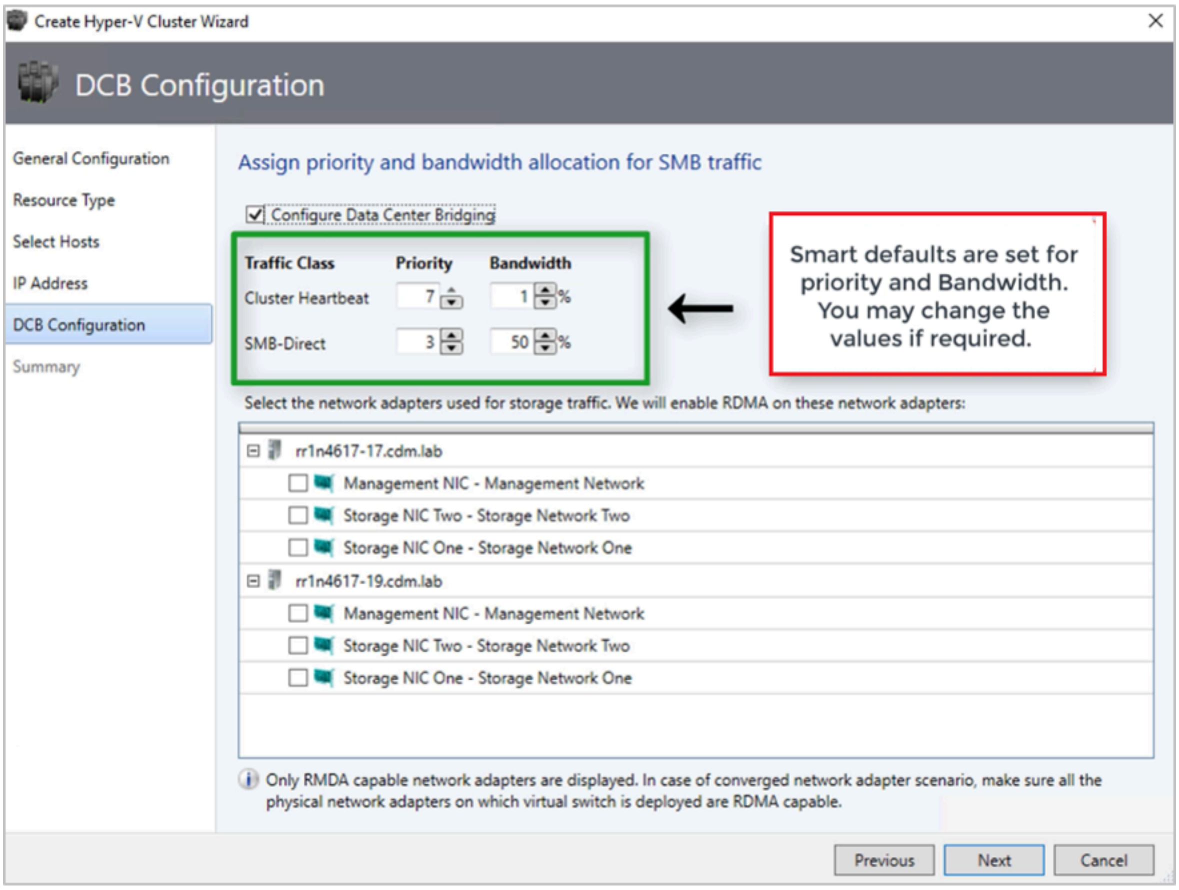
☑ Enable Storage Spaces Direct

Storage Spaces Direct will auto configure your storage by creating a global pool and global tiers.

2. In **DCB configuration**, select **Configure Data Center Bridging**.

3. Provide **Priority** and **Bandwidth** values for SMB-Direct and Cluster Heartbeat traffic.

> ⓘ **Note**
>
> Default values are assigned to Priority and Bandwidth. Customize these values based on your organization's environment needs.



Create Hyper-V Cluster Wizard

DCB Configuration

Assign priority and bandwidth allocation for SMB traffic

☑ Configure Data Center Bridging

Traffic Class	Priority	Bandwidth
Cluster Heartbeat	7	1 %
SMB-Direct	3	50 %

Smart defaults are set for priority and Bandwidth. You may change the values if required.

Select the network adapters used for storage traffic. We will enable RDMA on these network adapters:

- rr1n4617-17.cdm.lab
  - □ Management NIC - Management Network
  - □ Storage NIC Two - Storage Network Two
  - □ Storage NIC One - Storage Network One
- rr1n4617-19.cdm.lab
  - □ Management NIC - Management Network
  - □ Storage NIC Two - Storage Network Two
  - □ Storage NIC One - Storage Network One

Only RMDA capable network adapters are displayed. In case of converged network adapter scenario, make sure all the physical network adapters on which virtual switch is deployed are RDMA capable.

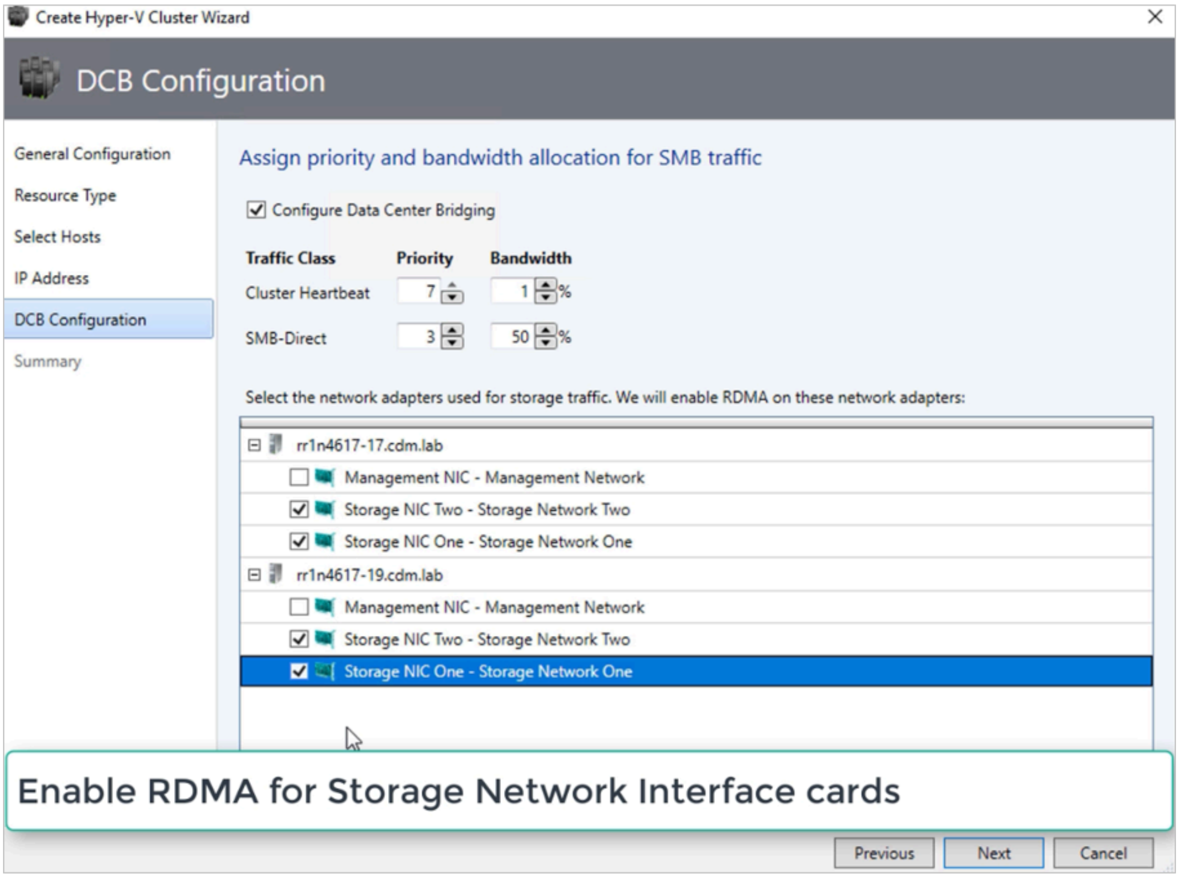
Default values:

Expand table

Traffic Class	Priority	Bandwidth (%)
Cluster Heartbeat	7	1
SMB-Direct	3	50

4. Select the network adapters used for storage traffic. RDMA is enabled on these network adapters.

> ⓘ **Note**
>
> In a converged NIC scenario, select the storage vNICs. The underlying pNICs must be RDMA capable for vNICs to be displayed and available for selection.



Assign priority and bandwidth allocation for SMB traffic

☑ Configure Data Center Bridging

Traffic Class	Priority	Bandwidth
Cluster Heartbeat	7	1 %
SMB-Direct	3	50 %

Select the network adapters used for storage traffic. We will enable RDMA on these network adapters:

- rr1n4617-17.cdm.lab
  - □ Management NIC - Management Network
  - ☑ Storage NIC Two - Storage Network Two
  - ☑ Storage NIC One - Storage Network One
- rr1n4617-19.cdm.lab
  - □ Management NIC - Management Network
  - ☑ Storage NIC Two - Storage Network Two
  - ☑ Storage NIC One - Storage Network One

Enable RDMA for Storage Network Interface cards

5. Review the summary and select **Finish**.

   An S2D cluster will be created, and the DCB parameters are configured on all the S2D Nodes.

   > ⓘ **Note**
   >
   > - DCB settings can be configured on the existing Hyper-V S2D clusters by visiting the **Cluster Properties** page and navigating to the **DCB configuration** page.
   > - Any out-of-band changes to DCB settings on any of the nodes will cause the S2D cluster to be noncompliant in VMM. A Remediate option will be provided in the **DCB configuration** page of cluster properties, which you can use to enforce the DCB settings configured in VMM on the cluster nodes.

Step 4: Manage the pool and create CSVs

You can now modify the storage pool settings and create virtual disks and CSVs.

1. Select **Fabric** > **Storage** > **Arrays**.

2. Right-click the cluster > **Manage Pool**, and select the storage pool that was created by default. You can change the default name and add a classification.

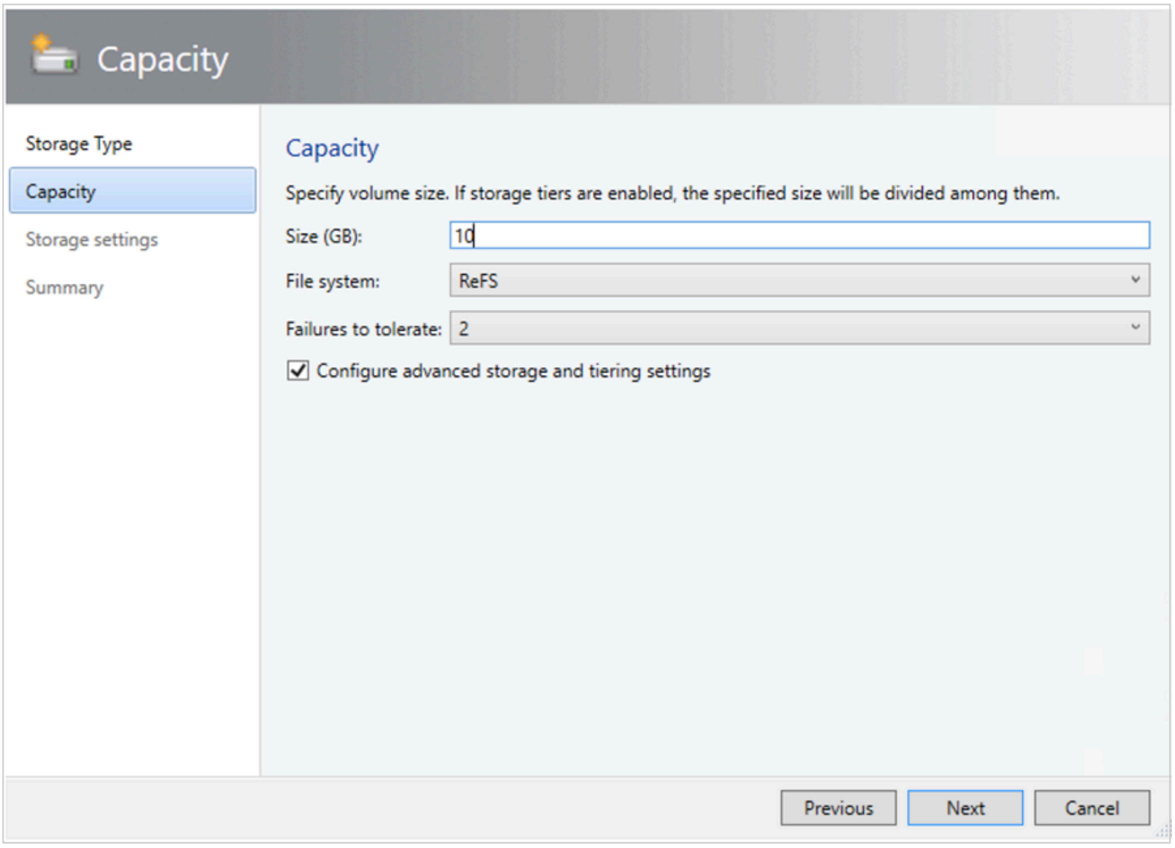
3. To create a CSV, right-click the cluster > **Properties** > **Shared Volumes**.

4. In the Create Volume Wizard > **Storage Type**, specify the volume name and select the storage pool.

5. In **Capacity**, you can specify the volume size, file system, and resiliency settings.

6. Select **Configure advanced storage and tiering settings** to set up these options.

7. Select **Next**.



Capacity

Specify volume size. If storage tiers are enabled, the specified size will be divided among them.

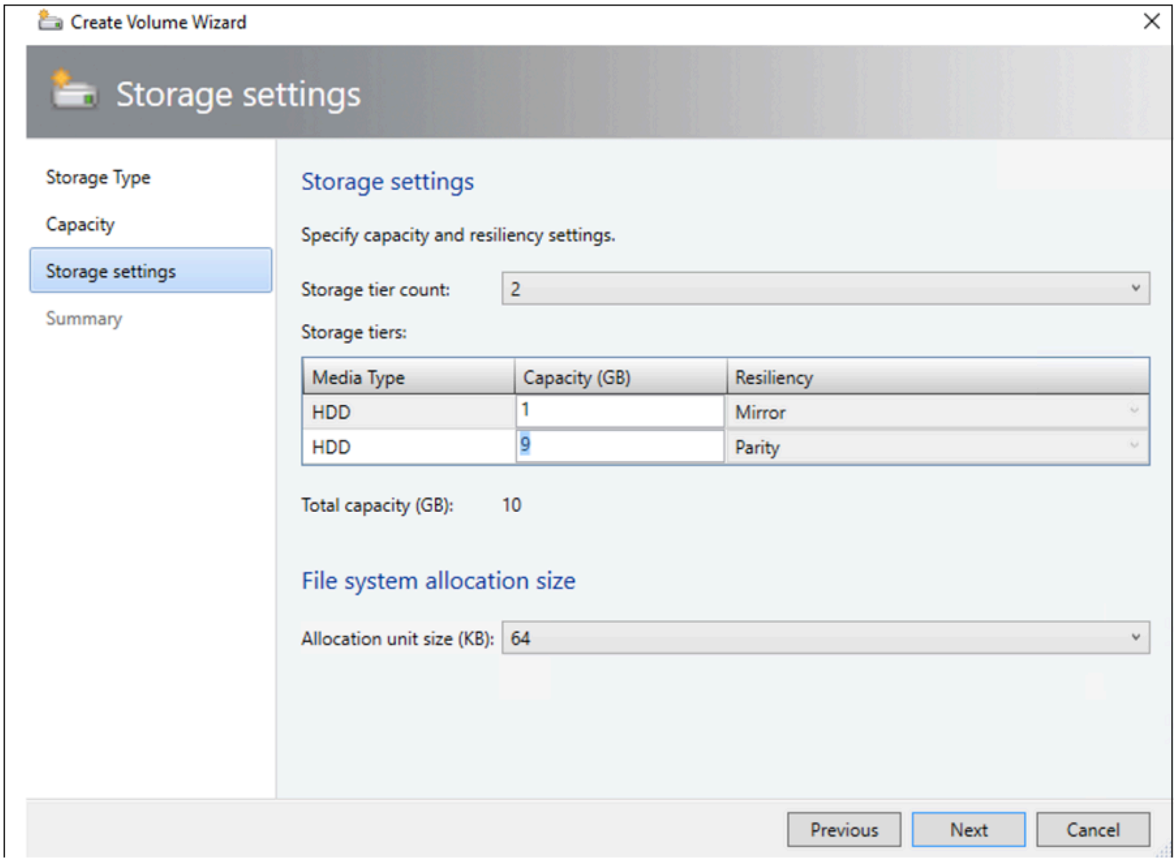
Size (GB): 10

File system: ReFS

Failures to tolerate: 2

☑ Configure advanced storage and tiering settings

8. In **Storage Settings**, specify the storage tier split, capacity, and resiliency settings.



Storage settings

Specify capacity and resiliency settings.

Storage tier count: 2

Storage tiers:

Media Type	Capacity (GB)	Resiliency
HDD	1	Mirror
HDD	9	Parity

Total capacity (GB): 10

File system allocation size

Allocation unit size (KB): 64

9. In **Summary**, verify the settings and finish the wizard. A virtual disk will be created automatically when you create the volume.

If you use PowerShell, the pool and the storage tier are automatically created with the **Enable-ClusterS2D autoconfig=true** option.

Step 5: Deploy VMs on the cluster

In a hyper-converged topology, VMs can be directly deployed on the cluster. Their virtual hard disks are placed on the volumes you created using S2D. You create and deploy these VMs just as you would any other VM.

Next steps

- Provision VMs
- Manage the cluster

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Deploy and manage Azure Stack HCI clusters in VMM

Article • 09/04/2024

This article provides information about how to set up an Azure Stack HCI cluster in System Center Virtual Machine Manager (VMM). You can deploy an Azure Stack HCI cluster by provisioning from bare-metal servers or by adding existing hosts. Learn more about the new Azure Stack HCI.

VMM 2022 supports Azure Stack HCI, version 20H2; Azure Stack HCI, version 21H2; and Azure Stack HCI, version 22H2 (supported from VMM 2022 UR1).

> ⓘ **Important**
>
> Azure Stack HCI clusters that are managed by Virtual Machine Manager must not join **the preview channel** yet. System Center (including Virtual Machine Manager, Operations Manager, and other components) does not currently support Azure Stack preview versions. For the latest updates, see the **System Center blog**.

Before you start

Ensure that you're running VMM 2022 UR1 or later.

What’s supported?

- Addition, creation, and management of Azure Stack HCI clusters. See detailed steps to create and manage HCI clusters.
- Ability to provision and deploy VMs on the Azure Stack HCI clusters and perform VM life cycle operations. VMs can be provisioned using VHD(x) files, templates, or from an existing VM. Learn more.
- Set up VLAN based network on Azure Stack HCI clusters.
- Deployment and management of SDN network controller on Azure Stack HCI clusters.
- Management of storage pool settings, creation of virtual disks, creation of cluster shared volumes (CSVs), and application of QoS settings.

- Moving VMs between Windows Server and Azure Stack HCI clusters works via Network Migration and migrating an offline (shut down) VM. In this scenario, VMM does export and import under the hood, even though it's performed as a single operation.

- The PowerShell cmdlets used to manage Windows Server clusters can be used to manage Azure Stack HCI clusters as well.

Register and unregister Azure Stack HCI clusters

With VMM 2022, we're introducing VMM PowerShell cmdlets to register and unregister Azure Stack HCI clusters.

Use the following cmdlets to register an HCI cluster:

PowerShell

```powershell
Register-SCAzStackHCI -VMHostCluster <HostCluster> -SubscriptionID <string>
```

Use the following command to unregister a cluster:

PowerShell

```powershell
Unregister-SCAzStackHCI -VMHostCluster <HostCluster> -SubscriptionID
<string>
```

For detailed information on the supported parameter, see Register-SCAzStackHCI and Unregister-SCAzStackHCI.

What’s not supported?

- Management of Azure Stack HCI stretched clusters is currently not supported in VMM.

- Azure Stack HCI is intended as a virtualization host where you run all your workloads in virtual machines. The Azure Stack HCI terms allow you to run only what's necessary for hosting virtual machines. Azure Stack HCI clusters must not be used for other purposes like WSUS servers, WDS servers, or library servers. Refer to Use cases for Azure Stack HCI, When to use Azure Stack HCI, and Roles you can run without virtualizing.

- Live migration between any version of Windows Server and Azure Stack HCI clusters isn't supported.

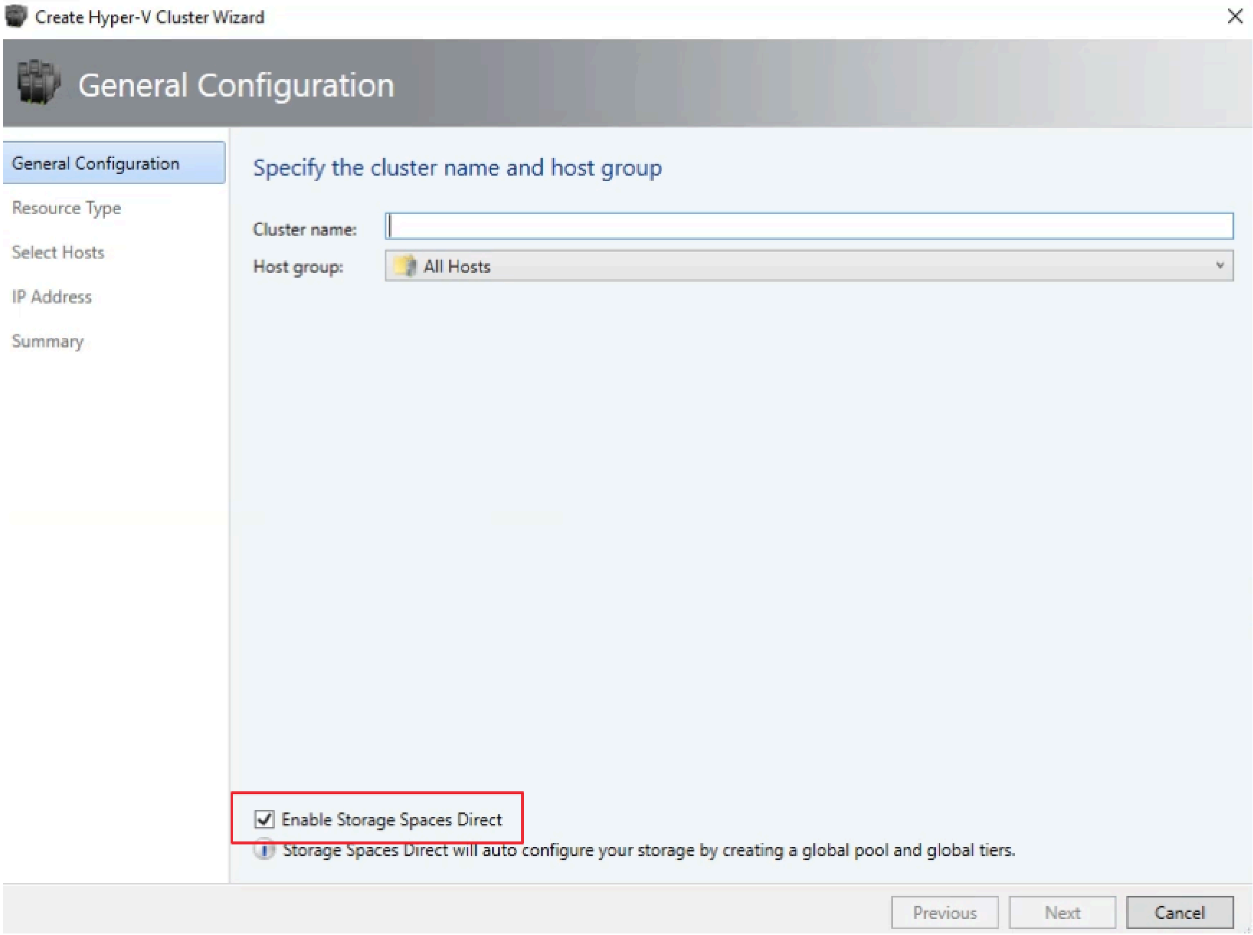
ⓘ Note

Live migration between Azure Stack HCI clusters works, as well as between Windows Server clusters.

- The only storage type available for Azure Stack HCI is Storage Spaces Direct (S2D). Creation or management of non-S2D cluster with Azure Stack HCI nodes isn't supported. If you need to use any other type of storage, for example SANs, use Windows Server as the virtualization host.

ⓘ Note

You must enable S2D when creating an Azure Stack HCI cluster. To enable S2D, in the cluster creation wizard, go to **General Configuration**. Under **Specify the cluster name and host group**, select **Enable Storage Spaces Direct** as shown below:



Create Hyper-V Cluster Wizard

General Configuration

Specify the cluster name and host group

Cluster name:

Host group: All Hosts

☑ Enable Storage Spaces Direct

Storage Spaces Direct will auto configure your storage by creating a global pool and global tiers.

After you enable a cluster with S2D, VMM does the following:

- The Failover Clustering feature is enabled.
- Storage replica and data deduplication are enabled.
- The cluster is optionally validated and created.

- S2D is enabled, and a storage array object is created in VMM with the same name as you provided in the wizard.

When you use VMM to create a hyper-converged cluster, the pool and the storage tiers are automatically created by running `Enable-ClusterStorageSpacesDirect -Autoconfig $True`.

After these prerequisites are in place, you provision a cluster, and set up storage resources on it. You can then deploy VMs on the cluster.

Follow these steps:

Step 1: Provision the cluster

You can provision a cluster by Hyper-V hosts and bare-metal machines:

Provision a cluster from Hyper-V hosts

If you need to add the Azure Stack HCI hosts to the VMM fabric, follow these steps. If they're already in the VMM fabric, skip to the next step.

ⓘ Note

- When you set up the cluster, select the **Enable Storage Spaces Direct** option on the **General Configuration** page of the **Create Hyper-V Cluster** wizard.
- In **Resource Type**, select **Existing servers running a Windows Server operating system**, and select the Hyper-V hosts to add to the cluster.
- All the selected hosts must have Azure Stack HCI installed.
- Since S2D is enabled, the cluster must be validated.

Provision a cluster from bare metal machines

ⓘ Note

Typically, S2D node requires RDMA, QoS, and SET settings. To configure these settings for a node using bare metal computers, you can use the post deployment script capability in PCP. Here's the sample PCP post deployment script. You can also use this script to configure RDMA, QoS, and SET while adding a new node to an existing S2D deployment from bare metal computers.

1. Read the prerequisites for bare-metal cluster deployment.

> ⓘ **Note**
>
> - The generalized VHD or VHDX in the VMM library must be running Azure Stack HCI with the latest updates. The **Operating system** and **Virtualization platform** values for the hard disk must be set.
> - For bare-metal deployment, you need to add a pre-boot execution environment (PXE) server to the VMM fabric. The PXE server is provided through Windows Deployment Services. VMM uses its own WinPE image, and you need to ensure that it's the latest. To do this, select **Fabric** > **Infrastructure** > **Update WinPE image**, and ensure that the job finishes.

2. Follow the instructions for provisioning a cluster from bare-metal computers.

Step 2: Set up networking for the cluster

After the cluster is provisioned and managed in the VMM fabric, you need to set up networking for cluster nodes.

1. Start by creating a logical network to mirror your physical management network.
2. You need to set up a logical switch with Switch Embedded Teaming (SET) enabled so that the switch is aware of virtualization. This switch is connected to the management logical network and has all of the host virtual adapters, which are required to provide access to the management network or configure storage networking. S2D relies on a network to communicate between hosts. RDMA-capable adapters are recommended.
3. Create VM networks.

Step 3: Configure DCB settings on the Azure Stack HCI cluster

> ⓘ **Note**
>
> Configuration of DCB settings is an optional step to achieve high performance during S2D cluster creation workflow. Skip to step 4 if you do not wish to configure DCB settings.

Recommendations

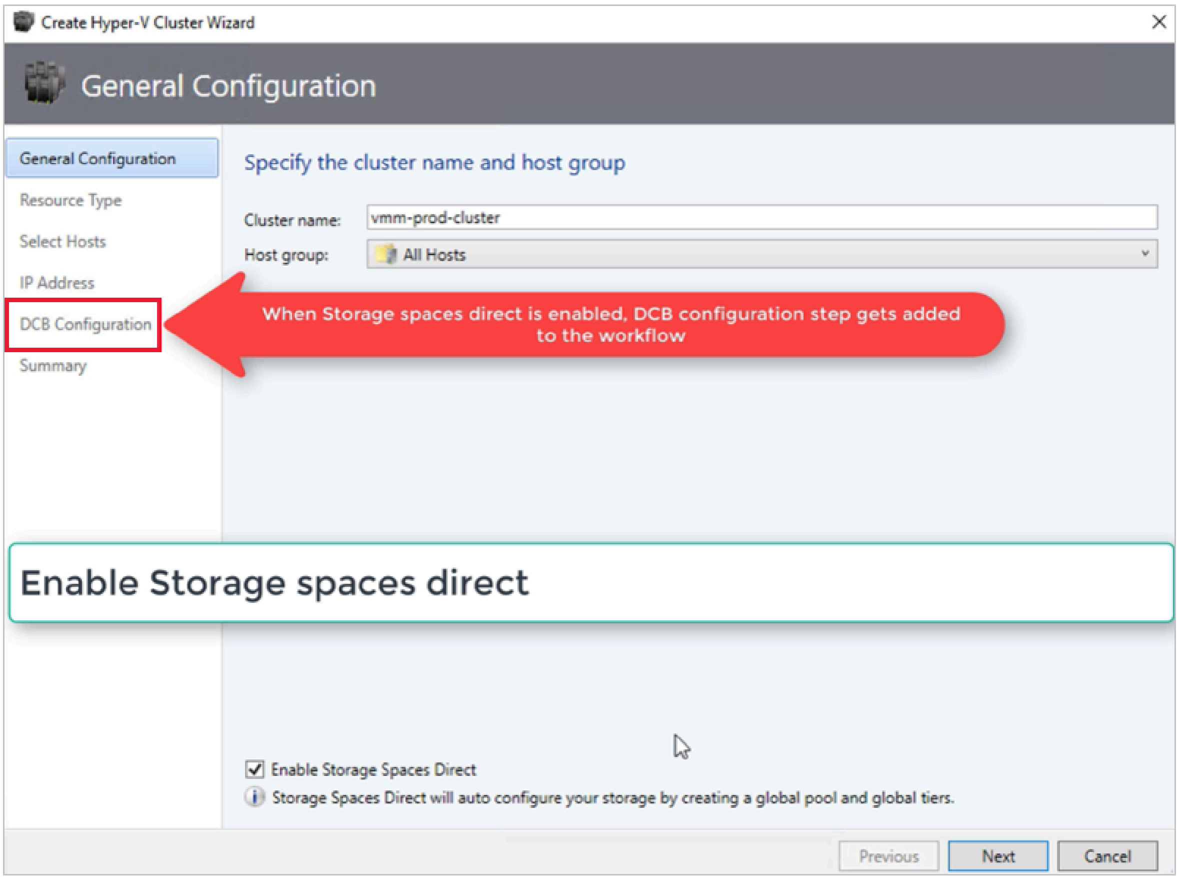
- If you've vNICs deployed, for optimal performance, we recommend you to map all your vNICs with the corresponding pNICs. Affinities between vNIC and pNIC are set randomly by the operating system, and there could be scenarios where multiple vNICs are mapped to the same pNIC. To avoid such scenarios, we recommend you to manually set affinity between vNIC and pNIC by following the steps listed here.
- When you create a network adapter port profile, we recommend you to allow **IEEE priority**. Learn more.

  You can also set the IEEE Priority using the following PowerShell commands:

  ```PowerShell
  Set-VMNetworkAdapterVlan -VMNetworkAdapterName 'SMB2' -VlanId '101' -
  Access -ManagementOS
  Set-VMNetworkAdapter -ManagementOS -Name 'SMB2' -IeeePriorityTag on
  ```

Use the following steps to configure DCB settings:

1. Create a new Hyper-V cluster, select **Enable Storage Spaces Direct**. *DCB Configuration* option gets added to the Hyper-V cluster creation workflow.



Create Hyper-V Cluster Wizard

General Configuration

Specify the cluster name and host group

Cluster name: vmm-prod-cluster

Host group: All Hosts

When Storage spaces direct is enabled, DCB configuration step gets added to the workflow

Enable Storage spaces direct

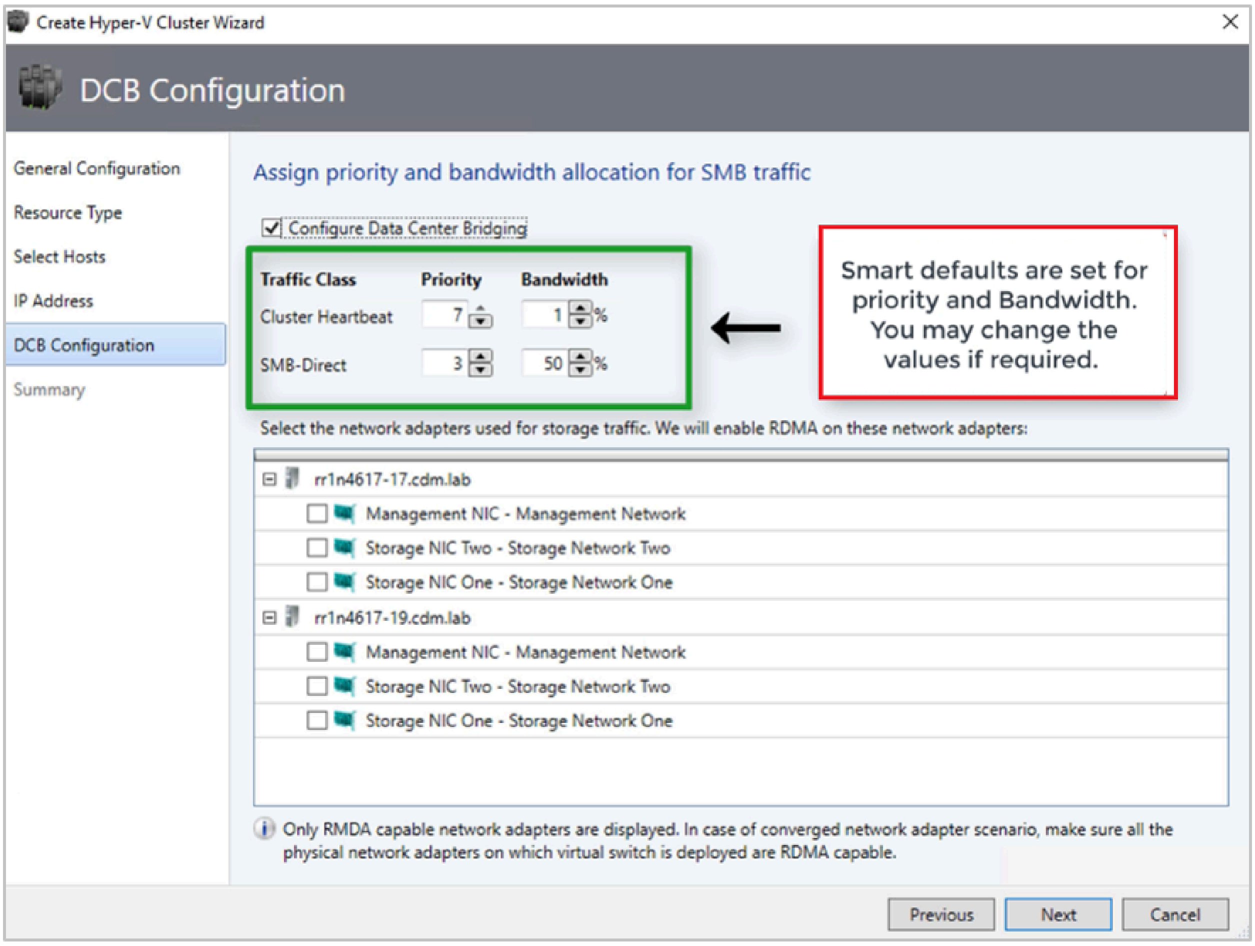
☑ Enable Storage Spaces Direct

Storage Spaces Direct will auto configure your storage by creating a global pool and global tiers.

2. In **DCB configuration**, select **Configure Data Center Bridging**.

3. Provide **Priority** and **Bandwidth** values for SMB-Direct and Cluster Heartbeat traffic.

> ⓘ Note
>
> Default values are assigned to **Priority** and **Bandwidth**. Customize these values based on your organization's environment needs.



Assign priority and bandwidth allocation for SMB traffic

☑ Configure Data Center Bridging

Traffic Class	Priority	Bandwidth
Cluster Heartbeat	7	1 %
SMB-Direct	3	50 %

Smart defaults are set for priority and Bandwidth. You may change the values if required.

Select the network adapters used for storage traffic. We will enable RDMA on these network adapters:

- rr1n4617-17.cdm.lab
  - □ Management NIC - Management Network
  - □ Storage NIC Two - Storage Network Two
  - □ Storage NIC One - Storage Network One
- rr1n4617-19.cdm.lab
  - □ Management NIC - Management Network
  - □ Storage NIC Two - Storage Network Two
  - □ Storage NIC One - Storage Network One

ⓘ Only RMDA capable network adapters are displayed. In case of converged network adapter scenario, make sure all the physical network adapters on which virtual switch is deployed are RDMA capable.

Default values:

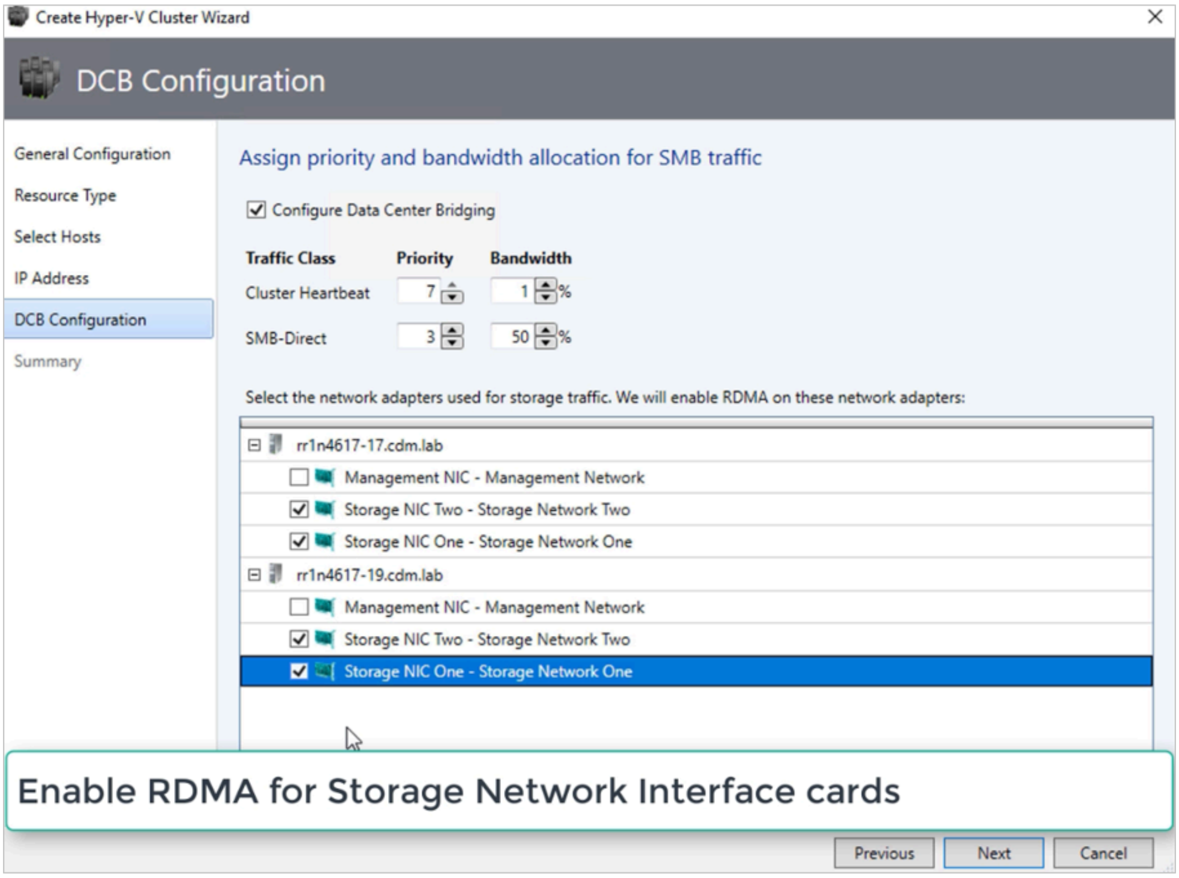
⛶ Expand table

Traffic Class	Priority	Bandwidth (%)
Cluster Heartbeat	7	1
SMB-Direct	3	50

4. Select the network adapters used for storage traffic. RDMA is enabled on these network adapters.

ⓘ Note

In a converged NIC scenario, select the storage vNICs. The underlying pNICs must be RDMA capable for vNICs to be displayed and available for selection.



Assign priority and bandwidth allocation for SMB traffic

☑ Configure Data Center Bridging

Traffic Class	Priority	Bandwidth
Cluster Heartbeat	7	1 %
SMB-Direct	3	50 %

Select the network adapters used for storage traffic. We will enable RDMA on these network adapters:

- rr1n4617-17.cdm.lab
  - □ Management NIC - Management Network
  - ☑ Storage NIC Two - Storage Network Two
  - ☑ Storage NIC One - Storage Network One
- rr1n4617-19.cdm.lab
  - □ Management NIC - Management Network
  - ☑ Storage NIC Two - Storage Network Two
  - ☑ Storage NIC One - Storage Network One

Enable RDMA for Storage Network Interface cards

5. Review the summary and select **Finish**.

An Azure Stack HCI cluster will be created and the DCB parameters are configured on all the S2D nodes.

ⓘ Note

- DCB settings can be configured on the existing Hyper-V S2D clusters by visiting the **Cluster Properties** page and navigating to the **DCB configuration** page.
- Any out-of-band changes to DCB settings on any of the nodes will cause the S2D cluster to be non-compliant in VMM. A Remediate option will be provided in the **DCB configuration** page of cluster properties, which you can use to enforce the DCB settings configured in VMM on the cluster nodes.

Step 4: Register Azure Stack HCI cluster with Azure

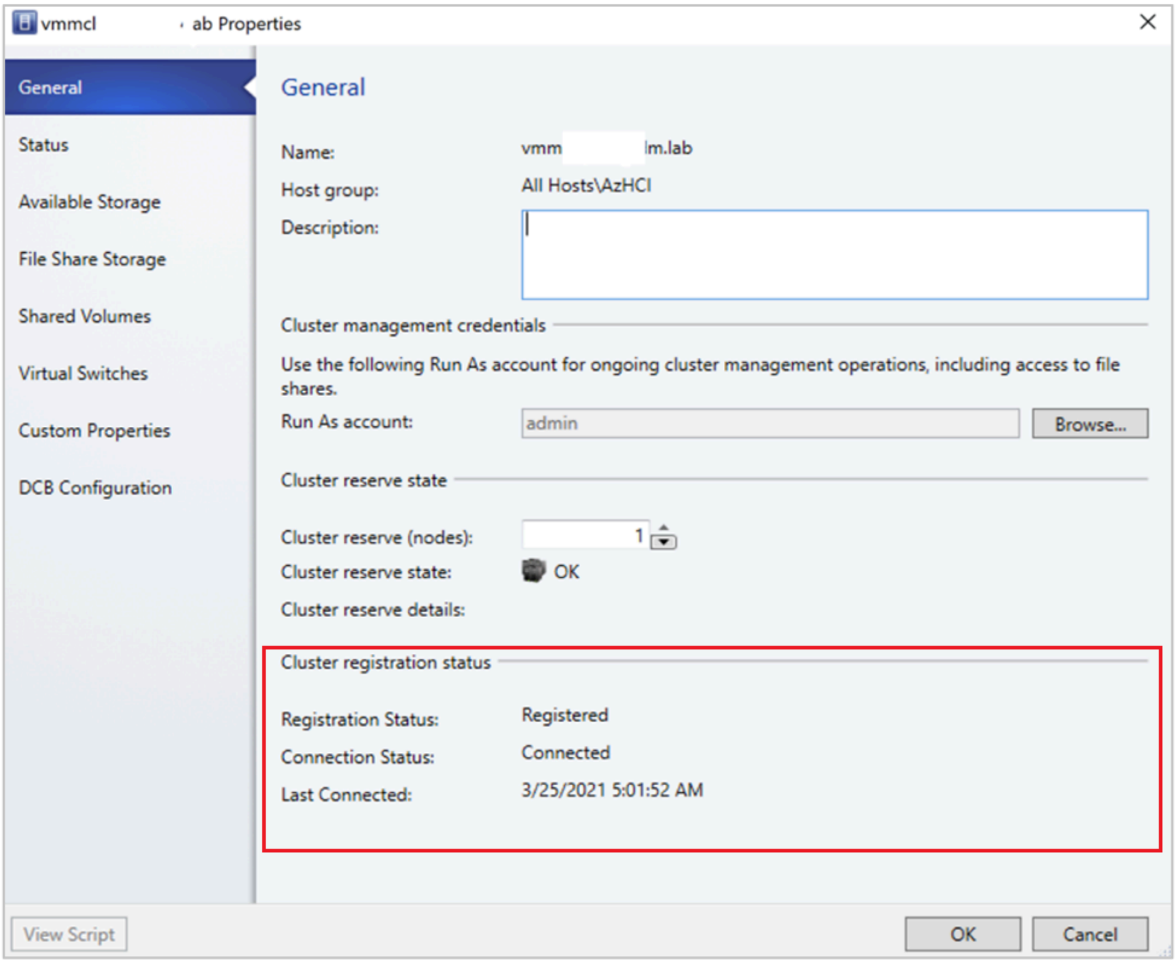
After creating an Azure Stack HCI cluster, it must be registered with Azure within 30 days of installation per Azure Online Service terms. If you're using System Center 2022, use `Register-SCAzStackHCI` cmdlet in VMM to register the Azure Stack HCI cluster with Azure. Alternatively, follow these steps to register the Azure Stack HCI cluster with Azure.

The registration status will reflect in VMM after a successful cluster refresh.

Step 5: View the registration status of Azure Stack HCI clusters

1. In the VMM console, you can view the registration status and last connected date of Azure Stack HCI clusters.

2. Select **Fabric**, right-click the **Azure Stack HCI** cluster, and select **Properties**.



General

Name: vmm lm.lab
Host group: All Hosts\AzHCI
Description:

Cluster management credentials

Use the following Run As account for ongoing cluster management operations, including access to file shares.

Run As account: admin

Cluster reserve state

Cluster reserve (nodes): 1
Cluster reserve state: OK
Cluster reserve details:

Cluster registration status

Registration Status: Registered
Connection Status: Connected
Last Connected: 3/25/2021 5:01:52 AM

3. Alternatively, run `Get-SCVMHost` and observe the properties of returned object to check the registration status.

Step 6: Manage the pool and create CSVs

You can now modify the storage pool settings and create virtual disks and CSVs.

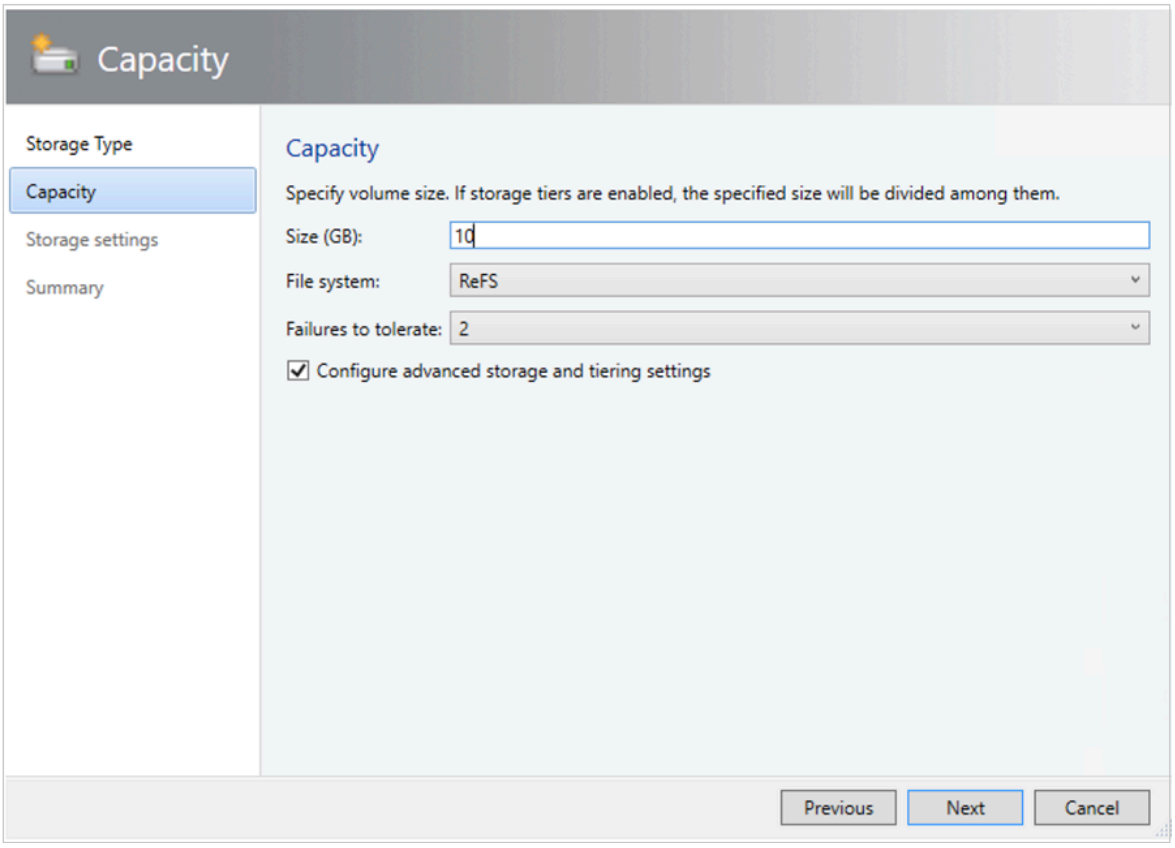
1. Select **Fabric** > **Storage** > **Arrays**.

2. Right-click the cluster > **Manage Pool**, and select the storage pool that was created by default. You can change the default name and add a classification.

3. To create a CSV, right-click the cluster > **Properties** > **Shared Volumes**.

4. In the **Create Volume Wizard** > **Storage Type**, specify the volume name and select the storage pool.

5. In **Capacity**, you can specify the volume size, file system, and resiliency (Failures to tolerate) settings.



Capacity

Specify volume size. If storage tiers are enabled, the specified size will be divided among them.

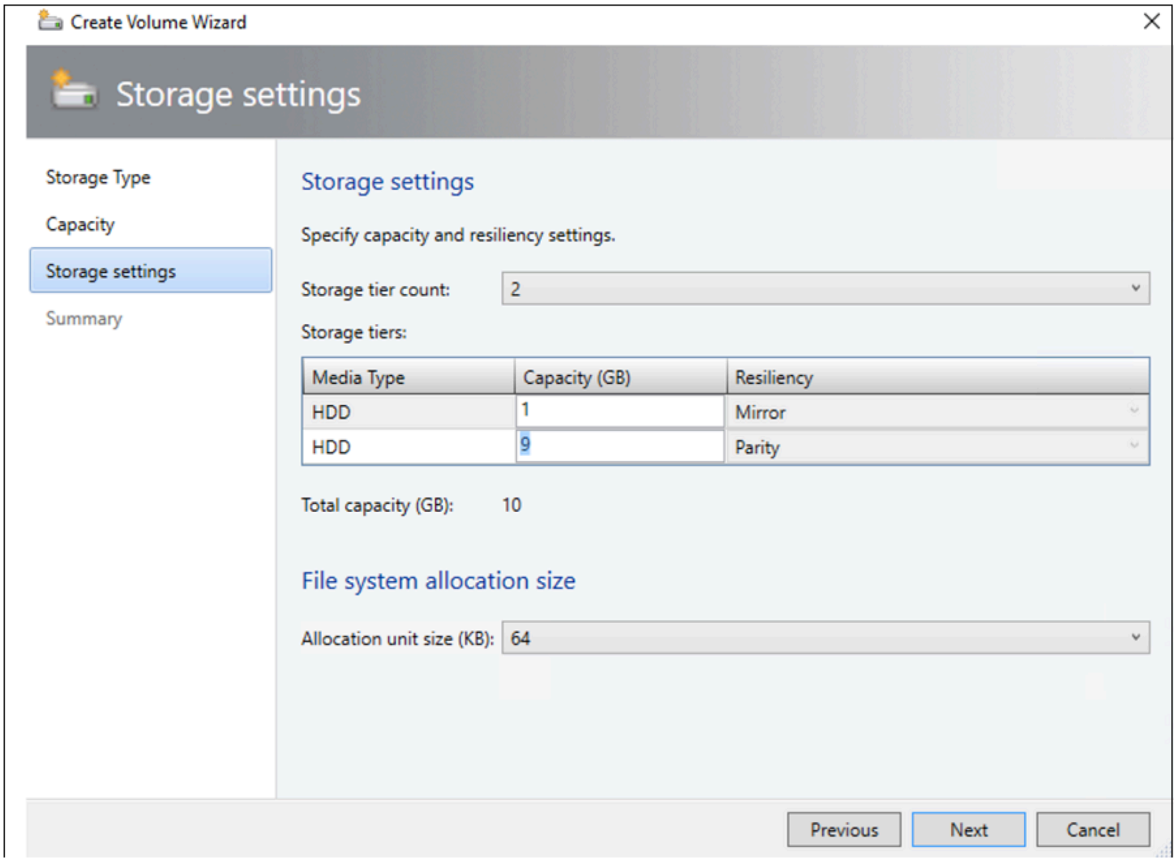
Size (GB): 10

File system: ReFS

Failures to tolerate: 2

☑ Configure advanced storage and tiering settings

6. Select **Configure advanced storage and tiering settings** to set up these options.



Storage settings

Specify capacity and resiliency settings.

Storage tier count: 2

Storage tiers:

Media Type	Capacity (GB)	Resiliency
HDD	1	Mirror
HDD	9	Parity

Total capacity (GB): 10

File system allocation size

Allocation unit size (KB): 64

7. In **Summary**, verify settings and finish the wizard. A virtual disk will be created automatically when you create the volume.

Step 7: Deploy VMs on the cluster

In a hyper-converged topology, VMs can be directly deployed on the cluster. Their virtual hard disks are placed on the volumes you created using S2D. You create and deploy these VMs just as you would create any other VM.

> ⓘ **Important**
>
> If the Azure Stack HCI cluster isn't registered with Azure or not connected to Azure for more than 30 days post registration, high availability virtual machine (HAVM) creation will be blocked on the cluster. Refer to step 4 and 5 for cluster registration.

Step 8: Migrate VMs from Windows Server to Azure Stack HCI cluster

Use Network migration functionality in VMM to migrate workloads from Hyper-V (Windows Server 2019 and later) to Azure Stack HCI.

ⓘ Note

Live migration between Windows Server and Azure Stack HCI isn't supported. Network migration from Azure Stack HCI to Windows Server isn't supported.

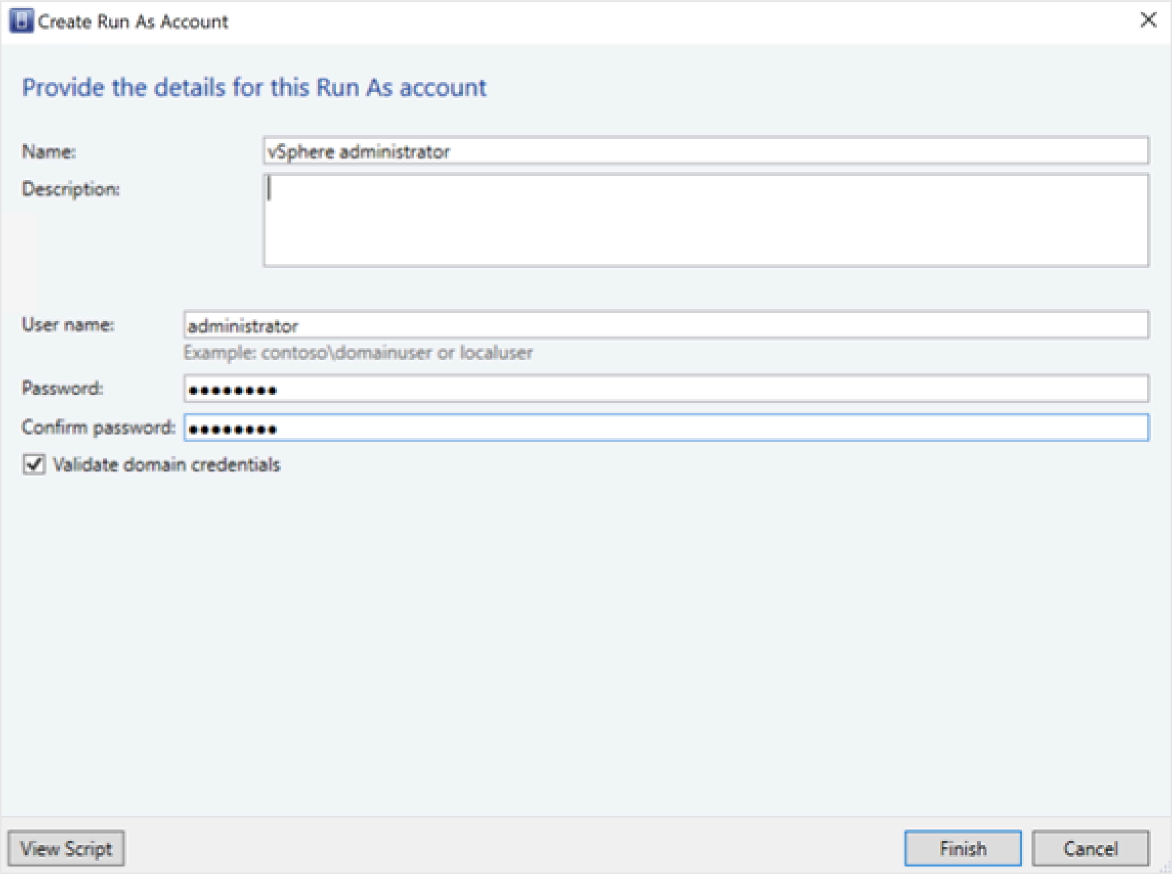
1. Temporarily disable the live migration at the destination Azure Stack HCI host.
2. Select VMs and Services > All Hosts, and then select the source Hyper-V host from which you want to migrate.
3. Select the VM that you want to migrate. The VM must be in a turned off state.
4. Select Migrate Virtual Machine.
5. In Select Host, review and select the destination Azure Stack HCI host.
6. Select Next to initiate network migration. VMM will perform imports and exports at the back end.
7. To verify that the virtual machine is successfully migrated, check the VMs list on the destination host. Turn on the VM and re-enable live migration on the Azure Stack HCI host.

Step 9: Migrate VMware workloads to Azure Stack HCI cluster using SCVMM

VMM offers a simple wizard-based experience for V2V (Virtual to Virtual) conversion. You can use the conversion tool to migrate workloads at scale from VMware infrastructure to Hyper-V infrastructure. For the list of supported VMware servers, see System requirements.

For prerequisites and limitations for the conversion, see Convert a VMware VM to Hyper-V in the VMM fabric.

1. Create **Run as account** for vCenter Server Administrator role in VMM. These administrator credentials are used to manage vCenter server and ESXi hosts.



Create Run As Account

Provide the details for this Run As account

Name: vSphere administrator

Description:

User name: administrator

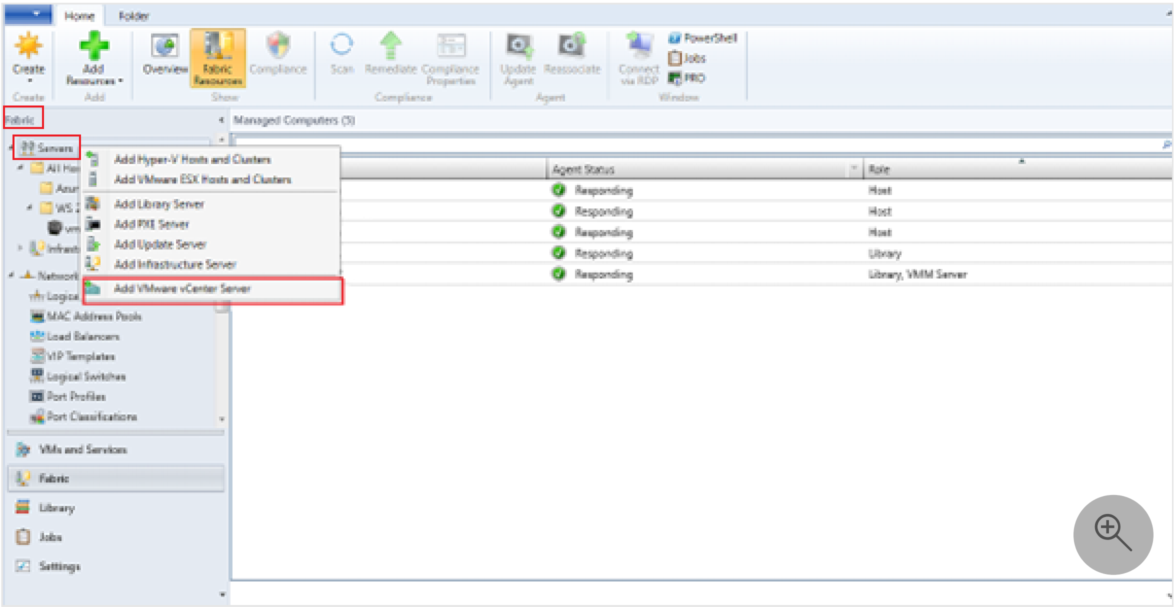
Example: contoso\domainuser or localuser

Password: ••••••••

Confirm password: ••••••••

☑ Validate domain credentials

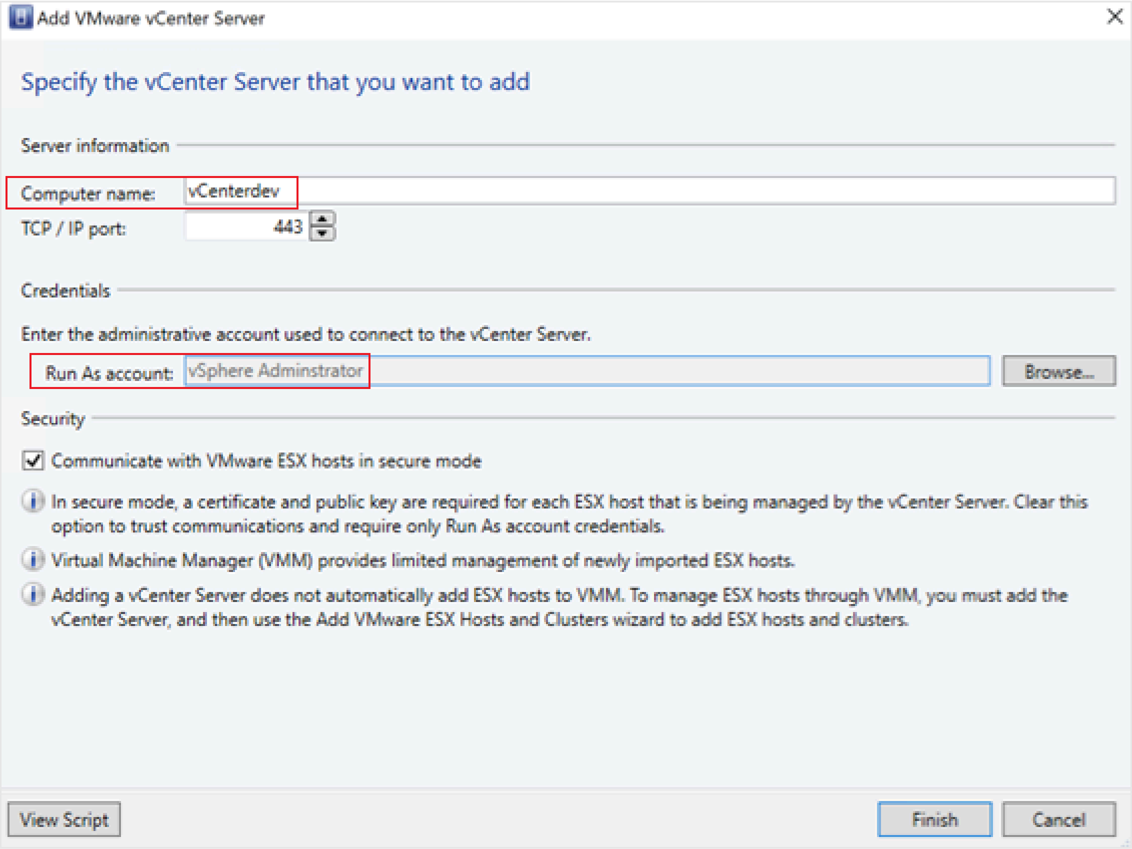
2. In the VMM console, under **Fabric**, select **Servers** > **Add VMware vCenter Server**.



3. In the **Add VMware vCenter Server** page, do the following:

    a. **Computer name**: Specify the vCenter server name.

b. **Run As account**: Select the Run As account created for vSphere administrator.



Add VMware vCenter Server

Specify the vCenter Server that you want to add

Server information

Computer name: vCenterdev

TCP / IP port: 443

Credentials

Enter the administrative account used to connect to the vCenter Server.

Run As account: vSphere Adminstrator

Security

☑ Communicate with VMware ESX hosts in secure mode

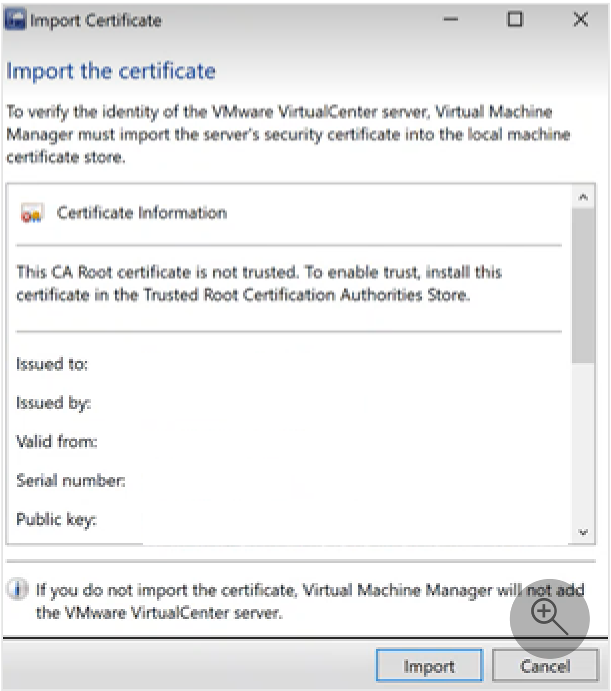
In secure mode, a certificate and public key are required for each ESX host that is being managed by the vCenter Server. Clear this option to trust communications and require only Run As account credentials.

Virtual Machine Manager (VMM) provides limited management of newly imported ESX hosts.

Adding a vCenter Server does not automatically add ESX hosts to VMM. To manage ESX hosts through VMM, you must add the vCenter Server, and then use the Add VMware ESX Hosts and Clusters wizard to add ESX hosts and clusters.

4. Select **Finish**.

5. In the **Import Certificate** page, select **Import**.



Import Certificate

Import the certificate

To verify the identity of the VMware VirtualCenter server, Virtual Machine Manager must import the server's security certificate into the local machine certificate store.

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities Store.

Issued to:

Issued by:

Valid from:

Serial number:

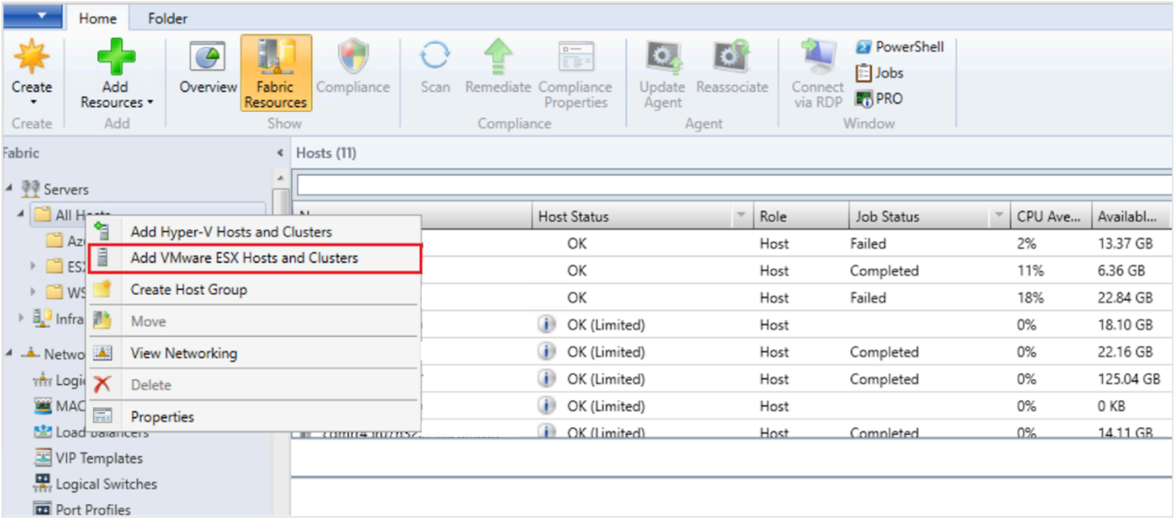
Public key:

If you do not import the certificate, Virtual Machine Manager will not add the VMware VirtualCenter server.

6. After the successful addition of the vCenter server, all the ESXi hosts under the vCenter are migrated to VMM.

Add Hosts

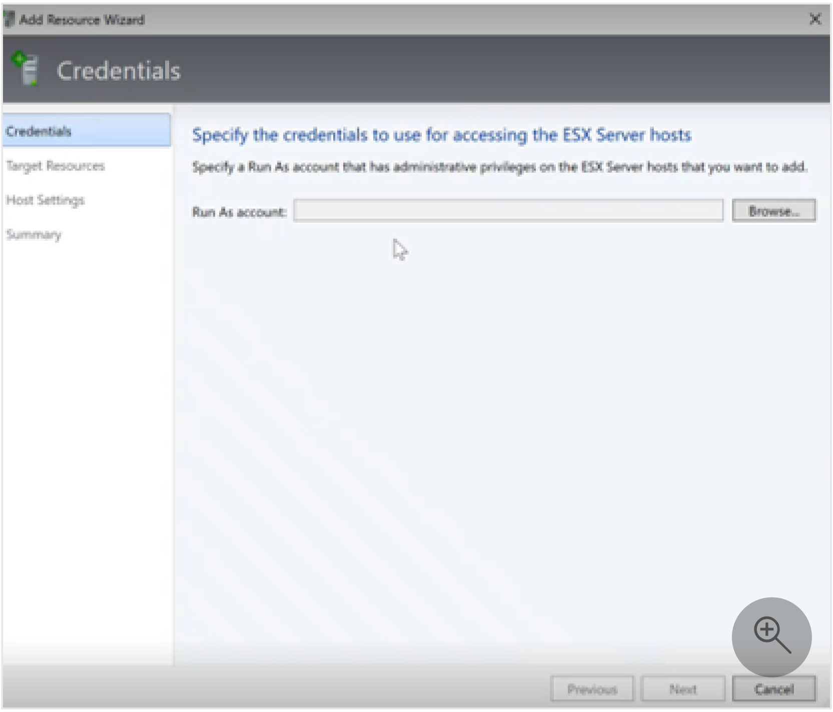
1. In the VMM console, under **Fabric**, select **Servers** > **Add VMware ESX Hosts and Clusters**.



Host Status	Role	Job Status	CPU Ave...	Availabl...
OK	Host	Failed	2%	13.37 GB
OK	Host	Completed	11%	6.36 GB
OK	Host	Failed	18%	22.84 GB
OK (Limited)	Host		0%	18.10 GB
OK (Limited)	Host	Completed	0%	22.16 GB
OK (Limited)	Host	Completed	0%	125.04 GB
OK (Limited)	Host		0%	0 KB
OK (Limited)	Host	Completed	0%	14.11 GB

2. In the **Add Resource Wizard**,

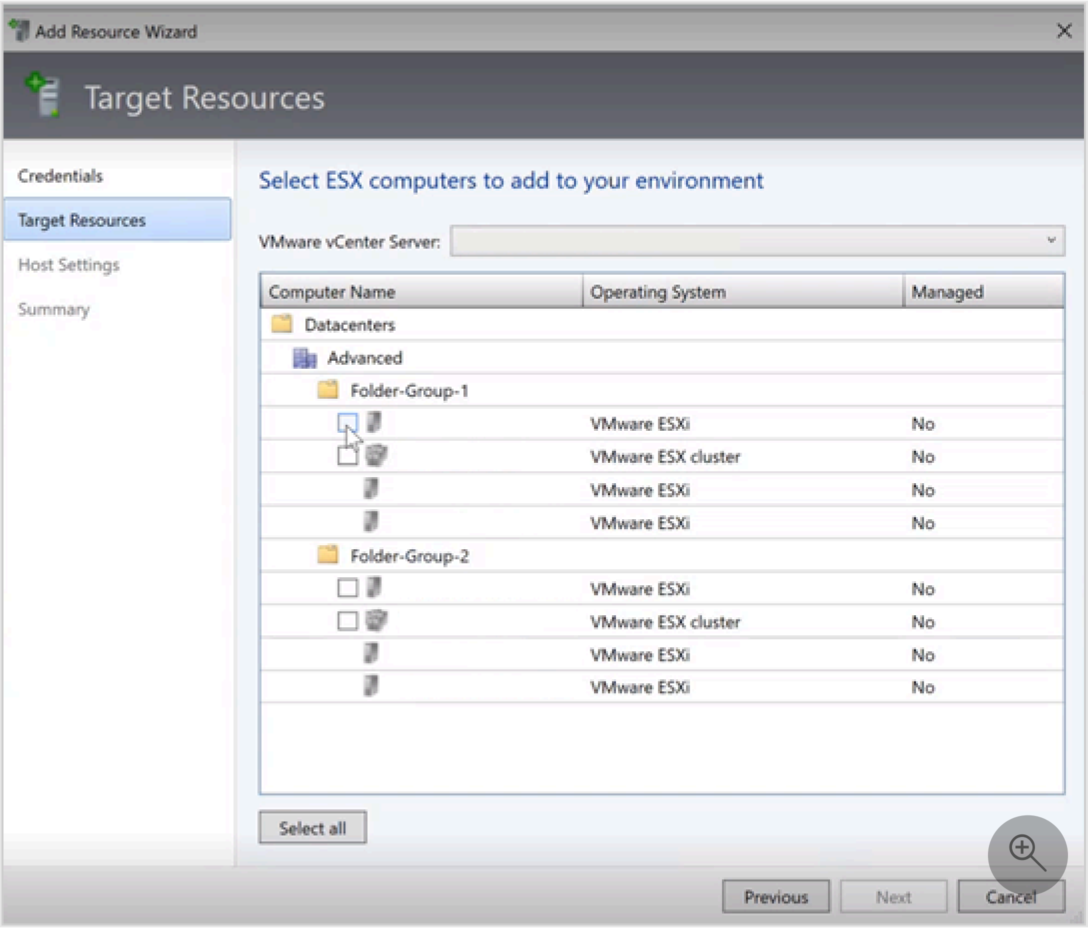
   a. Under **Credentials**, select the Run as account that is used for the port and select **Next**.



Specify the credentials to use for accessing the ESX Server hosts

Specify a Run As account that has administrative privileges on the ESX Server hosts that you want to add.

   b. Under **Target Resources**, select all the ESX clusters that need to be added to VMM and select **Next**.



Add Resource Wizard

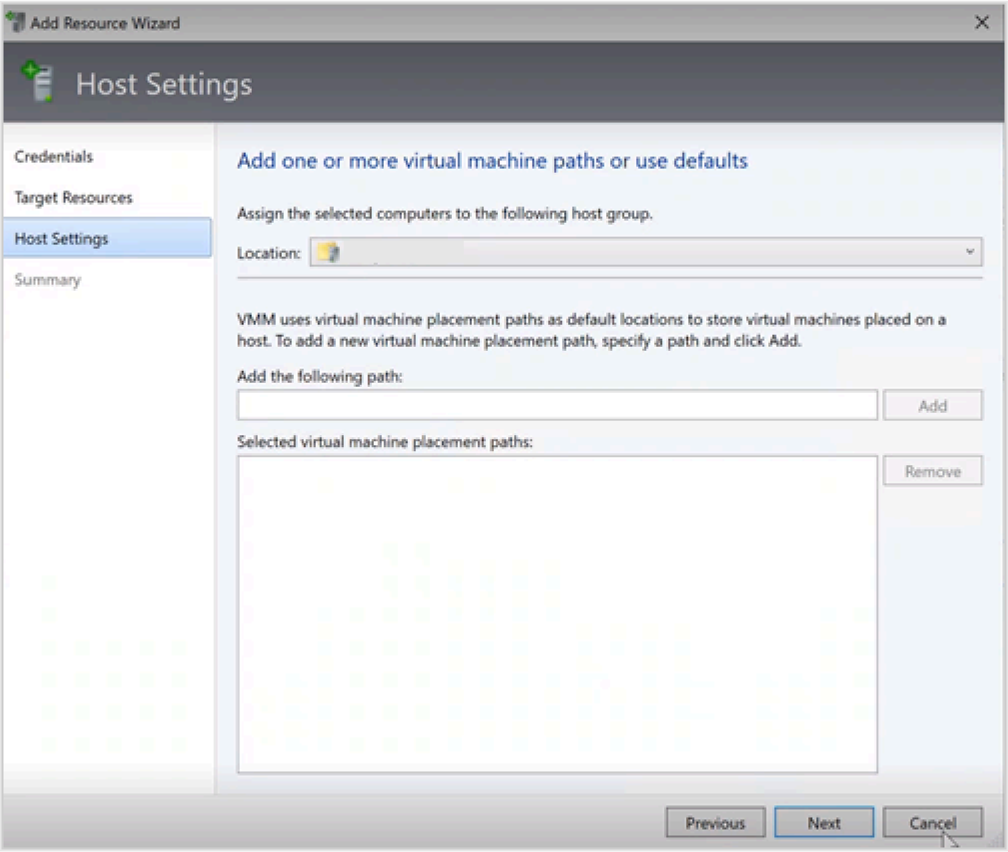
Target Resources

Select ESX computers to add to your environment

VMware vCenter Server:

Computer Name	Operating System	Managed
Datacenters		
Advanced		
Folder-Group-1		
□	VMware ESXi	No
□	VMware ESX cluster	No
	VMware ESXi	No
	VMware ESXi	No
Folder-Group-2		
□	VMware ESXi	No
□	VMware ESX cluster	No
	VMware ESXi	No
	VMware ESXi	No

c. Under **Host Settings**, select the location where you want to add the VMs and select **Next**.



Add Resource Wizard

Host Settings

Add one or more virtual machine paths or use defaults

Assign the selected computers to the following host group.

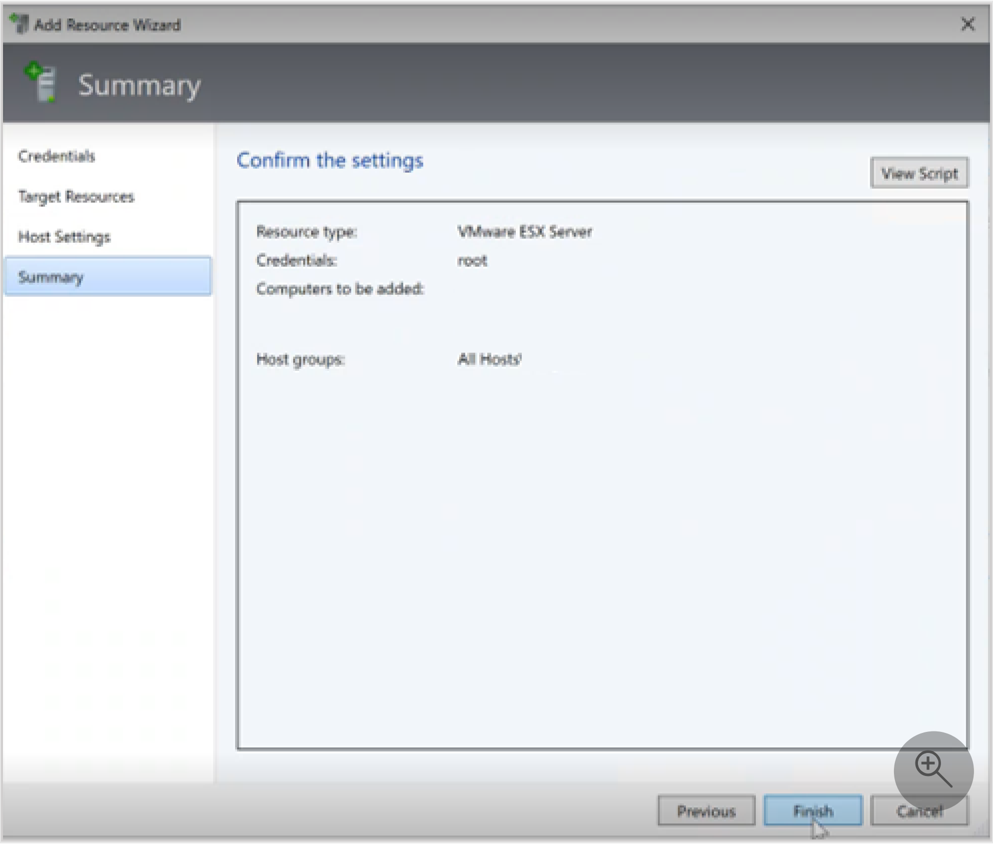
Location:

VMM uses virtual machine placement paths as default locations to store virtual machines placed on a host. To add a new virtual machine placement path, specify a path and click Add.

Add the following path:

Selected virtual machine placement paths:

d. Under **Summary**, review the settings and select **Finish**. Along with the hosts, associated VMs will also get added.

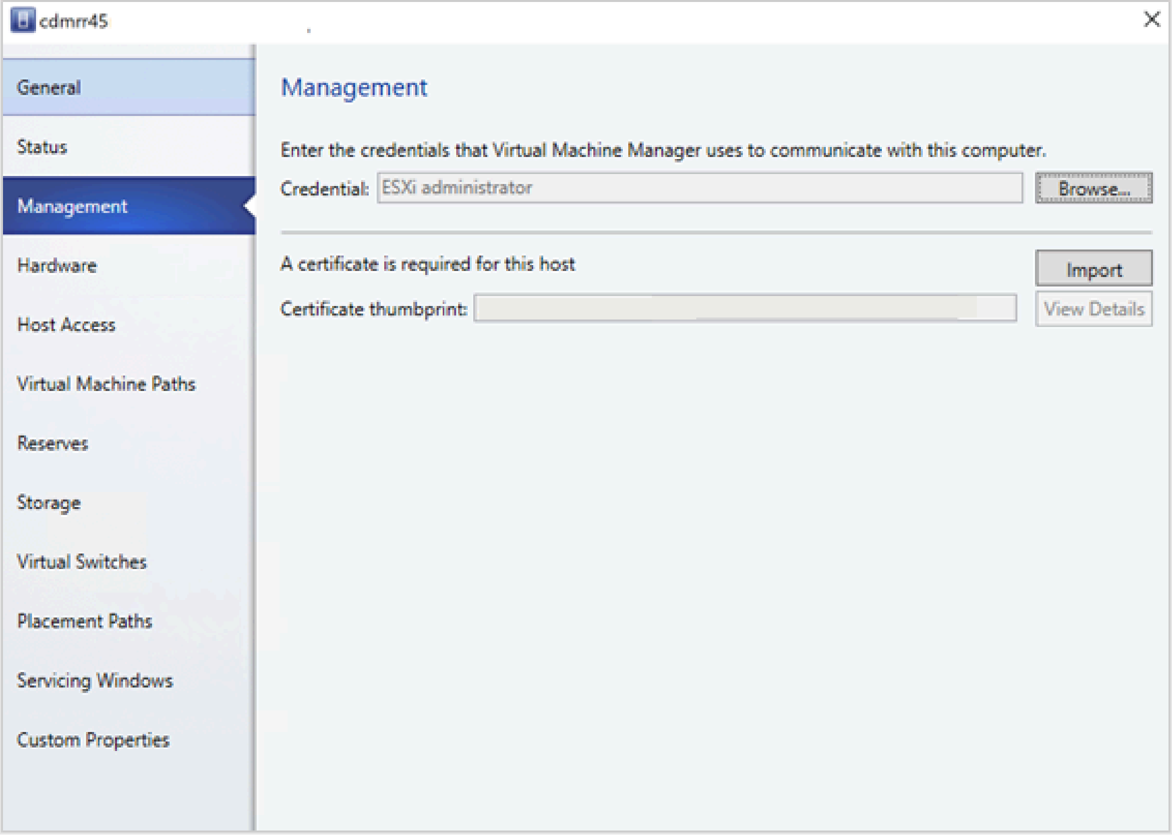


Resource type: VMware ESX Server
Credentials: root
Computers to be added:
Host groups: All Hosts\

Verify the status of ESXi host

1. If the ESXi host status reflects as **OK (Limited)**, right-click **Properties** > **Management**, select Run as account that is used for the port and import the certificates for the host.

   Repeat the same process for all the ESXi hosts.



Enter the credentials that Virtual Machine Manager uses to communicate with this computer.

Credential: ESXi administrator

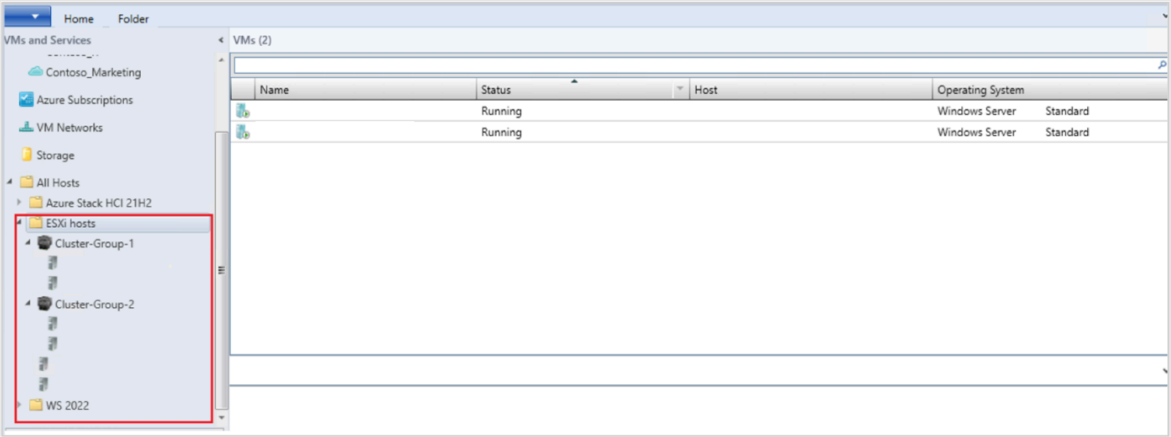
A certificate is required for this host

Certificate thumbprint:

After you add the ESXi clusters, all the virtual machines running on the ESXi clusters are auto discovered in VMM.

View VMs

1. Go to **VMs and Services** to view the virtual machines. You can also manage the primary lifecycle operations of these virtual machines from VMM.



VMs (2)

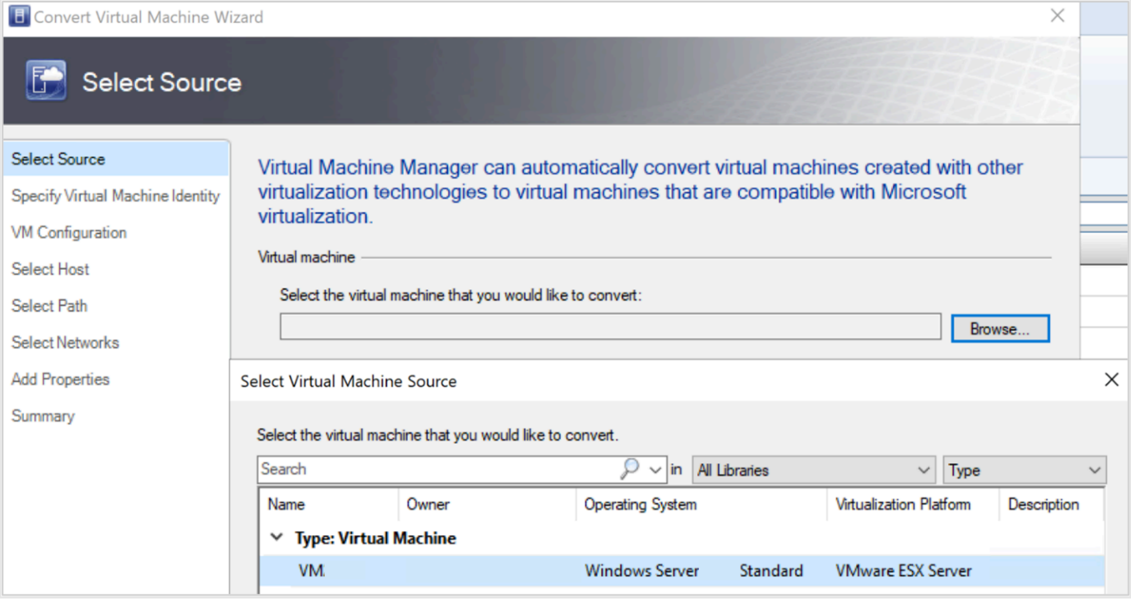
Name	Status	Host	Operating System	
	Running		Windows Server	Standard
	Running		Windows Server	Standard

2. Right-click the VM and select **Power Off** (online migrations aren't supported) that need to be migrated and uninstall VMware tools from the guest operating system.

3. Select **Home** > **Create Virtual Machines** > **Convert Virtual Machine**.

4. In the **Convert Virtual Machine Wizard**,

   a. Under **Select Source**, select the VM running in ESXi server and select **Next**.



Virtual Machine Manager can automatically convert virtual machines created with other virtualization technologies to virtual machines that are compatible with Microsoft virtualization.

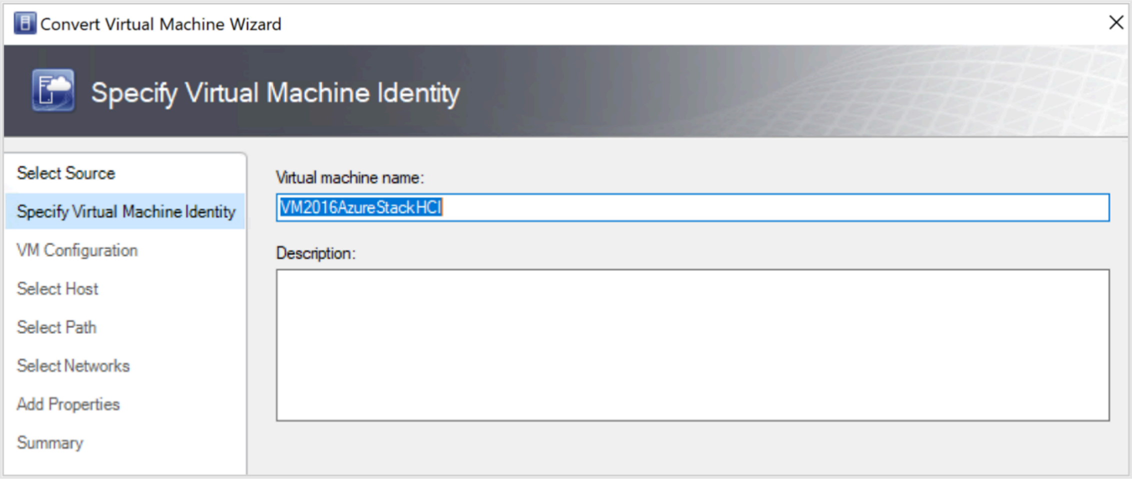
Virtual machine

Select the virtual machine that you would like to convert:

Select the virtual machine that you would like to convert.

Name	Owner	Operating System		Virtualization Platform	Description
Type: Virtual Machine					
VM		Windows Server	Standard	VMware ESX Server	

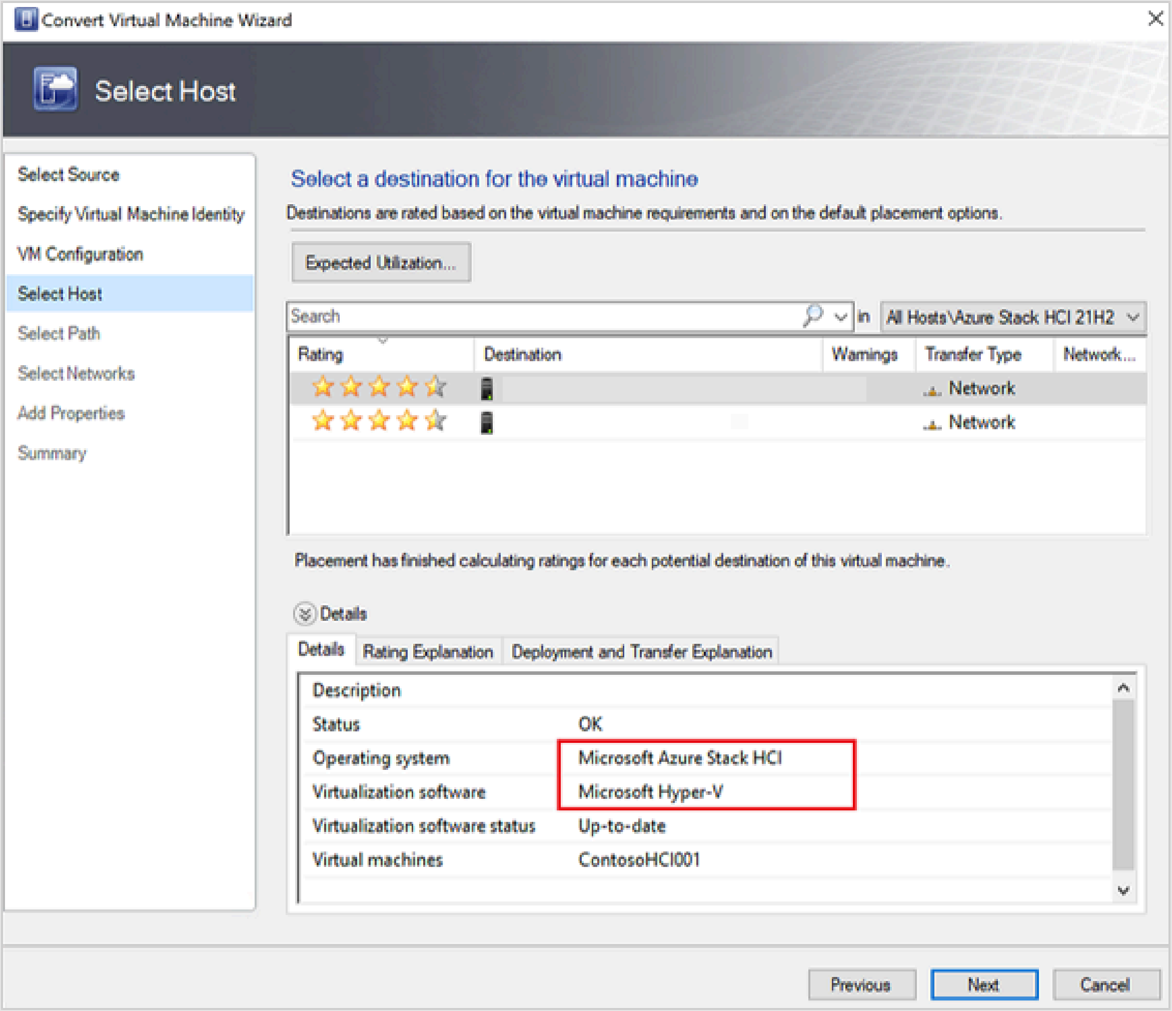
   b. Under **Specify Virtual Machine Identity**, enter the new name for the virtual machine if you wish to and select **Next**.


Convert Virtual Machine Wizard
Specify Virtual Machine Identity
Select Source
Specify Virtual Machine Identity
VM Configuration
Select Host
Select Path
Select Networks
Add Properties
Summary

Virtual machine name: VM2016AzureStackHCI

Description:

5. Under **Select Host**, select the target Azure Stack HCI node and specify the location on the host for VM storage files and select **Next**.



Select a destination for the virtual machine

Destinations are rated based on the virtual machine requirements and on the default placement options.

Rating	Destination	Warnings	Transfer Type	Network...
★★★★☆			Network	
★★★★☆			Network	

Placement has finished calculating ratings for each potential destination of this virtual machine.

Description	
Status	OK
Operating system	Microsoft Azure Stack HCI
Virtualization software	Microsoft Hyper-V
Virtualization software status	Up-to-date
Virtual machines	ContosoHCI001

6. Select a virtual network for the virtual machine and select **Create** to complete the migration.
The virtual machine running on the ESXi cluster is successfully migrated to Azure Stack HCI cluster. For automation, use PowerShell commands for conversion.

Next steps

- Provision VMs
- Manage the cluster

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

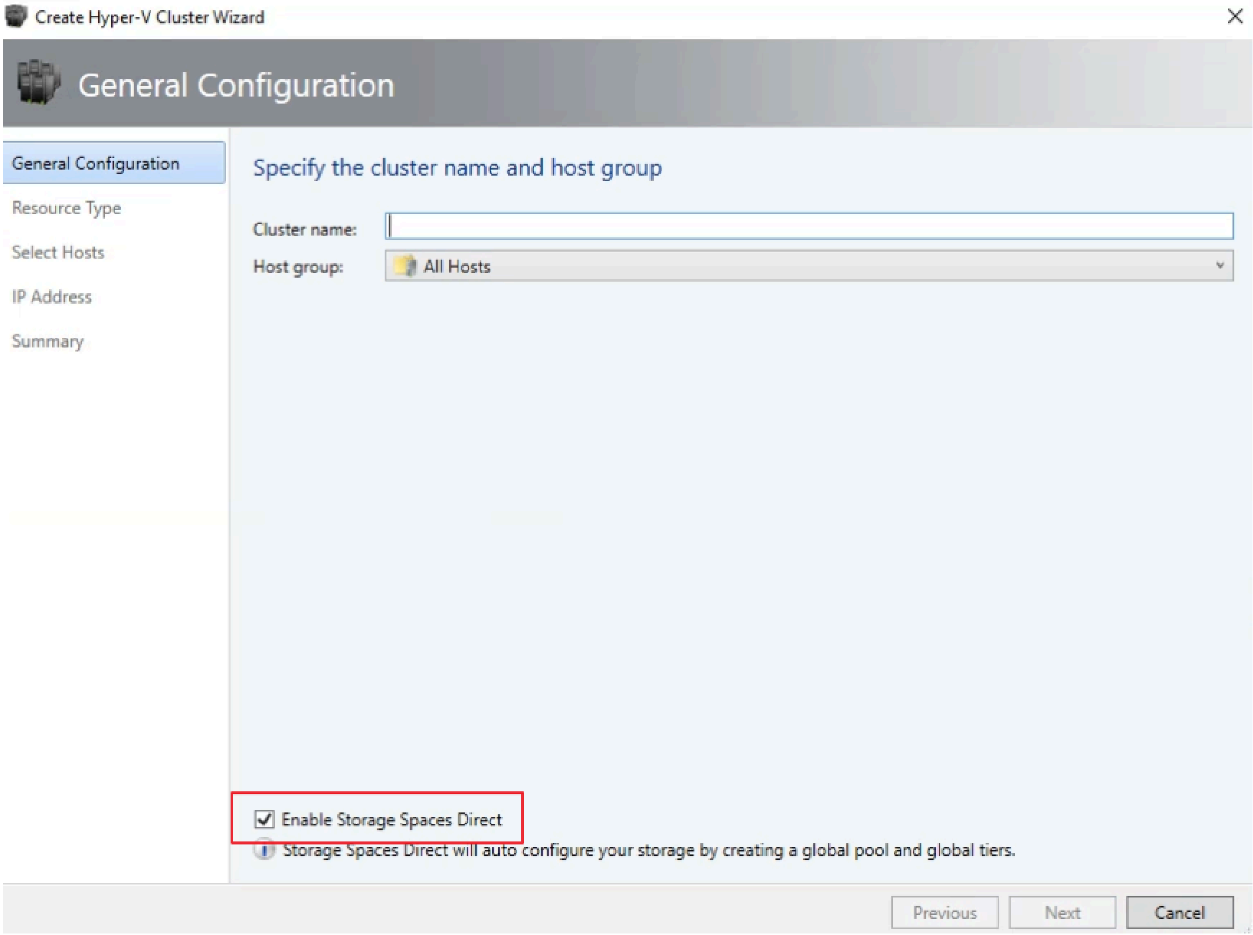
Deploy a Storage Spaces Direct disaggregated cluster in VMM

Article • 08/02/2024

Read this article to set up a disaggregated cluster running Storage Spaces Direct (S2D) in System Center Virtual Machine Manager (VMM). Learn more about S2D.

You can deploy a disaggregated S2D cluster by provisioning a cluster running Hyper-V hosts, and a separate storage cluster running scale-out file server (SOFS) with S2D.

> ⓘ Note
>
> You must enable S2D before adding the storage provider to VMM. To enable S2D, go to **General Configuration** > **Specify the cluster name and host group** and select the **Enable Storage Spaces Direct** option as shown below:



Cluster name:

Host group: All Hosts

☑ Enable Storage Spaces Direct

Storage Spaces Direct will auto configure your storage by creating a global pool and global tiers.

After you enable a disaggregated cluster with S2D, VMM does the following:

1. The File Server role and the Failover Clustering feature are enabled.
2. Storage replica and data deduplication are enabled.

3. The cluster is optionally validated and created.
4. S2D is enabled, and a storage array is created with the same name you provide in the wizard.

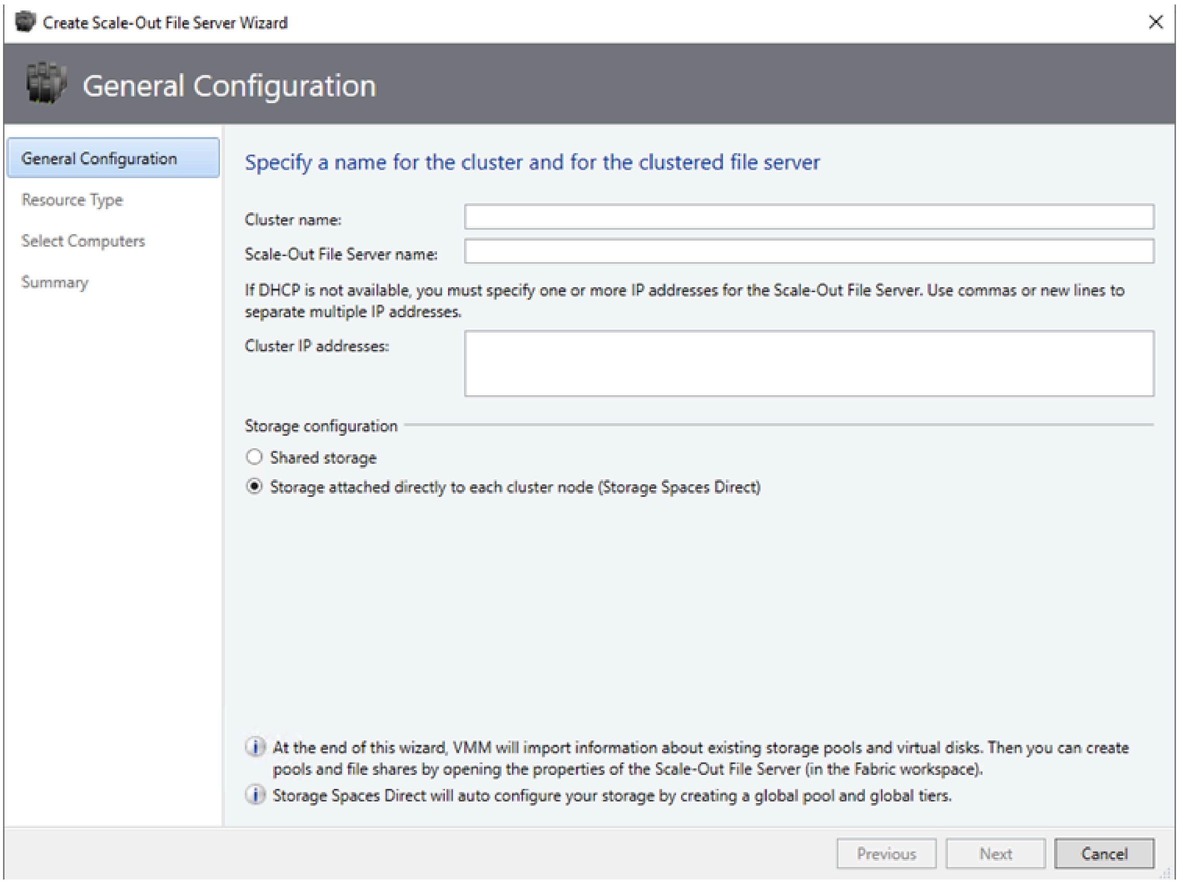
Step 1: Provision a SOFS cluster

You can provision a SOFS cluster from servers in the VMM fabric or add an existing SOFS cluster to the fabric

Provision a SOFS cluster

1. Select **Fabric Resources** > **Create** > **File Server Cluster**.

2. In **General Configuration**, specify a cluster name, select a host group, and select **Storage attached directly to each cluster node (Storage Spaces Direct)**.



Create Scale-Out File Server Wizard

General Configuration

Specify a name for the cluster and for the clustered file server

Cluster name:

Scale-Out File Server name:

If DHCP is not available, you must specify one or more IP addresses for the Scale-Out File Server. Use commas or new lines to separate multiple IP addresses.

Cluster IP addresses:

Storage configuration

○ Shared storage

● Storage attached directly to each cluster node (Storage Spaces Direct)

At the end of this wizard, VMM will import information about existing storage pools and virtual disks. Then you can create pools and file shares by opening the properties of the Scale-Out File Server (in the Fabric workspace).

Storage Spaces Direct will auto configure your storage by creating a global pool and global tiers.

3. In **Resource Type**, specify the RunAs account with local admin permissions on the servers you want to add to the cluster, and specify whether to add existing Windows servers or bare-metal machines.

4. In **Cluster Nodes**, define a list of computers to add to the cluster.

5. In **Summary**, confirm the settings and then select **Finish**.

If you want to add additional nodes to the SOFS cluster, VMM automatically discovers any disks associated with the node. When you modify a storage pool and select the new disks to add, VMM makes those disks available to the hosts and VMs that use the share supported by that pool. Learn more about adding nodes to a SOFS.

Add an existing SOFS cluster with S2D enabled

1. Select **Fabric** > **Add Resources** > **Storage Devices**.
2. In the Add Resource Wizard, select **Windows-based File Server**.
3. In **Discovery Scope**, specify the cluster IP address or FQDN. Provide a Run As account with cluster access, and specify if the cluster is in a different domain.
4. In **Storage Device**, select the SOFS to add to the VMM fabric. You must only assign a classification to the pool after you add the provider.
5. In **Summary**, check the settings and complete the wizard.

Step 2: Manage the pool and create file shares

After the SOFS cluster is provisioned and managed by VMM, you can modify the storage pool and create the storage.

1. Select **Fabric** > **Storage** > **Arrays**.
2. Right-click the cluster > **Manage Pool**, and select the storage pool that was created by default. You can change the default name and add a classification
3. After the pool appears with the new name if needed, select **Create File Share**.
4. In the Create File Share Wizard > **General**, specify a name for the share and select the pool from which storage must be taken.
5. In **Capacity**, specify the share size and settings.
6. In **Summary,** verify the settings. After the share is created, a new CSV is added under the storage pool.

Step 3: Allocate the storage in Hyper-V

1. In the Hyper-V host properties > **Storage**, specify the file share path.
2. Now, you can create VMs that use this file share.

Next steps

- Provision VMs
- Manage the cluster

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Manage Storage Spaces Direct clusters

Article • 08/22/2024

This article explains how to manage Storage Spaces Direct (S2D) clusters in the System Center Virtual Machine Manager (VMM) fabric.

Configure cluster settings

You can view and configure cluster settings, which include cluster status, failure management, and available storage.

Add a node to a hyper-converged cluster

You can add a new node on a hyper-converged S2D cluster in the VMM fabric. The new node can be an existing Hyper-V server or a bare-metal physical server.

> ⓘ **Note**
>
> Typically, S2D node requires Remote Direct Memory Access (RDMA), Quality of Service (QoS), and switch embedded teaming (SET) settings. To configure these settings for a node using bare-metal computers, you can use the post-deployment script capability in the physical computer profile (PCP). Here's the **sample PCP post-deployment script**. You can also use this script to configure RDMA, QoS, and SET when you add a new node to an existing S2D deployment from bare-metal computers.

- When you add a new node on a hyper-converged cluster, VMM automatically discovers disks on the new node and enables S2D.
- VMM disables maintenance mode on disks before adding them.

Control storage resources with QoS

Quality of Service in Windows Server provides a way to specify minimum and maximum resources that can be assigned to Hyper-V VMs using scale-out file share storage. QoS mitigates *noisy neighbor* issues and ensures that a single VM doesn't consume all storage resources.

Set up QoS policies for a file server or for specific virtual disks on the server.

Configure DCB settings on S2D clusters

With the advent of converged networking, organizations are using Ethernet as a converged network for their management and storage traffic. It's important for Ethernet networks to support a similar level for performance and losslessness compared to that of dedicated fiber channel networks. This similar level of support becomes more important when the use of S2D clusters is considered.

RDMA, in conjunction with data center bridging (DCB), helps to achieve a similar level of performance and losslessness in an Ethernet network compared to fiber channel networks.

The DCB settings must be consistent across all the hosts and the fabric network (switches). A misconfigured DCB setting in any one of the host or fabric devices is detrimental to the S2D performance.

To configure a DCB setting, use this procedure.

Next steps

Set storag3 QoS for clusters

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage storage QoS for clusters

Article • 08/02/2024

This article describes how to manage storage quality-of-service (QoS) policies for clusters in System Center Virtual Machine Manager (VMM).

Assign storage QoS policy for clusters

Windows server 2016 and later allows the deployments to use the storage QoS feature with any VHDs residing on a Cluster Shared Volume (CSV). In VMM 2016, the management of SQoS is limited to VHDs residing on the S2D hyper-converged type clusters and Scale-Out File Servers only (SOFS). Also, the scope of QoS policies is based on the storage arrays, which isn't scalable to the scenarios like SAN, where VMM only manages the compute cluster.

VMM supports QoS on all managed clusters and also SOFS running on Windows Server 2016 and later.

> ⓘ **Note**
>
> VMM 2022 supports Azure Stack Hyper Converged Infrastructure (HCI, version 20H2 and 21H2).

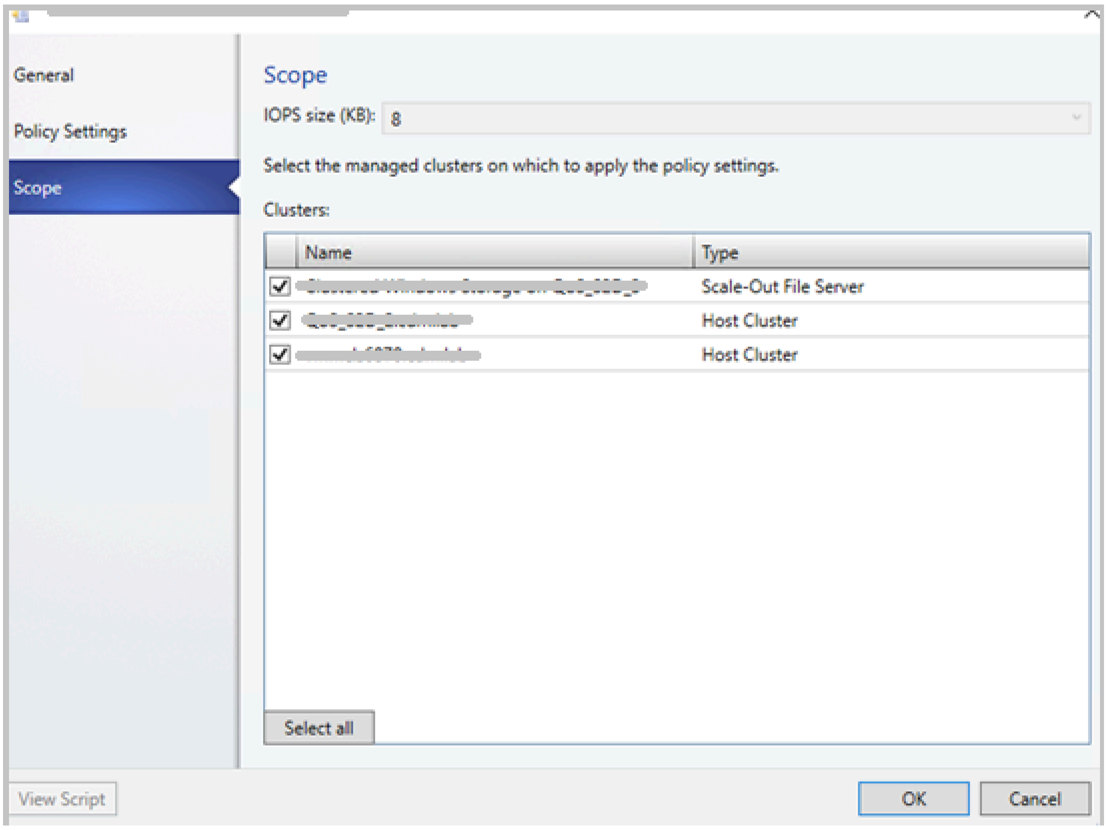
Use these steps:

1. Select **Fabric** > **Storage** > **QoS Policies** > **Create Storage QoS Policy**.

2. In the wizard > **General**, specify a policy name.

3. In **Policy Settings**, specify how the policy must apply. Select **All virtual disk instances share resources** to specify that the policy must be applied to all virtual disks on the file server (pooled, single instance). Select **Resources allocated to each virtual disk instance** to specify that the policy is applied separately to each specified virtual disk (multi-instance). Specify the minimum and maximum IOPS. A setting of 0 means that no policy is enforced.

4. In **Scope**, select the managed cluster under **Clusters** to which you want to apply the policy.



Scope

IOPS size (KB): 8

Select the managed clusters on which to apply the policy settings.

Clusters:

	Name	Type
☑	[redacted]	Scale-Out File Server
☑	[redacted]	Host Cluster
☑	[redacted]	Host Cluster

5. In **Summary**, verify the settings and finish the wizard.

On Upgrade

After upgrade, existing deployments that are managing their QoS with VMM can seamlessly migrate to the new QoS scoping based on the cluster name.

PowerShell cmdlets

The following new parameters are added:

Expand table

Affected cmdlet	Parameter	Details
New-SCStorageQoSPolicy	-HostCluster	Specifies an array of HostCluster objects for QoS policy scope. **Optional**.
New-SCVIrtualDiskDrive	-StorageQoSPolicy	Allows you to select the storage QoS policy for the Virtual Disk Drive. **Optional**.
Set-SCStorageQoSPolicy	-HostCluster	Specifies an array of HostCluster objects to be added in the QoS policy scope. **Optional**.
Get-SCStorageQoSPolicy	-HostCluster	Specifies a HostCluster object for which we want to query the QoS policies. **Optional**.

Assign a storage QoS Policy from templates

Templates usage is a common way for deploying VMs and Services on a cloud.

You can select storage QoS policies from a template as well. For information on how to assign storage QoS policies from templates, see the related procedure in the create a VM template article.

Next steps

Manage QoS

System requirements for System Center Virtual Machine Manager

Article • 07/10/2024

This article provides details of the system requirements for System Center 2022 - Virtual Machine Manager (VMM).

VMM 2022 system requirements

The following sections describe the scalability information, hardware, software, and SQL Server requirements for VMM 2022, and summarize the support for the servers managed in the VMM fabric.

Capacity limits

The following table provides the scale limits that were tested for System Center Virtual Machine Manager 2022. There are various factors that affect the scale limits, such as hardware configuration, network, topology, and others.

The planning guide provides the details about how these factors can be adapted to specific requirements.

Expand table

Entity	Recommended maximum count
Physical hosts	1000
Virtual Machines	25000
Services	1000
User roles	1000
Clouds	20
Virtual networks	2000
logical networks	20
Library resources	1000
Library Objects (templates, profiles)	100

Hardware

⛶ Expand table

Hardware	VMM server	VMM database	VMM library	VMM console
Processor (minimum)	8 core Pentium 4, 2 GHz (x64)	8 core Pentium 4, 2.8 GHz	4 core Pentium 4, 2.8 GHz	2 core Pentium 4, 1 GHz CPU
Processor (recommended)	16-core, 2.66 GHz CPU	16 core 2.6 GHz CPU	4 core 2.8 GHz CPU	2 core 2 GHz CPU
RAM (minimum)	4 GB	8 GB	2 GB	4 GB
RAM (recommended)	16 GB	16 GB	4 GB	4 GB
Hard drive (minimum)	4 GB	50 GB	Based on size/amount of stored files	4 GB
Hard drive (recommended)	10 GB	200 GB	Based on size/amount of stored files	10 GB

Server operating system

⛶ Expand table

Operating system	VMM server	Remote VMM library	Remote VMM database
Windows Server 2022 Desktop experience	Y	Y	If supported by SQL Server version
Windows Server 2022 Server Core	Y	Y	If supported by SQL Server version

> ⓘ **Note**
>
> Ensure that VMM server operating system is the same as the managed host operating system in case of deployment of Hyper Converged Infrastructure.

VMM console operating system

Expand table

Operating system	Supported
Windows 10 Enterprise	Y
Windows 11 Enterprise	Y
Window Server 2016 Standard, Datacenter	Y
Windows Server 2019 (with desktop experience)	Y
Window Server 2019 Standard, Datacenter, Server Core with FOD	Y
Windows Server 2022 Standard, Datacenter	Y

SQL Server

> **Note**
>
> - For the supported versions of SQL, use the service packs that are currently in support by Microsoft.
> - For the below supported SQL versions, Standard, Enterprise, and Datacenter (64-bit) editions are supported based on the availability.

Expand table

SQL version	Supported
SQL Server 2016 and SPs as detailed here	Y
SQL Server 2017 as detailed here	Y
SQL Server 2019 as detailed here	Y
SQL Server 2022 as detailed here (Supported from VMM 2022 UR1)	Y
SQL Server command line utilities	Install the SQL Server 2016 Command-Line Utilities from the Microsoft® SQL Server® 2016 Feature Pack or Install the SQL Server 2017 Command-Line Utilities from

SQL version	Supported
	the Microsoft® SQL Server® 2017 Feature Pack. or Install the SQL Server 2019 Command-Line Utilities from the Microsoft® SQL Server® 2019 Feature Pack. or Install the SQL Server 2022 Command-Line Utilities from the Microsoft® SQL Server® 2022 Feature Pack. Not required for VMM installation

Virtualization

⛶ Expand table

VM	Supported
VMM management server	The VMM management server can be installed on a VM. If you use dynamic memory, set the start RAM of the VM to at least 4096 MB. Don't install on a server running Hyper-V. You can deploy the VMM management server (physical or VM) in a highly available cluster.
VMM console	You can install the VMM console on a VM.

Installation components

These components should be installed on the server before you install VMM.

⛶ Expand table

Component	VMM server	VMM console
Active Directory	The VMM management server must be a domain member. The computer name shouldn't exceed 15 characters.	A computer with the VMM console installed should be a domain member.
Windows ADK	Download Windows ADK for Windows 11 and Windows Server 2022 and download windows	Not applicable

Component	VMM server	VMM console
	PE Add-on for ADK	
PowerShell	PowerShell 5.1	PowerShell 5.0, 5.1
.NET (minimum)	4.6	4.5

> ⓘ **Note**
>
> If you run into ADK file path issue while installing VMM, copy the files from the *amd64* folder in ADK root folder to the ADK root folder itself. The default ADK folder path is *C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\WSIM*, but it can be different based on your choice of folder path during ADK installation.

Servers in the VMM fabric

Expand table

Operating system	Hyper-V host	SOFS	Update server	PXE server
Windows Server 2016 Standard and Datacenter (Core)	Y	Y	N	N
Windows Server 2016 Standard and Datacenter (With Desktop experience)	Y	Y	Y	Y
Hyper-V Server 2016	N	N	N	N
Windows Server 2019 Standard and Datacenter (With Desktop experience)	Y	Y	Y	Y
Windows Server 2019 Standard and Datacenter (Core)	Y	Y	N	N
Hyper-V Server 2019	N	N	N	N
Azure Stack Hyper Converged Infrastructure (HCI, version 20H2)	Y	N	N	N
Azure Stack Hyper Converged Infrastructure (HCI, version 21H2)	Y	N	N	N

Operating system	Hyper-V host	SOFS	Update server	PXE server
Azure Stack Hyper Converged Infrastructure (HCI, version 22H2) (Supported from VMM 2022 UR1)	Y	N	N	N
Windows Server 2022	Y	Y	Y	Y

VMware servers in the VMM fabric

Expand table

VMware	Supported
ESX	ESX/ESXi 6.5, 6.7 7.0, 8.0 (supported from VMM 2022 UR1)
vCenter	6.5, 6.7 7.0, 8.0 (supported from VMM 2022 UR1)
Supported	Features and limitations

VMs in the VMM fabric

Expand table

Guest operating system	Supported
Hyper-V VMs	Any guest running on supported Hyper-V hosts. Learn more about support for 2022 and earlier versions.
VMware VM	Any VM running on supported VMware servers. Learn more .

Next steps

Plan VMM installation

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Plan VMM installation

Article • 08/02/2024

This article helps you to plan all the elements required for a successful System Center Virtual Machine Manager (VMM) installation and includes information for releases VMM 2016 and later. Use these requirements as applicable for the VMM version you plan to install.

For more information on the supported versions of hardware and software, see the system requirements article for the version you install.

Deployment requirements

Verify the following system requirements:

- **VMM management server**: Verify hardware and operating system requirements.
- **SQL Server**: Review supported SQL Server versions.
- **VMM console**: Review operating system requirements and if you want to run the VMM console on a separate computer.
- **VMM library**: Review the hardware requirements for remote VMM library shares.
- **Virtualization hosts**: Review the supported operating systems for Hyper-V and SOFS servers in the VMM fabric. Review requirements for VMware servers.
- **Other fabric servers**: Review the supported operating systems for update and PXE (used for bare-metal deployment) servers.

Additional deployment requirements

Expand table

Component	Details
Command-line utilities for SQL Server	SQL Server 2014 feature pack for release earlier to 2019, 2016/2017 feature pack for 2019 If you want to deploy VMM services using SQL Server data-tier apps, install the related command-line utilities on the VMM management server. The version you install should match the SQL Server version.
Windows Assessment and Deployment Kit (ADK)	Windows ADK for Windows 10. You can install from setup, or download it. You only need the **Deployment Tools** and **Windows Preinstallation Environment** options.

Component	Details
	If you run into ADK file path issue while installing VMM, copy the files from the *amd64* folder in ADK root folder to the ADK root folder itself. The default ADK folder path is *C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\WSIM*, but it can be different based on your choice of folder path during ADK installation.
Guest operating system	Windows operating systems supported by Hyper-V. Linux (CentOS, RHEL, Debian, Oracle Linux, SUSE, Ubuntu)
PowerShell	Supported versions
.NET	Supported versions
Host agent	VMM 2016/2019 Needed for hosts managed in VMM.
Monitoring	System Center Operations Manager 2016. You also need SQL Server Analysis Services 2014 or a later version.
VMware	vCenter 5.1, 5.5, 5.8, 6.0, 6.5 vCenter 7.0 and 8.0 (Supported from 2022 UR1 and 2019 UR5) ESXi 5.5, 6.0, 6.5 ESXi 7.0 and 8.0 (Supported from 2022 UR1 and 2019 UR5) vCenter and ESXi servers running these versions can be managed in VMM.
Bare metal provisioning	System Management Architecture for Server Hardware (SMASH) (v1 or higher) over WS-MAN. Intelligent Platform Interface 1.5 or higher Data Center Manager Interface (DCMI) 1.0 or higher. Required to discover and deploy physical bare-metal servers.

SPN

If the VMM user installing VMM, or running VMM setup, doesn't have permissions to write the service principal name (SPN) for the VMM server in Active Directory, setup will finish with a warning. If the SPN isn't registered, other computers running the VMM console won't be able to connect to the management server, and you won't be able to deploy a Hyper-V host on a bare metal computer in the VMM fabric. To avoid this issue, you need to register the SPN as a domain administrator before you install VMM, as follows:

1. Run these commands from <SystemDrive>\Windows\System32>, as a domain administrator:

    - `setspn -u -s SCVMM/<MachineBIOSName> <VMMServiceAccount>`
    - `setspn -u -s SCVMM/<MachineFQDN> <VMMServiceAccount>`

    For a cluster, <MachineBIOSName> should be <ClusterBIOSName> and <MachineFQDN> should be <ClusterFQDN>

2. On the VMM server (or on each node in a cluster), in the registry, navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Setup**.

3. Set **VmmServicePrincipalNames** to **SCVMM/<MachineBIOSName>,SCVMM/<MachineFQDN>**. For a cluster: **SCVMM/<ClusterBIOSName>,SCVMM/<ClusterFQDN>**.

If you can't do this, you can also register the SPN during VMM installation. A domain administrator can provide the SPN write permissions to VMM service user or setup user.

> ⓘ **Note**
>
> This approach isn't the preferred one. The permission allows the delegated user to register any servicePrincipalName with no restrictions.

Hence, the delegated user should be highly trusted, and the account credentials must be kept secure. To do this:

1. Run adsiedit as a domain administrator.
2. Navigate to find the VMM service user. Right-click **Properties** > **Security** > **Advanced**. Then select **Add**, and in **Select a principal**, specify the user who will be granted the permissions.
3. Select **Write servicePrincipalName** > **OK**.

When you install VMM with this user account, SPN will be registered.

VMM management server

- You can't run the VMM management server on Nano server (applicable to Windows Server releases prior to 2019).

- The management server computer name can't exceed 15 characters.
- Don’t install the VMM management server, or other System Center components other than agents, on servers running Hyper-V.
- You can install the VMM management server on a VM. If you do, and you use the Dynamic Memory feature of Hyper-V, then you must set the startup RAM for the virtual machine to be at least 2,048 megabytes (MB).

- We recommend that you use a dedicated SCVMM management server and not install any other System Center components and management tools on the same server.
- If you want to manage more than 150 hosts, we recommend the following:
  - Add one or more remote computers as library servers, and don't use the default library share on the VMM management server.
  - Don't run the SQL Server instance on the VMM management server.

- For high availability, the VMM management server can be installed on a failover cluster. Learn more.

SQL Server and database

- The instance of SQL Server that you're using must allow for case-insensitive database objects.

- The SQL Server’s computer name can't exceed 15 characters in length.

- If the VMM management server and the SQL Server computer aren't members of the same Active Directory domain, then a two-way trust must exist between the two domains.

- When you install SQL Server, select the **Database Engine Services** and **Management Tools - Complete** features.

- You can perform an in-place upgrade to a supported version of SQL Server (without moving the VMM database). Ensure that no jobs are running when you perform the upgrade, or jobs can fail and need to be restarted manually.

- For the VMM database, for better performance, don't store database files on the disk that is used for the operating system.

- If you're using Software Defined Networking (SDN) in VMM, then all networking information is stored in the VMM database. Because of this, you might want to consider high availability for the VMM database, using the following guidelines:

- Failover clustering is supported and is the recommended configuration for availability within a single geographical area or datacenter. Read more.
- Use of Always On Availability Groups in Microsoft SQL Server is supported, but it's important to review the differences between the two availability modes, synchronous-commit and asynchronous-commit. Learn more.
  - With asynchronous-commit mode, the replica of the database can be out of date for a period of time after each commit. This can make it appear as if the database were back in time, which might cause loss of customer data, inadvertent disclosure of information, or possibly elevation of privilege.
  - You can use synchronous-commit mode as a configuration for remote-site availability scenarios.

- The SQL Server service must use an account that has permission to access Active Directory Domain Services (AD DS). For example, you can specify the Local System Account or a domain user account. Don't specify a local user account.

- You don't need to configure collation. During deployment, Setup automatically configures CI collation according to the language of the server operating system.

- Dynamic port is supported.

- If you want to create the VMM database prior to VMM installation:

  - Ensure that you have permissions or create a SQL database, or ask the SQL Server admin to do it.

  - Configure the database as follows:

    1. Create a new database with settings: Name: VirtualManagerDB; Collation: Latin1_General_100_CI_AS, but aligned with the specific SQL Server instance collation.
    2. Grant db_owner permissions for the database to the VMM service account.
    3. In VMM setup, you'll select the option to use an existing database and specify the database details and VMM service account as the database user.

Library server

- If you run the library server on the VMM management server, then you must provide additional hard disk space to store objects. The space required varies based on the number and size of the objects you store.
- The library server is where VMM stores items such as virtual machine templates, virtual hard disks, virtual floppy disks, ISO images, scripts, and stored virtual

machines. The optimal hardware requirements that are specified for a VMM library server vary, depending on the quantity and size of these files. You'll need to check CPU usage and other system state variables to determine what works best in your environment.

- If you want to manage Virtual hard disks in the .vhdx file format, the VMM library server must run Windows Server 2012 or later.
- VMM doesn't provide a method for replicating physical files in the VMM library or a method for transferring metadata for objects that are stored in the VMM database. Instead, if necessary, you need to replicate physical files outside of VMM, and you need to transfer metadata by using scripts or other means.
- VMM doesn't support file servers that are configured with the case-sensitive option for Windows Services for UNIX because the Network File System (NFS) case control is set to **Ignore**.

Account and domain requirements

When you install VMM, you must configure the VMM service to use any one of the following accounts:

- The Local System account (can't be used for a highly available VMM deployment) or
- A domain user account or
- A Group Managed Service Account (gMSA)

Ensure the following before you prepare an account:

- VMM service account should have *log on as a service* permission on the VMM server.

- You can't change the identity of the Virtual Machine Manager service account after installation. This includes changing from the local system account to a domain account, from a domain account to the local system account, or changing the domain account to another domain account. To change the Virtual Machine Manager service account after installation, you must uninstall VMM (selecting the Retain data option if you want to keep the SQL Server database), and then reinstall VMM by using the new service account.
- If you specify a domain account, the account must be a member of the local Administrators group on the computer.
- If you specify a domain account, it's recommended that you create an account that is designated to be used for this purpose. When a host is removed from the VMM management server, the account that the System Center Virtual Machine Manager service is running under is removed from the local Administrators group of the

host. If the same account is used for other purposes on the host, this can cause unexpected results.

- If you plan to use shared ISO images with Hyper-V virtual machines, you must use a domain account.
- If you're using a disjointed namespace, you must use a domain account. For more information about disjointed namespaces, see Naming conventions in Active Directory for computers, domains, sites, and OUs.
- If you're installing a highly available VMM management server, you must use a domain account.
- The computer on which you install the VMM management server must be a member of an Active Directory domain. In your environment, you might have user accounts in one forest and your VMM servers and host in another. In this environment, you must establish a two-way trust between the two cross-forest domains. One-way trusts between cross-forest domains aren't supported in VMM.
- To create and use gMSA, review the article on gMSA and create the gMSA as per the guidance available. Ensure that the servers on which the VMM Management service would be installed have permissions to retrieve the password of gMSA account.

> ⓘ **Note**
>
> You do not need to specify the ‘Service Principle Name (SPN)’ when creating gMSA. VMM service sets the appropriate SPN for gMSA.

Distributed key management

By default, VMM encrypts some data in the VMM database by using the Data Protection Application Programming Interface (DPAPI). For example, Run As account credentials, passwords in guest operating system profiles, and product key information in virtual hard disks properties. Data encryption is tied to the specific computer on which VMM is installed, and the service account that VMM uses. If you move your VMM installation to another computer, VMM won't retain the encrypted data, and you'll need to enter it manually.

To ensure that VMM retains encrypted data across moves, you can use distributed key management to store encryption keys in Active Directory. If you move your VMM installation, VMM retains the encrypted data because the new VMM computer has access to the encryption keys in Active Directory. To set up distributed key management, you should coordinate with your Active Directory administrator.

ⓘ Note

- You must create a container in AD DS before you install VMM. You can create the container by using ADSI Edit (installed from **Server Manager** > **Remote Server Administration Tools**.)
- You create the container in the same domain as the user account with which you're installing VMM. If you specify that the VMM service uses a domain account, that account must be in the same domain. For example, if the installation account and the service account are both in the corp.contoso.com domain, you must create the container in that domain. So, if you want to create a container that is named VMMDKM, you specify the container location as CN=VMMDKM,DC=corp,DC=contoso,DC=com. The account with which you're installing VMM needs Full Control permissions to the container in AD DS. The permissions must apply to this object and to all descendant objects.

- If you're installing a highly available VMM management server, you must use distributed key management to store encryption keys in Active Directory. You need distributed key management because if VMM fails over to a node, that node will need access to the encryption keys.
- When you configure the service account and distributed key in setup, you must type the location of the container in AD DS, for example: CN=VMMDKM,DC=corp,DC=contoso,DC=com

Next steps

Install VMM

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Plan a highly available VMM deployment

Article • 07/10/2024

This article helps you to plan a highly available System Center Virtual Machine Manager (VMM) deployment.

For resilience and scalability, you can deploy VMM in high availability mode as follows:

- Deploy the VMM management server in a failover cluster.
- Make library server file shares highly available.
- Deploy the SQL Server VMM database as highly available.

Plan a highly available SQL Server deployment

- You should set up SQL Server before you deploy the VMM management servers.
- We recommend you use a highly available SQL Server installation on a failover cluster and configure SQL Server Always On availability groups. You shouldn't install SQL Server on the VMM cluster.
- Review the best practices for failover cluster node prerequisites.
- Always On availability groups are supported in VMM. Use **synchronous commit** for higher protection with more overhead. If you use **asynchronous-commit** mode, the secondary database can lag the primary database making some data loss possible.
- The database server must be in the same domain as the VMM server or in a domain with a two-way trust.
- Using a clustered database with VMM requires Kerberos authentication. To support this, the SQL Server instance must associate a Service Principal Name (SPN) with the account that the SQL Server will be running on.

Plan a highly available VMM management server

- Don't install on a Hyper-V host parent partition. You can install VMM on a VM.
- Before you start, you need to set up the VMM service account and distributed key management. Learn more
- Only one instance of VMM can be deployed to a failover cluster of up to 16 nodes.

- The user who creates the cluster has **Create Computers objects** permission to the OU or the container where the servers that will form the cluster reside. If this isn't possible, ask a domain admin to pre-stage a cluster computer object for the cluster.

- Requirements for computers running as VMM management nodes:
  - All cluster nodes that will act as VMM servers must be running either Windows Server 2019 or Windows Server 2022.
  - Each cluster node must be joined to a domain and must have a computer name that doesn't exceed 15 characters.
  - The VMM service network name must not exceed 15 characters.
  - Windows ADK needs to be installed on each computer. Install from setup or the download center. Select **Deployment Tools** and **Windows Preinstallation Environment** when you install.
  - If you plan to deploy VMM services that use SQL Server data-tier applications, install the related command line utilities on your VMM management server. The command line utility is available in the SQL Server 2012 feature pack or SQL Server 2014 feature pack or SQL Server 2016 feature pack or SQL Server 2017 feature pack or SQL Server 2019 feature pack.

> ⓘ Note
>
> Deploying a highly available SCVMM management server in a Stretched clusters configuration is not supported.

Plan a highly available VMM library

You can create highly available library servers to ensure that file-based resources, templates, and profiles are resilient and available.

- VMM doesn't automatically create the VMM library as highly available when you deploy VMM in high availability mode. You need to create highly available library servers by deploying the library on a file server cluster.
- You'll need to set up a file server failover cluster. Deploying highly available library shares on the VMM cluster isn't supported.
- Computers you'll configure as file servers should be running Windows Server 2012 R2 or later. We recommend that all nodes have the same version of Windows.
- All nodes you want to add as file servers should be in the same domain.
- Ensure that the hardware and software you want to use for the library meets the system requirements.

- The user who creates the cluster has **Create Computers objects** permission to the OU or the container where the servers that will form the cluster reside. If this isn't possible, ask a domain admin to pre-stage a cluster computer object for the cluster.
- The account you use to create the cluster should be a domain user on all the computers you want to add as file server nodes.
- The library server can't be a scale-out file server (SOFS). It must be on a failover cluster that doesn't use the SOFS cluster role. This is because when you deploy the library, the VMM agent is deployed on the host. For SOFS, there are multiple hosts in a cluster provides shares, which makes it complicated for agent deployment. When you have a standalone or clustered library server, you can use storage on SOFS by creating shares on it.
- You can deploy the library shares on a cluster with physical nodes or a guest cluster.
- If you want to add clustered storage when you create the cluster, ensure that all the computers can access the storage.
- If you want to deploy a distributed VMM library in different datacenters, you need to set up a scheduled copy between the two library shares. No replication is available.

Next steps

- Set up a highly available VMM deployment

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Identify VMM ports and protocols

Article • 07/10/2024

As part of your System Center Virtual Machine Manager (VMM) deployment, you need to allow access for the ports and protocols that the VMM server and components will use. It's important to plan this in advance. Some of the port settings are configured in VMM setup, and if you want to modify them after you set up VMM for the first time, you'll need to reinstall to do so.

Set up exceptions

1. Identify where you need to create firewall exceptions, in accordance with the table below.
2. On the server you identify, select **Start** > **Next** > **Administrative Tools** > **Windows Firewall with Advanced Security**.
3. In the **Windows Firewall with Advanced Security on Local Computer** pane, select on **Inbound Rules**.
4. In **Actions**, select **New Rule**.
5. In the **New Inbound Rule Wizard** > **Rule Type**, select **Port**, and then select **Next**.
6. In **Protocol and Ports**, specify the port settings in accordance with the table below and continue in the wizard to create the rule.

Port and protocol exceptions

Expand table

Connect	Port/protocol	Details	Configure
VMM server to VMM agent on Windows Server-based hosts/remote library server	80: WinRM; 135: RPC; 139: NetBIOS; 445: SMB (over TCP)	Used by the VMM agent Inbound rule on hosts	Can't modify
VMM server to VMM agent on Windows Server-based hosts/remote library server	443:HTTPS	BITS data channel for file transfers Inbound rule on hosts	Modify in VMM setup
VMM server to VMM agent on Windows	5985:WinRM	Control channel	Modify in VMM setup

Connect	Port/protocol	Details	Configure
Server-based hosts/remote library server		Inbound rule on hosts	
VMM server to VMM agent on Windows Server-based hosts/remote library server	5986:WinRM	Control channel (SSL) Inbound rule on hosts	Can't modify
VMM server to VMM guest agent (VM data channel)	443:HTTPS	BITS data channel for file transfers Inbound rule on machines running the agent The VMM guest agent is a special version of the VMM agent. It's installed on VMs that are part of a service template and on Linux VMs (with or without a service template).	Can't modify
VMM server to VMM guest agent (VM control channel)	5985:WinRM	Control channel Inbound rule on machines running the agent	Can't modify
VMM host to host	443:HTTPS	BITS data channel for file transfers Inbound rule on hosts and VMM server	Modify in VMM setup
VMM server to VWware ESXi servers/Web Services	22:SFTP Inbound rule on hosts	Can't modify	
VMM server to load balancer	80:HTTP; 443:HTTPS	Channel used for load balancer management	Modify in load balancer provider
VMM server to remote SQL Server database	1433:TDS	SQL Server listener Inbound rule on SQL Server	Modify in VMM setup

Connect	Port/protocol	Details	Configure
VMM server to WSUS update servers	80/8530:HTTP; 443/8531:HTTPS	Data and control channels Inbound rule on WSUS server	Can't modify from VMM
VMM library server to Hyper-V hosts	443:HTTPS	BITS data channel for file transfers Inbound rule on hosts - 443	Modify in VMM setup
VMM console to VMM	WCF:8100 (HTTP); WCF:8101 (HTTPS); Net.TCP: 8102	Inbound rule on VMM console machine	Modify in VMM setup
VMM server to storage management service	WMI	Local call	
Storage management service to SMI-S provider	CIM-XML	Provider-specific	
VMM server to Baseboard Management Controller (BMC)	443: HTTP (SMASH over WS-Management)	Inbound rule on BMC device	Modify on BMC device
VMM server to Baseboard Management Controller (BMC)	623: IPMI	Inbound rule on BMC device	Modify on BMC device
VMM server to Windows PE agent	8101:WCF; 8103:WCF	8101 is used for control channel, 8103 is used for time sync	Modify in VMM setup
VMM server to WDS PXE provider		8102: WCF	Inbound rule on PXE server
VMM server to Hyper-V host in untrusted/perimeter domain	443:HTTPS (BITS)	BITS data channel for file transfers Inbound rule on VMM server	
Library server to Hyper-V host in untrusted/perimeter domain	443:HTTPS	BITS data channel for file transfers Inbound rule on VMM library	
VMM server to Windows file server	80: WinRM; 135: RPC; 139: NetBIOS; 445: SMB (over TCP)	Used by the VMM agent Inbound rule on file server	

Connect	Port/protocol	Details	Configure
VMM server to Windows file server	443:HTTPS	BITS used for file transfer Inbound rule on file server	
VMM server to Windows file server	5985/5986:WinRM	Control channel Inbound rule on file server	

ⓘ Note

In addition to the above ports, VMM relies on the default dynamic port range for all its communication with Hyper-V hosts, file servers, and library servers. Learn more about the dynamic port range. We recommend that you reconfigure the firewalls to allow traffic between servers in the dynamic port range of 49152 through 65535.

ⓘ Note

System Center Virtual Machine Manager uses NTLM authentication protocol to perform management operations. Using Kerberos authentication protocol isn't recommended as it may break a few VM operations.

Next steps

You can modify some of these ports and protocols during VMM installation.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Plan the VMM compute fabric

Article • 07/10/2024

This article describes how to plan the System Center Virtual Machine Manager (VMM) compute fabric. The VMM compute fabric consists of the VMM library, virtualization hosts, host groups, and other infrastructure servers.

Plan the VMM library

Before you start:

- You should verify system requirements for the VMM library before you install VMM.
- VMM deploys the default library share on the VMM server. After the setup is complete, you can't remove or relocate the default library share. So consider its location before you install VMM.
- If you're using a SAN, the library server should have the same SAN as the hosts that use the library. This ensures that the library server and the hosts can access the same LUNs on the SAN for faster file transfers.
- If you connect to a library from virtualization hosts across a LAN, the library server should be as close as possible to the hosts.
- If you're planning to add more library servers, you can create library groups to organize them. You can use library groups to align servers with host groups in the VMM fabric. As a best practice, you should align each library server with the host group that uses the resources of that library.

Plan virtualization hosts

VMM supports Hyper-V and VMware virtualization hosts. When you're adding, provisioning, and managing hosts in the VMM fabric, consider these points:

- The topology of Hyper-V hosts. VMM can work with Hyper-V hosts that are in the same domain as the VMM server, in a domain with a two-way trust, or in a domain without a two-way trust. VMM can also work with Hyper-V hosts that are in a perimeter network, or in a disjointed namespace.
- The topology of VMware hosts. VMM works with VMware hosts located anywhere in your environment.
- The number and type of guest operating systems running on the host.
- The system configuration of the VMs running on the host.
- The types of apps running on the guest operating systems.

- The VM workloads that will run on the host.
- The processor requirements for the host. You need enough processing capacity to run the VMs.
- The memory requirements for the host. After you use VMM to allocate host RAM to a VM, that memory isn't available for other resources. You also need adequate memory to run the host operating system and any other apps.
- The storage requirements for the host. You need adequate storage for the host itself and also for the VMs running on it. Remember, you need to take extra space into account for VM paging files, dynamically expanding virtual hard disks, saving the contents of VM RAM when the VM is in a saved state, and VM checkpoints.
- The network requirements for the host. If VMs are running apps that need high availability, you'll need to consider the network requirements.

Plan host groups

Host groups act as containers for virtualization hosts and virtual machines. You apply settings at the group level, including setting resources at the host level, specifying hosts for self-service users, and storage and network options. Planning for host groups is especially important in a large-scale deployment, where host groups can help you to effectively manage resource provisioning and management.

You can base your host groups on settings that make sense for your organization. For example:

- For branch offices in your organization.
- To match your Active Directory structure.
- To reflect functions such as development, test, production, or research.
- To limit the hosts used for administrative tasks. For example, you could restrict the placement of virtual machines by selecting a particular host group.
- To reserve host resources to determine the CPU, memory, disk space, disk I/O capacity, and network capacity that will always be available to the host operating system.
- To automatically place virtual machines on the most suitable host. Automatic placement is also used to deploy the virtual machines that users create in virtual machine self-service.
- To designate self-service hosts on which users can create and operate their own virtual machines. You add self-service policies to a host group to enable users or groups to create, operate, and manage their own virtual machines within a controlled environment on the hosts in the host group.

Host groups are hierarchical. For example, you can create a child host group of an existing host group to override host reserves inherited for a parent host group, or to amend VM permissions inherited from the self-service policies of a parent host group.

- All host groups belong to the root host group - All Hosts.
- Each host or host group is identified by its host path, a sequence of host group names that specifies the location of a host or host group within the hierarchy of host groups in the navigation pane. For example, the host path All Hosts\New York\Site21\VMHost05 indicates that the host VMHost05 belongs to the host group Site21, which is a child host group of the host group New York.
- When you change the host reserves for a parent host group, you can choose whether to cascade the host reserve settings to hosts in all its child host groups. If you choose to cascade the host reserve settings, all the host reserve settings for the parent host group overwrite all previous settings for all hosts in all the child host groups of the parent host group.
- If a parent host group is used for virtual machine self-service, each of its child host group automatically inherits self-service policies from the parent host group. However, you can add a self-service policy for the same user or group to both a parent host group and its child host group. By adding policies to both parent and child, you can assign the same users different templates, set different virtual machine permissions, and assign a different virtual machine quota on a subset of hosts within the parent host group.
- You can use a host group to isolate a host. For example, if you have a host with guest operating systems that are running mission-critical applications, you can isolate that host by placing it in its own host group. This way you can ensure that there are no self-service policies applied on the host group and that the system resources set aside for running the host's operating system are appropriate, thus maximizing the host resources available for use by the guest operating systems.

Next steps

- Learn about deploying the library in high availability mode if required.
- Manage the VMM library

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Plan the VMM networking fabric

Article • 07/10/2024

This article describes how to plan your networking fabric in System Center Virtual Machine Manager (VMM).

Networking components

VMM networking contains many components, summarized in the following table:

⛶ Expand table

Networking component	Details
Logical networks	In VMM, your physical networks are defined as logical networks. Logical networks are a useful way of abstracting your underlying physical network infrastructure. Logical network settings will match or mirror your physical network environment. For example, the IP addresses and VLAN properties will match exactly, a network site in a logical network will contain configuration settings for the site. By default, VMM creates logical network automatically when you add a Hyper-V host to the fabric if a suitable network can't be found. You can disable this option. To abstract logical networks from the VMs that use them, VMM provides **VM networks**. You connect the virtual adapter of a VM to a VM network.
MAC address pools	You can create MAC address pools for VMs running on virtualization hosts in the VMM fabric. When you use static MAC address pools, VMM can automatically generate and assign MAC addresses to VMs. You can use a standard pool or configure a custom pool.
Load balancers	VMM supports adding hardware load balancers or using NLB to load balance requests to a service tier.
VIP templates	Virtual IP (VIP) templates contain load balancing information for a particular type of traffic. For example, you could have a template that specifies how to balance HTTPS traffic on a specific load balancer.
Logical switches	Logical switches are containers for virtual switch settings. You apply logical switches to hosts so that you have consistent switch settings across all hosts. VMM tracks switch settings on hosts deployed with logical switches to ensure compliance.

Networking component	Details
Port profiles	Port profiles act as containers for the properties you want a network adapter to have. Instead of configuring properties per network adapter, you set up in the port profile and apply that profile to an adapter. There are two types of port profiles. Virtual port profiles contain settings that are applied to virtual network adapters connect to VMs or used by virtualization hosts. Uplink port profiles are used to define how a virtual switch connects to a logical network.
Port classifications	Port classifications are abstract containers for virtual port profile settings. This abstraction means that admins and tenants can assign a port classification to a VM template, while the VM's logical switch determines which port profile should be used. Profiles and then both admins and tenant can select a suitable classification. VMM contains many default port classifications. For example, there's a classification for VMs that needs high bandwidth and a different one for VMs that need low bandwidth. Port classifications are linked to virtual port profiles when you configure logical switches.

Plan logical networks

During deployment, you need to create logical networks and set up network sites and IP addressing in each network. Then you create VM networks based on those logical networks.

Here's what you need to plan:

1. **Automation creation**: Decide whether you want to let VMM create logical networks. VMM will automatically create a logical network each time you add a virtualization host. VMM doesn't create network sites in the automatically created logical network. You can turn off this option in **Settings** > **General** > **Network Settings** and clear **Automatic creation of logical networks**.
2. **Logical network capacity**: If you're going to create logical networks manually, figure out what you'll need to represent your physical network topology. For example, if you need a management network and a network used by VMs, you should create two logical networks.
3. **Logical network types**: Figure out the type of logical network you need. You'll configure VM networks on top of logical networks and those VM networks can provide network virtualization with the ability to create multiple virtual networks on shared physical networks, or VM networks can provide isolation with VLANS and PVLANS. When you configure the logical network, you need to indicate the type of network you need.

4. **Network sites**: Determine how many network sites you need in the logical network. You could plan around host groups and host locations. For example, a Seattle host group and a New York host group. You don't need network sites if you don't have VLANs and you're using DHCP to allocate IP addresses.
5. **VLANs/subnets**: Figure out the VLANs and IP subnets you need in the logical network. These will mirror what you have in your physical network topology.
6. **IP addressing**: If you're using static IP address assignment, determine which logical networks need static address pools.

Here's what you need to do:

1. Identify baseline logical networks: Identify a set of initial logical networks that mirror the physical networks in your environment.
2. Identify additional logical networks for specific requirements: Define logical networks with specific purpose or perform a particular function within your environment. One of the benefits of logical networks is that you can separate computer and network services with different business purposes without needing to change your physical infrastructure.
3. Determine isolation requirements: Identify which logical networks need to be isolated and how that isolation will be enforced, either through physical separation, VLAN/PVLAN, or network virtualization. Remember, that you need isolation if the logical network is going to be used by multiple tenants. If you have a single tenant or customer, isolation is optional. In turn, if you don't need isolation you only need a single VM network that maps to the logical network.
4. Determine the network sites, VLANs, PVLANs, and IP pools that need to be defined for each logical network you've identified.
5. Figure out which logical network will associate with which virtualization hosts.

Plan logical networks, network sites, and IP address pools

Use the following table to plan for the logical networks, VM networks, and IP address pools you'll need to support a virtualized infrastructure.

Expand table

Item to review or determine	Description and (as needed) links within this article
Logical networks already created by default by VMM	When you add a Hyper-V host to VMM, logical networks can be created by default, based on DNS suffixes.

Item to review or determine	Description and (as needed) links within this article
How many logical networks you need, and the purpose of each	Plan to create logical networks to represent the network topology for your hosts. For example, if you need a management network, a network used for cluster heartbeats, and a network used by virtual machines, create a logical network for each.
Categories that your logical networks fall into	Review the purposes of your logical networks and categorize them: - **No isolation**: For example, a cluster-heartbeat network for a host cluster. - **VLAN**: Isolation provided by your VLANs. - **Virtualized**: Provides a foundation for Hyper-V network virtualization. - **External**: Managed through a network manager (vendor network-management console or virtual switch extension manager) outside of VM. - **IPAM**: Managed through an IP Address Management (IPAM) server.
How many network sites are needed in each logical network	One common way to plan network sites is around host groups and host locations. For example, for a **Seattle** host group and a **New York** host group, if you had a MANAGEMENT logical network, you might create two network sites called **MANAGEMENT - Seattle** and **MANAGEMENT - New York**.
Which VLANs and/or IP subnets are needed in each network site	The VLANs and IP subnets you assign should match your topology.
Which logical networks (or specifically, which network sites) will need IP address pools	Determine which logical networks will use static IP addressing or load balancing, and which logical networks will be the foundation for network virtualization. For these logical networks, plan for IP address pools.

Logical networks created by default

In the VMM console, **Fabric** >**Networking** > **Logical networks**, you might see logical networks created by VMM by default. VMM creates these networks to ensure that when you add a host, you have at least one logical network for deploying virtual machines and services. No network sites are created automatically.

To illustrate how these settings work, suppose that you haven't changed the settings and you add a Hyper-V host to VMM management. In this case, VMM automatically creates logical networks that match the first DNS suffix label of the connection-specific DNS suffix on each host network adapter. On the logical network, VMM also creates a VM network that is configured with **no isolation**. For example, if the DNS suffix for the host network adapter was corp.contoso.com, VMM would create a logical network named **corp**, and on it, a VM network named **corp** that is configured with no isolation.

Guidelines for network sites: VLAN and IP subnet settings

The main guideline specifying VLANs and IP subnets for network sites is to reflect your network topology. For details, see the following table.

> ⓘ Note
>
> Network sites are sometimes referred to as **logical network definitions**, for example, in Windows PowerShell commands.

⛶ Expand table

Purpose of logical network	Guideline for network sites in that logical network
Static IP: Logical network that will use static IP addressing, for example, a network that supports host cluster nodes	Create at least one network site and associate at least one IP subnet with the network site.
DHCP (but not VLANs): Logical network that doesn't include VLANs, with all computers or devices using DHCP	No network sites are necessary.
VLANs: Logical network for VLAN-based independent networks	- If the VLANs use static IP addressing, create corresponding network sites that specify VLAN and IP subnet information. - If the VLANs use DHCP, create corresponding network sites that specify only VLAN information (no subnets).
Network virtualization: Logical network that will be the foundation for VM networks using network virtualization	Create at least one network site and associate at least one IP subnet with the site. The IP subnet is necessary because this logical network will need an IP address pool. Assign a VLAN to the network site if appropriate.
Load balancing: Logical network that will include a load balancer that is managed by VMM	Create at least one network site and associate at least one IP subnet with the network site.

ⓘ Note

For an external network, that is, a network managed through a vendor network-management console or virtual switch extension manager outside of VMM, you can configure settings through the vendor network-management console and allow them to be imported from the vendor network-management database into VMM.

Guidelines for IP address pools

In general, create IP address pools where you'll use static IP addressing or load balancing; also create IP address pools on logical networks that will be the foundation for VM networks supporting network virtualization. VMM uses IP address pools to assign IP addresses to Hyper-V hosts that you deploy through VMM, and to Windows-based virtual machines that you deploy through VMM, regardless of the type of host they're running on (Hyper-V or VMware ESX).

The following table provides detailed guidelines. Additional information about IP address pools is provided after the table.

Expand table

Purpose of logical network	Guideline for creating IP address pools for that logical network, or for VM networks built on that logical network
Static IP: Logical network with **no isolation** and requiring static IP addressing. For example, a network that supports host cluster nodes	Create one or more IP address pools for the logical network. For a logical network with **no isolation**, if you create a VM network on the logical network, any IP address pools will automatically become available on the VM network. In other words, the VM network will give direct access to the logical network.
VLANs: Logical network for VLAN-based independent networks using static IP addressing (rather than DHCP)	Create IP address pools on the logical network—one IP address pool for each VLAN where static IP addressing will be used. Later, when you create the VM networks that represent the VLANs, the IP address pools will automatically become available on those VM networks.
Network virtualization: Logical network that will be the foundation	Create IP address pools on the logical network that provides the foundation for the VM networks. Later, when you create the VM networks, you'll also create IP

Purpose of logical network	Guideline for creating IP address pools for that logical network, or for VM networks built on that logical network
for VM networks using network virtualization	address pools on them (and see the important note after this table). If you use DHCP on the VM networks, VMM will respond to a DHCP request with an address from an IP address pool. The process of creating an IP address pool for a VM network is similar to the process of creating an IP address pool for a logical network.
Load balancing: Logical network that will be the foundation for a VM network, where you'll use load balancing in a **service tier** (part of a set of virtual machines deployed together as a VMM **service**)	Create a static IP address pool on the VM network, and in it, define a reserved range of IP addresses. When you use VMM to deploy a load-balanced service tier that uses the VM network, VMM uses the reserved range of IP addresses to assign virtual IP (VIP) addresses to the load balancer.

ⓘ **Important**

If you configure a virtual machine to obtain a static IP address from an IP address pool, you must also configure the virtual machine to use a static MAC address. You can either specify the MAC address manually (during the **Configure Settings** step) or have VMM automatically assign a MAC address from a MAC address pool.

This requirement for static MAC addresses is necessary because VMM uses the MAC address to identify which network adapter to set the static IP address to, and this identification must happen before the virtual machine starts. Identifying the network adapter is especially important if a virtual machine has multiple adapters. If the MAC addresses were assigned dynamically through Hyper-V, VMM could not consistently identify the correct adapter to set a static IP address on.

VMM provides static MAC address pools by default, but you can customize the pools.

- When you create a static IP address pool, you can configure associated information, such as default gateways, Domain Name System (DNS) servers, DNS suffixes, and Windows Internet Name Service (WINS) servers. All these settings are optional.
- IP address pools support both IPv4 and IPv6 addresses. However, you can't mix IPv4 and IPv6 addresses in the same IP address pool.

ⓘ Note

After a virtual machine has been deployed in VMM, you can view the IP address or addresses assigned to that virtual machine. To do this, right-click the listing for the virtual machine, select **Properties**, and select the **Hardware Configuration** tab. Select the network adapter, and in the results pane select **Connection details**.

Next steps

- Set up the networking fabric

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Supported storage arrays

Article • 07/10/2024

This article provides details of the supported arrays for System Center 2022 - Virtual Machine Manager (VMM).

Supported storage arrays in VMM 2022

Virtualized workloads in System Center - Virtual Machine Manager (VMM) need storage resources that meet capacity and performance requirements. VMM recognizes local and remote storage. It supports storage on block-level storage devices that expose logical unit numbers (LUNs) using fiber channel, iSCSCI, and SAS connections, and network file shares.

Expand table

Device	Protocol	Min Controller Firmware	SMI-S	Details
Hewlett Packard Enterprise 3PAR	SMI-S	3PAR: 3PAR v. 3.2.2 MU3 or later 3PAR 8000 & 20000, 7000 & 10000	SMI-S CIM version 1.5	Link
NEC / NEC Storage M-Series M320, M320F, M520, M720, M720F	iSCSI/FC	010A M320/M320F Storage Control Software revision 1028 or later M520/M720/M720F Storage Control Software revision 1224 or later	SMI-S 1.6.1	Link
DELL SC Series	iSCSI/FC	SCOS: 7.4.2 or later DSM: 2019 R1 or later DSM 2020 R1 (20.1.1) or later	SMI-S version 1.6	Link
HPE Primera	SMI-S	4.0.0	4.0.0	Link
Pure Storage	iSCSI/FC	Purity 5.3.0+ 6.0.0+ and 6.1.0+	version 1.6.1	Link

Device	Protocol	Min Controller Firmware	SMI-S	Details
FlashArray - X, C, M				

ⓘ Note

Known issue: Deletion of thinly provisioned storage volume (LUN) fails for HPE Primera through VMM 2022.

Workaround: Delete LUN directly from the array.

ⓘ Note

If you would like us to certify a new storage device, reach out to systemcenterfeedback@microsoft.com.

Next steps

- Learn more about configuring storage in the VMM fabric.
- Learn more about array SMI-S Conformance Testing Program

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Upgrade System Center Virtual Machine Manager

Article • 07/10/2024

This article provides the upgrade information for System Center 2022 - Virtual Machine Manager (VMM).

Upgrade to System Center 2022 - Virtual Machine Manager

The following sections provide information about how to upgrade to VMM 2022. These include prerequisites, upgrade instructions, and tasks to complete after the upgrade finishes.

> ⓘ Note
>
> - You can upgrade to VMM 2022 from VMM 2019; upgrade from 2016 isn't supported.
> - During VMM Installation, ensure that SQL Database isn't part of any Availability Group.

Requirements and limitations

- You should be running VMM on System Center 2019.
- Ensure that the server meets all the requirements for VMM 2022 and that prerequisites are in place. Learn more.
- Ensure that you're running a supported version of SQL Server.
- If your current VMM deployment is integrated with Azure Site Recovery, note that:
  - Site Recovery settings can't be upgraded. After the upgrade, you need to redeploy.
  - Verify Hyper-V host support for VMM 2022.

Before you start

Ensure the following:

1. Complete any jobs that are currently running in VMM.

ⓘ **Note**

The jobs history is deleted during the upgrade.

2. Close any connections to the VMM management server, including the VMM console and the VMM command shell.
3. Close any other programs that are running on the VMM management server.
4. Ensure that there are no pending restarts on VMM servers.
5. Perform a full backup of the VMM database.
6. If the current SQL Server database used Always On availability groups:
   - If the VMM database is included in the availability group, remove it in SQL Server Management Studio.
   - Initiate a failover to the computer that is running SQL Server on which the VMM database is installed.
7. If you're running Operations Manager with VMM, disconnect the connection between the VMM and the Operations Manager server.

Upgrade sequence for System Center components

If you're running more than one System Center components, they should be upgraded in a specific order as shown below:

1. Service Management Automation
2. Orchestrator
3. Service Manager
4. Data Protection Manager
5. Operations Manager
6. Configuration Manager
7. Virtual Machine Manager
8. Service Provider Foundation

Upgrade a standalone VMM server

ⓘ **Note**

When you're upgrading a standalone VMM server, we recommend that you install VMM 2022 on the same server that had VMM 2019.

If you're using Distributed Key Management, you can choose to install VMM 2022 on a different server.

Use the following procedures:

- Back up and upgrade the OS
- Install VMM 2022

Back up and upgrade OS

1. Back up and retain the VMM database.
2. Uninstall the VMM. Ensure to remove both the management server and the console.
3. Upgrade the management OS to Windows Server 2022.
4. Install Windows 11 or Windows Server 2022 version of ADK.

Uninstall the VMM

1. Go to **Control Panel** > **Programs** > **Program and Features**, select **Virtual Machine Manager** and select **Uninstall**.
2. On the **Uninstall wizard,** select **Remove Features**, then select both **VMM management Server** and **VMM Console** under the features to remove list.
3. On the database options page, select **Retain database**.
4. Review the summary and select **Uninstall**.

Install VMM 2022

1. In the main setup page, select **Install**.
2. In **Select features to install**, select the VMM management server, and then select **Next**. The VMM console will be automatically installed.
3. In **Product registration information**, provide the appropriate information and then select **Next**. If you don't enter a product key, VMM will be installed as an evaluation version that expires after 180 days from the installation date.
4. In **Please read this license agreement**, review the license agreement, select the **I have read, understood, and agree with the terms of the license agreement** checkbox, and then select **Next**.
5. In **Usage and Connectivity Data**, select either of the options, and then select **Next**.

6. If the **Microsoft Update** page appears, select whether you want to use Microsoft Update and select **Next**. If you've already chosen to use Microsoft Update on this computer, this page won't appear.
7. In **Installation location**, use the default path or enter a different installation path for the VMM program files and then select **Next**.
8. In **Database configuration**:

   - Learn more if you need to upgrade the VMM SQL Server.
   - If you're using a remote SQL instance, specify the SQL server computer name.
   - If SQL server runs on the VMM server, enter the name of the VMM server, or enter **localhost**. If the SQL Server is in a cluster, enter the cluster name.
   - Don't specify a port value if you're using a local SQL server or if your remote SQL server uses the default port (1433).
   - Select **Existing Database** and select the database that you retained (backed up) from your previous installation. Provide credentials with permissions to access the database. When you're prompted to upgrade the database, select **Yes**.

9. In **Configure service account and distributed key management**, specify the account that the VMM service will use.

> ⓘ Note
>
> You can't change the identity of the VMM service account after installation.

10. Under **Distributed Key Management**, select whether to store encryption keys in Active Directory.

> ⓘ Note
>
> Choose the settings for the service account and distributed key management carefully. Based on your selection, encrypted data, such as passwords in templates, might not be available after the upgrade and you'll need to enter them manually.

11. In **Port configuration**, use the default port number for each feature or provide a unique port number that is appropriate in your environment.

> ⓘ Note
>
> You can't change the ports that you assign during the installation of a VMM management server unless you uninstall and then reinstall the VMM management

server. Also, don't configure any feature to use port 5986; this port number is preassigned.

12. In **Library configuration**, select whether to create a new library share or to use an existing library share on the computer. The default library share that VMM creates is named **MSSCVMMLibrary**, and the folder is located at **%SYSTEMDRIVE%\ProgramData\Virtual Machine Manager Library Files**. **ProgramData** is a hidden folder, and you can't remove it. After the VMM management server is installed, you can add library shares and library servers by using the VMM console or by using the VMM command shell.
13. In **Upgrade compatibility report**, review the settings and select **Next** to proceed with the upgrade.
14. In **Installation Summary**, review the settings and select **Install** to upgrade the server. **Installing features** page appears and displays the installation progress.
15. In **Setup completed successfully**, select **Close** to finish the installation. To open the VMM console, check **Open the VMM console when this wizard closes** or you can select the Virtual Machine Manager Console icon on the desktop.

ⓘ **Note**

Once the upgrade is successful, upgrade the host agent manually by using the VMM. It is recommended to maintain the server and the agent in the same version.

If there's any issue with the setup, check the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder.

During the setup, VMM enables the following firewall rules. These rules remain in effect even if you uninstall the VMM later.

- Windows Remote Management
- Windows Standards-Based Storage Management

Upgrade a highly available VMM server

You can upgrade a highly available (HA) VMM server 2019 to 2022.

The following two modes of upgrade are supported:

- Mixed mode with no additional VMM servers
- Mixed mode with additional VMM servers

ⓘ Note

SQL Server upgrade can be performed any time, independent of VMM upgrade.

Mixed mode upgrade with no additional VMM servers

This procedure requires no additional VMM servers, but has increased risk for downtime in some scenarios. For example, when you have two node HA VMM and the active VMM node fails while you're upgrading the passive. In this scenario, your VMM server won't have a failover node available.

Follow these steps:

1. Back up and retain the VMM database.
2. Uninstall the VMM on the passive node.
3. On the passive VMM node, upgrade the management OS to Windows server 2022.
4. Upgrade to the Windows 11 or Windows Server 2022 version of the ADK.
5. Install VMM 2022 on the passive node by using the following steps:

- In the main setup page, select **Install**.
- In **Select features to install**, select **VMM management server** and then select **Next**. The VMM console will be automatically installed.
- When prompted, confirm that you want to add this server as a node to the highly available deployment.
- On **Database Configuration** page, if prompted, select to upgrade the database.
- Review the summary and complete the installation.

6. Fail over the active VMM node to the newly upgraded VMM server.
7. Repeat the procedure on other VMM nodes.
8. Update the cluster functional level by using the **Update-ClusterFunctionalLevel** command.
9. [Optional] Install the appropriate SQL Command line utilities.

Mixed mode upgrade with additional VMM servers

This procedure requires additional VMM servers; however, it ensures almost no downtime in all the scenarios.

Follow these steps:

1. Back up and retain the VMM database.

2. Add the same number of additional servers (with Windows Server 2022 Management OS) that equals to the server number present in the HA cluster.
3. Install Windows 11/Windows Server 2022 version of the ADK on the newly added 2022 servers.
4. Install VMM 2022 on one of the newly added servers by using the details in **step 5** in Mixed mode upgrade with no additional VMM servers.
5. Repeat the installation steps for all the other newly added servers.
6. Fail over the active VMM node to one of the newly added servers.
7. Uninstall VMM from the 2019 nodes, and remove these nodes from the cluster after failover.
8. Update the cluster functional level by using the **Update-ClusterFunctionalLevel** command.
9. [Optional] Install the appropriate SQL Command line utilities.

> ⓘ **Note**
>
> Once the HA VMM upgrade is successful, upgrade the host agent manually by using the VMM.

Update VMM agents

After the upgrade, you need to update the VMM agents on your Hyper-V hosts and in your VMM library servers.

1. Select **Fabric** > **Servers** > **All Hosts**.
2. In the **Hosts** pane, right-click a column heading and then select **Agent Version Status**.
3. Select the host with the VMM agent that you want to update. On the **Hosts** tab, in the **Host** group, select **Refresh**. If a host needs to have its VMM agent updated, the **Host Status** column will display **Needs Attention**, and the **Agent Version Status** column will display **Upgrade Available**.
4. Right-click the host with the VMM agent that you want to update, and then select **Update Agent**. In **Update Agent**, provide the necessary credentials and then select **OK**.
5. The **Agent Version Status** column will display a value of **Upgrading**. After the VMM agent is updated successfully on the host, the **Agent Version Status** column will display a value of **Up-to-date**, and the **Agent Version** column will display the updated version of the agent. After you refresh the host again, the **Host Status** column for the host will display a value of **OK**.

6. You can update the VMM agent on a VMM library server in a similar manner. To view a list of VMM library servers, select **Fabric** > **Servers** > **Library Servers**.

Reassociate hosts and library servers

After the upgrade, you might need to reassociate virtual machine hosts and VMM library servers with the VMM management server.

Follow these steps:

1. Select **Fabric** > **Servers** > **All Hosts**.
2. In the **Hosts** pane, ensure that the **Agent Status** column is displayed. If it isn't displayed, right-click a column heading and select **Agent Status**.
3. In the host group, select **Refresh**. If a host needs to be reassociated, the Host Status column displays **Needs Attention**, and the **Agent Status** column displays **Access Denied**. Right-click the host that you want to reassociate and then select **Reassociate**.
4. In **Reassociate Agent** page, provide credentials and then select **OK**. The Agent Status displays the status as **Reassociating**. After the host is reassociated successfully, the status changes to **Responding**.
5. Refresh the host; the host status columns now display **OK**. After you've reassociated the host, you might need to update the VMM agent on the host.

Upgrade the VMM SQL Server database

There are a couple of reasons you might want to upgrade the VMM SQL Server database:

- You're upgrading VMM to System Center 2022, and the current SQL Server database version isn't supported.
- You want to upgrade a VMM standalone server to a high availability server, and SQL Server is installed locally.
- You want to move the SQL Server database to a different computer.

Collect database information

Before you upgrade, collect information about the VMM database:

1. Record the database connection in the VMM console > **Settings** > **General** > **Database Connection**.

2. Record the account information in Server Manager > **Tools** > **Services**. Right-click **System Center Virtual Machine Manager** > **Properties** > **Log On**. This is the domain or local account that was assigned as the service account when VMM was installed. You can check if it's local in **Tools** > **Computer Manager** > **Local Users and Groups** > **Users**.
3. Check whether you used distributed key management when you installed VMM, or if encryption keys are stored locally on the VMM server.
4. If you're moving the VMM database, but not upgrading the VMM, check which update rollups have been applied on the VMM server.

Upgrade a standalone database

1. Back up the existing VMM database, and copy the backup to a computer running a supported version of SQL Server.
2. Use SQL Server tools to restore the database.

- If you're upgrading VMM, you'll specify the new SQL Server location in VMM setup > **Database Configuration**.
- If you want to upgrade the database without upgrading VMM, you need to uninstall, and then reinstall VMM. When you uninstall, on the **Database Options** page, select **Retain database**. Then reinstall with the same settings you used for the original installation. On the **Database Configuration**, specify the new SQL Server details. After reinstall, apply the update rollups and check that the deployment is working as expected.

Upgrade a highly available database

1. Record the source version of the existing database and the version you want to upgrade to.
2. Create a backup of the highly available SQL Server database from the active node of the SQL Server cluster.
3. Upgrade passive SQL Server nodes to the new version. After the upgrade, optionally install SQL Server Management Studio if you want to manage the SQL Server from this node.
4. Fail over the highly available SQL server role from the currently active node to the upgraded node. After failover, you can use SQL Server Management Studio to validate the running database version.
5. Repeat the upgrade for the other nodes in the HA SQL cluster. As an additional validation, you can fail over the SQL Server database roles to ensure that everything works as expected.

Migrate a SQL Server cluster as part of the VMM upgrade

1. Take a backup of the highly available VMM database from the active node of the existing SQL cluster.
2. Note the VMM role name to use when reinstalling the VMM server role. Uninstall VMM server from the existing VMM cluster nodes with the retain database option. When uninstalling VMM server from last node, you can get a message about unsuccessful SPN registration. This is a known issue with no functional impact.
3. Restore the backed-up DB into another SQL cluster running supported SQL version. Add the user on which VMM service is running as User to this new DB with membership to db_owner.
4. While upgrading VMM Server as part of SQL Cluster migration, give the Parameters corresponding to the new SQL Cluster.

Redeploy Azure Site Recovery

If Azure Site Recovery was integrated into your VMM 2019 deployment, you need to redeploy it with VMM 2022 for replication to Azure or replication to a secondary site.

Connect to Operations Manager

After the upgrade, reconnect VMM to the Operations Manager.

Renew certificates for PXE servers

If you have a PXE server in the VMM fabric, you need to remove it from the fabric, and then add it again. This is to renew the PXE server certificate and avoid certificate errors.

Next steps

Learn about deploying the latest update rollups.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Install VMM

Article • 08/02/2024

This article describes how to install the System Center Virtual Machine Manager (VMM) management server.

Before you start

- Review the system requirements and planning information. Learn about system requirements.
- Ensure that you have at least local admin permissions on the computer before you run the setup.
- The service account should be an administrator on the VMM server.

> ⓘ **Note**
>
> During VMM Installation, ensure that the SQL Database isn't part of any Availability Group.

Run setup

> ⓘ **Note**
>
> The service account for VMM can be:
>
> - A local account.
> - A user account used for service.
> - A group managed service account.
> - If you're using a local account, you can't have VMM in a highly available configuration.
> - If you're using gMSA account, the format should be *domainFQDN\gMSAAccount$*.

1. Close any open programs and ensure that no restarts are pending on the computer.
2. To start the Virtual Machine Manager Setup wizard, on your installation media, right-click **setup.exe** and then select **Run as administrator**.

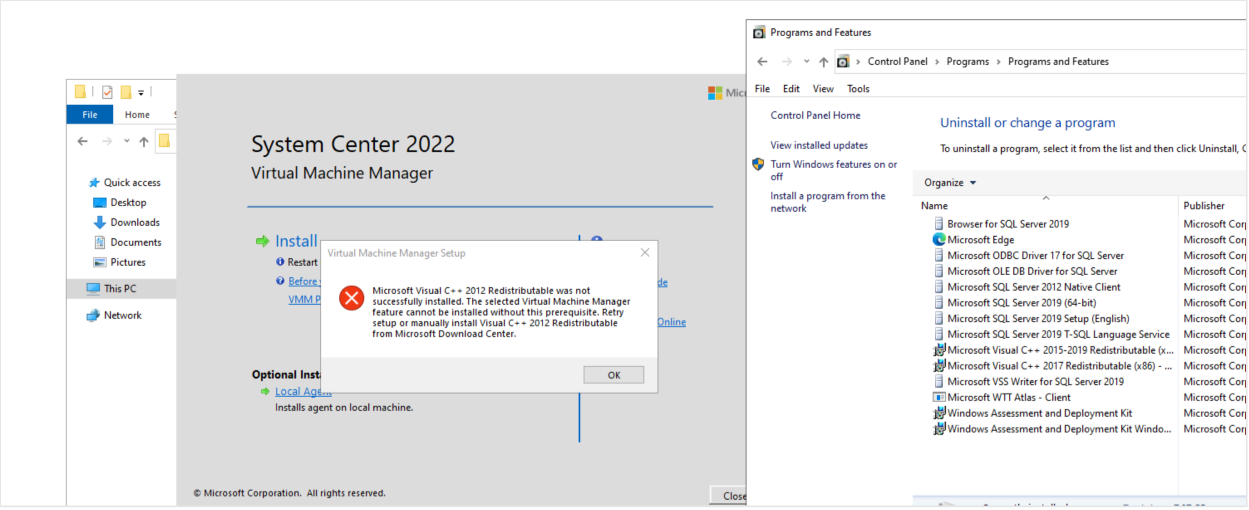
3. In the main setup page, select **Install**.
4. On the **Select features to install** page,
   Select the **VMM management server** checkbox, and then select **Next**. The VMM console installs automatically. If you're installing on a cluster node, you'll be asked if you want to make the management server highly available.
5. On the **Product registration information** page, provide the appropriate information and select **Next**. If you don't enter a product key, VMM installs as an evaluation version that expires in 180 days after installation.
6. On the **Please read this license agreement** page,
   Review the license agreement, select the **I have read, understood, and agree with the terms of the license agreement** checkbox, and then select **Next**.
7. On the **Diagnostic and Usage Data** page,
   Review Microsoft's data collection policy and how to disable data collection. Then select **Next**.
8. If the **Microsoft Update** page appears,
   Select whether you want to use Microsoft Update, and then select **Next**. If you've already chosen to use Microsoft Update on this computer, the page won't appear.
9. On the **Diagnostic and Usage Data** page,
   Review Microsoft's data collection policy and how to disable data collection and then select **Next**.
10. On the **Installation location** page,
    Use the default path or enter a different installation path for the VMM program files, and then select **Next**. The setup program checks the computer on which you're installing the VMM management server to ensure that the computer meets the appropriate hardware and software requirements. If the computer doesn't meet a prerequisite, a page that contains information about the prerequisite and how to resolve the issue appears.
11. On the **Database configuration** page,

    - If you're using a remote SQL instance, specify the name of the computer that's running the SQL Server.
    - If you're installing the VMM management server on the same computer that's running the SQL Server, then in the **Server name** box, either enter the name of the computer (for example, **vmmserver01**) or **localhost**.
    - If the SQL Server is in a cluster, enter the cluster name.

12. Don't specify a **Port** value if you don't have a remote instance of the SQL Server or if you have a remote SQL Server that uses the default port (1433).
13. Specify the SQL Server instance name and whether to use an existing or new database. You need an account with permissions to connect to the instance.

14. On the **Configure service account and distributed key management** page, Specify the account that the VMM service uses. You can't change the identity of the VMM service account after installation. Learn more about distributed key management here.
15. Under **Distributed Key Management**, select whether to store encryption keys in Active Directory or not.
16. On the **Port configuration** page,
    Use the default port number for each feature or provide a unique port number that's appropriate in your environment. You can't change the ports that you assign during the installation of a VMM management server unless you uninstall and then reinstall the VMM management server. Also, don't configure any feature to use port 5986 because that port number is preassigned.
17. On the **Library configuration** page,
    Select whether to create a new library share or to use an existing library share on the computer. The default library share that VMM creates is named *MSSCVMMLibrary*, and the folder is located at **%SYSTEMDRIVE%\ProgramData\Virtual Machine Manager Library Files**. **ProgramData** is a hidden folder, and you can't remove it. After the VMM management server is installed, you can add library shares and library servers by using the VMM console or by using the VMM command shell.
18. On the **Installation summary** page,
    Review your selections and then select **Install**. The **Installing features** page appears and displays the installation progress.
19. On the **Setup completed successfully** page,
    a. Select **Close** to finish the installation.
    b. To open the VMM console, ensure that **Open the VMM console when this wizard closes** is checked or select the **Virtual Machine Manager Console** icon on the desktop.

> ⓘ **Note**
>
> If VMM 2022 and SQL 2019 are installed on the same machine, the following error appears: Reboot the machine for successful installation.



System Center 2022

Virtual Machine Manager

Installs agent on local machine.

© Microsoft Corporation. All rights reserved.

Virtual Machine Manager Setup

Microsoft Visual C++ 2012 Redistributable was not successfully installed. The selected Virtual Machine Manager feature cannot be installed without this prerequisite. Retry setup or manually install Visual C++ 2012 Redistributable from Microsoft Download Center.

OK

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, C

Name	Publisher
Browser for SQL Server 2019	Microsoft Cor
Microsoft Edge	Microsoft Cor
Microsoft ODBC Driver 17 for SQL Server	Microsoft Cor
Microsoft OLE DB Driver for SQL Server	Microsoft Cor
Microsoft SQL Server 2012 Native Client	Microsoft Cor
Microsoft SQL Server 2019 (64-bit)	Microsoft Cor
Microsoft SQL Server 2019 Setup (English)	Microsoft Cor
Microsoft SQL Server 2019 T-SQL Language Service	Microsoft Cor
Microsoft Visual C++ 2015-2019 Redistributable (x...	Microsoft Cor
Microsoft Visual C++ 2017 Redistributable (x86) - ...	Microsoft Cor
Microsoft VSS Writer for SQL Server 2019	Microsoft Cor
Microsoft WTT Atlas - Client	Microsoft Cor
Windows Assessment and Deployment Kit	Microsoft Cor
Windows Assessment and Deployment Kit Windo...	Microsoft Cor

During Setup, VMM enables the following firewall rules. These rules remain in effect even if you later uninstall VMM.

- Windows Remote Management
- Windows Standards-Based Storage Management

ⓘ Note

If Setup doesn't finish successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** is a hidden folder.

ⓘ Note

If you run into ADK file path issue while installing VMM, copy the files from the *amd64* folder in ADK root folder to the ADK root folder itself. The default ADK folder path is *C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\WSIM*, but it can be different based on your choice of folder path during ADK installation.

Install VMM from a command prompt

You can install VMM from a command prompt. The installation media contains `.ini` files for all the VMM features:

- **VMServer.ini**: Settings for the VMM management server.
- **VMClient.ini**: Settings for the VMM console.
- **VMServerUninstall.ini**: Uninstallation settings for the VMM management server.

Each of these files contains key/value pairs with default values. These entries are commented out. Remove the comment symbol (#) and change the value.

1. Edit the `VMServer.ini` file with the options in the table below this procedure.
2. After you edit, open an elevated command prompt and run setup.exe with the following parameters. For example, to use a `VMServer.ini` file that is stored in C:\Temp with a SQL Server administrator account of *contoso\SQLAdmin01* and a VMM service account of *contoso\VMMadmin14*, use the following command: **setup.exe /server /i /f C:\Temp\VMServer.ini /SqlDBAdminDomain contoso /SqlDBAdminName SQLAdmin01 /SqlDBAdminPassword password123 /VmmServiceDomain contoso /VmmServiceUserName VMMadmin14 /VmmServiceUserPassword password456 /IACCEPTSCEULA**

VMServer.ini values

Expand table

Option	Values	Default
ProductKey	Product key in the format: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx	xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
UserName	Optional display name for the user who is installing the features. UserName isn't the user account for the installation.	Administrator
CompanyName	Optional display name for the organization that is installing the features.	Microsoft Corporation
ProgramFiles	Location for VMM files.	C:\Program Files\Microsoft System Center\Virtual Machine Manager
CreateNewSqlDatabase	0: Use an existing Microsoft SQL Server database. 1: Create a new SQL Server database.	1
SqlInstanceName	Name of the new or existing instance of SQL Server.	MICROSOFT$VMM$
SqlDatabaseName	Name of the new or existing SQL Server database.	VirtualManagerDB

Option	Values	Default
RemoteDatabaseImpersonation	0: Don't impersonate the administrator account for SQL Server. The user that runs setup.exe must be an administrator for the server that is hosting the SQL Server. 1: Impersonate the administrator account for SQL Server by using the provided credentials. The user who runs setup.exe must provide values for the SqlDBAdminName, SqlDBAdminPassword, and SqlDBAdminDomain parameters.	0
SqlMachineName	Name of the server that is hosting SQL Server. Don't specify localhost. Instead, specify the actual name of the computer.	<sqlmachinename>
(various ports)	Ports used by VMM	IndigoTcpPort: 8100 IndigoHTTPSPort: 8101 IndigoNETTCPPort: 8102 IndigoHTTPPort: 8103 WSManTcpPort: 5985 BitsTcpPort: 443
CreateNewLibraryShare	0: Use an existing library share. 1: Create a new library share.	1
LibraryShareName	Name of the file share to be used or created.	MSSCVMMLibrary
LibrarySharePath	Location of the existing file share or the new file share to be created.	C:\ProgramData\Virtual Machine Manager Library Files
LibraryShareDescription	Description of the share.	Virtual Machine Manager Library Files
SQMOptIn	0: Don't opt in for **Diagnostic and Usage Data**.	1

Option	Values	Default
	1: Opt in for **Diagnostic and Usage Data**.	
MUOptIn	0: Don't opt in to Microsoft Update. 1: Opt in to Microsoft Update.	0
VmmServiceLocalAccount	0: Use a domain account for the VMM service (scvmmservice). 1: Use the Local System account for the VMM service. To use a domain account, when you run setup.exe, provide values for the VMMServiceDomain, VMMServiceUserName, and VMMServiceUserPassword parameters.	0
TopContainerName	Container for Distributed Key Management (DKM); for example, *CN=DKM,DC=contoso,DC=com*.	VMMServer
HighlyAvailable	0: Don't install as highly available. 1: Install as highly available.	0
VmmServerName	Clustered service name for a highly available VMM management server. Don't enter the name of the failover cluster or the name of the computer on which the highly available VMM management server is installed.	<VMMServerName>
VMMStaticIPAddress	IP address for the clustered service name for a highly available VMM management server if you're not using Dynamic Host Configuration Protocol (DHCP). Both IPv4 and IPv6 are supported.	<comma-separated-ip-for-HAVMM>
Upgrade	0: Don't upgrade from a previous version of VMM. 1: Upgrade from a previous version.	1

Setup-exe parameters

Expand table

Parameter	Details
/server	Specifies installation of the VMM management server.
/i or /x	Specifies whether to install (/i) or uninstall (/x) the server.
/f <filename>	Specifies the .ini file to use. Be sure that this parameter points to the correct .ini file. If setup.exe doesn't find an .ini file, it performs the installation by using its own default values.
/VmmServiceDomain <domainName>	Specifies the domain name for the account that is running the VMM service (scvmmservice). Use this parameter only if you set VmmServiceLocalAccount to 0 in VMServer.ini.
/VmmServiceUserName <userName>	Specifies the username for the account that is running the VMM service (scvmmservice). Use this parameter only if you set VmmServiceLocalAccount to 0 in VMServer.ini.
/VmmServiceUserPassword <password>	Specifies the password for the account that is running the VMM service (scvmmservice). Use this parameter only if you set VmmServiceLocalAccount to 0 in VMServer.ini.
/SqlDBAdminDomain <domainName>	Specifies the domain name for the administrator account for the SQL Server database. Use this parameter if the current user doesn't have administrative rights to SQL Server.
/SqlDBAdminName <userName>	Specifies the username for the administrator account for the SQL Server database. Use this parameter if the current user doesn't have administrative rights to SQL Server.
/SqlDBAdminPassword <password>	Specifies the password for the administrator account for the SQL Server database. Use this parameter if the current user doesn't have administrative rights to SQL Server.
/IACCEPTSCEULA	Notes acceptance of the Microsoft Software License Terms. This is a mandatory parameter. For example, to use a VMServer.ini file that is stored in C:\Temp with a SQL Server administrator account of contoso\SQLAdmin01 and a VMM service account of contoso\VMMadmin14, use the following command: **setup.exe /server /i /f C:\Temp\VMServer.ini /SqlDBAdminDomain contoso /SqlDBAdminName SQLAdmin01 /SqlDBAdminPassword password123 /VmmServiceDomain contoso /VmmServiceUserName VMMadmin14 /VmmServiceUserPassword password456 /IACCEPTSCEULA**

Uninstall VMM or the VMM console

1. Ensure that the VMM console and VMM command shell are closed.

2. On the computer on which the VMM management server is installed, select **Start** and then select **Control Panel**.

3. Under **Programs**, select **Uninstall a program**. Under **Name**, right-click **Microsoft System Center Virtual Machine Manager**.

4. On the **What would you like to do?** page, select **Remove features**.

5. On the **Select features to remove** page, select the **VMM management server** checkbox, and then select **Next**. If you want to uninstall the VMM console, select the **VMM console** checkbox.

   > ⓘ **Note**
   >
   > If you've a highly available VMM deploy, you must remove both the VMM server and the VMM console.

6. On the **Database options** page, select whether you want to retain or remove the VMM database, and, if necessary, credentials for the database, and then select **Next**.

7. On the **Summary** page, review your selections and select **Uninstall**. The **Uninstalling features** page appears, and uninstallation progress is displayed.

8. After the VMM management server is uninstalled, on the **The selected features were removed successfully** page, select **Close**.

The following firewall rules, which were enabled during VMM Setup, remain in effect after you uninstall VMM:

- File Server Remote Management

- Windows Standards-Based Storage Management firewall rules

If there's a problem with setup completing successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** is a hidden folder.

Uninstall VMM from the command line

To uninstall VMM, edit the *VMServerUninstall.ini* file as described. Then run setup.exe for the uninstall. For example, to uninstall using an ini file stored in C:\Temp with an account contoso.SQLAdmin01 type: **setup.exe /server /x /f C:\Temp\VMServerUninstall.ini**

/SqlDBAdminDomain contoso /SqlDBAdminName SQLAdmin01
/SqlDBAdminPassword password123

VMServerUnisntall.ini

Expand table

Option	Details	Default value
RemoteDatabaseImpersonation	0: Local SQL Server installation. 1: Remote SQL Server installation. When you run setup.exe, provide a value for the SqlDBAdminName, SqlDBAdminPassword, and SqlDBAdminDomain parameters unless the user who is running setup.exe is an administrator for SQL Server.	0
RetainSqlDatabase	0: Remove the SQL Server database. 1: Don't remove the SQL Server database To remove the SQL Server database, when you run setup.exe, provide a value for the SqlDBAdminName, SqlDBAdminPassword, and SqlDBAdminDomain parameters unless the user who is running Setup is an administrator for SQL Server.	0
ForceHAVMMUninstall	0: Don't force uninstallation if setup.exe can't verify whether this node is the final node of the highly available installation. 1: Force the uninstallation.	

Support for gMSA account

Group Managed Service Account (gMSA) helps improve the security posture and provides convenience through automatic password management, simplified service principle name (SPN) management, and the ability to delegate the management to other administrators.

VMM supports the use of gMSA for *Management server service account*.

> ⓘ Note
>
> gMSA, when used as VMM Service account, needs to have *logon as a service* and *Replace a process level token* permissions.

Prerequisites

1. Review this article and create gMSA as per the guidance available in the article.

2. Ensure that the servers on which VMM Management service would be installed have permissions to retrieve the password of the gMSA account.

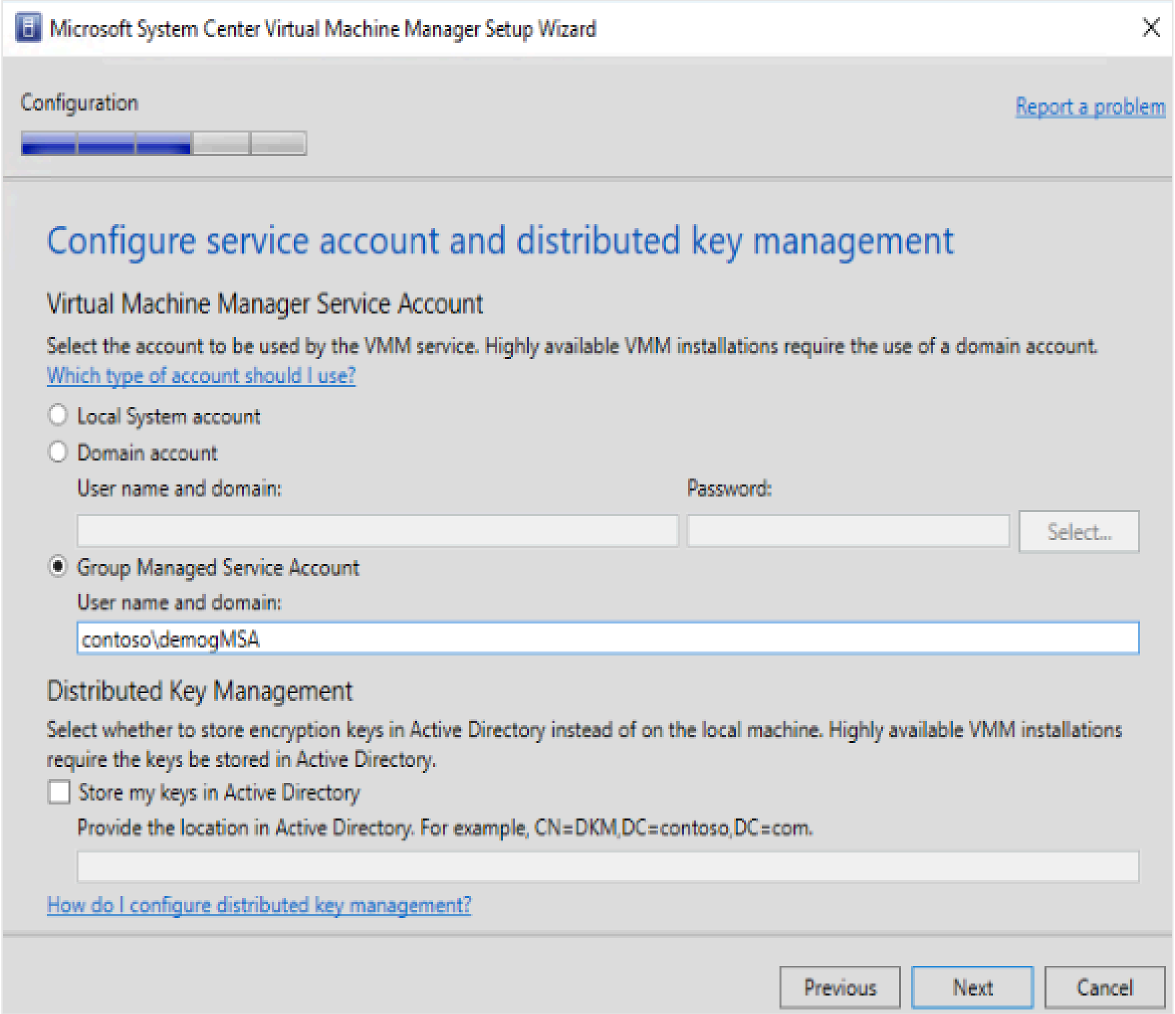
   > ⓘ Note
   >
   > You don't need to specify the SPN when creating the gMSA. VMM service sets the appropriate SPN on the gMSA.

Use the following steps:

1. Start the VMM installation setup.

2. On the **Service account configuration** page, select **Group Managed Service Account** as the option for VMM service account.

3. Enter the gMSA account details in *Domain\gMSA account* format.



Microsoft System Center Virtual Machine Manager Setup Wizard
Configuration
Report a problem

Configure service account and distributed key management

Virtual Machine Manager Service Account

Select the account to be used by the VMM service. Highly available VMM installations require the use of a domain account.

Which type of account should I use?

○ Local System account

○ Domain account

User name and domain:

Password:

● Group Managed Service Account

User name and domain: contoso\demogMSA

Distributed Key Management

Select whether to store encryption keys in Active Directory instead of on the local machine. Highly available VMM installations require the keys be stored in Active Directory.

□ Store my keys in Active Directory

Provide the location in Active Directory. For example, CN=DKM,DC=contoso,DC=com.

How do I configure distributed key management?

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Install the VMM Console

Article • 07/10/2024

This article describes how to install the System Center Virtual Machine Manager (VMM) console on a remote computer and connect to the VMM server. When you install the VMM management server, the console is installed on it automatically.

> ⓘ Note
>
> The default timeout value for a VMM client session is 330 seconds, and it's specific to each client. To update the timeout value, create *IndigoSendTimeout* registry in all the client machines from where the timeout needs to be configured. The registry is located at **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Administrator Console\Settings**.
>
> The registry is of type DWORD (32-bit), the minimum value is 330 seconds, and the maximum is 900 seconds (15 minutes).

Before you start

- Check the supported operating systems for the console that are detailed in the system requirements.
- Review and ensure you meet the system requirements. Learn about system requirements.
- Ensure that you have at least local administrator permissions on the computer on which you're installing the console.
- The VMM version of the console must match the System Center version of the VMM server. For example, to connect to a VMM server running System Center 2022, the VMM console version must also be 2022.
- You can only install one version of the console on a single machine.

Run setup

1. Review the planning instructions. Then, right-click setup.exe for VMM > **Run as administrator**.
2. On the main setup page, select **Install** and on the **Select features to install** page, select the **VMM console** checkbox, and then select **Next**. On the **Please read this**

notice page, select the **I agree with the terms of this notice** checkbox, and then select **Next**.

3. Review the information on the **Diagnostic and Usage Data** page, and then select **Next**. On the **Microsoft Update** page, select whether you want to use Microsoft Update, and then select **Next**. This page won't appear if updates are already installed.
4. On the **Installation location** page, enter an installation path for the VMM program files or use the default path, and then select **Next**. Setup checks that the computer meets the console installation requirements.
5. On the **Port configuration** page, enter the port that you want to use for the VMM console to communicate with the VMM management server, and then select **Next**. The port setting that you assign for the VMM console should match the port setting that you assigned for the VMM console during the installation of the VMM management server. The default port setting is 8100. Also, don't assign port number 5986 because it's preassigned.
6. On the **Installation summary** page, review the settings and select **Install**. The **Installing features** page appears and displays the installation progress.
7. On the **Setup completed successfully** page, select **Close** to finish the installation. Select **Open the VMM console when this wizard closes** to open the console after the wizard finishes. If setup doesn't finish successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** is a hidden folder.

If you want to uninstall the console, do the following:

1. In the Control Panel, select to uninstall a program and select Microsoft System Center Virtual Machine Manager.
2. In **Select features to remove**, select **VMM console**. On the VMM management server, you can't uninstall the console without uninstalling VMM management.
3. In **Summary**, review the settings and select **Uninstall**.

Install the console from the command prompt

You can install the VMM administrator console from the command line by using the VMClient.ini file to customize the installation options. You can set the parameters as follows:

⛶ **Expand table**

Parameter	Value
ProgramFiles	Specify the location in which to store program files.
IndigoTCpPort	Specify the port number used to communicate with the VMM server.
MUOptIn	0: Don't opt in to Microsoft Update. 1: Opt in.
VmmServerForOpsMgrConfig	Specify the name of the System Center Operations Manager server.
IACCEPTSCUELA	Specifies that you have read, understood, and accepted the terms of use.

Install the console as follows:

1. Copy the VMClient.ini file from the amd64\Setup folder to a local folder.
2. Edit the VMClient.ini file. Remove the comment indicator (#) only if you want to edit the entry. Otherwise, setup uses the values in the .ini file as the default values.
3. Run setup as follows: setup.exe /client /i /f <path>, where:

   - /client - specifies console installation
   - /i or /x - specify whether to install (/i) or uninstall (/x) the console.
   - /f <filename> - specifies the ini file to use. Make sure this is correct. If setup doesn't find the ini file, it installs with default values.
   - path: location of ini file.
   - Don't use the /opsmgr parameter

Example: **setup.exe /client /i /f C:\Temp\VMClient.ini**.

Connect to a VMM management server

1. On the remote machine desktop, select the VMM console icon if the console isn't open.
2. Specify the server name and port on which the VMM server is listening (8100 by default). For example, **vmmserver01:8100**.
3. You can use the account with which you're signed in to the remote machine or specify a different account to connect to VMM. Select **Automatically connect with these settings** if you want to connect to the same VMM server each time.
4. Select **Connect**. **Select User Role** appears if the credentials you're using belong to more than one VMM user roles.

Enable enhanced console session in VMM

Article • 07/10/2024

This article provides information on how to configure enhanced console session in System Center Virtual Machine Manager (VMM).

Console connect in VMM provides a way to connect to the VM without a network connection to it. For information on deploying VMM console, see install VMM console. In System Center 2016 Operations Manager, the console connect in VMM supported only basic session where clipboard text can only be pasted through the **Type Clipboard Text menu** option.

VMM supports enhanced console session. With console connected through enhanced session, **Cut (Ctrl + X)**, **Copy (Ctrl + C)**, and **Paste (Ctrl + V)** operations on the ANSI text and files are available on the clipboard, thereby copy/paste commands for text and files are made possible from and to the VM.

Before you start

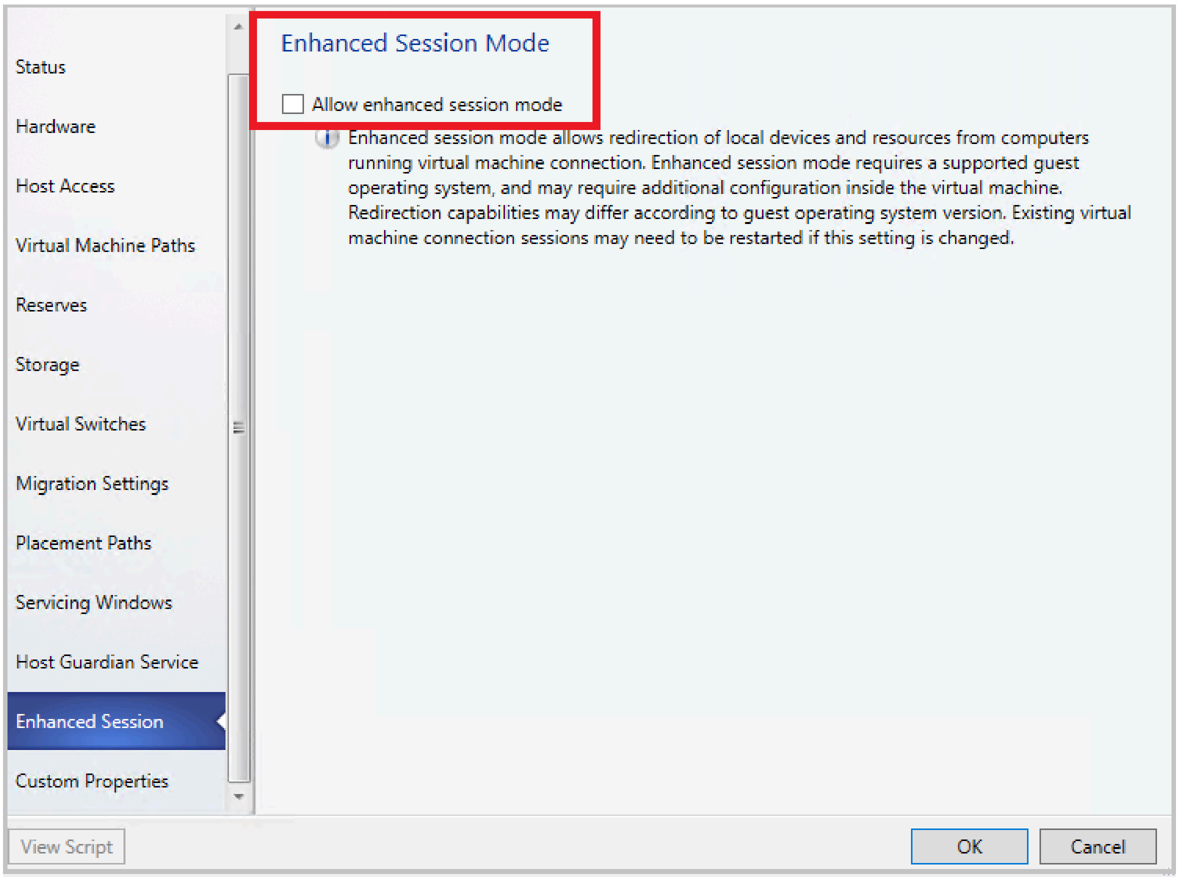
Ensure the following prerequisites:

1. The operating system of the host on which the VM is running should be Windows Server 2016 and later.
2. The Hyper-V host must have Enhanced session mode policy setting turned ON.
3. The computer from which you connect to the VM must run on Windows 10, Windows 8.1, Windows Server, Windows Server 2016, or later.
4. The virtual machine must have remote desktop services enabled and run Windows 10, Windows 11, Windows Server 2016, or later as the guest operating system.

Enable the enhanced console session

Use the following steps:

1. Right-click the host in **VMs & Services** and navigate to the **Enhanced Session** option.
2. Select **Allow enhanced session mode** and select **OK**.



Enhanced Session Mode

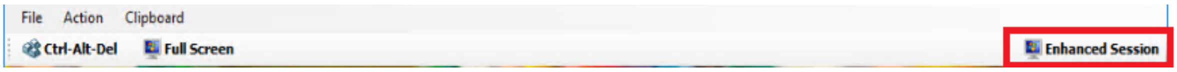
□ Allow enhanced session mode

Enhanced session mode allows redirection of local devices and resources from computers running virtual machine connection. Enhanced session mode requires a supported guest operating system, and may require additional configuration inside the virtual machine. Redirection capabilities may differ according to guest operating system version. Existing virtual machine connection sessions may need to be restarted if this setting is changed.

3. In the VMM console, navigate to the VM on this host.

4. Right-click the VM and select **Connect via Console**.

5. Once you see the VM console, look for the **Enhanced Session** option at the top right of the page. Select it to launch the Enhanced Session window.



ⓘ **Note**

This action will close the current session and open a new session. You will be redirected to the sign in screen in the new session.

6. To switch back to the basic session, select **Basic Session** at the top right.

Once the Enhanced Session Mode policy is enabled on the host:

- Close any open console sessions to view the **Enhanced Session** option.
- For a VM that is booting for the first time from a VHD/VHDX, the enhanced session option doesn't show up when you attempt to connect through console. Restart the VM and refresh the VM properties in VMM for the Enhanced Session option to appear in the console connect window.

Next steps

Use local resources on Hyper-V VM with VMConnect

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Deploy VMM for high availability

Article • 08/02/2024

For resilience and scalability, you can deploy System Center Virtual Machine Manager (VMM) in a high availability mode.

Before you start

Prepare for a high availability deployment by considering the following:

- Only one instance of VMM can be deployed to a failover cluster of up to 16 nodes.
- Requirements for computers running as VMM management nodes:
  - All cluster nodes that are VMM servers must be running Windows Server 2016.
  - Each cluster node must be joined to a domain and must have a computer name that doesn't exceed 15 characters.
  - The VMM service network name must not exceed 15 characters.
  - Windows ADK needs to be installed on each computer. Install from setup or the download center. Select **Deployment Tools** and **Windows Preinstallation Environment** when you install.
  - If you plan to deploy VMM services that use SQL Server data-tier applications, install the related command-line utilities on your VMM management server. The command line utility is available in the SQL Server 2012 feature pack or SQL Server 2014 feature pack or SQL Server 2016 feature pack.
- Don't install on a Hyper-V host parent partition. You can install VMM on a VM.
- Before you start, set up the VMM service account and distributed key management. Learn more

Deploy high availability components

- Deploy the VMM management server in a failover cluster.
- Make library server file shares highly available.
- Deploy the SQL Server VMM database as highly available.

Next steps

Deploy a highly available VMM management server.

Deploy a highly available VMM management server

Article • 08/02/2024

This article describes the steps for deploying a highly available System Center Virtual Machine Manager (VMM) server.

Before you start

- Read the planning steps for a highly available deployment.
- This procedure presumes you're setting up a single failover cluster with two or more file servers.

Set up the failover cluster

Follow these steps to set up the failover cluster:

1. Select **Server Manager** > **Manage** > **Add Roles and Features**.
2. In **Select installation type**, select **Role-based or feature-based installation**.
3. In **Select destination server**, select the server you want to configure for failover clustering. On **Select features**, select **Failover Clustering**.
4. Select **Add Feature** to install the failover cluster management tools.
5. In **Confirm installation selections**, select **Install**. A server restart isn't needed.
6. Repeat for each server you want to add as a node in the file server cluster.
7. After you've added at least two nodes in the cluster, you can run cluster validation tests. Open **Failover Cluster Manager** and under **Management**, select **Validate Configuration**.
8. In **Select Servers or a Cluster**, specify the NetBIOS or FQDN of a node you're adding and select **Add**. In **Testing Options**, select **Run all tests (recommended)**.
9. In **Summary**, if the tests completed correctly, select **Create the cluster now using the validated nodes**. Select **View Report** to troubleshoot any issues.
10. In **Access Point for Administering the Cluster**, specify the cluster name. For example, **VMMLibrary**. When the cluster is created, this name is registered as the cluster computer object (CNO) in Active Directory. If you specify a NetBIOS name for the cluster, the CNO is created in the same location where the computer objects for the cluster node reside (either the default Computers container or an OU). You can specify a different location by adding the distinguished OU name. For example, CN=ClusterName, OU=Clusters, DC=Contoso. For more information, see distributed key management.

11. If the server isn't configured to use DHCP, specify a static IP address for the cluster. Select each network you want to use for cluster management, and in **Address**, select the IP address. This is the IP address that is associated with the cluster in DNS.
12. In **Confirmation**, review the settings. Clear **Add all eligible storage to the cluster** if you want to configure storage later. Select **Next** to create the cluster.
13. In **Summary**, confirm that the cluster was created and that the cluster name is listed in Failover Cluster Manager.

Install VMM on the first cluster node

1. On either node of the cluster you created, run the VMM setup and select **Install**.
2. VMM detects its installation on a cluster node and asks you if you want to make the VMM server highly available. Select **Yes**.
3. In **Select features to install**, select the VMM management server and the VMM console.
4. In **Product registration information**, specify organizational details and the product key.
5. In **EULA and CEIP**, accept the End User License Agreement (EULA) and specify whether you want to participate in Customer Experience Improvement Program (CEIP).
6. In **Installation Location**, accept the default settings.
7. In **Prerequisites**, VMM checks whether all the prerequisites are met and installs the missing components. If you don't have the Windows ADK installed, download and install it.
8. In **Database configuration**, specify the database to use for VMM. The database should be highly available and deployed in a separate failover cluster. This dialog appears if VMM isn't clustered or if it's clustered but not using Always On Availability Groups. Specify the cluster name.
9. In **Cluster configuration**, specify the name of the VMM cluster. For example, **HAVMMM**.
10. In **Configure service account and distributed key management**, specify the service account and key location you created earlier. VMM Run As accounts are stored as encrypted in the VMM database. For a high availability deployment, you need to access encrypted keys from a central location. So you should have created a distributed key management container in Active Directory before you ran setup. Learn more about distributed key management container here.
11. In **Port configuration**, modify the port settings if required.
12. Finish installing VMM. You can't specify a library share right now. In a highly available deployment, you create the library share after the installation is complete.

Install VMM on the second cluster node

1. Run setup and confirm that you want to **add this server as a node** to the highly available deployment.
2. In the wizard, specify the service account password. You don't need to specify other information.

Next steps

Deploy SQL Server for VMM high availability.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Deploy SQL Server for VMM high availability

Article • 08/02/2024

This article describes the steps for deploying a highly available SQL Server database for System Center Virtual Machine Manager (VMM). You set up a SQL Server cluster and configure the SQL Server VMM database with Always On Availability Groups.

Before you start

Read the planning information for a highly available VMM deployment. It includes prerequisites and issues you should be aware of.

Set up availability groups

SQL Server Always On availability groups support failover environments for a discrete set of user databases (availability databases). Each set of availability databases is hosted by an availability replica. To set up an availability group, you must deploy a Windows Server Failover Clustering (WSFC) cluster to host the availability replica and enable Always On availability on the cluster nodes. You can then add the VMM SQL Server database as an availability database.

- Learn more about Always On prerequisites
- Learn more about setting up a WSFC for Always On availability groups
- Learn more about setting up an availability group

Configure the VMM database with Always On Availability Groups

1. On the VMM server, stop the VMM service. For a cluster, in Failover Cluster Manager, stop the VMM role.

2. Connect to the machine that hosts the VMM database, and in SQL Server Management Studio, right-click the VMM database > **Properties**. In **Options**, set the **Recovery model** for the database to **Full**.

3. Right-click the VMM database > **Tasks** > **Back Up** and take a backup of the database.

4. In SQL Server Management Studio > **Always On High Availability** > right-click the availability group name > **Add Database**.

5. In **Add Database to Availability Group** > **Select Databases**, select the VMM database.

6. In **Select Data Synchronization**, leave the **Full** default.

7. In **Connect to Replicas** > **Connect**, specify permissions for the availability group destination.

8. Prerequisites are checked in **Validation**. In **Summary**, when you select **Next**, Always On availability support is initiated for the VMM database. The VMM database is copied and from this point Always On keeps the VMM database synchronized between the SQL Server Always On cluster nodes.

9. Change VMM connection string in the path *HKLM\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings\Sql\ConnectionString* from *Server* to *SQLListenerName*. Also, update the following:

   - *HKLM\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings\Sql\MachineName* with *SQLListenerName*
   - *HKLM\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings\Sql\InstanceName* with *SQLListenerName*.
   - *HKLM\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings\Sql\MachineFQDN* with *SQLListenerFQDN*.

10. Restart the VMM service or cluster role. The VMM server should be able to connect to the SQL Server.

11. VMM credentials are only stored for the main SQL Server, so you need to create a new login on the secondary node of the SQL Server cluster with the following characteristics:

    - The login name is identical to the VMM service account name.
    - The login has the user mapping to the VMM database.
    - The login is configured with the database owner credentials.

Run a failover

To check that Always On is working as expected for the VMM database, run a failover from the primary to secondary node in the SQL Server cluster.

1. In SQL Server Management Studio, right-click the availability group on the secondary server > **Failover**.
2. In **Fail Over Availability Group** > **Select New Primary Replica**, select the secondary server.
3. In **Summary**, select **Finish**.
4. Now move it back by initiating a failover to the secondary node computer that is running SQL Server and verify that you can restart the VMM service (scvmmservice).
5. Repeat the last two steps for every secondary node in the cluster that is running SQL Server.
6. If this is a high availability VMM setup, continue to install other high availability VMM nodes.

> ⓘ **Note**
>
> If you're experiencing high latency or timeout errors in a multi-subnet scenario, change the VMM connection string in the path *HKLM\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings\Sql\ConnectionString*, add MultiSubnetFailover=True, and restart the VMM service.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Deploy a highly available VMM library

Article • 08/02/2024

This article describes the steps for deploying a highly available System Center Virtual Machine Manager (VMM) library. You set up a Windows failover cluster running the File Server role. Then you create file shares on the cluster, and assign them as VMM library shares.

Before you start

Read the planning steps for a highly available VMM deployment.

Set up the failover cluster

This procedure presumes you're setting up a single failover cluster with two or more file servers.

1. Select **Server Manager** > **Manage** > **Add Roles and Features**.
2. In **Select installation type**, select **Role-based or feature-based installation**.
3. In **Select destination server**, select the server you want to configure for failover clustering. On **Select features**, select **Failover Clustering**. Select **Add Feature** to install the failover cluster management tools.
4. In **Confirm installation selections**, select **Install**. A server restart isn't needed.
5. Repeat for each server you want to add as a node in the file server cluster.
6. After you've added at least two nodes in the cluster, you can run cluster validation tests (you'll need at least two nodes in the cluster). Open **Failover Cluster Manager** and under **Management**, select **Validate Configuration**.
7. In **Select Servers or a Cluster**, specify the NetBIOS or FQDN of a node you're adding and select **Add**. In **Testing Options**, select **Run all tests (recommended)**.
8. In **Summary**, if the tests completed correctly, select **Create the cluster now using the validated nodes**. Select **View Report** to troubleshoot any issues.
9. In **Access Point for Administering the Cluster**, specify the cluster name. For example, **VMMLibrary**. When the cluster is created, this name will be registered as the cluster computer object (CNO) in Active Directory. If you specify a NetBIOS name for the cluster, the CNO is created in the same location where the computer objects for the cluster node reside (either the default Computers container or an OU). You can specify a different location by adding the distinguished OU name. For example, CN=ClusterName, OU=Clusters, DC=Contoso.

10. If the server isn't configured to use DHCP, specify a static IP address for the cluster. Select each network you want to use for cluster management, and in **Address** select the IP address. This is the IP address that will be associated with the cluster in DNS.
11. In **Confirmation**, review the settings. Clear **Add all eligible storage to the cluster** if you want to configure the storage later. Select **Next** to create the cluster.
12. In **Summary**, confirm that the cluster was created and that the cluster name is listed in Failover Cluster Manager.

If you want to build a guest cluster to deploy the file server, read Rudolf Vesely's useful blog post.

Set up the file server role

1. On each computer you'll set up as a file server node, in **Failover Cluster Manager**, select **Configure Role**.
2. In the **High Availability Wizard** > **Select Role**, select **File Server**.
3. In **File Server Type**, select **File Server for general use**.
4. In **Client Access Point**, enter the cluster name (in our procedure this was **VMMLibrary**) and the cluster IP address.
5. In **Select storage**, specify the shared storage you want to use.
6. Confirm the settings and finish the wizard.

Create a file share

1. In **Failover Cluster Management** > cluster name > **Roles**, select the file server and select **Add File Share**.
2. In **New Share Wizard** > **Select Profile**, select **SMB Share - Quick**.
3. In **Share Location**, select the file server.
4. In **Share Name**, specify the share name and description.
5. In **Other Settings**, leave the default settings.
6. In **Permissions**, grant full access to the SYSTEM and Administrators accounts and to the VMM admin account. In **Confirmation**, review the settings and select **Create**.

Add the share as a VMM library

1. Open the VMM console > **Library** > **Add Library Server**.
2. In **Add Library Server Wizard** > **Enter Credentials**, specify a domain account with permissions for the file cluster.

3. On the **Select Library Servers** page, enter the domain in which the file cluster is located and in **Computer name**, specify the name you assigned to file server cluster or select **Search** to find it. Select **Add** > **Next**.
4. On the **Add Library Servers** page, select the library shares you want to add. If you want to add the default library resources to the share, select **Add Default Resources**. In addition to default resources, this adds the ApplicationFrameworks folder to the share.
5. On the **Summary** page, review settings and select **Add Library Servers**. In **Library** > **Library Servers**, verify the library server and share are listed.
6. After the share is created, you can copy resources to the library share.

Next steps

Set up TLS for VMM.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up TLS for VMM

Article • 08/02/2024

This article describes how to set up Transport Security Layer (TLS) protocol version 1.2 with System Center Virtual Machine Manager (VMM) server.

> ⓘ **Note**
>
> Virtual Machine Manager will use the protocol configured at the Operating System Level. For example, if TLS 1.0, TLS 1.1, and TLS 1.2 are enabled at the Operating System Level, then Virtual Machine Manager will select one of the three protocols in the following order of preference:
>
> 1. TLS version 1.2
> 2. TLS version 1.1
> 3. TLS version 1.0
>
> The Schannel SSP then selects the most preferred authentication protocol that the client and server can support.

Before you start

- Security fixes should be up to date on the VMM server and the server running the VMM database.
- The VMM server should be running .NET version 4.6. Follow these instructions to determine which version of .NET is installed.
- To work with TLS 1.2, System Center components generate SHA1 or SHA2 self-signed certificates. If SSL certificates from a certificate authority (CA) certificates are used, they should use SHA1 or SHA2.

Install a SQL Server update for TLS 1.2 support

1. Open KB 3135244.
2. Download and install the update for your SQL Server version.
   - You don't need this update if you're running SQL Server 2016.
   - SQL Server 2008 R2 doesn't support TLS 1.2.

Configure the VMM server to use TLS 1.2

Disable all SCHANNEL protocols except for TLS 1.2.

Manually modify the registry

1. Open the Registry Editor, and navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols.
2. Right-click **Protocol**, select **New** > **Key**. Enter the key and press Enter. Perform this procedure to create the following keys:

   - **SSL3**
   - **TLS 1.0**
   - **TLS 1.1**
   - **TLS 1.2**

3. After you've created these keys, you need to create the **Client** and **Server** keys under them.

   - For **SSL3**, select **New** > **Key**. Enter **Client** and press Enter. Again, for **SSL3**, select **New** > **Key** again. Then enter **Server** and press **Enter**.
   - Repeat the action to create the **Client** and **Server** keys under **TLS 1.0**, **TLS 1.1**, and **TLS 1.2**.

4. After you've created the **Client** and **Server** keys, you need to create DWORD values under them, in order to enable and disable protocols. Do this as follows:

   - Enable the TLS 1.2 protocol. To do this, in **TLS 1.2**, under the **Client** key, create the DWORD value **DisabledByDefault**, and set the value to 0. Now create a DWORD value **Enabled**, and set the value to 1. Create the same DWORD values under the **Server** key.
   - Now disable the other protocols. To do this, in **SSL3**, **TLS 1.0** and **TLS 1.1**, under the **Client** key, create the DWORD value **DisabledByDefault**, and set the value to 1. Now create a DWORD value **Enabled**, and set the value to 0. Create the same DWORD values under the **Server** key.

Modify the registry with a PowerShell script

Instead of modifying the registry values manually, you can use the following PowerShell script.

```
$ProtocolList       = @("SSL 2.0", "SSL 3.0", "TLS 1.0", "TLS 1.1", "TLS 1.2")
$ProtocolSubKeyList = @("Client", "Server")
$DisabledByDefault  = "DisabledByDefault"
$registryPath       =
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\"

foreach ($Protocol in $ProtocolList)
{
    foreach ($key in $ProtocolSubKeyList)
    {
        $currentRegPath = $registryPath + $Protocol + "\" + $key
        Write-Output "Current Registry Path: `"$currentRegPath`""

        if (!(Test-Path $currentRegPath))
        {
            Write-Output " `'$key`' not found: Creating new Registry Key"
            New-Item -Path $currentRegPath -Force | out-Null
        }
        if ($Protocol -eq "TLS 1.2")
        {
            Write-Output " Enabling - TLS 1.2"
            New-ItemProperty -Path $currentRegPath -Name $DisabledByDefault -Value
"0" -PropertyType DWORD -Force | Out-Null
            New-ItemProperty -Path $currentRegPath -Name 'Enabled' -Value "1" -
PropertyType DWORD -Force | Out-Null
        }
        else
        {
            Write-Output " Disabling - $Protocol"
            New-ItemProperty -Path $currentRegPath -Name $DisabledByDefault -Value
"1" -PropertyType DWORD -Force | Out-Null
            New-ItemProperty -Path $currentRegPath -Name 'Enabled' -Value "0" -
PropertyType DWORD -Force | Out-Null
        }
        Write-Output " "
    }
}

Exit 0
```

Configure VMM to use TLS 1.2

1. Open the registry editor on the VMM server. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NetFramework\v4.0.30319**.
2. Create the DWORD value **SchUseStrongCrypto** and set the value to 1.
3. Now navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft .NetFramework\v4.0.30319**.
4. Under this location, create the same DWORD value **SchUseStrongCrypto** and set the value to 1.
5. Restart the server for the settings to take effect.

Modify the registry with a PowerShell script

You can modify the registry settings using the following PowerShell script.

```
# Tighten up the .NET Framework
$NetRegistryPath = "HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319"
New-ItemProperty -Path $NetRegistryPath -Name "SchUseStrongCrypto" -Value "1" -
PropertyType DWORD -Force | Out-Null

$NetRegistryPath = "HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319"
New-ItemProperty -Path $NetRegistryPath -Name "SchUseStrongCrypto" -Value "1" -
PropertyType DWORD -Force | Out-Null
```

Next steps

Learn more about the TLS 1.2 protocol.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Deploy and manage update rollups in VMM

Article • 08/02/2024

This article provides information about how to install, verify, and remove update rollups for System Center Virtual Machine Manager (VMM).

> ⓘ **Note**
>
> Update rollups are installed automatically if Microsoft updates are set to Automatic. If they aren't installed automatically, you can install them manually.

Obtain and install update rollups

The following sections provide information about how to obtain and install the update rollups manually through Microsoft updates, Microsoft Download Center, and through VMM command line.

Back up the VMM database

1. In the VMM console, select **Settings**.
2. On the Home tab, select **Backup**.
3. In the VMM backup page, in the **Path** text box, specify the location for the backup file, and select **OK**.

> ⓘ **Note**
>
> Ensure that the job completes successfully; otherwise review the error details, and redo the backup. For more information, see Back up the VMM database.

Install update rollups from Microsoft updates

Follow these steps on a computer that has a VMM component installed and the latest updates are yet to be installed:

1. Under **Settings** > **Update & Security**, select **Windows Update**.
2. In the **Windows Update** window, select **Check Online for updates from Microsoft Update**.

3. Select **Important updates are available**.
4. Select the update rollup package and select **OK**.
5. Select **Install updates** to install the update package.

Install update rollups from Microsoft Download Center

To manually download the update rollups from the Microsoft Download Center, visit the Microsoft Download Center, search for the desired KB and manually download the update rollup packages.

Install update rollups through command prompt

To manually install an update rollup package through an elevated command prompt, run the following command:

msiexec.exe/update <package_name>

ⓘ Note

In the **<package_name>** placeholder, enter the actual package name.

ⓘ Note

There may be additional installation steps specific to an update rollup release. Check update rollup KB guide to ensure you complete all the installation steps.

Check the installation of an update rollup

Use the following procedure to check if an update rollup is successfully installed:

1. Under **Control Panel** > **Programs** > **Programs and Features** > **View installed updates**.
2. Verify that an update entry was created after the update rollup was installed.
    - For example, the Update Rollup 2 was released as update 3209586. You should be able to see this detail under **View installed updates** if you've installed this update rollup and if it was successfully installed.
3. Verify that the binary's version has the correct build number.
4. See the following to check the build number for a specific update rollup:

- List of build numbers for VMM

ⓘ Note

Not all the binaries have the current update rollup build number. However, if you don't have the binaries listed with the relevant update rollup build number, it's likely that the update rollup didn't install successfully.

Remove an update rollup

ⓘ Important

1. It isn't recommended that you remove the update rollups. Prior to removing, check all the available options if you can avoid the uninstall. You may also contact Microsoft Support to check and ensure if uninstallation is required.
2. It's recommended that you back up your VMM database before you attempt to remove an update rollup.
3. When you remove, the VMM binaries roll back to their earlier versions. However, the VMM database doesn't roll back.
4. If you've one or more hotfixes installed on the server, ensure that you replace the hotfix binary with the official update rollup binary before you start the removal.

Remove an update rollup using the control panel

1. Go to **Control Panel** > **Programs** > **Programs and Features**. For quick access, enter **appwiz.cpl** in **Run**; it opens the **Programs and Features** in **Control Panel**.
2. Select **View installed updates**.
3. Find the update that you want to remove, right-click the update, and then select **Uninstall**.

Remove an update rollup using the command line

ⓘ Note

To remove an update using the command line, you must have the following two globally unique identifiers (GUIDs) available:

- RTM product GUID
- Patch GUID

RTM Product GUIDs

- SCVMM Server: {EBC28D9B-9565-46F3-A248-E26F07F81A98}
- SCVMM Admin Console amd64: {B703D43A-ABF6-4A36-84CC-00D77FF8570B}
- SCVMM Admin Console i386: {F5D46892-E1BD-4E0A-BD6E-DAA1900BA786}
- SCVMM Guest Agent amd64: {3E71E1FB-AF93-4110-A8EB-973132A3B16B}
- SCVMM Guest Agent i386: {57D2C983-23BF-4840-B784-BDDAC2DC932B}

Patch GUIDs

To find the patch GUID, right-click the update, select **Properties**. On the **Details** tab, select the **Revision number**. This is the patch GUID.

When you know the RTM product GUID and the patch GUID, run the following command to remove the update: **Msiexec /I {< RTM Product GUID >} MSIPATCHREMOVE={< Patch GUID >}**

Verify the successful removal of an update rollup

Use the following procedure to check if the update rollup was successfully removed:

1. Check whether the update was removed from **Programs and Features**.
2. Verify that binaries were reverted successfully. To do this, go to the VMM installation directory, and verify that there's no binary that has the build version of the update rollup that you uninstalled.

ⓘ Note

When you uninstall the server and console updates from the VMM server, the order of uninstallation isn't important.

Restore the database backup in VMM

ⓘ Note

1. You can create a database backup at any time. But the database should be restored only if you uninstalled the latest update rollup on the server. If you uninstalled an older update rollup, you don't have to restore the VMM database.
2. Ensure that you restore the database backup that you created prior to the update rollup installation.

For information on how to restore the database backup, see this article.

Post-restore tasks

This section applies only if you add a host or a library server after you create a database backup and before you uninstall an update rollup.

After the VMM database is recovered, you must do the following actions:

- Remove any hosts that were removed from VMM since the last backup.
- If a host was removed since the last backup, the host shows a status of **Needs Attention** in the VMM console. Also, the virtual machines on that host show a status of **Host Not Responding**.
- Remove the virtual machines that were removed from the VMM since the last backup. If a host has a virtual machine that was removed since the last backup, the virtual machine shows a status of **Missing** in the VMM console.
- Add any hosts that were added to the VMM since the last backup.
- If you restored the VMM database to a different computer, you must re-associate the hosts that have a status of **Access Denied** in the VMM console.
  - A computer is considered different if it has a different security identifier (SID). For example, if you reinstall the operating system on the computer, the computer has a different SID, even if it has the same computer name.

For more information on post-restore tasks, see this article.

ⓘ Note

You must follow these steps for any other fabric resource, such as storage providers, library servers, and so on, that you add after you create a database backup.

Back up and restore VMM

Article • 08/02/2024

This article describes the backup and recovery process in a System Center Virtual Machine Manager (VMM) environment and provides some recommendations.

Before you start

- Don't use checkpoints for disaster recovery. Checkpoints don't create full duplicates of the hard disk contents, nor do they copy data to a separate volume.
- You can use a checkpoint to serve as temporary backup before updating an operating system on a virtual machine. This allows you to roll back the update if it has adverse effects.
- You should use a backup application to back up and recover your data in catastrophic data loss. One option is System Center Data Protection Manager (DPM).
- Data such as Remote Access Authorization (RAA) passwords and the product key can be entered when you reinstall VMM. However, some encrypted data such as Virtual Machine Roles can't be re-entered.
- You can't back up and restore such data if you use the Data Protection application programming interface (DPAPI) for backing up VMM.
- The data will be lost if the VMM management server fails.

Create and implement a backup plan

Basic elements of a backup plan include a list of what needs to be backed up and an outline of what is changed frequently (and therefore need to be backed up frequently) in your environment.

Back up the VMM database

The VMM database contains information such as configurations, service templates, profiles, virtual machine templates, services, scale-out services, and other critical data that is required for VMM to function correctly. Back up the VMM database regularly.

The VMM database can be stored on the VMM management server or on a separate server running Microsoft SQL Server. To back up the VMM database, you can use one or more of the following:

- SQL Server tools. For more information, see Create a Full Database Backup (SQL Server).

- Other backup tools that are used in your environment.

- The VMM console or a Windows PowerShell cmdlet, as described in the procedures that follow.

In addition to backing up the database, we recommend that you create a system state backup of the VMM management server so that you can re-create the server with the same security identifier (SID) in a catastrophic data loss. The SID is an integral part of how VMM is authorized on virtual machine hosts.

> ⓘ **Important**
>
> - There are several ways to recover the VMM database file that you create through either of the following backup procedures. One way, which requires the VMM management server to be functioning, is to use the **SCVMMRecover.exe** tool, as described in Backup-SCVMMServer (although **SCVMMRecover.exe** is not a cmdlet). Another way, which doesn't require the VMM management server to be functioning, is to restore using SQL Server tools for restoring and attaching a database file.
> - To use the following procedures, you must be a member of the Administrator user role.

You can back up the VMM database in the following ways:

1. By using the VMM console
2. By using cmdlets in Windows PowerShell

Select the required tab for steps to back up the VMM database by:

Using the VMM console

Follow these steps to back up the VMM database by using the VMM console:

1. In the **Settings** workspace, on the **Home**, in the **Backup** group, select **Backup**.

2. In the **Virtual Machine Manager Backup** dialog, specify the location for the backup file. Select a folder that isn't a root directory and that SQL Server can access.

You can check the status of the backup in the **Jobs** workspace.

For information about how to recover the backup, see the **Important** note before this procedure.

Back up hosts and virtual machines

Virtual machine hosts are Hyper-V hosts, VMware ESXi hosts, and host clusters on which virtual machines and services are deployed. To back up virtual machine hosts and clusters, use Microsoft System Center Data Protection Manager (DPM) or another backup application that takes advantage of Volume Shadow Copy Service (VSS) to copy host and virtual machine data to a remote file server share.

> **Important**
>
> We recommend that you back up virtual machine configuration files (.vmc) daily.

Inventory your hosts, and then back up all the hosted virtual machines. To get the list of hosts that are being managed by VMM, run the following cmdlet from a Windows PowerShell command line:

```
$vmhost = get-scvmmserver <VMM management server name> | get-scvmhost
```

For more information, see Get-SCVMMServer and Get-SCVMHost.

Back up all the configuration and resource files on each VMM host by using backup software that supports the VMM VSS writer. Backup software that supports VMM can minimize the number of steps required to archive and restore virtual machines, help minimize downtime, and help ensure consistency of the data that is being archived or restored.

Back up library servers

The VMM library includes file-based resources, such as virtual hard disks, ISO images, scripts, driver files, and application packages that are stored on library servers. These resources are closely associated with resources in the VMM database that aren't file-based, such as virtual machine and service templates and profiles. All these resources should be backed up.

To back up the data on library servers, use System Center Data Protection Manager (DPM) or another backup application that takes advantage of Volume Shadow Copy Service (VSS) to copy host and virtual machine data to a remote file server share. For a list of VMM library servers, run the following cmdlet from the Windows PowerShell command line:

```
$libraryservers = get-scvmmserver <VMM management server name> | get-
sclibraryserver
```

For more information, see Get-SCVMMServer and Get-SCLibraryServer.

Back up all the files on library shares to a shared folder on a remote file server, including the files with the following extensions:

- .vhd and .vhdx
- .iso
- .vmx
- .ps1
- .vmc
- .vsv

Back up VMM private clouds

To orchestrate and automate the replication and failover of virtual machines located in VMM clouds, you can use Azure Site Recovery Manager. You can replicate in the following ways:

- From one on-premises VMM site to another, using Hyper-V replication or SAN replication.

- From an on-premises VMM site to Azure, using Hyper-V replication.

Back up registry keys, encryption keys, and credentials

Use the following guidelines to back up registry keys, encryption keys, and non-VMM managed credentials:

- **Registry keys**: VMM uses multiple registry keys to store important settings. Settings are stored in the following registry key and its subkeys:

HKLM\Software\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings.

You should back up this entire section of the registry with the possible exception of the SQL subkey. If you back up the SQL subkey, you capture the database name, location, and other details at the time of backup, which might not match the VMM database details that you want at the time of recovery.

To back up registry keys, you can use the Regedit **Export** function, or any other tool that is used in your environment to back up registry keys.

- **Encryption keys in Active Directory Domain Services**: If distributed key management (DKM) is configured, then you're storing VMM-related encryption keys in Active Directory Domain Services (AD DS). To back up these keys, back up Active Directory on a regular basis.

- **Non-VMM managed credentials**: Some credentials that are related to VMM are managed by the Windows Credential Manager on the VMM management server. To access the Credential Manager, in the Control Panel, select **All Control Panel Items**, and then select **Credential Manager**. Select **Back up Credentials** to back up any VMM-related credentials.

Back up non-Microsoft user interface add-ins and other non-Microsoft applications

You can use non-Microsoft user interface (UI) add-ins to extend the functionality of the VMM console. The data that is used by a UI add-in might be stored on the local server or on a remote computer, and it might be configured with a specific set of permissions. Consult the backup guidelines of your specific UI add-in.

For any other non-Microsoft applications, refer to the application's specific backup guidelines.

Restore the VMM environment

Restore the VMM database if necessary

If the VMM database must be restored, restore it first, using the process that corresponds to your backup method. For example, to restore using SQL Server tools, see Restore and Recovery Overview (SQL Server).

If the VMM database is the only element that you need to restore, and you want information about the **SCVMMRecover.exe** tool, see Backup-SCVMMServer.

You can restore the VMM server on the same or a different computer. Select the required tab for steps to restore the VMM server on:

The same computer

If you're using the same computer for the VMM server, perform a system state restore on that computer (otherwise, skip this section). If you do this, the SID of the VMM server remains the same, and fewer steps are required to restore your VMM environment.

After you've restored the VMM server, take the following steps:

1. Remove any hosts or virtual machines from the VMM console that were removed after the last backup. If a host has been removed after the last backup, then it appears as **Not Responding** and all virtual machines on the host appear as **Host Not Responding**. If the host is present but a virtual machine has been removed after the last backup, then the virtual machine appears as **Missing**.

2. Add any hosts or virtual machines that were added after the last backup.

Update hosts with the new VMM management server

1. Open the VMM console.

2. Review the lists of hosts and virtual machines, as needed, to prepare for later steps in this procedure:

   - To review the list of servers, in the **Fabric** workspace, on the left, select **Servers**.

   - To review the list of virtual machines, in the **VMs and Services** workspace, on the left, select **All Hosts**.

3. Remove any hosts or virtual machines from the VMM console that were removed after the last backup. If a host has been removed after the last backup, then it appears as **Not Responding** and all the virtual machines on the host appear as **Host Not Responding**. If the host is present but a virtual machine has been removed after the last backup, then the virtual machine appears as **Missing**.

4. Add any hosts or virtual machines that were added after the last backup.

5. Identify the managed computers that are marked as **Access Denied**, right-click each one, select **Reassociate**, and then provide the administrative credentials.

6. If you're restoring a VMM management server that was also a library server, then the new computer lists the original VMM server as the default library server. From the **Library** view, remove the original library server, and then add the new computer as a library server.

You might also need to re-associate servers in the perimeter network (also known as DMZ, demilitarized zone, and screened subnet), as described in the next section.

Reassociate servers in a perimeter network

After you restore a VMM server, servers on a perimeter network might initially appear as **Not Responding**. In that case, perform the following steps:

1. Sign in to each server on the perimeter network, and then locate the VMM account. The VMM account is a local administrator account with a 10-character username of **scvmm** plus 5 random characters.

2. Change the password of the VMM account on each server.

3. On the VMM management server, in the **Host Properties** dialog, select **Options**, and then assign each server the same password that you created in step 2.

Restore VMM library servers

To restore a library server after data loss, restore the file server shares, and then restore the data back onto the shares.

After you restore the VMM management server and the VMM database, library servers are listed in the VMM console. As needed, re-associate these listings with the physical library servers.

1. If the newly restored computer has the same name as the original computer, install the Virtual Machine Manager agent locally on that computer, and then re-associate that computer with the VMM management server.
2. If the newly restored computer has a different name than the original computer, use the VMM console to remove the original computer from the list of managed computers, and then add the new computer.

Restore registry keys, Active Directory objects, and non-VMM managed credentials

Use the following guidelines to restore registry keys, Active Directory objects, and non-VMM managed credentials:

- **Registry keys**: To restore registry keys that were previously backed up, you can use the Regedit **Import** function or any other tool that is used in your environment to back up and restore registry keys. However, don't restore the SQL subkey if the database name, location, and other details that it contains don't match what you want for the VMM database at the time you're restoring the registry keys.

- **Active Directory objects**: If distributed key management (DKM) is enabled in your VMM environment, VMM stores some data in Active Directory, such as RAA passwords, product key information, and Virtual Machine Role data. After reinstalling VMM, if needed, you can re-enter some of the data that was stored in Active Directory, such as RAA passwords and product key information. After you reinstall VMM and (if necessary) restore Active Directory, the data in Active Directory continues to be accessible to VMM.

- **Non-VMM managed credentials**: In Control Panel, select **All Control Panel Items**, and then select **Credential Manager**. Select **Restore Credentials** to restore any VMM-related credentials that were previously backed up.

Post-restore tasks

Depending on your VMM configuration, you might need to do some of the following tasks after you restore your VMM environment:

Configure Always On Availability Groups

If the VMM database was configured by using SQL Server Always On Availability Groups, you must complete a few tasks to ensure that the database is correctly configured with an availability group.

Install additional VMM consoles

If you had to replace any servers on which VMM consoles were installed, reinstall the consoles on those servers.

Update virtual machine templates

All the virtual machine templates that were restored must correctly specify the virtual hard disk that contains the operating system.

1. In the VMM console, open the **Library** workspace, expand **Templates**, and then select **VM Templates**.

2. In the **Templates** pane, right-click the virtual machine template that you want to update, select **Properties** > **Hardware Configuration** to update the settings.

Restore Microsoft Azure Hyper-V Recovery Manager

If Microsoft Azure Hyper-V Recovery Manager is implemented in the VMM environment, then you must perform a few steps to restore the Microsoft Azure Hyper-V Recovery Manager Provider.

Review add-ins, driver packages, and certificates

After you restore VMM, review the following items to ensure that you've taken the necessary steps for your add-ins, driver packages, and certificates:

- **Non-Microsoft user interface add-ins**: To restore any non-Microsoft user interface add-ins or any other non-Microsoft party applications, consult the respective application's restore guidelines.

- **Driver packages**: Driver packages that were previously added to the VMM library might not be discovered correctly after a restore. They might have to be removed and re-added.

- **Certificates**: Any VMM-related certificates on hosts must be updated with the information of the new VMM management server.

> ⓘ **Note**
>
> After you reinstall VMM, VMM updates the account control lists (ACLs) that became outdated due to the failure. No further intervention is required.

Feedback

Set up the library in the VMM compute fabric

Article • 08/02/2024

Read this article to understand the System Center Virtual Machine Manager (VMM) library and how to interact with it.

The VMM library is a file share that includes a catalog of resources that are used to deploy virtual machines and services in the VMM fabric. The library stores:

- **File-based resources** such as virtual hard disks, ISO images, and scripts, driver files, and application packages (SQL Server data-tier applications and Web Deploy).
- **Non-file-based resources** such as virtual machine templates and service templates that are used to create VMs and services.
- **Offline virtual machines** are stored in the library.

When you install VMM by default, a single library share is created on the VMM management server. You can add additional shares. For high availability, you can deploy a failover cluster of file servers. Scale out file server (SOFS) isn't supported. You interact with libraries and library resources using the **Library** view in the VMM console.

What can I do in the library?

Expand table

Resource type	What can I add?
File-based resources	Virtual hard disks (.vhd/.vhdx/.vmdk), ISO image files (.iso) PowerShell scripts (.ps1), SQL Server scripts (.sql), Web Deploy (MSDeploy) packages (.zip), SQL Server data-tier apps - DACS (.dacpac), driver files (.inf), answer files (.inf, xml), virtual floppy disks (.vfd/.flp)
Templates and profiles	Templates help you to quickly create VMs and services with consistent settings. You create and add profiles with specific settings to templates. **VM templates** are used to create a single VM. A template can be created from an existing virtual hard disk, another VM template in the library, or from a VM deployed on a host. **Service templates** are used to create multiple VMs and can include settings for Windows Server roles and features. In addition to using hardware and guest OS profiles, service templates can use application and SQL Server profiles.

Resource type	What can I add?
	Hardware profiles define hardware settings such as CPU, memory, and priority of VM for resource allocation on host. **Guest OS profiles** define operating system settings that will be applied when a VM is created from a template. **Application profiles** provide instructions required to install an app. VMM supports these mechanisms for app deployment - data-tier apps (DAC) and WebDeploy (MSDeploy), running a script created for Windows installer (.msi), setup.exe, Windows PowerShell Desired State Configuration (DSC), Puppet, and Chef. **SQL Server profiles** provide instructions for customizing a SQL Server instance for a SQL Server DAC.
Equivalent objects	Equivalent objects are user-defined groupings of library resources that are considered equivalent. After you've marked objects as equivalent, when you point to a specific virtual disk on a library share in a template or profile, VMM can substitute any equivalent object when a VM or service is created. This means you can author templates and profiles without relying on specific physical resources, and resources can be serviced without affecting the availability of templates and profiles. VMM supports virtual disks, .iso images, and custom resources as equivalent objects.
Cloud libraries	Read-only library shares that are assigned to a private cloud and a stored node where self-service users with appropriate permissions can store VMs and services. You can add resources to cloud libraries to make them available for private cloud users.
Self-service user content	Self-service users can upload their own resources that can be used when they author templates. Users can share resources with other self-service users.
Stored VMs and services	Users can store their VMs that aren't in use in the stored node of the cloud library.
Update catalog and baselines	If you manage updates through VMM, then WSUS update baselines are stored in the library.
Custom resources	Add custom resources so that resources that would otherwise not be indexed show up in the library. To do this, create a folder with a .CR extension and save it to a library share. Folder contents are available to all users who can access the share. Examples of custom resources include pre- and post-execution scripts and custom installation packages.
Manage replicated	You can manage library servers, which are replicated. You can use any replication technologies, such as DFSR, to manage the replicated shares through VMM.

Resource type	What can I add?
library shares	

Learn more about managing replicated library shares.

Next steps

Learn about adding file-based resources to the library.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Add file-based resources to the VMM library

Article • 08/02/2024

After you've set up the System Center Virtual Machine Manager (VMM) library, use this article if you want to add file-based resources to the library and mark objects in the library as equivalent.

You can add file-based resources to the library as follows:

- Copy files to the share in the VMM console
- Import and export file-based resources between library shares
- Copy files to the library share from outside the VMM console

> ⓘ **Note**
>
> Sysprep the virtual hard disk and then add it to the VMM library Learn more.

Copy files to the share in the VMM console

1. Go to **Library** > **Library Servers**.
2. Right-click a library share > **Explore**.
3. Copy files to the share.

Import and export files between libraries

1. Select **Library** > **Import Physical Resource**.
2. Select whether to import a resource or custom resources, select the destination library server, share, and optionally a folder. Select **OK** > **Import**. Verify the import in **Library Servers** > target location > **Physical Library Objects**.
3. To export, select **Export Physical Resource**.
4. Right-click a library share > **Explore**. Select the resources you want to export (select and hold the SHIFT key for multiple), and select **OK**. Select a destination folder and select **OK** > **Export**.
5. Copy files to the share.

Mark objects as equivalent

You can group library resources together, so they're considered equivalent. Then when you create templates and profiles and point to a specific virtual disk on a library share, VMM can substitute any equivalent object when a VM or service is created. This means you can author templates and profiles without relying on specific physical resources, and resources can be serviced without affecting the template and profile availability.

VMM supports virtual disks, .iso images, and custom resources as equivalent objects. Equivalent resources must be the same file type.

You'll need to be an admin, delegated admin, or self-service user to mark objects as equivalent. Delegated admins can mark on library shares within their scope. Self-service users can mark objects in their user role data path.

1. Select **Library** > **Library servers**.
2. For admins and delegated admins, the **Library Server** column indicates the location of each resource. Self-service users must expand **Self Service User Content** > **Type** to sort library resources.
3. Right-click the resources > **Mark Equivalent**.
4. In **Equivalent Library Objects**, enter the family name and release value to create a new equivalent set, or select a family name to add to an existing set. Objects must have the same family name, release value, and namespace (automatically assigned by VMM) to be equivalent.

Next steps

Learn about adding profiles to the VMM library.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Add profiles to the VMM library

Article • 08/02/2024

Use this article to learn about System Center Virtual Machine Manager (VMM) profiles and how to add them to the VMM library.

A VMM profile contains settings that are used when you create a new virtual machine or virtual machine template. Profiles make deployment easier by helping you to quickly create VMs with consistent settings. Profiles can be used to restrict the settings that are available to self-service users who create new VMs.

⛶ Expand table

Profile	Details	Used for VM templates	Used for service templates
Hardware profile	Defines hardware configuration settings, such as CPU, memory, network adapters, a video adapter, a DVD drive, and the VM priority when resources are allocated on a VM host.	Yes	No
Guest operating system profile	Defines operating system configuration settings that are applied to a VM, including the type of operating system, the computer name, administrator password, domain name, product key, time zone, answer file, and RunOnce file.	Yes	No
Application profile	Provides instructions for installing an application. VMM supports multiple mechanisms for application deployment. Two of these mechanisms are for specific application packaging technologies: data-tier applications (DAC) and WebDeploy (MSDeploy). A third mechanism enables you to install any application by running a script. You can use scripts that are created for Windows Installer (MSI), Setup.exe installation programs, Windows PowerShell Desired State Configuration (DSC), Puppet software, and Chef software.	No	Yes
SQL Server profile	Provides instructions for customizing an instance of Microsoft SQL Server for a SQL Server DAC when a virtual machine is deployed as part of a service.	No	Yes
Capability profile	Defines limits and capabilities for a specific set of resources; for example, settings for network adapters, processor ranges, and memory. Capability profiles are	Yes	Yes

Profile	Details	Used for VM templates	Used for service templates
	used for hardware profiles or in cloud deployment. For example, you could configure a private cloud and assign it a Hyper-V capability profile that requires all resources to the highly available. In this example, you need to set up library resources, such as hardware profiles, to align with the capability. To learn more, review this article .		
Physical computer profile	Defines settings used to provision servers.	No	No

Create a hardware profile

1. In the VMM console, select > **Library** > **Create** > **Hardware Profiles**.
2. In **New Hardware Profile** > **General**, enter a profile name. You can create a hardware profile with the default settings but you probably want to tailor them. In **Hardware Profile**, you can specify the hardware settings.
3. In **Compatibility**, you can specify that a capability profile must be assigned to the hardware profile. Remember, capability profiles help limit available options when you're creating a new VM.
4. In **General**, you can define how many virtual processors to assign to the VM. You can specify memory, startup, and dynamic memory range. Startup specifies the memory that is assigned to the VM during startup. After startup, this memory can be reclaimed back from the VM in accordance with the minimum memory settings.
5. In **Bus Configuration**, you add and remove hardware that supports storage device.
6. In **Network Adapters**, you specify the number of network adapters in the VM, whether they'll have a static IP address or an address allocated from a pool, the MAC address, and port profile. The port profile can be used to control how bandwidth is used on the adapters.
7. In **Advanced**, you can specify high availability and performance settings. In **Availability**, specify whether the VM must be highly available in deployed in a cluster. In **BIOS**, select the order of virtual device and when **Num Lock** is enabled for password entry. In **CPU Priority**, specify relative priority of CPU usage for the VM. If you set to High, the VM has more access to resources than those set to Low. In **Virtual NUMA**, specify when the VM can use virtual NUMA. In **Memory Weight**, specify the relative memory priority for the VM.
8. After you've finished creating the hardware profile, you can right-click it to configure additional properties. In **Dependencies**, you see any dependencies for

the profile. For example, if a library-based file is required, you will see it here. In **Access**, you can see the roles or users who have permissions to use this profile. In **Validation Errors**, you can check for errors.

9. After you've created the hardware profile, you can use it when you configure a virtual machine template or create a virtual machine. You can select a complete hardware profile, or select it and then tweak settings for the individual VM or template.

Create a guest OS profile

1. In the VMM console, select > **Library** > **Create** > **Guest OS Profiles**.
2. In **New Guest OS Profile** > **General**, enter a profile name. In **Guest OS Profile**, specify the OS settings.
3. In **General Settings** > **Operating System**, specify the VM operating system. In **Identity Information**, specify the actual machine name of the VM. You probably want a unique name so that you can specify a wildcard to generate a new name for each VM. You can also use characters ### to set an increasing numeric value. For example, if you enter ContosoVM-##, it generates machines named ContosoVM-01, ContosoVM-02, and so on. In **Admin Password**, specify local admin permissions require a password. You can use the predefined Run As account. In **Product Key**, enter the key for the OS installation. If you add an answer file under **Scripts**, you can select the **Product key provided by answer file** settings. In **Time Zone**, specify the time location for the VM.
4. In **Roles and Features**, specify what needs to be installed on the VM.

> ⓘ **Note**
>
> This setting is only used for the profile used in a VM template, which is then used in a service template.

5. In **Networking**, specify domain settings for the VM and credentials to use for joining the domain.
6. In **Scripts**, specify any scripts you want to use for the VM. Scripts must be located on the library share. For example, an installation answer file. The **GUIRunOnce** option allows you to run a script the first time a user signs in to the VM.
7. After you've created the guest OS profile, you can right-click it to configure additional properties. In **Dependencies**, you can see any dependencies for the profile. For example, Run As accounts. In **Access**, you see the roles or users who have permissions to use this profile.

8. After you've created the hardware profile, you can use it when you configure a virtual machine template or create a VM.

Create an application profile

1. In the VMM console, select > **Library** > **Create** > **Application Profiles**.
2. In **New Application Profile** > **General**, enter a profile name. In **Application Configuration**, you can specify the app settings.
3. In **Application Configuration** > **OS Compatibility**, specify the guest operating systems that are compatible with the application profile.
4. Select **Add** and select the type of application or script that you want to apply to the profile. To deploy any app type, select **General**. To deploy SQL Server DAC packages or script, select **SQL Server Application Host** so that you can add packages and scripts to the profile. To deploy Web applications, select **Web Application Host** so that you can add Web Deploy packages and scripts to the profile.
5. If you selected **General**, you can add more than one more of the application or script to the profile.
6. For applications, you can specify settings such as certificate, ports, and folders. You can also specify that the deployment of the app must be managed by a script. You can specify the script name and specify when it must run.
7. Select **Scripts** to add an unlimited number of scripts and properties such as parameters and security settings. For example, you can configure a script to create a guest cluster out of multiple VMs deployed by the VMM. For example, you can specify that one script must run at Creation: First VM (to form the cluster on the first virtual machine) and a different script to run at Creation: VMs After First (to add additional virtual machines to the cluster).
8. After you're done, verify that the profile was created in **Library** > **Profiles** > **Application Profiles**.
9. You use application profiles in service templates. For example, you could create a number of VM templates with hardware and OS profiles. Then you create a service template that includes those VM templates and the application profiles to create a set of VMs that are configured and deployed together as a single entity.

Create a SQL Server profile

1. In the VMM console, select > **Library** > **Create** > **SQL Server Profiles**.
2. In **New SQL Server Profile** > **General**, enter a profile name. In **SQL Server Configuration**, you can specify the app settings.

3. In **Application Configuration** > **Add** > **SQL Server Deployment**. A SQL Server deployment corresponds to a single instance of SQL Server. If you want multiple instances of SQL Server on the same VM, you need to create multiple deployments.
4. In **SQL Server Deployment**, select **Deployment 1** and specify the deployment name and the SQL Server instance details. The RunAs account is optional; the VMM service account is used if you don't specify it.
5. In **Configuration**, enter the path to the SQL Server installation file (setup.exe) and the SQL Server admins.
6. In **Service Account**, specify which accounts to use.

Create a capability profile

The exact settings for a capability profile depend on the profile in use. As an example, let's configure the Hyper-V capability profile to specify high availability for resources used in a private VMM cloud.

1. In the VMM console, select > **Library** > **Create** > **Capability Profiles**.
2. In **Create Capability Profile** > **General**, enter a profile name. In **Capabilities**, specify the profile settings.
3. In **Capabilities** > **Fabric Compatibility**, select **Hyper-V virtualization host**. You could also elect to set up a custom capability profile.
4. Set up the hardware configuration settings for the profile. The settings are similar to those used in a hardware profile. However, in capability profiles, these settings represent limits rather than exact values.
5. In **Advanced** > **Availability**, select **Highly available VM mode** > **Use default** > **Required**.
6. Complete the wizard. After you've created the profile, you can select and enable it in **VMs and Services** > cloud name > **Properties** > **Capability Profiles**.
7. Remember that all the other profiles and templates used for VMs in the cloud need to match the capability profile requirements and the high availability setting.

Create a physical computer profile

VMM can be used to provision physical computers into Hyper-V hosts or into a scale-out file server (SOFS). When you're provisioning physical computers, you can use a physical computer profile to specify settings for the machine. Create a physical computer profile as follows:

1. In the VMM console, select > **Library** > **Create** > **Physical Computer Profile**.

2. In **New Physical Computer Profile** > **Profile Definition**, enter a profile name and description.

3. In **OS Image**, select a virtual hard disk from the library share. It must be running Windows Server 2016 or later. To create the hard disk, you can create a VM, install the guest operating system, and then use Sysprep with **/generalize** and **/oobe**. If the disk is dynamic, VMM converts it to a fixed disk during deployment. We recommend that you use a fixed disk type to help protect user data and increase performance.

4. In **Hardware Configuration**, set up network adapters, disks and partitions, and any drivers.
5. In **Network Adapters**, select **Connectivity Properties** to set up consistent device naming (CDN) for the adapter. Specify whether to allocate an IP address with DHCP or from a static pool. If it's a physical network adapter connected to a logical switch, this option isn't available.
6. In **Disk**, specify the partitioning scheme for the first disk. Select Master Boot Record (MBR) for BIO. or GUID Partition Table (GPT) for EFI. Specify a volume label, what free disk space to use, and what to designate as the boot partition. VMM copies the .vhd or .vhdx file to the boot partition and automatically creates a system partition on the same disk.
7. In Driver filter, specify the driver files to be applied to the operating system during deployment. You can filter drives with plug and play IDs or with specific tags. With the tag option, you need to add driver files to the library and assign the corresponding tags to the library share before deployment.
8. In **OS Configuration**, set up the domain, the password for the local admin, name, and organization, product team, time zone, and an answer file for additional setup options. In GUIRunOnce, you can specify commands or scripts that must run the first time a user signs into the machine.
9. Verify the settings in **Summary** and select **Finish**. You can check the physical computer profile in **Library** > **Profiles** > **Physical Computer Profiles**.

Next steps

Learn about creating VM templates and service templates in the VMM library and adding profiles to them.

Feedback

Add VM templates to the VMM library

Article • 08/02/2024

Read this article to learn about VM templates and how to manage them in the System Center Virtual Machine Manager (VMM) library.

Templates help you to create VMs with consistent settings. VMM provides two types of templates:

- VM templates are database objects that are stored in the VMM library. They're used to quickly set up VMs.
- Service templates define how a service is configured. They include information about the VMs that are deployed as part of the service, which applications to install on VMs, and the network settings that must be used. Service templates usually contain VM templates.

There are two methods for creating a VM template:

- From an existing virtual hard disk or VM template in the VMM library.

  > ⓘ **Note**
  >
  > Ensure the virtual hard disk was Sysprepped.

- From an existing VM deployed on a host.

Before you start

- You can base a new VM template on an existing VM template or on a virtual hard disk that is stored in the library. You can configure hardware settings, guest operating system settings, application installation, and Microsoft SQL Server instances. You can configure each of these settings manually or you can import the settings from an existing profile.
- Static IP address settings are available only when you deploy a VM from a VM template.
- If you create a VM template based on Linux, some of the Linux-specific settings, such as operating system specialization, work only if you deploy the Linux-based VM on a Hyper-V host.
- The option to create a VM template that's based on an existing VM on a host isn't applicable for Linux-based virtual machine templates.

- Application deployment, SQL Server deployment, and configurable service settings only apply when you deploy a VM as part of a service.
- If you grant rights for a particular template to a user that doesn't have rights to the Run As account that's specified in the template, then the user can potentially extract the credentials for the Run As account from the template during deployment.
- Before creating a template based on a VM, you'll need to create a new local administrator account on that VM. Using the default built-in administrator account will cause Sysprep to fail. In addition, ensure that the VM isn't joined to a domain.

Create a VM template based on an existing VHD or VM template in the library

1. Select **Library** > **Create** > **Create VM Template**.
2. In the Create VM Template Wizard, select **Source** > **Use an existing VM template or virtual hard disk stored in the library**. Select the disk or template in **Select VM Template Source**.
3. In **Identity**, enter a template name and description.
4. In **Configure Hardware**, specify the hardware settings. You can select to use an existing hardware profile.

> ⓘ Note
>
> The profile and hardware options will depend on which VM you're configuring - Generation 1 or Generation 2 VMs. To learn more, review how to create a hardware profile.

5. In **Configure Operating System**, specify the machine settings. You can use a guest OS profile or configure specific settings. To learn more, review how to create a guest OS profile.
6. In **Configure Applications**, set up app settings. This isn't relevant if you're using the VM template to deploy VMs that aren't part of a service. To learn more, review how to create an application profile. If you're configuring a SQL Server setup in **Configure SQL Server**, review how to create a SQL Server profile.
7. In **Summary**, review the settings and select **View Script** if you want to see the script that will be used to create the template. Then select **Create**. In **Jobs**, you can track the template being created. Wait for the **Completed** status.
8. When you create a VM, you'll be able to create it based on the template you've created.

Create a VM template based on a VM deployed on a host

1. Select **Library** > **Create** > **Create VM Template**.
2. In the Create VM Template Wizard > select **Source** > **From an existing virtual machine that is deployed on a host**. Select the VM in **Select VM Template Source**.
3. In **Identity**, enter a template name and description.

> ⓘ **Note**
>
> The template will destroy the source VM, and data on it could be lost. Clone it if it's important to you.

4. In **Configure Hardware**, select **Next**.

5. In **Configure Operating System**, specify the guest operating system settings. You can use a guest OS profile or configure specific settings. To learn more, review how to create a guest OS profile.

6. In **Select Library Server**, select the library server for the VM you're using for the template and in **Select Path**, specify the share/folder.

7. In **Summary**, review the settings and select **Create**. In **Jobs**, you can track the template being created. Wait for the **Completed** status.

You can create VMs based on the template you've created.

Assign a storage QoS policy template

1. After step 3 in the previous procedure, in **Configure Hardware**, select **Advanced** under **Bus configuration**, and select appropriate option under **Storage QoS Policy**.

2. Proceed with the rest of the steps to complete the wizard.

Next steps

Learn how to create VMs based on the template you've created.

Feedback

Add service templates to the VMM library

Article • 08/02/2024

Read this article to learn about setting up service templates in the System Center Virtual Machine Manager (VMM) library.

Service templates group VMs together to provide an app. They contain information about a service, including the VMs that are deployed as part of the service, the applications installed on VMs, and the network settings that must be used. You can add VM templates, network settings, applications, and storage to a service template.

Service templates can be single or multi-tier:

- A single tier service contains one VM used as a specific app.
- A multi-tier service contains multiple VMs. For example, you could create a three-tier service with a backend tier running a SQL Server database, a middle tier running the business server, and a third tier running a frontend web interface.
- Tiers can be added based on a copy of an existing VM template (which can be customized) or a virtual hard disk in the library.

You set up service templates using the VMM service template designer.

Before you start

You can create service templates if you have VMM admin or delegated admin permissions, or if you have a self-service user account with **Author** enabled.

Create a service template

1. Select **Library** > **Create** > **Create Service Template**.
2. In **New Service Template** > **Name**, specify a template name. In **Release**, indicate the template version.
3. To configure a tier using the predefined templates, select the designer workload and select a preconfigured tier pattern (blank, 1, 2, or 3 tiers). Select **Save and Validate** to save the template. After it's created, you can select a template object to modify its name, release version, or users/roles that can access it.
4. When the tier appears in the workspace, drag a VM template to it. The properties of the VM template are applied to the tier.

> ⓘ Note
>
> This doesn't establish a link between the tier and the template. Changing the template properties does not modify the tier properties.

> ⓘ Note
>
> You can also select **Add Machine Tier** to add a tier manually. This opens the **Create Machine Tier Template** wizard. In **Select Source**, select a source for the tier. You can use an exact copy of an existing VM template or to customize an existing VM template. Select **Browse** to select the template or hard disk. In **Additional Properties**, you'll configure the tier properties described in the next step.

5. You can select a tier to access its properties in the details pane of the designer. Select **View All Properties** to modify all the properties in a single view. Here's what you can modify when you select to view all:

   - In **General**, specify:
     - The order in which tiers are deployed and serviced. For example, if you need the database tier to be running in order to run a frontend web app, you'd set the database tier to 1.
     - Whether you want to be able to add additional VMs to the tier in order to scale out (you can scale out to five VM instances in a tier).
     - More than one upgrade domain to minimize service interruptions when a tier is updated. VMM will update VMs in the tier according to their upgrade domains. VMM upgrades an upgrade domain at a time. It shuts down VMs in the domain, updates them, brings them online, and moves to the next domain to reduce impact.
     - The creation of an availability set for the tier. The availability set helps VMs in the service remain available during maintenance. VMM tries to separate VMs in the same availability set by placing them on separate hosts.
   - In **Configure Hardware**, you'll see the hardware settings for the associated VM template. You can select an alternative hardware profile or configure hardware settings manually. To learn more, review how to create a hardware profile.
   - In **Configure Operating System**, you'll see the operating system settings for the associated VM template. You can select an alternative guest OS profile or configure settings manually. To learn more, review how to create a guest OS profile.

- In **Application Configuration** or **SQL Server Configuration**, you can select an application/SQL Server profile or configure settings for a new profile. Learn more about application and SQL Server profiles.

Add a VM network to the service template

You'll need to configure network settings for a tier by connecting the tier adapters to one or more VM networks. To do this, you'll add a logical network component and then use the connector tool to connect it to the adapter.

1. In the Service Template Designer, select **Service Template Components** > **Add VM Network**.
2. When the network appears as a component, use the Connector to connect to the appropriate NIC.

Next steps

Set up load balancing for a service tier.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage the VMM library

Article • 08/02/2024

Read this article to learn how to manage the System Center Virtual Machine Manager (VMM) library by refreshing it, moving files around, and removing orphaned resources.

Refresh the library

By default, VMM refreshes library shares once every hour.

- You can change the default refresh settings in **General** > **Library Settings** > **Settings** > **Modify** to 336 hours (14 days). You can also disable automatic library refreshes.
- To manually refresh, select **Library** > library server or share > **Refresh share**.

During a library refresh, the following occurs:

- VMM adds these file types to the **Library** view: virtual hard disks (except for those attached to a stored VM), virtual floppy disks, ISO images, answer files, and PowerShell scripts. Snapshots imported into the library with Hyper-V and VMware VMs are displayed on the **Checkpoints** tab of the VM properties. The snapshot files aren't displayed.
- VMM indexes but doesn't display these file types:
  - Files associated with stored VMs (VM configuration file, attached virtual hard disks, saved state files, imported snapshots, checkpoints).
  - Files associated with VM templates.
  - Configuration files:
    - Hyper-V (.exp -export, .vsv -savedstate, .bin)
    - Virtual Server (.vmd, .vsv)
    - VMware (.vmtx, .vmx)

Transfer files

You've direct access to copy and move library files through Windows Explorer. Each file in a library share has a unique GUID and is periodically indexed during library refreshes. After a file is refreshed, you can move it to any other location on a library share managed by VMM and refresh automatically tracks the file movement. After the move, file metadata is updated during the next library refresh.

In addition, you can allow unencrypted file transfers to and from a library server.

- To transfer unencrypted file transfers, the feature must be allowed on both the source and destination servers.
- To enable the option, select **Library** > **Library Server** and navigate to the server. Select **Actions** > **Library Server** > **Properties** and select **Allow unencrypted file transfers**.

Disable and remove file-based resources

You can remove a file-based resource either temporarily or permanently from the library.

- To disable resources, select **Library** > **Library servers** > and select the library share. Select the resource and select **Actions** > **Disable**. Select **Enable** to re-enable.
- To remove files, we recommend you use VMM rather than simply deleting the file resources. When you remove the file in the library, any resources that use the file are updated automatically. To remove a file, select **Library** > **Library servers** > and select the library share. Select the resource and select **Actions** > **Remove**. Select **Yes** to confirm.

Remove a library server or share

There are circumstances in which you need to remove a library server or share. For example, if you're no longer using the resources on a share or you temporarily want to remove those resources.

- To remove a library share, select **Library** > **Library servers** > and select the library share. In Actions, select **Library Share** > **Remove**. Select **Yes** to confirm.

> ⓘ **Note**
>
> Removing a share doesn't delete the files on it. They're no longer indexed by library refreshes.

- To remove a library server, select **Library** > **Library servers**. Select **Actions** > **Library Server** > **Remove**.

Ensure that you specify an account with administrative permissions on the server.

- VMM provides a list of dependent resources. If you proceed with removing the chosen Library Server, VMM removes any references to the removed files on the dependent resources. When you remove a library server, the **Library Server** role is removed from the VMM agent running on the server. If the server isn't performing any other VMM roles, the agent is removed.

- If you remove a highly available library server, the cluster is removed from the **Library** view. The individual cluster nodes aren't removed, but they're not displayed in the library. To remove the nodes from VMM, remove the VMM agent from each computer.

Remove orphaned resources

When you remove a library share from VMM management and there are templates that reference resources that were located on the library share, a representation of the library resource appears in the VMM library as an orphaned resource.

To remove orphaned resources, modify the templates that reference the orphaned resources to use valid library resources in the VMM library. If you add the library share again, VMM doesn't automatically reassociate the template with the physical library resource. You must complete these steps to correct the template issues and to remove any orphaned resources.

1. Select **Library** > **Orphaned Resources**.
2. You won't be able to delete an orphaned resource until the templates that reference it are updated to valid references. To view the templates, right-click the orphaned resource > **Properties**. To update the template, select it and then in the **Properties** dialog, locate the resource that's missing > **Remove**.
3. Add a new resource that's valid.
4. When you have completed these steps for all the templates, close the **Properties** dialog. To verify there aren't any dependencies, right-click the orphaned resource > **Properties** > **Dependencies**. Then right-click the orphaned resource > **Delete**.

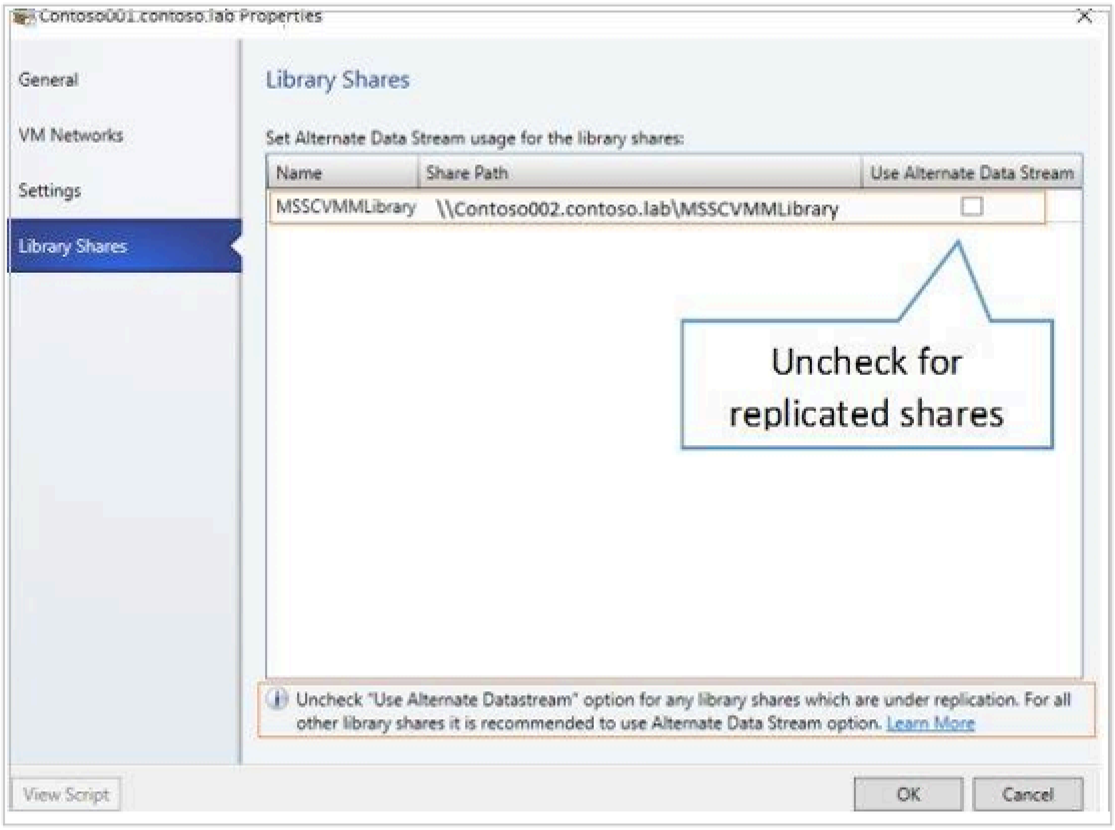
Manage replicated library shares

VMM supports the management of library servers, which are replicated. You can use any replication technologies, such as DFSR, to replicate shares and manage the shares through VMM.

For effective management of replicated shares using VMM, disable the usage of *alternate data stream* for both the source and destination library shares. You can do this while adding new library shares or by editing properties of the existing library shares. *Alternate data stream* is enabled by default. Disable this option only when using replication across library shares.

VMM generates a GUID for all the library objects managed by VMM. This metadata is written into *Alternate Data Stream* of the file. VMM uses *Alternate Data Stream* to identify library objects as the same objects, while they're moved across folders in library shares or in scenarios where a library object is renamed. Disabled *Alternate Data stream* impacts the identification of object as the same object in the scenarios mentioned above.

However, for effective management of replicated library shares using VMM, it's required to disable the *Alternate Data Stream* option.



Library Shares

Set Alternate Data Stream usage for the library shares:

Name	Share Path	Use Alternate Data Stream
MSSCVMMLibrary	\\Contoso002.contoso.lab\MSSCVMMLibrary	☐

Uncheck for replicated shares

Uncheck "Use Alternate Datastream" option for any library shares which are under replication. For all other library shares it is recommended to use Alternate Data Stream option. Learn More

Rename/move library files in replicated library shares

If you've opted to disable writing to *Alternate Data Stream*, some scenarios like rename/move to different library share might be effective. To ensure these scenarios work fine, use the following steps:

1. Ensure the file that you want to rename/move is replicated across all the library shares.
2. Refresh all the replicated library shares.
3. Rename/move the library file in the parent library share.

ⓘ Note

Storing VMs and VMWare VM templates isn't supported on library shares with *UseAlternateDataStream* set to false.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Set up host groups in the VMM compute fabric

Article • 08/09/2024

Read this article to learn about setting up and managing host groups in the System Center Virtual Machine Manager (VMM) fabric.

A VMM host group is a logical entity that groups fabric resources together. You can group virtual machine hosts or clusters or create nested host groups. After you've created host groups, you can assign and configure resources at the host group level. Those resources are then applied to all hosts and clusters in the group.

You can create host groups based on different criteria. For example, based on physical location, hardware capabilities, or specific workloads. You can assign permissions for host groups to the VMM admin, delegated administrators, and read-only admin user roles. Members of these user roles can view and manage the fabric resources that are assigned to them at the host group levels. When you create private clouds in VMM, you select which host groups will be included in the cloud, and then allocate resources in the host groups to the cloud.

Create host groups

1. Select **Fabric** > **Servers** > **All Hosts** > **Create Host Group**.
2. Enter a group name. To create a host group at a specific location in the tree, right-click the desired parent node, and then select **Create Host Group**.

After you've created a host group, you can modify the following properties for the group.

Expand table

Tab	Property
General	Configure the host group name, the location in the host group hierarchy, the description, and whether to allow unencrypted BITS file transfers.
Placement Rules	VMM automatically identifies the most suitable host to which you can deploy virtual machines. However, you can specify custom placement rules. By default, a host group uses the placement settings from the parent host group.
Host Reserves	Host reserve settings specify the amount of resources that VMM sets aside for the host operating system to use. For a virtual machine to be placed on a host,

Tab	Property
	the host must be able to meet the virtual machine’s resource requirements without using host reserves. You can set host reserves for individual host groups and for individual hosts. The host reserve settings for the root host group, All Hosts, sets the default host reserves for all hosts. You can configure reserve values for the following resources: CPU Memory Disk I/O Disk space Network I/O
Dynamic Optimization	Configure dynamic optimization and power optimization settings. Dynamic optimization balances the virtual machine's load within a host cluster. Power optimization enables VMM to evacuate hosts of a balanced cluster and turn them off to save power.
Network	View inheritance settings, and configure whether to inherit network logical resources from parent host groups. The network logical resources include the following: IP address pools Load balancers Logical networks MAC address pools
Storage	View and allocate storage to a host group.
Custom Properties	Manage custom properties for the following object types: Virtual machine Virtual machine template Host Host cluster Host group Service template

Tab	Property
	Service instance Computer tier Cloud

Next steps

After you've created host groups, you can deploy Hyper-V hosts in the VMM fabric.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Add Windows servers as Hyper-V hosts or clusters in the VMM compute fabric

Article • 08/09/2024

This article describes adding an existing Windows Server as a Hyper-V host server or cluster to the System Center Virtual Machine Manager (VMM) fabric and configuring the host and cluster properties.

The article is relevant for adding Windows Server computers with or without the Hyper-V role. If you add a Windows Server that doesn't have Hyper-V installed, VMM will install the Hyper-V role as long as the server meets the prerequisites.

Before you start

The prerequisites for adding an existing Hyper-V host server or cluster depend on whether Hyper-V is installed and where the server is located.

Expand table

Host location	Prerequisite
Server without Hyper-V	If you want to add a server that doesn't have Hyper-V installed, it must meet the prerequisites for Hyper-V installation. The server must be running supported version of Windows Server. If you want to add the VMM management server as a managed Hyper-V host, the Hyper-V role must be installed on the server before you add it. You can't add a highly available VMM server as a managed Hyper-V host cluster. If you want to add a Hyper-V cluster, the instructions in this article presume that the cluster already exists. Read this article if you want to create a cluster from the existing Hyper-V hosts in the VMM fabric. This article assumes that the server you want to add already has an operating system running on it. If you want to add a bare-metal computer as a Hyper-V host or cluster, read this article.
Same domain as VMM server, or two-way trusted domain	You must specify account credentials for an account that has administrative rights on the computers that you want to add. You can enter a username and password or specify a Run As account. If you use Group Policy to configure Windows Remote Management (WinRM) settings, note these settings:

Host location	Prerequisite
	WinRM Service settings must be configured through Group Policy and can only apply to hosts that are in a trusted Active Directory domain. Specifically, VMM supports the configuration of the Allow automatic configuration of listeners, Turn On Compatibility HTTP Listener, and Turn on Compatibility HTTPS Listener Group Policy settings. VMM doesn't support other WinRM Service policy settings. If you enable the **Allow automatic configuration of listeners** policy setting, you must configure it to allow messages from any IP address. In other words, in the policy setting, the IPv4 filter and IPv6 filter (depending on whether you use IPv6) must be set to *****. WinRM Client settings can't be configured through Group Policy. These policy settings might override client properties that VMM requires for the VMM agent to work correctly. If you enable any unsupported WinRM Group Policy settings, installation of the VMM agent can fail.
Untrusted domain	VMM doesn't support configuring Windows Remote Management (WinRM) Group Policy settings (Service or Client) on hosts that are in an untrusted Active Directory domain. If WinRM Group Policy settings are enabled, installation of the VMM agent—required on the hosts might fail. In an untrusted domain, when VMM installs the agent on the servers or clusters, it also generates a certificate. The certificate is used to help secure communications with the host. When VMM adds the host or cluster, the certificate is automatically imported into the VMM management server trusted certificate store.
Disjoined namespace (DNS suffix doesn't match the domain of which it's a member)	The System Center Virtual Machine Manager service must be running as the local system account or as a domain account that has permission to register a Service Principal Name (SPN) in Active Directory. When you try to add a computer that is in a disjointed namespace, VMM checks Active Directory to see if an SPN exists. If it doesn't, VMM tries to create one. If the permissions are OK, VMM adds the missing SPN automatically. Otherwise, host addition fails and you'll need to add the SPN manually. To do this, enter: **setspn -A HOST/**. For example, setspn –A HOST/hypervhost03.contosocorp.com hypervhost03. If the host cluster is in a disjointed namespace and the VMM management server is not, add the DNS suffix for the host cluster to the TCP/IP connection settings on the VMM management server. If you use Group Policy to configure Windows Remote Management (WinRM) settings, review the following requirements:

Host location	Prerequisite
	WinRM Service settings must be configured through Group Policy and can only apply to hosts that are in a trusted Active Directory domain. Specifically, VMM supports the configuration of the Allow automatic configuration of listeners, Turn On Compatibility HTTP Listener, and Turn on Compatibility HTTPS Listener Group Policy settings. VMM doesn't support other WinRM Service policy settings. If you enable the Allow automatic configuration of listeners policy setting, you must configure it to allow messages from any IP address. In other words, in the policy setting, the IPv4 filter and IPv6 filter (depending on whether you use IPv6) must be set to *. WinRM Client settings can't be configured through Group Policy. These policy settings might override client properties that VMM requires for the VMM agent to work correctly. If you enable any unsupported WinRM Group Policy settings, installation of the VMM agent can fail.
Perimeter network or workgroup	You'll need to install the VMM agent locally on the target host. To do this run VMM setup as an administrator and select **Optional Installations** > **Local Agent**. In **Security File Folder** select **This host in on a perimeter network** and enter an encryption key. In **Host network name** specify how the VMM server will contact the host server and note the computer name or IP address. Finish the wizard. Check that a file SecurityFile.txt is located on the VMM server. By default, it's located in C:\Program Files\Microsoft System Center version\Virtual Machine Manager.

ⓘ Note

- After the VMM agent installation on the host, the local computer account gets automatically added to the local Administrators group. This is not a mandatory requirement for VMM agent; If needed, you can manually remove the local computer account from the Administrators group on the host.
- Adding a cluster under a perimeter network isn't supported.

Add servers

1. In the VMM console, open **Fabric** > **Servers**.

2. Select **Add group** > **Add Resources** > **Hyper-V hosts and Clusters**.

3. In the **Add Resource Wizard** > **Resource location**, select where the server you want to add is located.

   - If you're adding a host in a perimeter network, select **Windows Server computer in a perimeter network**.

4. In **Credentials**, specify credentials for a domain account that has administrative permissions on all hosts that you want to add. (For computers in an untrusted domain, you must use a Run As account.)

   > ⓘ **Note**
   >
   > The above provided credentials or Run As account must be a local administrator on the host machines. If a Run As account is provided, then it will be used while adding the host as well as for providing future access to the host during its lifetime. If the credentials are entered manually, then they'll only be used while adding the host. Once the host has been successfully added, the VMM service account will be added as local administrator on the host and used to provide any future access to it. The VMM service account needs admin privileges on the host machines to create the shielded VM.

5. In **Discovery scope** specify:

   - **Same domain or domains with two-way trust**:
     - If you select **Specify Windows Server** computers by names, in **Computer names** enter names or IP addresses, one per line. If you're adding a Hyper-V host cluster, specify the name or IP address of the cluster or of any cluster node.
     - If you select **Specify an Active Directory** query to search for Windows Server computers, you can enter or generate a query.
     - **Untrusted domain**: Discovery page doesn't appear.
     - **Disjointed namespace**: Enter the host FQDN and select **Skip AD verification**.

6. In **Target resources**, specify the computers you want to add. Repeat for all hosts. If discovery succeeds, the host will be listed under **Computer name**. Add as follows:

   - **Trusted domain or disjointed namespace**: Select the checkbox next to each computer that you want to add, and select **Next**. If you specified a cluster name or cluster node in the previous step, select the checkbox next to the

  cluster name. (The cluster name is listed together with the associated cluster nodes).
  - **Untrusted domain**: Enter the FQDN or IP address of the server or cluster that you want to add, and select **Add**. For a cluster, you can enter an FQDN or IP address of the cluster or of one of the cluster nodes.
  - **Perimeter network/workgroup**: Enter the NETBIOS name or IP address of the host in the perimeter network. Enter the encryption key you created when you installed the agent on the host, and in the Security file path, enter the path to the SecurityFile.txt file.

7. In the **Host settings** > **Host group** list, select the host group to which you want to assign the host or host cluster. If the host is already associated with a different VMM management server, select **Reassociate this host with this VMM environment**. If the host was associated with a different VMM management server, it will stop working on that server.

   - For a standalone host, in **Add the following path**, enter a path on the host for storing files for virtual machines that are deployed on the host, and select **Add**. Repeat to add more than one path. If the path doesn't exist, it's created automatically. If you leave the box empty, the default is %SystemDrive%\ProgramData\Microsoft\Windows\Hyper-V. As a best practice, don't add default paths that are on the same drive as the operating system files.
   - For a cluster, don't specify default virtual machine paths. VMM automatically manages the paths that are available for virtual machines based on the shared storage that's available to the host cluster

8. On the **Summary** page, confirm the settings, and select **Finish**. The **Jobs** dialog appears to show the job status. Wait for a Completed status. Verify that the host or cluster was added in the host group > host or cluster name. The status must be **OK**.

Configure properties for Hyper-V hosts

After you've added Hyper-V hosts and servers in the VMM fabric, there are a number of properties you can configure for standalone hosts and clusters.

Expand table

Tab	Settings
General	View identity and system information for the host. This includes information such as processor information, total and available memory and storage, the operating system, the type of hypervisor, and the VMM agent version. Enter a host description. Configure whether the host is available for placement. Configure the remote connection port. By default, the port is set to 2179.
Hardware	View or modify settings for CPU, memory, graphics processing units (GPUs), storage (including whether the storage is available for placement), network adapters, DVD/CD-ROM drives and Baseboard Management Controller (BMC) settings.
Status	Lists health status information for the host. Includes areas such as overall health, Hyper-V role health, and VMM agent health. In the **Status** pane, you can also do the following: View error details. Refresh the health status. Select **Repair all**. VMM will try to automatically fix any errors.
Virtual Machine Paths/Virtual Machines	Shows the virtual machines that reside on the host, together with status information. Also enables you to register virtual machines on the host.
Reserves	Enables you to override host reserve settings from the parent host group and configure reserved resources for the host. Configurable resources include CPU, memory, disk space, disk I/O, and network capacity.
Storage	Shows storage allocated to a host and enables you to add and remove storage logical units or file shares.
Virtual Switches	Enables you to configure virtual switches.
Placement Paths/Placement	Enables you to configure the default virtual machine paths and default parent disk paths that will be used during virtual machine placement on the host.
Servicing Windows	Enables you to select servicing windows.
Custom Properties	Enables you to assign and manage custom properties.

Properties for Hyper-V clusters

⛶ Expand table

Tab	Settings
General	View the name, host group, and description. You can also configure the **Cluster reserve (nodes)** setting and view the cluster reserve state. The **Cluster reserve (nodes)** setting specifies the number of node failures a cluster must be able to sustain while still supporting all virtual machines deployed on the host cluster. If the cluster can't withstand the specified number of node failures and still keep all the virtual machines running, the cluster is placed in an overcommitted state. When overcommitted, the clustered hosts receive a zero rating during virtual machine placement. An administrator can override the rating and place a highly available virtual machine on an overcommitted cluster during a manual placement.
Status	View detailed status information for the host cluster: Cluster validation test runs and successes. Includes a link to the latest validation report (if available). Note that accessing the report requires administrative permissions on the cluster node where the report is located. For host clusters, you can perform an on-demand cluster validation through VMM. To do this, in the **Fabric** workspace, locate and select the host cluster. Then, on the **Host Cluster** tab, select **Validate Cluster**. Cluster validation begins immediately. Online elements in the cluster: cluster core resources, disk witness in quorum, and the cluster service on each node.
Available Storage	Shows available storage, that is, storage logical units that are assigned to the host cluster but aren't Cluster Shared Volumes (CSVs). You can also do the following: Add and remove storage logical units that are managed by VMM. Convert available storage to shared storage (CSV).
Shared Volumes	Shows the shared volumes (CSVs) that are allocated to the host cluster. You can also do the following: Add and remove CSVs that are managed by VMM. Convert CSVs to available (non-CSV) storage.
Custom Properties	Custom properties that you manage.

Run a script on a remote host using Run Script command

Article • 09/10/2024

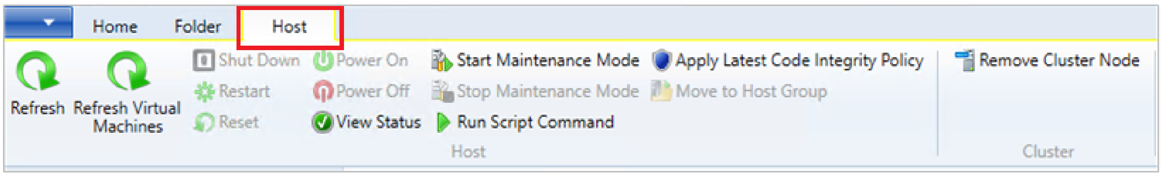
System Center Virtual Machine Manager (VMM) supports the ability to execute commands remotely, on a host using the Run Script command feature. This feature is useful in scenarios where you want to start a service or collect information from a remote host.

You can also run the script on the host using the custom resources that you added to the VMM library. Custom resources can consist of batch files that can execute specific commands against the server, but the use of custom resources isn't required.

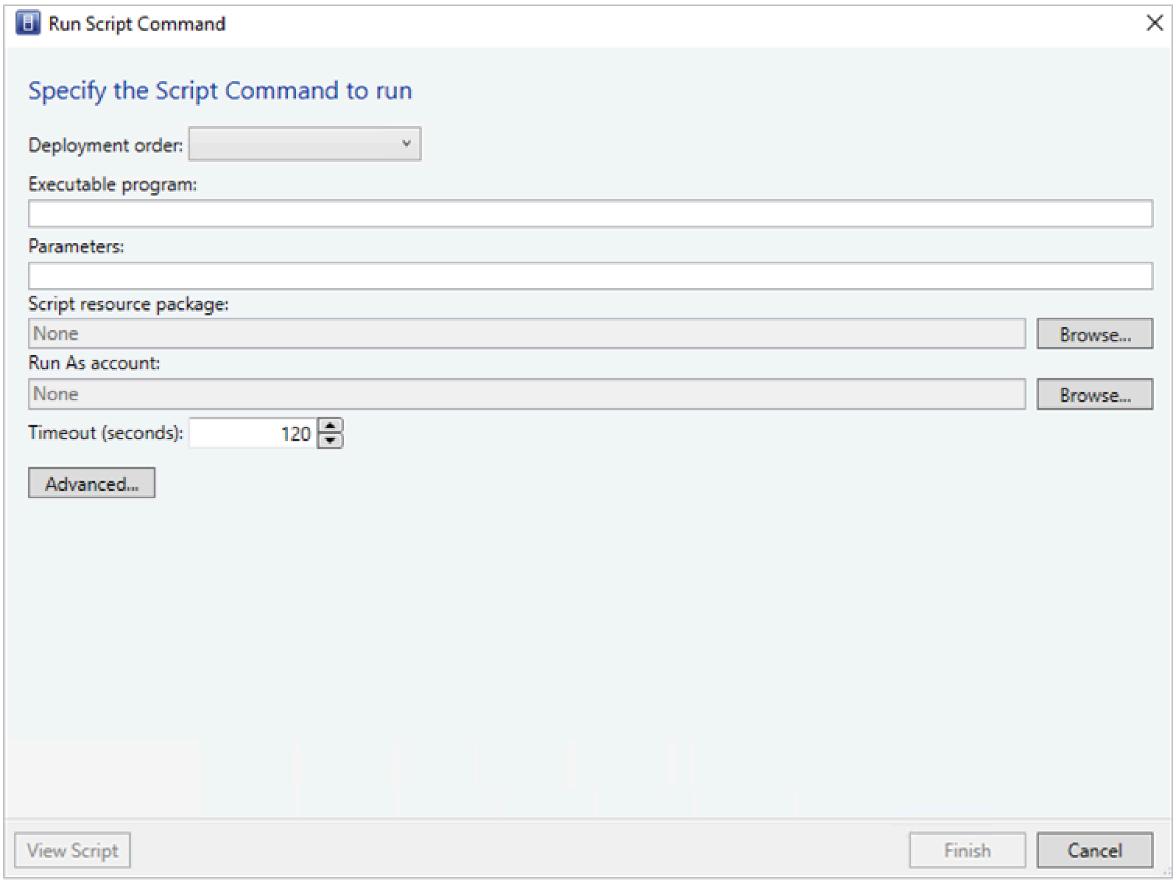
Example scenario 1 - Start a service

The following example scenario provides information on how you can start a service **sftlist** on a VMM host using the Run Script command feature.

1. In the VMM console, on the toolbar, select **Host** and select **Run Script Command**.



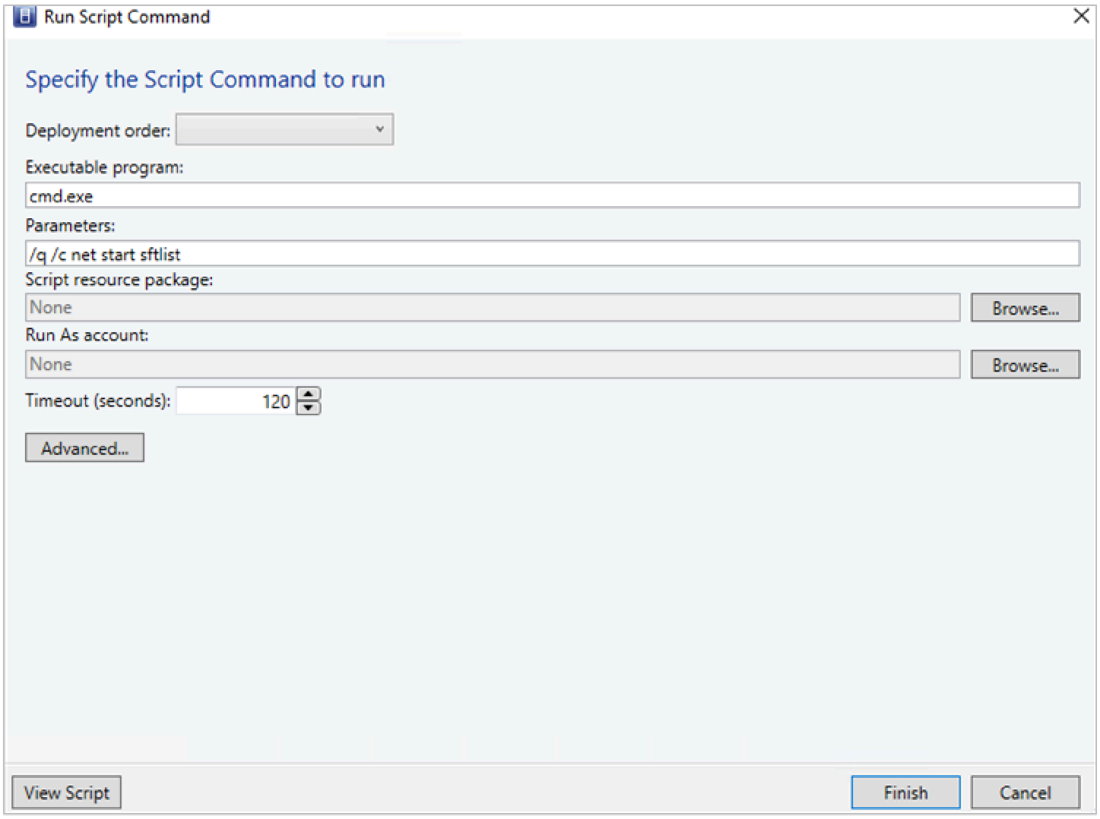
The **Run Script Command** page appears:



2. As an example, enter the following details against the options displayed:

- **Deployment Order**: Select the deployment order from the dropdown menu.
- **Executable program**: cmd.exe
- **Parameters**: /q /c net start sftlist
- **Script resource package** and **Run As account**: None

  The **/q** turns off the echo for the command line and **/c** carries out the command and then terminates. If you don't use these switches, the outcome will be a return code 0 from the cmd.exe process and won't display the actual result of the command in the job.



Specify the Script Command to run

Deployment order:

Executable program: cmd.exe

Parameters: /q /c net start sftlist

Script resource package: None

Run As account: None

Timeout (seconds): 120

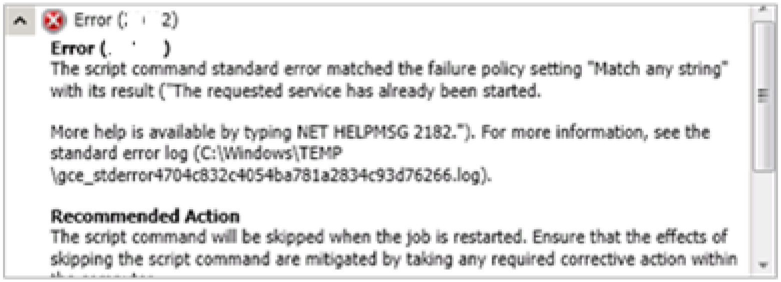
3. Select the **Timeout** seconds for this command.

4. Select **Advanced..** and specify the output file and log file location for any errors.

5. Select **Finish**.

Monitor the job in the VMM console for the result. If there's any error, go through the error file log and follow the recommendations as applicable.

Here is a sample error message

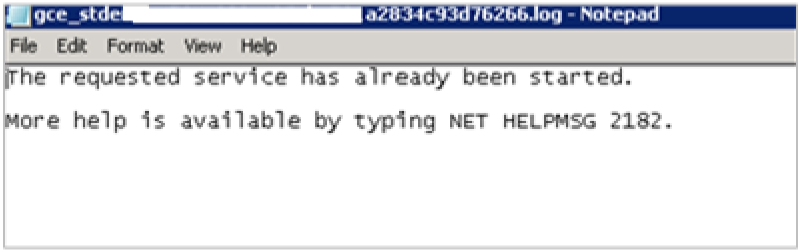


Error (; 2)

Error (.)
The script command standard error matched the failure policy setting "Match any string" with its result ("The requested service has already been started.

More help is available by typing NET HELPMSG 2182."). For more information, see the standard error log (C:\Windows\TEMP \gce_stderror4704c832c4054ba781a2834c93d76266.log).

Recommended Action
The script command will be skipped when the job is restarted. Ensure that the effects of skipping the script command are mitigated by taking any required corrective action within


gce_stde a2834c93d76266.log - Notepad
File Edit Format View Help

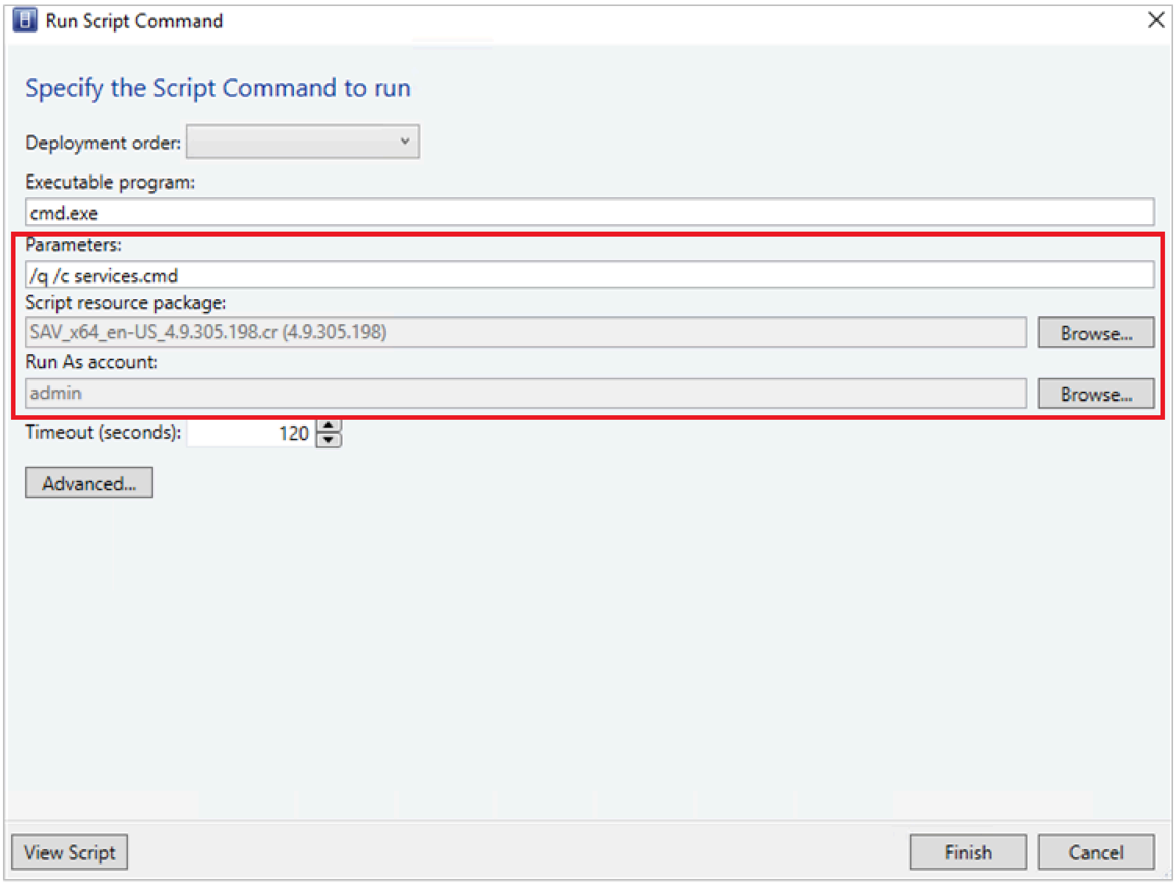
```
The requested service has already been started.

More help is available by typing NET HELPMSG 2182.
```

Example scenario 2 - Start a service using custom resources

In this example, at step 2, we use the following values; rest of the steps remain the same.

- **Deployment Order**: Select the deployment order from the dropdown menu.
- **Executable program**: cmd.exe
- **Parameters**: /q /c services.cmd
- **Script resource package**: SAV_x64_en-US-4.9.305.198.cr(4.9.305.198)
- **Run As account**: Admin

  For this example, we included a batch file named **services.cmd** under a custom resource folder named **SAV_x64_en-US-4.9.305.198.cr(4.9.305.198)**, and specified the **Run As account** as Admin.



Run Script Command

Specify the Script Command to run

Deployment order:

Executable program: cmd.exe

Parameters: /q /c services.cmd

Script resource package: SAV_x64_en-US_4.9.305.198.cr (4.9.305.198)

Run As account: admin

Timeout (seconds): 120

The batch file performs a net stop sftlist/y and then a net start sftlist. In this scenario, the custom resource folder is transferred to the agent host and copied under windows\temp. A folder with the format, **scvmm.xxxxxxxx**, is created to contain all the files. From here, it executes the batch file, and the agent returns the corresponding outcome to VMM and displays it in the job. If the script generates an error, it creates a log under the specified location.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Provision a cluster from Hyper-V standalone hosts in the VMM fabric

Article • 09/10/2024

Use the instructions in this article to create a cluster from standalone Hyper-V host servers that are managed in the System Center Virtual Machine Manager (VMM) fabric.

Before you start

⛶ Expand table

Prerequisite	Details
VMM	You'll need a VMM host group set up in the fabric. This is needed to allocate shared storage logical units if VMM needs to assign shared storage to the cluster nodes.
Hyper-V	You must have two or more standalone Hyper-V hosts in the VMM fabric that are in the same VMM host group. The hosts must meet the requirements for failover clustering. All the hosts that will be in the cluster must be running the same operating system. All hosts must belong to the same VMM host group. You must have a domain account (to use as the basis for a Run As account) for creating the cluster. The account must have administrative permissions on the servers that will become cluster nodes and must belong to the same domain as those servers. Also, the account requires **Create Computer objects** permission in the container that is used for Computer accounts in the domain.
Storage	Storage must be discovered and classified in the Fabric workspace of the VMM console. Then, either storage pools or logical units or both must be allocated to the host group or the parent host group chosen for your set of hosts. If the shared storage isn't managed by VMM, disks must be available to all nodes in the cluster before you can add them. You'll need to provision one or more logical units to all hosts that you want to cluster, and mount and format the storage disks on one of the hosts. To access shared storage, the Multipath I/O (MPIO) feature must be installed on each Hyper-V host. VMM doesn't add this automatically. You can add MPIO using the server manager. If MPIO is installed, VMM will automatically enable it for supported storage arrays using the Microsoft provided Device Specific Module

Prerequisite	Details
	(DSM). If you already installed vendor-specific DSMs for supported storage arrays and then add the host VMM, the vendor-specific MPIO settings will be used to communicate with those arrays. If you add a host to VMM management before you add the MPIO feature, you must add the MPIO feature, and then manually configure MPIO to add the discovered device hardware IDs. Or you can install vendor-specific DSMs. If you're using iSCSI SAN as your shared storage, the Microsoft iSCSI initiator service must be installed and running (set to automatic) on each Hyper-V host. VMM uses the iSCSI initiator service to configure shared storage on the Hyper-V nodes automatically when the cluster is created. There's no need to discover iSCSI portals on each Hyper-V node if VMM manages the shared storage. If you're using a Fibre Channel storage array network (SAN), each host must have a host bus adapter (HBA) installed, and zoning must be correctly configured. For more information, see your storage array vendor’s documentation. By default, when VMM manages the assignment of logical units, VMM creates one storage group per host, either a standalone host or a host cluster node. However, for some storage arrays, it's preferable to use one storage group for the entire cluster, where host initiators for all cluster nodes are contained in a single storage group. To support this, you must set the CreateStorageGroupsPerCluster property to $true using the Set-SCStorageArray cmdlet.
Networking	For all Hyper-V hosts that you want to cluster, if the hosts are configured to use static IP addresses on a particular network, ensure that the static IP addresses on all hosts are in the same subnet. If you've already created a network configuration in VMM that is relevant to the cluster and have applied that configuration to network adapters in the hosts, ensure that the configuration is applied consistently across all the hosts you want to cluster. For example, if you've designated a specific set of network adapters (one per host) as management adapters for the cluster, ensure that the name of the logical network and VM network associated with those network adapters is consistent. When VMM is identifying networks that the cluster can use, it will only recognize networks with consistent settings on every node.

Create a cluster

1. In the VMM console, select **Fabric** > **Create** > **Hyper-V Cluster** to open the Create Hyper-V Cluster wizard.
2. In **General**, specify a cluster name and choose the host group in which the existing Hyper-V hosts are located.
3. In **Resource Type**, select the Run As account that you'll use to create the cluster. The account 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 **Existing Windows servers** is selected, and if you don't need support from Microsoft for this cluster, you can select **Skip cluster validation**.

4. In **Nodes**, select the Hyper-V host servers that you want to include in the cluster. You can select multiple hosts using the CTRL key or a range using SHIFT.
5. In **IP address** (if it appears), enter the IP address you want to use for the cluster.
6. In **Storage**, select the data disks you want the cluster to use. The list of available disks includes the logical units associated with the host group that you selected at the beginning of the wizard.

    - If you assigned storage out-of-band, disks that aren't managed by VMM are displayed and selected as available disks, with the checkbox next to each disk dimmed and unavailable.
        - If you're using a non-Microsoft clustered file system (CFS) solution, ensure that you're aware which disks are CFS disks. Don't select those disks for the cluster. If you do, cluster creation will fail.
        - If the number of selected hosts for the cluster is even, the smallest disk that is larger than 500 megabytes (MB) is automatically chosen as the witness disk and is unavailable for selection.

7. In **Virtual Switches**, you can select the logical networks to use when VMM automatically creates virtual switches on the Hyper-V nodes. The external virtual switches on destination Hyper-V nodes. VMM will automatically create the virtual switches on all the Hyper-V nodes.
8. In **Summary**, confirm the settings and then select **Finish**. You can monitor the cluster status on the **Jobs** page. After the job finishes, you can verify cluster information by right-clicking **Properties** > **Status** tab on the cluster. You can also right-click the cluster and select **Validate Cluster**.

Here's what VMM does after you create the cluster:

1. Validates that all hosts meet the prerequisites, such as required operating system and domain membership
2. Enables the Failover Clustering feature on each host
3. Unmasks the selected storage logical units to each host
4. Runs the cluster validation process
5. Creates the cluster with quorum settings, configures any cluster static IP settings that you specified, and enables Cluster Shared Volumes (CSVs)
6. Assign the logical unit as a CSV on the cluster for each logical unit that is designated as a CSV.

Next steps

Provision VMs

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Provision a Hyper-V host or cluster from bare metal computers

Article • 08/09/2024

Use this article to provision a Hyper-V host or cluster from bare metal computers with nothing installed on them, in the System Center Virtual Machine Manager (VMM) fabric.

In addition to adding existing Windows Servers to the fabric as Hyper-V hosts and clusters, VMM can discover physical bare metal machines, automatically install an operating system, and provision them as Hyper-V server hosts and clusters.

Here's how you do this:

1. **Verify prerequisites**: Ensure you've all the prerequisites before you start.
2. **Initial configuration**: Set up the BIOS on the machine to support virtualization, set the BIOS boot order to boot from a Pre-Boot Execution Environment (PXE)-enabled network adapter as the first device, and configure the sign-in credentials and IP address settings for the BMC on each computer. You need to create DNS entries and Active Directory account for the machine names, and we recommend you allow time for DNS replication to occur.
3. **Prepare the PXE server environment**: Add the PXE server to VMM management (as described in Prerequisites: creating hosts, host clusters, Scale-Out File Server clusters from bare metal in VMM, and How to add a PXE server to VMM.)
4. **Add resources to VMM library**: Add resources that include a generalized virtual hard disk with an appropriate operating system (as listed in Prerequisites: creating hosts, host clusters, or Scale-Out File Server clusters from bare metal in VMM) to use as the base image and optional driver files to add to the operating system during installation.
5. **Create profiles**: In the library, create one or more physical computer profiles. These profiles include configuration settings, such as the location of the operating system image and hardware and operating system configuration settings.
6. **Create Hyper-V host or cluster**: You run different wizards depending on whether you want to set up a standalone host or cluster.

Before you start

ⓘ **Note**

VMM doesn't support bare metal provisioning of physical Machines in disjoint namespace. As a workaround, follow these steps:

1. Provision the bare metal in a non-disjoint namespace domain.
2. Remove the provisioned host from VMM.
3. Join the host to the disjoint namespace domain of interest.
4. Add the host back to VMM. Use this procedure.

Ensure the following prerequisites:

Expand table

Component	Prerequisite	Details
Physical computer	Support for discovery	Each physical computer must have a baseboard management controller (BMC) installed that enables out-of-band management. Through a BMC, you can access the computer remotely, independent of the operating system and control system functions, such as the ability to turn the computer off or on. BMC requirements: The BMCs must use one of the supported out-of-band management protocols, and the management protocol must be enabled in the BMC settings. The supported protocols are: Intelligent Platform Management Interface (IPMI) versions 1.5 or 2.0; Data Center Management Interface (DCMI) version 1.0; System Management Architecture for Server Hardware (SMASH) version 1.0 over WS-Management (WS-Man); custom protocols such as Integrated Lights-Out (iLO) The BMCs must use the latest version of firmware for the BMC model. The BMCs must be configured with sign-in credentials and must use either static IP addressing or DHCP. If you use DHCP, we recommend that you configure DHCP to assign a constant IP address to each BMC, for example, using DHCP reservations. The VMM management server must be able to access the network segment on which the BMCs are configured.
Physical computer	Hyper-V role requirements	Computer that supports the Hyper-V role must use x64-based processors and have the appropriate basic input/output system (BIOS) settings enabled.

Component	Prerequisite	Details
Physical computers	DNS	If your environment has multiple Domain Name System (DNS) servers, where DNS replication can take some time, we strongly recommend that you create DNS entries for the computer names that are assigned to the physical computers, and allow time for DNS replication to occur. Otherwise, deployment of the computers can fail.
Physical computer	BIOS/EFI	Determine whether the computers use Extensible Firmware Interface (EFI) or BIOS. If you've computers of each type, you must create a separate profile for each type.
Physical computers	Operating system	You can add a Windows Server 2016 node to a Windows Server 2012 R2 cluster, subject to the requirements specified previously; however, you can't add a Windows Server 2012 R2 node to a Windows Server 2016 cluster. **Note:** VMM 2019 UR3 and later supports Azure Stack Hyper Converged Infrastructure (HCI, version 20H2).
PXE server	Deployment requirements	You must have a PXE server configured with Windows Deployment Services. If you've an existing PXE server in your environment configured with Windows Deployment Services, you can add that server to VMM. Then you can use it for provisioning in VMM (and VMM recognizes only the resulting servers). All other requests continue to be handled by the PXE server according to how it's configured. If you don't have an existing PXE server, you can deploy the Windows Deployment Services role on a server running a supported operating system (Windows Server 2012 R2 or later). When you install Windows Deployment Services, you must install both the Deployment server and Transport server options. You don't need to add images. During host deployment, VMM uses a virtual hard disk that you've created and stored in the library. In addition, you don't need to configure settings on the PXE response tab. VMM provides its own PXE provider. The PXE server must be in the same subnet as the physical computers that you want to provision. When you add a PXE server, you must specify account credentials for an account that has local administrator permissions on the PXE server. You can enter a username

Component	Prerequisite	Details
		and password or specify a Run As account. If you want to use a Run As account, you can create the RunAs account before you begin, or during deployment.
PXE server	Boot order	On each computer, set the BIOS boot order to boot from a Pre-Boot Execution Environment (PXE)-enabled network adapter as the first device.
Virtual hard disk	Operating system	Ensure that you've a generalized virtual hard disk in a VMM library share. It must be running Windows Server 2012 R2 or later. We recommend that for production servers, you use a fixed disk (.vhd or .vhdx file format) to increase performance and to help protect user data. By default, when you create a physical computer profile, VMM converts a dynamic disk to a fixed disk. If you plan to assign customer drivers, they must exist in the library. To create the virtual hard disk, you can create a virtual machine, install the guest operating system, and then use sysprep with the /generalize and the /oobe options. The operating system on the virtual hard disk that you deploy on hosts or clusters must support the boot from virtual hard disk (VHD) option. If you use Remote Desktop Services (RDS) to manage servers, we recommend that you enable the RDS connections in the image. You can also enable RDS by using an answer file in the physical computer profile.
Networking	Logical networks	If you've already configured logical networks or logical switches in VMM, you can include those configurations in a physical computer profile. To include a logical switch that you want to apply to physical NICs in a physical computer profile (for hosts or host clusters), you must first take certain steps. Ensure that you've installed the intended number of NICs on the host computer or computers. In addition, before you create the physical computer profile in VMM, create the logical switch. To include static IP addressing controlled through a logical network in a physical computer profile, configure the logical network. The logical network must include at least

Component	Prerequisite	Details
		one network site and static IP address pool. The network site must also be available to the host group or to a parent host group where you want to assign the hosts that you're creating from bare metal. To include a virtual NIC for hosts in a physical computer profile (for hosts or host clusters), you must first take certain steps. Ensure that you've installed the intended number of physical NICs on the computer or computers that are to become hosts. In addition, on the VMM management server, install all necessary virtual switch extensions and extension providers, create at least one VM network, and create a logical switch. In the logical switch, as a best practice, include one or more port classifications for the virtual ports.
Physical computer profile	Answer file	If you want a physical computer profile to include references to an answer file (Unattend.xml file) or to custom resources (for example, an application installer that is referenced in post-deployment script commands), create the answer file or obtain the custom resources before deployment, and add them to a VMM library share. Within a library share, place custom resources in one or more folders with a .CR (custom resource) extension. VMM recognizes them as custom resources. For example, you might want to create an answer file to enable Remote Desktop Services and place it on a library share. Then you can select that file when you configure a physical computer profile. By default, when you deploy servers or clusters from bare metal, VMM automatically performs the following (no answer file or post-deployment commands needed): Installs the Hyper-V role for Hyper-V hosts. Installs the Hyper-V role, failover cluster feature, and multipath I/O (MPIO) for Hyper-V clusters.
Accounts	You need two Run As accounts. A Run As account for joining computers to the domain. You can create a Run As account in the Settings workspace.	

Component	Prerequisite	Details
	A Run As account for access to the baseboard management controller (BMC) on each computer.	

Add a PXE server to the VMM fabric

1. Select **Fabric** > **Servers** > **Add** > **Add Resources** > **PXE Server**.
2. In Computer name, specify the PXE server name.
3. Add the credentials for an account that has local administrator permissions on the PXE server. You can specify an existing Run As account (or select **Create Run As Account** to create a new one); manually enter user credentials in the format domain_name\user_name. Select **Add**.
4. In **Jobs**, verify that the job status is Completed and close the dialog. The job sets up the new PXE server, installs the VMM agent on the PXE server, imports a new Windows Preinstallation Environment (Windows PE) image, and adds the machine account for the PXE server to VMM.
5. Verify that the PXE server is added in **Fabric** > **Servers** > **PXE Servers** > **Home** > **Show** > **Fabric Resources** > **PXE Servers**. The agent status must be **Responding**.

Add and assign driver files

If you plan to assign custom drivers, the driver files must exist in the library. You can tag the drivers in the library so that you can later filter them by tag. After the files are added, when you configure a physical computer profile, you can specify the driver files. VMM installs the specified drivers when it installs the operating system on a physical computer.

In the physical computer profile, you can select to filter the drivers by tags, or you can select to filter drivers with matching Plug and Play (PnP) IDs on the physical computer. If you select to filter the drivers by tags, VMM determines the drivers to apply by matching the tags that you assign to the drivers in the library to the tags that you assign in the profile. If you select to filter drivers with matching PnP IDs, you don't need to assign custom tags.

1. Locate a driver package that you want to add to the library.
2. In the library share that is located on the library server that is associated with the group where you want to deploy the physical computers, create a folder to store

the drivers, and then copy the driver package to the folder.

3. We strongly recommend that you create a separate folder for each driver package, and that you don't mix resources in the driver folders. If you include other library resources, such as .iso images, .vhd files, or scripts with an .inf file name extension in the same folder, the VMM library server is unable to discover the resources. Also, when you delete an .inf driver package from the library, VMM deletes the entire folder where the driver .inf file resides.
4. In the VMM console, open the Library workspace. In the **Library** > **Library Servers**, expand the library server where the share is located, right-click the share, and then select **Refresh**. After the library refreshes, the folder that you created to store the drivers appears.
5. Now assign tags if required. In **Library**, expand the folder that you created to store the drivers in the previous procedure, and then select the folder that contains the driver package.
6. In the **Physical Library Objects**, right-click the driver .inf file, and then select **Properties**.
7. In the **Driver File Name Properties** > **Custom tags**, enter custom tags separated by a semicolon, or select **Select** to assign available tags or to create and assign new ones. If you select **Select** and then select **New Tag**, you can change the name of the tag after you select **OK**. For example, if you added a network adapter driver file, you could create a tag that is named ServerModel NetworkAdapterModel, where ServerModel is the server model and NetworkAdapterModel is the network adapter model.

Create a physical computer profile

1. Select **Library** > **Home** > **Create** > **Physical Computer Profile**.
2. In the **New Physical Computer Profiles Wizard** > **Profile Description**, enter a name and description and select **VM host**.
3. In **OS Image** > **Virtual hard disk file** > **Browse**, select the generalized virtual hard disk that you added to the library share. By default, if the disk is dynamic VMM converts it to a fixed disk during host deployment. We recommend that for production servers, you use a fixed disk to increase performance and help protect user data.
4. In **Hardware Configuration** > **Management NIC**, select the network adapter used to communicate with VMM and whether to use DHCP or a static address. If you want to use Consistent Device Naming (CDN) for the adapter or configure logical switches and ports, select **Physical Properties**. Select **Add** to add the adapter.
5. In **Disk**, specify the partitioning scheme for the first disk. You can use GPT if the physical computer profile is EFI. In **Partition Information**, select the volume label,

whether to use all remaining free space or a specific size, and whether to designate the partition as the boot partition. You can also add a new disk or partition. During deployment, VMM copies the virtual hard disk file to the boot partition and automatically creates a system partition on the same disk.

6. In **Driver filter**, filter the driver filters to be applied to the operating system during host deployment. You can filter by Plug and Play ID or by specific tags. If you select to filter drivers with matching tags, ensure that you've added driver files to the library and assigned the corresponding tags.
7. In **OS Configuration**, specify the domain that the Hyper-V host or cluster must join, and specify local admin credentials and identity information. Add the product key for installation and set the time zone. In GUIRunOnce, specify one or more commands to run when the user signs in to the Hyper-V host for the first time.
8. In **Host Settings**, specify the path of the host to store the files that are associated with virtual machines placed on the host. Don't specify drive C because it's not available for placement. If you don't specify a path, VMM placement determines the most suitable location.
9. In **Summary**, verify the settings. Wait until **Jobs** shows a status of completed, and then verify the profile in **Library** > **Profiles** > **Physical Computer Profiles**.

PCP post deployment settings

After you successfully create and deploy the PCP, you can configure additional settings such as RDMA, QoS, and SET using the PCP post deployment script.

Sample script

Here's the sample script to configure RDMA, SET, and QoS.

PowerShell

```
# Install data center bridging
Install-WindowsFeature Data-Center-Bridging

#Enable RDMA, assuming customer chosen switch name for storage as
Storage1Switch and Storage2Switch
Enable-NetAdapterRDMA "Storage1Switch"
Enable-NetAdapterRDMA "Storage2Switch"

# set Qos Policy
New-NetQosPolicy "SMB" -NetDirectPortMatchCondition 445 -
PriorityValue8021Action 3

# Enable net qos flow control
Enable-NetQosFlowControl  -Priority 3
```

```
# Disable net qos flow control other than 3
Disable-NetQosFlowControl  -Priority 0,1,2,4,5,6,7

# Enable net adapter qos on all adapters
Enable-NetAdapterQos  -InterfaceAlias "*"

# set qos traffic class
New-NetQosTrafficClass "SMB"  -Priority 3  -BandwidthPercentage 50  -
Algorithm ETS

# Install windows feature
Install-WindowsFeature –Name Hyper-V

Install-WindowsFeature –Name RSAT-Hyper-V-Tools

# set net adapter property "encapsulated overhead"
NetAdapterAdvancedProperty -Name "*" -DisplayName "Encapsulated Overhead" -
DisplayValue "160"

#disable ipv6
netsh int ipv6 isatap set state disabled

#Configure SET team mapping between virtual network adapter to physical
network adapters. (Note: to get names of adapters, use command Get-
NetAdapater. For team mapping use command
$physicalAdapters = Get-NetAdapter -Physical
$virtualStorageAdapter1 = Get-VMNetworkAdapter -ManagementOS | Where-Object
{$_.Name -eq "Storage1Switch"}
$virtualStorageAdapter1 = Get-VMNetworkAdapter -ManagementOS | Where-Object
{$_.Name -eq "Storage2Switch"}

Set-VMNetworkAdapterTeamMapping -ManagementOS -PhysicalNetAdapterName
$physicalAdapters[0].Name -VMNetworkAdapterName $virtualStorageAdapter1.Name
Set-VMNetworkAdapterTeamMapping -ManagementOS -PhysicalNetAdapterName
$physicalAdapters[1].Name -VMNetworkAdapterName $virtualStorageAdapter2.Name

#Set firewall rules.
[System.String[]]$Alias=@("vEthernet (WssdStorage2)", "vEthernet
WssdStorage1)");
$Profile ='Any'
$Name="File and Printer Sharing"
$rules = Get-NetFirewallRule -DisplayGroup $Name

foreach ($rule in $rules)
     {
         $rule | Get-NetFirewallAddressFilter | Set-NetFirewallAddressFilter
-
         LocalAddress Any -RemoteAddress Any
     }

 Set-NetFirewallRule -DisplayGroup $Name -Enabled True -Profile $Profile –
InterfaceAlias $Alias
 $Profile='Any'
 $Name=='FPS-LLMNR-In-UDP'
 Set-NetFirewallRule -Name $Name -Enabled True -Profile $Profile
 [System.String[]]$Alias=@("Storage2Switch", "Storage1Switch",
"ManagementSwitch");
 $Profile ='Any'
 $Name="Windows Remote Management"
 Set-NetFirewallRule -DisplayGroup $Name -Enabled True -Profile $Profile -
InterfaceAlias $Alias

 #Set assurance settings
 reg add HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard /v
EnableVirtualizationBasedSecurity /t REG_DWORD /d 1 /f
 reg add HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard /v
RequirePlatformSecurityFeatures /t REG_DWORD /d 2 /f
 reg add HKLM\SYSTEM\CurrentControlSet\Control\LSA /v LsaCfgFlags /t
REG_DWORD /d 1 /f
 reg add HKLM\SYSTEM\CurrentControlSet\Control\LSA /v DisableRestrictedAdmin
/t REG_DWORD /d 0 /f
```

Provision a Hyper-V host from bare metal

When you deploy a Hyper-V host from bare metal, VMM does the following:

1. Discovers the physical computer through out-of-band management.
2. Deploys an operating system image on the computer through the physical computer profile.
3. Enables the Hyper-V role on the computer.
4. Brings the computer under VMM management as a managed Hyper-V host.

Provision as follows:

1. Select **Fabric** > **Servers** > **Home** > **Add** > **Add Resources** > **Hyper-V Hosts and Clusters**.
2. In the **Add Resource Wizard** > **Resource location**, select **Physical computers to be provisioned as virtual machine hosts**.
3. In **Credentials and Protocol** select the Run As account with permissions to access the BMC. In the **Protocol** list, select the out-of-band management protocol that your BMCs use. If you want to use Data Center Management Interface (DCMI), select **Intelligent Platform Management Interface (IPMI)**. Although DCMI 1.0 isn't listed, it's supported. Ensure the correct port is selected.
4. In **Discovery Scope**, specify the IP address scope that includes the IP addresses of the BMCs. You can enter a single IP address, an IP subnet, or an IP address range.

   - If you're provisioning a single computer, you can either specify a single IP address, or specify an IP address range that both starts and ends with the intended IP address. If you specify a single IP address, when you select **Next**, the computer is restarted.

  - If you specify an IP address range, when you select **Next**, information about the computer is displayed, and you can confirm that you specified the computer that you meant to.

5. If you specified a single IP address on the previous page, skip this step. Otherwise, the **Target Resources** page appears. Review the list of discovered BMCs (identified by IP addresses) and select the ones you want to provision as hosts. If you don't see all the BMCs that you expect, confirm that they are on a network accessible to the VMM server, and as needed, select **Refresh**.
6. In **Provisioning Options**, select a host group for new Hyper-V hosts. Select the physical computer profile you want to apply.
7. In **Deployment Customization**, review the list of computers again, and provide information for each computer that you want to include.

   - If you see a computer that you don't want to include, select the BMC (identified by IP address) and then select **Remove**.
   - To configure computers, select the BMC IP address.
   - Specify a unique computer name, without wildcard characters.
   - Select or clear **Skip Active Directory for this computer name**. The Active Directory check prevents deployment if the computer account already exists. This helps prevent deploying a computer with the same name as an existing computer. If you skip the Active Directory check, and there's an existing computer account in AD DS other than the Run As account that was specified in the physical computer profile, the deployment process fails to join the computer to the domain.

8. For the computer you're configuring, select a network adapter (on the left). You can modify the configuration or fill in more information.
9. You can specify the MAC address of the management NIC (not the BMC) and static IP settings for this network adapter. If you specify an address, select a logical network and an IP subnet if applicable. If the selected IP subnet includes IP address pool, you can check **Obtain an IP address corresponding to the selected subnet**. Otherwise, enter an IP address that's within the logical network or its subnet. If you select an IP subnet, ensure that it corresponds to the physical location where you're deploying the host and to the network that the adapter is connected to. Otherwise, the deployment can fail.
10. Configure the adapter settings for each network adapter.

> ⓘ **Note**
>
> If the number of physical network adapters in a computer doesn't match the number of physical network adapters that are defined in the physical computer

profile, you must specify any information that is missing for the adapters. If you decide not to provision this computer right now (for example, if physical hardware needs to be installed or uninstalled), you can select the computer's BMC IP address from the list and then select **Remove**.

11. Repeat the configuration for each BMC IP address in the list. When you've filled in information for all the computers you want to provision, select **Next**.
12. In **Summary**, confirm the settings, and then select **Finish** to deploy the new Hyper-V hosts and bring them under VMM management. Depending on your settings, the **Jobs** dialog might appear. Ensure that all the steps in the job have a status of **Completed**, and then close the dialog.
13. To confirm that the host was added, select **Fabric** > **Servers** > **All Hosts** > host group, and verify that the new Hyper-V host appears in the group.

Provision a Hyper-V cluster from bare metal

When you deploy a Hyper-V cluster from bare metal, VMM does the following:

1. Discovers the physical computers through out-of-band management.
2. Deploys an operating system image on the computers using the selected physical computer profile.
3. Installs the failover clustering feature, and the Hyper-V role and MPIO feature.
4. Brings the provisioned cluster under VMM management.

Provision as follows:

1. Select **Fabric** > **Servers** > **Add** > **Add Resources** > **Hyper-V Hosts and Clusters**.

2. In **General Configuration**, specify a name for the host cluster. Choose a storage configuration if required:

   - For shared storage, select **Storage connected to the cluster using shared SAS, FC, or iSCSI**.
   - For Storage Spaces Direct, select **Disk subsystem directly connected to individual nodes in the cluster**.

3. In **Resource Type** > select **Physical computers to be provisioned**:

   - Specify the administrator Run As account to use for creating the cluster.
   - Select the physical computer profile (which provides the domain name and administrator Run As account for each node).
   - Next to the **BMC Run As** account box, select **Browse**, and select a Run As account that has permissions to access the BMC.

- In the **Out-of-band management** protocol list, select the protocol that your BMCs use. If you want to use Data Center Management Interface (DCMI), select Intelligent Platform Management Interface (IPMI). Although DCMI 1.0 isn't listed, it's supported. Ensure that the correct port is selected.
- If the **Skip cluster validation** option appears, and you don't need support from Microsoft for this cluster, you can skip validation.

4. In **Discovery Scope**, specify the IP address scope that includes the IP addresses of the BMCs. You can enter a single IP address, an IP subnet, or an IP address range. Deep discovery provides detailed information about a computer (for example, MAC addresses of network adapters) but restarts the computer, and requires additional time. You can allow or skip deep discovery.

5. If you specified a single IP address on the previous page, skip this step. Otherwise, the **Target Resources** page appears. Review the list of discovered BMCs (identified by IP addresses) and select the ones you want to include in the cluster.

6. If you don't see all the BMCs that you expect, confirm that they're on a network accessible to the VMM server, and as needed, select **Refresh**. Allow or skip deep discovery. Deep discovery provides detailed information about a computer (for example, MAC addresses of network adapters) but restarts the computer, and requires additional time. Then select **Next**.

7. In **Deployment Customization**, provide information for each computer that you want to include. If you see a computer that you don't want to include, select the BMC (identified by IP address) and then select **Remove**.

   - To configure computers, select the BMC IP address. Specify a unique computer name, without wildcard characters.
   - Select or clear **Skip Active Directory for this computer name**. The Active Directory check prevents deployment if the computer account already exists.

   > ⓘ **Note**
   >
   > If you skip the check and there's an existing computer account in AD other than the Run As account that was specified in the physical computer profile, the deployment process fails to join the computer to the domain.

   - For the computer you're configuring, select a network adapter. You can modify the configuration or fill in more information.
   - You can specify the MAC address of the management NIC (not the BMC) and static IP settings for this network adapter. If you specify an address, select a

logical network and an IP subnet if applicable. If the selected IP subnet includes IP address pool, you can check **Obtain an IP address corresponding to the selected subnet**. Otherwise, enter an IP address that is within the logical network or its subnet. If you select an IP subnet, ensure that it corresponds to the physical location where you're deploying the host and to the network that the adapter is connected to. Otherwise, deployment can fail.

8. Configure the network adapter settings for each network adapter.

> ⓘ **Note**
>
> If the number of physical network adapters in a computer doesn't match the number of physical network adapters that're defined in the physical computer profile, you must specify any information that's missing for the adapters. If you decide not to provision this computer right now (for example, if physical hardware needs to be installed or uninstalled), you can select the computer's BMC IP address from the list and then select **Remove**.

9. Repeat the configuration for each BMC IP address in the list.
10. When you've filled in the needed information for all the computers you want to provision, select Next.
11. In **Summary**, confirm the settings, and then select **Finish** to deploy the new Hyper-V hosts and bring them under VMM management. Depending on your settings, the Jobs dialog might appear. Ensure that all the steps in the job have a status of Completed, and then close the dialog.
12. To confirm that the host was added, select **Fabric** > **Servers** > **All Hosts** > and locate and select the new host cluster. In the **Hosts** pane, in the **Host Status** column, verify that each node in the cluster is OK.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Create a guest cluster from a VMM service template

Article • 09/10/2024

Use this article if you want to create a guest failover cluster using a System Center Virtual Machine Manager (VMM) service template.

A guest failover cluster consists of multiple VMs that are deployed in a cluster and use shared storage. Services in VMM are used to group together virtual machines to provide an app. Service templates contain information about a service, including the VMs that are deployed as part of the service, the applications to install on VMs, and the network configuration that must be used. You can add VM templates, network settings, applications, and storage to a service template. Learn more.

You can use service templates to create a guest cluster. That cluster can then be configured to run an app, such as SQL Server.

Before you start

- VMs in a guest cluster can only be deployed to Hyper-V host clusters running Windows Server 2016 or later. Otherwise, deployment will fail.

- You can deploy a guest failover cluster that uses shared .vhdx files on a Hyper-V failover cluster. In this scenario, if Hyper-V uses Cluster Shared Volumes (CSVs) on block-level storage, then the shared .vhdx files are stored on a CSV that's configured as shared storage.
- Alternatively, Hyper-V can use SMB file-based storage deployed by Scale-Out File Server (SOFS) as the location of the shared .vhdx files.
- No other shared storage types are supported for guest clusters. Non-Microsoft SMB storage isn't supported.
- You need many scripts to create the guest cluster, including a script to run on the first VM in the cluster and a script to run on the other VMs so that they can join the cluster. Script settings are specified in the service template application settings.
- To configure shared disks for the cluster, you'll need to use new .vhdx files. Don't reuse from a previous cluster. Ensure that the hard disk files are in the VMM library.
- Identify a single path in SCSI-based storage where all the .vhdx files for the guest cluster will be placed at deployment time. You can use storage classifications to control the placement of .vhdx files, but you'll need at least one location in the classification with the capacity to hold all the .vhdx files. VMM doesn't deploy the .vhdx files to multiple locations.

- You can vary the location of .vhdx files at deployment time, even if you use the same service template to deploy multiple guest clusters. To do this, you'll need to deploy the guest clusters to a host group and not a cloud. Then at deployment, you specify a single path for all the shared .vhdx files for the cluster. This overrides the location specified in the VM template.
- You'll need a virtual hard disk file that contains the operating system (prepared with Sysprep) that you want the VMs in the guest cluster to use. When each node is created, VMM uses a copy of the virtual hard disk file for the system disk of the node.

Specify scripts that run when a guest cluster is created

1. Set up an application profile.
2. In **New Application Profile** > **General** > **Compatibility**, leave the default **General** setting enabled.
3. In **Application Configuration** > **OS Compatibility**, select one or more editions of a server operating system.
4. Add the scripts you need for creating the first node of the cluster and then adding other nodes. Provide the scripts as follows:

   - For a script that will run on the first node of the cluster when it's created (and not on other nodes), **for Script command type**, select **Creation: First VM**.
   - For a script that'll run on later nodes of the cluster when they're created (and not on the first node), for **Script command type**, select **Creation: VMs After First**.
   - For each script, specify the executable name and the parameters through which the script will run and the Run As account.
   - Configure other settings as needed, including how long the script must run before timing out, failure, and restart policies.
   - A script can contain settings to be entered when you're configuring the service for deployment. To format this type of setting, enter the parameter in the **Parameters** field in the following format: @<SettingLabel>@ (for example, enter @ClusterName@). Example: a script FormCluster.exe that runs with Cmd.exe and the /q and /c parameters and requires the cluster name would be Executable Program: **Cmd.exe**, Parameters: **/q /c FormCluster.cmd @ClusterName@**
   - You can also add scripts to delete the cluster in an orderly way. **Script command type** would be **Deletion: VMs Before Last** or **Deletion: Last VM**.

- You can also add a script of type **Pre-Install** that'll run on the first VM and on later VMs that are created as part of the service tier.

5. Select **OK** to save settings and verify that the profile was created in **Profiles** > **Application Profiles**. The profile will appear in the **Profiles** pane.

Create a VM template

Create a VM template that includes settings for a shared .vhdx file. This file must be deployed to shared storage that has SCSI channels available for each cluster node to provide the same access to the file for each node.

1. In the VMM library, verify that you have a virtual hard disk that contains the operating system (created using SysPrep) you want to use for VM in the guest cluster. It mustn't be blank.
2. Create a VM template.
3. In the **Create VM Template Wizard** > **Select Source**, select **Use an existing VM template or virtual hard disk stored in the library** > **Browse**.
4. In **Select VM Template Source**, select the virtual hard disk you want to use.
5. In **Configure Hardware**, specify a hardware profile or hardware settings.
6. To configure the guest cluster to use a shared .vhdx, in **Bus Configuration** select **SCSI adapter 0**, and then next to **New**, select **Disk**. The new disk appears as a listing under the SCSI adapter. Select the disk and select **Share the disk across the service tier**.
7. Clear **Contains the operating system for the virtual machine**. Select **Browse** and select the .vhdx file that you want VMM to deploy to shared storage and select **OK**. Repeat for each additional node in the cluster. Add the same disk each time but ensure that the SCSI channel is unique for each node.
8. In **Network Adapters**, select the adapter and select **Enable guest specified IP addresses**. This enables the nodes (VMs) in the cluster to specify the IP addresses for the cluster itself and for applications that you configure to run in the cluster.
9. In **Advanced** > **Availability**, select **Make this virtual machine highly available**. With this setting, enable the VM is created as a clustered instance on the host cluster so that if one host fails, the VM will fail over to another host in the cluster.
10. Select **Manage availability sets** > **Create**. The availability set you create will be used by all the nodes in the guest cluster. This means that VMM will attempt to keep the VMs on separate hosts so that if one host fails VMs on a different host can provide services.
11. In **Configure Operating System**, open the **Guest OS profile** list and select a guest operating system profile or **Create new Windows operating system customization settings**. Your selection determines whether additional wizard pages are displayed.

- Under **Identity Information** > **Computer name**, you can provide a pattern to generate computer names. For example, if you enter server####, the computer names that are created are server0001, server0002, and so on. The use of a pattern ensures that when you add additional virtual machines to a service, the computer names that are generated are related and identifiable. If you use this method to specify the computer name, you can't use it in combination with a name prompt parameter (@<name>@). You can use one method or the other, but not both.
- Under **Networking**, you can specify Active Directory settings using the FQDN or using at signs (@) before and after the domain name; for example, @Domain@. Using the at signs (@) in this way, the necessary information can be entered when the virtual machine is deployed as part of a service. You don't need a trust relationship between the domain in which the service is deployed and the VMM management server domain.

12. Finish the wizard to create the VM template.

Include the VM template in a service template

1. Create a service template, and add the VM template to the appropriate template tier.
2. After you save and validate the template, right-click the tier object in the service template designer and select **Properties**.
3. In **Application Configuration**, add the application profile you created. When the service is deployed, the scripts in the application profile will run. Save and validate the service template.
4. Right-click the service template again > **Properties**.
5. In **General**, select **This machine tier can be scaled out** and specify a value greater than 1 for **Default instance count** and **Maximum instance count**. The maximum must be set to less or equal to the number of SCSI channels you configured in the VM template. The default count must be less than the maximum.
6. In **Number of upgrade domains**, specify the same value as that in **Maximum instance count**. For example, if you specify a default count of 3 and a maximum count of 3, the guest cluster will have three nodes. The number of upgrade domains must also be set to 3 so that updates are performed in three stages, one node (VM) at a time. This leaves at least two VMs in the guest cluster running during planned maintenance.
7. Save and validate the service template.

After you've set up the guest cluster, you're ready to deploy the service.

Next steps

Deploy VMs from a template.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Set up networking for Hyper-V hosts and clusters in the VMM fabric

Article • 08/09/2024

This article describes how to set up network settings for Hyper-V hosts and clusters in the System Center Virtual Machine Manager (VMM) compute fabric.

You can apply network settings to a Hyper-V host or cluster using a logical switch. Applying a logical switch ensures that logical networks and other network settings are consistently assigned to multiple physical network adapters.

Before you start

- If you want to configure network settings manually, ensure that you've set up logical networks before you begin. In addition, ensure that the network sites within your logical networks are configured to use the host group of the host you want to assign them to. Check this in **Fabric** > **Servers** > **All Hosts** and select the host group. In **Hosts**, select the host > **Properties**.
- If you want to use a logical switch, you need to create the logical switch and port profiles.

Configure network settings with a logical switch

To do this, you'll need to configure the logical switch and port profiles you'll apply. Then you need to indicate what the physical network adapter is used for and configure network settings by applying a logical switch. The network adapters that you configure can be physical or virtual adapters on the hosts.

Specify what the network adapter is used for

Regardless of any port profiles and logical switches you're using in your network configuration, you must specify whether a network adapter in a host is used for virtual machines, host management, neither, or both. (The host must already be under management in VMM.)

1. Open **Fabric** > **Servers** > **All Hosts** > host-group-name > **Hosts** > **Host** > **Properties** > **Hardware**.

2. Under **Network adapters**, select the physical network adapter that you want to configure.

   - If you want to use this network adapter for virtual machines, ensure that **Available for placement** is checked.
   - If you want to use this network adapter for communication between the host and the VMM management server, ensure that **Used by management** is checked. You must ensure that you've at least one network adapter available for communication between the host and the VMM management server.

3. You don't need to configure individual settings in **Logical network connectivity** because you're using a switch.

Apply a logical switch

1. Open **Fabric** > **Servers** > **All Hosts** > *host group* > **Hosts** > **Host** > **Properties** > **Virtual Switches**.

2. Select the logical switch you created. Under **Adapter**, select the physical adapter that you want to apply the logical switch to.

3. In the **Uplink Port Profile** list, select the uplink port profile that you want to apply. The list contains the uplink port profiles that have been added to the logical switch that you selected. If a profile seems to be missing, review the configuration of the logical switch, and then return to this property tab. Select **OK** to finish.

   > ⓘ **Note**
   >
   > If you didn't create the virtual switch earlier and did it now, the host might temporarily lose network connectivity when VMM creates the switch.

4. Repeat the steps as needed. If you apply the same logical switch and uplink port profile to two or more adapters, the two adapters might be teamed depending on a setting in the logical switch. To find out if they'll be teamed, open the logical switch properties, select the **Uplink** tab, and view the **Uplink mode** setting. If the setting is **Team**, the adapters will be teamed. The specific mode in which they'll be teamed is determined by a setting in the uplink port profile.

5. After applying the logical switch, you can check the network adapter settings and verify whether they're in compliance with the switch:

   - Select **Fabric**> **Networking** > **Logical Switches** > **Home** > **Show** > **Hosts**.

- In **Logical Switch Information for Hosts**, verify the settings. **Fully compliant** indicates that the host settings are compliant with the logical switch. **Partially compliant** indicates some issues. Check the reasons in **Compliance errors**. **Non compliant** indicates that none of the IP subnets and VLANs defined for the logical network are assigned to the physical adapter. Select the switch > **Remediate** to fix this.
- If you've a cluster, check each node.

Set affinity between vNICs and pNICs

This section provides the information on how to set affinity between virtual network adapters (vNICs) and physical network adapters (pNICs). Affinity between pNICs and vNICs brings in flexibility to route network traffic across teamed pNICs. With this feature, you can increase throughput by mapping RDMA capable physical adapter with RDMA settings enabled vNIC. Also, you can route specific type of traffic (for example, live migration) to a higher bandwidth physical adapter. In HCI deployment scenarios, by specifying affinity, you can use SMB multichannel to meet high throughput for SMB traffic.

Before you begin

Ensure the following:

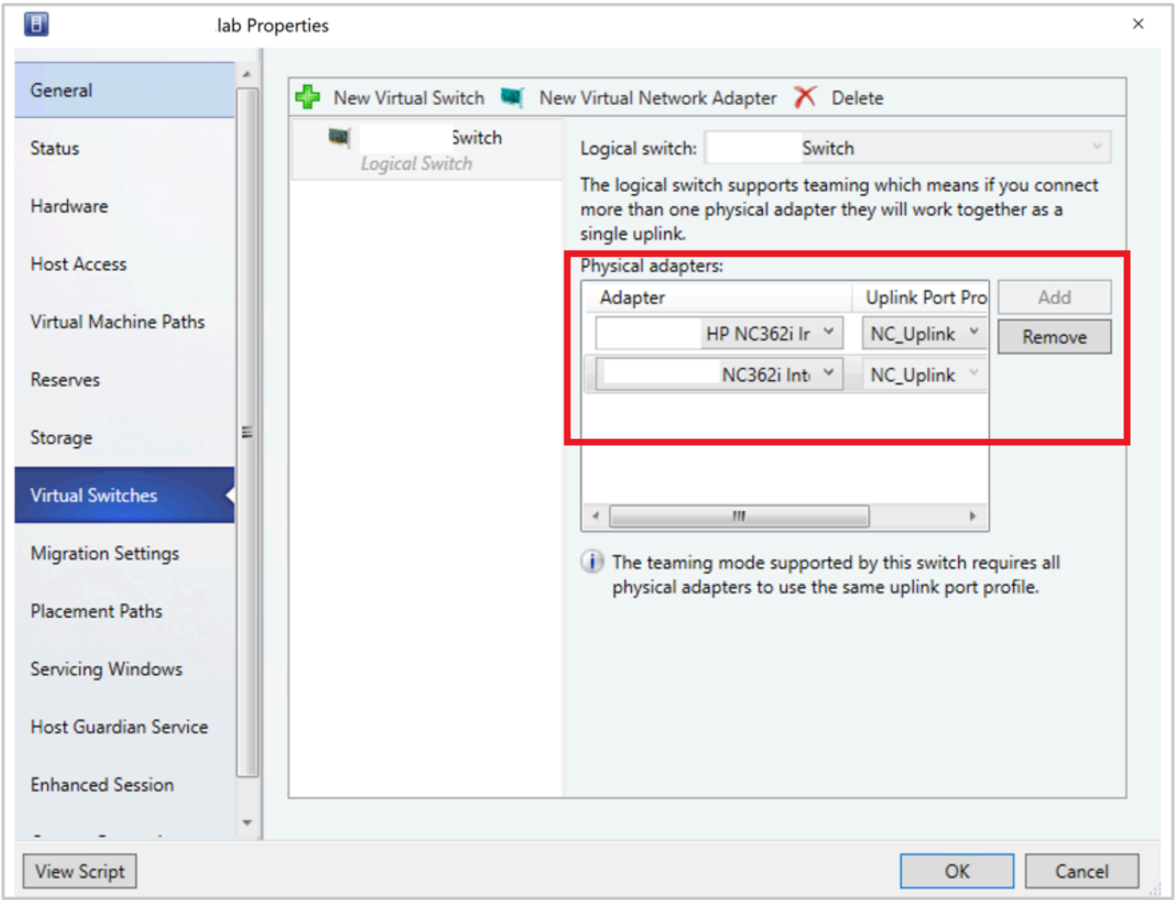
1. Logical switch is deployed on a host.
2. SET teaming property is enabled in the logical switch.

Follow these steps:

For a host, affinity between vNIC and pNIC can be set at virtual switch level. You can define affinity either when you add a new virtual network adapter to the virtual switch or when you modify the properties of an existing virtual network adapter.

1. Open **Fabric** > **Servers** > **All Hosts** > **host group** > **Hosts** > **Host**. Right-click **Host**, select **Properties**, and navigate to **Virtual Switches** tab.

2. Verify that the physical adapters to be teamed are added here. Affinity can be mapped only for physical adapters that are added here.



Logical switch: Switch

The logical switch supports teaming which means if you connect more than one physical adapter they will work together as a single uplink.

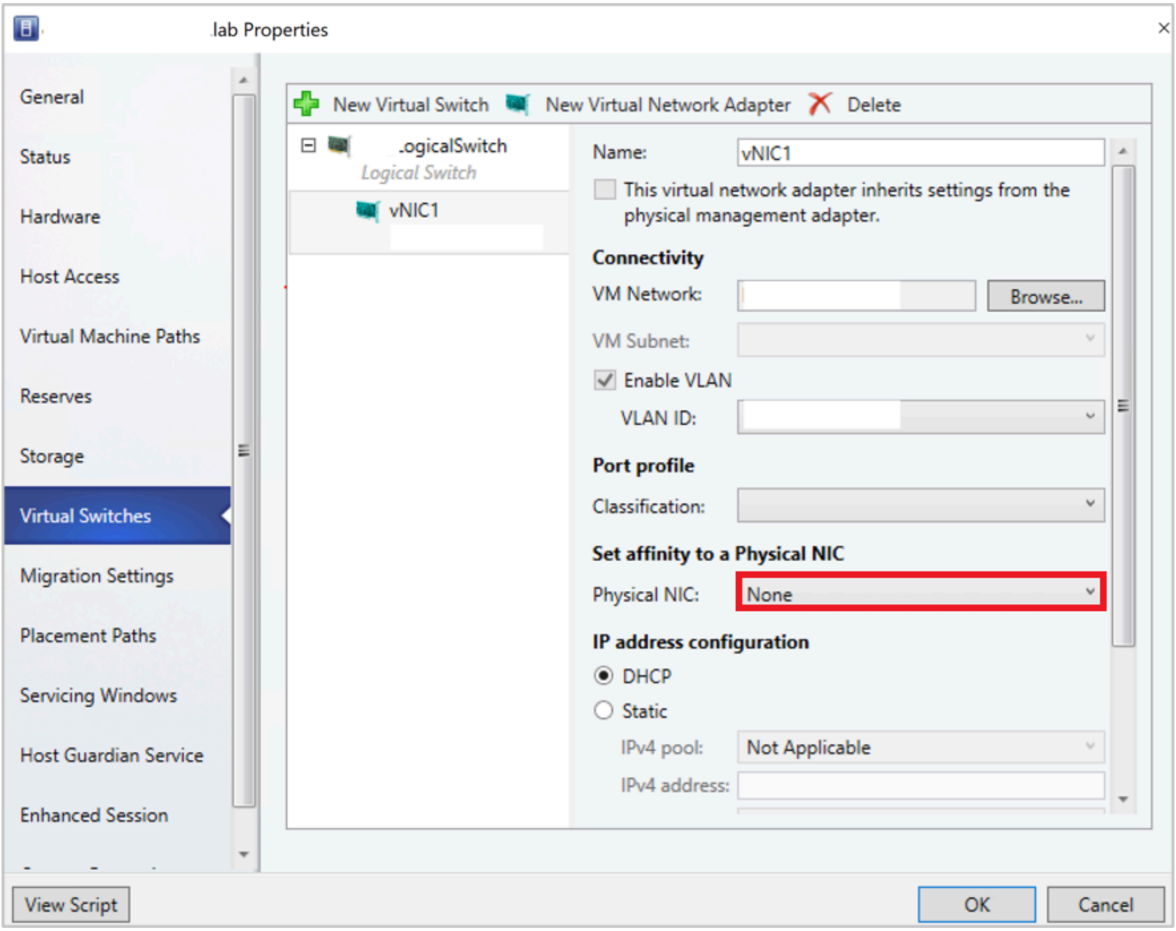
Physical adapters:

Adapter	Uplink Port Pro
HP NC362i Ir	NC_Uplink
NC362i Int	NC_Uplink

The teaming mode supported by this switch requires all physical adapters to use the same uplink port profile.

3. Select **New virtual network adapter** to add a new vNIC to the virtual switch.

4. By default, the affinity value is set as **None**. This setting corresponds to the existing behavior, where the operating system distributes the traffic from vNIC to any of the teamed physical NICs.



Name: vNIC1

□ This virtual network adapter inherits settings from the physical management adapter.

Connectivity

VM Network:

VM Subnet:

☑ Enable VLAN

VLAN ID:

Port profile

Classification:

Set affinity to a Physical NIC

Physical NIC: None

IP address configuration

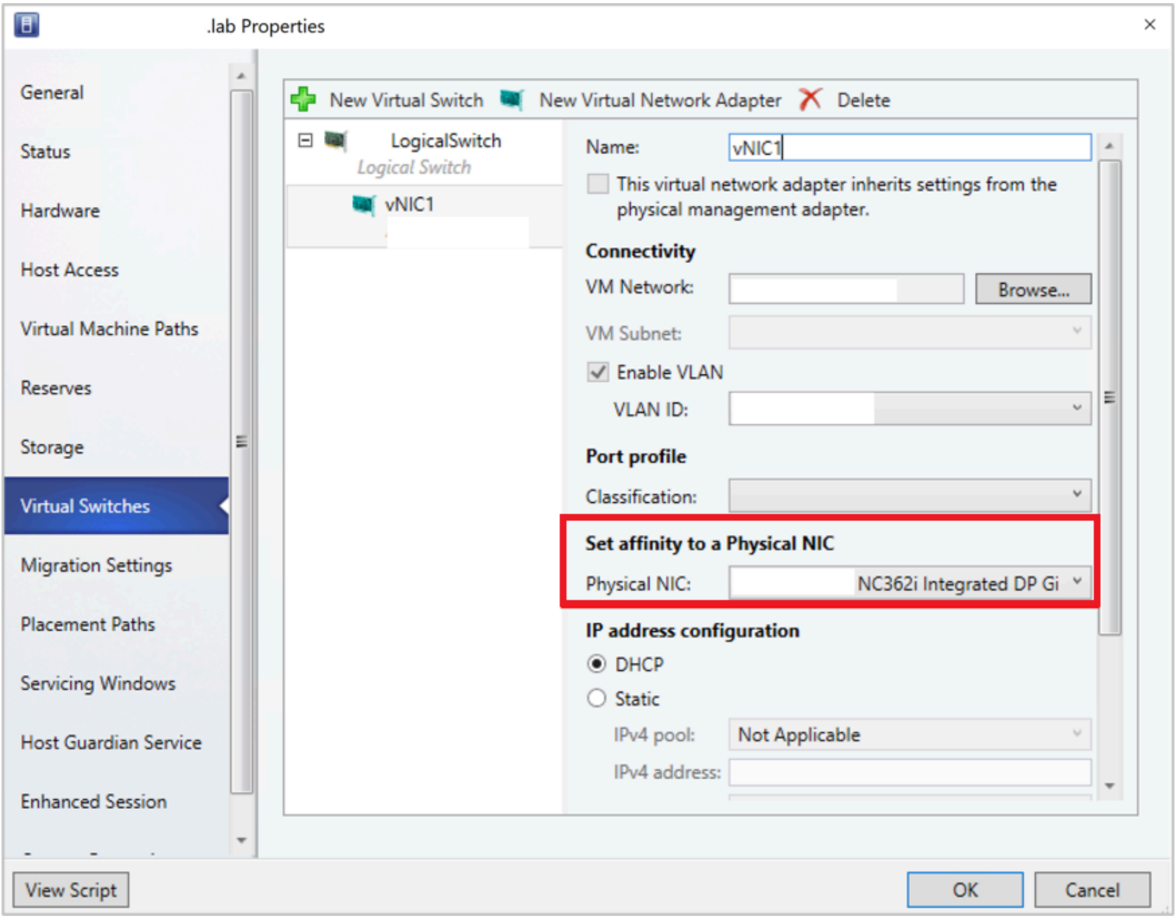
● DHCP

○ Static

IPv4 pool: Not Applicable

IPv4 address:

5. Set the affinity between a vNIC and physical NIC by selecting a physical adapter from the dropdown menu.



Name: vNIC1

□ This virtual network adapter inherits settings from the physical management adapter.

Connectivity

VM Network:

VM Subnet:

☑ Enable VLAN

VLAN ID:

Port profile

Classification:

Set affinity to a Physical NIC

Physical NIC: NC362i Integrated DP Gi

IP address configuration

● DHCP

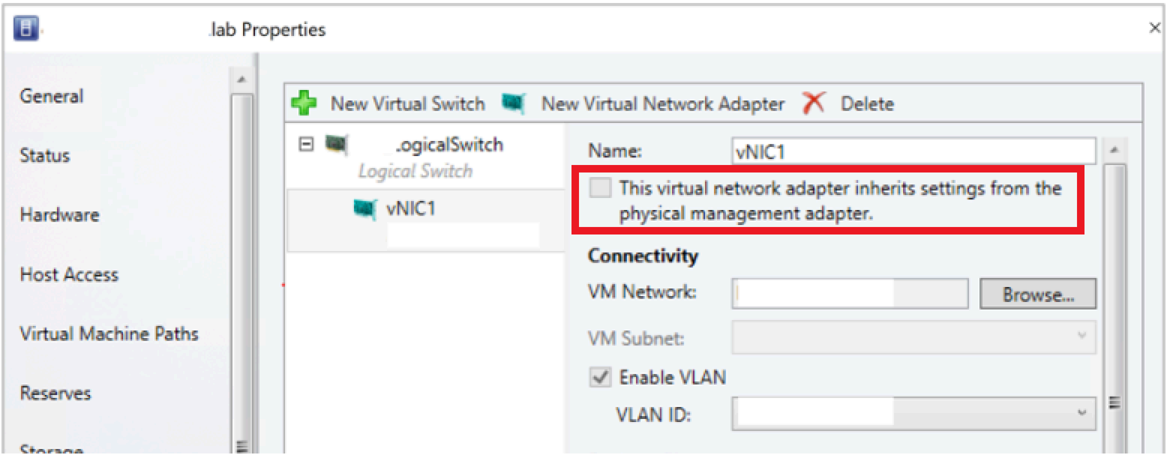
○ Static

IPv4 pool: Not Applicable

IPv4 address:

6. Once the affinity is defined, traffic from the vNIC is routed to the mapped physical adapter.

> ⓘ Note
>
> - We recommend you to not remove any of the physical adapters post teaming, as it could break the assigned affinity mappings.
> - If the option **This virtual adapter inherits the properties from the physical management adapter** is checked, affinity can't be defined for vNICs that handle management traffic.



Name: vNIC1

☐ This virtual network adapter inherits settings from the physical management adapter.

Connectivity

VM Network:

VM Subnet:

☑ Enable VLAN

VLAN ID:

Frequently asked questions

Q: I've deployed a SET enabled switch and teamed three physical adapters pNIC1, pNIC2, and pNIC3. I've set affinity between vNIC1 and pNIC1. For some reasons, if pNIC1 goes down, will there be no traffic flow from vNIC1?

A: No, traffic will continue to flow from vNIC1 to any of physical adapters (pNIC2 and pNIC3). When a physical adapter for which you've defined an affinity goes down, the default behavior of SET switch overrides affinity behavior. This means the operating system will map the traffic from vNIC1 to any of the active physical adapters (pNIC2 or pNIC3).

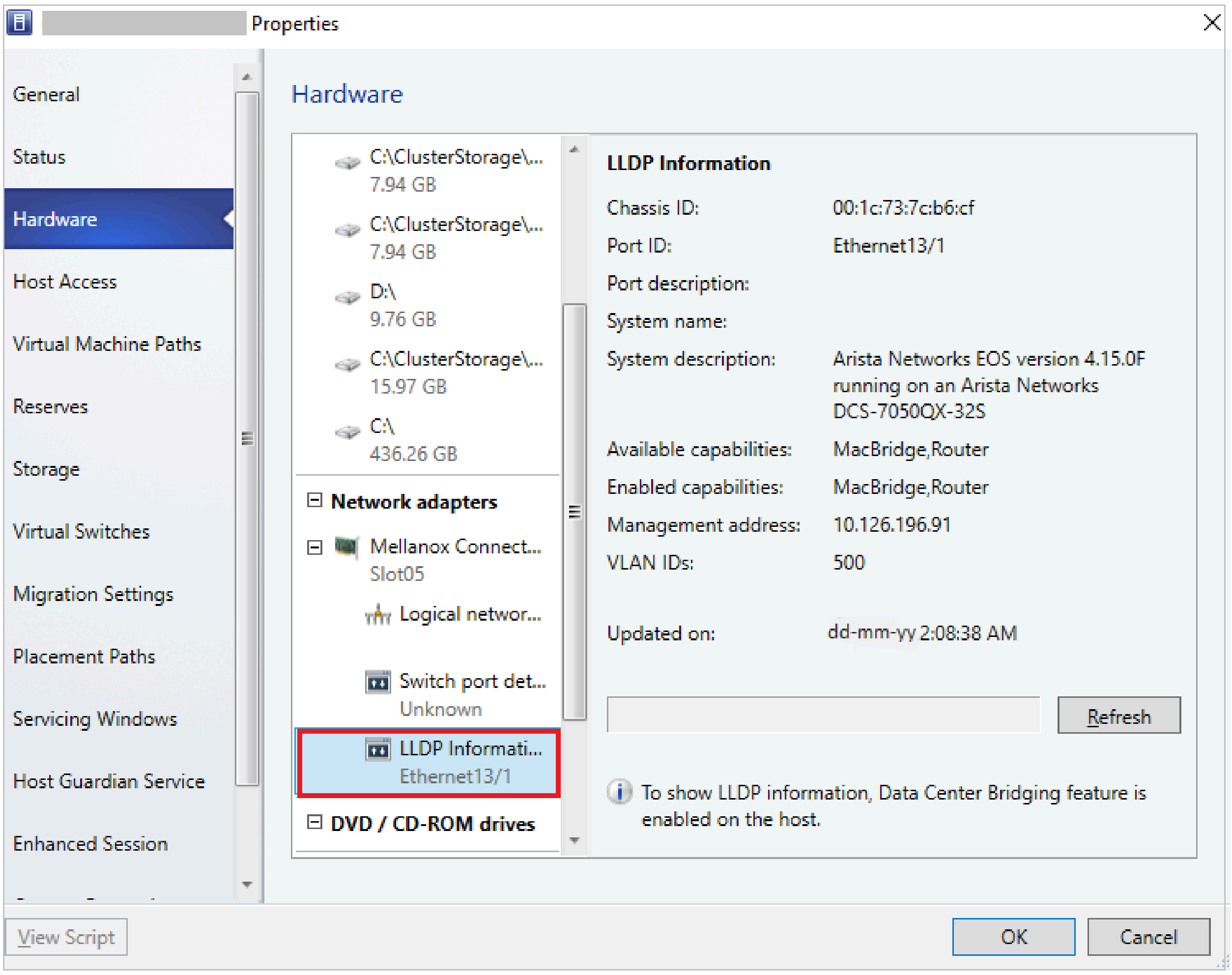
Monitor physical network devices

VMM supports Link Layer Discovery Protocol (LLDP). You can now use the LLDP information to remotely monitor physical network device properties and information. You can view this information using the VMM console and PowerShell.

Console view

To get the details of network devices from the VMM console, go to **View** > **Host** > **Properties** > **Hardware Configuration** > **Network adapter**.

> ⓘ **Note**
>
> The details displayed contain a time stamp (updated on). To get the current details, refresh the page.



LLDP Information

Chassis ID: 00:1c:73:7c:b6:cf

Port ID: Ethernet13/1

Port description:

System name:

System description: Arista Networks EOS version 4.15.0F running on an Arista Networks DCS-7050QX-32S

Available capabilities: MacBridge,Router

Enabled capabilities: MacBridge,Router

Management address: 10.126.196.91

VLAN IDs: 500

Updated on: dd-mm-yy 2:08:38 AM

ⓘ To show LLDP information, Data Center Bridging feature is enabled on the host.

The following LLDP information is displayed:

⛶ Expand table

Information displayed	Description
Chassis ID	Switch chassis ID
Port ID	Switch port to which NIC is connected
Port Description	Details related to the port such as *Type*

Information displayed	Description
System Name Manufacturer	Manufacturer, Software version details
System Description	Detailed system description
Available Capabilities	Available system capabilities (such as switching, routing)
Enabled Capabilities	Enabled system capabilities (such as switching, routing)
VLAN ID	Virtual LAN identifier
Management Address	IP management address

PowerShell

Use the following PowerShell command to view/refresh the LLDP details:

PowerShell

```
Set-SCVMHostNetworkAdapter -RefreshLLDP
```

ⓘ Note

By default, LLDP Packet wait time is set as 30 seconds. You can modify this value by modifying the registry key at **Software\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings\LLdpPacketWaitIntervalSeconds**. The minimum value you can set is 5 seconds, and the maximum value is 300 seconds.

Next steps

Set up storage for Hyper-V hosts.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Add storage to Hyper-V hosts and clusters

Article • 08/09/2024

This article describes how to allocate provisioned storage to Hyper-V hosts and clusters in the System Center Virtual Machine Manager (VMM) fabric.

Before you start

Before you can allocate provisioned storage to hosts and cluster, it must be discovered and classified in the VMM fabric:

1. Discover and classify storage:
    - Add and classify block storage devices. Learn about classification.
    - Add file storage
2. Allocate block storage to host groups. You can allocate an entire storage pool or a specific logical unit (LUN).
3. Ensure that you've completed these steps before you allocate storage to hosts:
    - **MPIO**: If you're using Fiber Channel or iSCSI storage, the Multipath I/O (MPIO) feature must be enabled on each host.
        - If MPIO is already enabled before you add the host, VMM will automatically enable it for supported storage arrays using Microsoft DSM. If you've vendor-specific DSMs, these will be used.
        - If you add a host to VMM and enable MPIO later, you need to configure it manually to add the discover device hardware IDs.
    - **HBA and zoning**: If you're using Fiber Channel storage array network (SAN), each host must have a host bus adapter (HBA) installed and zoning must be correctly configured.
    - **iSCSI**: If you're using an iSCSI SAN, ensure that iSCSI portals have been added, and that the iSCSI initiator is logged into the array.

      Ensure that the Microsoft iSCSI Initiator Service on each host is started and set to **Automatic**.
    - **Storage group**: Explain to your storage administrator how VMM manages storage.
        - In VMM, a storage group binds together host initiators, target ports, and logical units.

    - A storage group contains one or more host initiator IDs (IQN or WWN) (WWN).
    - A storage group also contains one or more target ports and one or more logical units. Logical units are exposed to the host initiators through the target ports.
    - By default, when VMM manages the assignment of logical units, VMM creates one storage group per host, either a standalone host or a host cluster node.
    - For some storage arrays, it's preferable to use one storage group for the entire cluster, where host initiators for all cluster nodes are contained in a single storage group. To do this, you need to set the CreateStorageGroupsPerCluster property to $true using the Set-SCStorageArray cmdlet.

Allocating storage

- You can allocate file storage directly to hosts and clusters.
- You can add LUNs to hosts and clusters.
- If you already provisioned LUNs on a host group, you can assign these to hosts and clusters.
- If you provisioned a storage pool on a host group, you can create LUNs during the procedure to add storage to a cluster.
- If you want to use shared storage that isn't managed by VMM, the storage disks must be available to all hosts or nodes before you can add them. You need to provision one or more LUNs to all hosts you want to cluster, and then mount and format the storage disks on one of the nodes.

  > ⓘ **Note**
  >
  > VMM doesn't support or block the use of asymmetric storage, where a workload can use disks that are shared between a subset of the cluster nodes. Each cluster node must be a possible owner of the cluster disk.

- After adding iSCSI storage to a host, you need to create a new session to the storage.

Allocate file storage to a standalone host

You can assign file shares on any host on which you want to create VMs that will use the file share as storage.

1. Select q**Fabric** > **Servers** > **All Hosts**, and select the host or cluster node you want to configure.

2. Select **Host** > **Properties** > **Host Access**. Specify a Run As account. By default, the Run As account that was used to add the host to VMM is listed. In the **Run As** account box, configure the account settings. You can't use the account that you use for the VMM service.

   > ⓘ **Note**
   >
   > - If you used a domain account for the VMM service account, add the domain account to the local Administrators group on the file server.
   > - If you used the local system account for the VMM service account, add the computer account for the VMM management server to the local Administrators group on the file server. For example, for a VMM management server that is named VMMServer01, add the computer account VMMServer01$.
   > - Any host or host cluster that accesses the SMB 3.0 file share must have been added to VMM using a Run As account. VMM automatically uses this Run As account to access the SMB 3.0 file share.
   > - If you specified explicit user credentials when you added a host or host cluster, you can remove the host or cluster from VMM, and then add it again using a Run As account.

3. Select **Host Name Properties** > **Storage** > **Add File Share**.

4. In **File share path**, select the required SMB 3.0 file share, and then select **OK**.

5. To confirm that the host has access, open the **Jobs** workspace to view the job status. Or open the host properties again, and then select the **Storage** tab. Under **File Shares**, select the SMB 3.0 file share. Verify that a green check mark appears next to **Access to file share**.

6. Repeat this procedure for any standalone host that you want to access the SMB 3.0 file share or for all nodes in a cluster

Assign a logical unit to a standalone host

You can either assign an existing unit or create a new one and assign it.

1. In **Fabric** > **Servers** > **All Hosts**, right-click the host that you want to configure > **Properties**.

2. If you want to create a new logical unit:

   - On the toolbar, next to **Disk**, select **Add**. Next to **Logical unit**, select **Create Logical Unit**.
   - In **Create Logical Unit** > **Storage pool**, choose the pool from which you want to create the logical unit. Specify a name (alphanumeric only), a description, and the unit size. Select **OK** to finish.

3. To assign an existing logical unit to the host, on the toolbar, next to **Disk**, select **Add**, and select the logical unit you want to assign.

4. In the **Logical unit** list, verify that the logical unit that you just created is selected.

5. In **Format new disk**, if you want to format the disk, select **Format this volume as NTFS volume with the following settings**, and specify the settings.

   > ⓘ **Note**
   >
   > If you select **Force format even if a file system is found**, all the existing data on the volume will be overwritten. If the logical unit has existing data, and you do not use the **Force Format** option, the VMM job to assign the logical unit will complete with a warning. VMM assigns the logical unit to the host. You can format the disk later.

6. In **Mount Point**, select the mount options. Select **OK** to assign the logical unit to the host.

7. VMM registers the storage logical unit to the host and mounts the storage disk.

   - To view the associated job information, open the **Jobs** workspace.
   - To verify that the logical unit was assigned, view the information on the **Storage** tab in the **Host Name** > **Properties** dialog. The newly assigned logical unit appears under **Disk**. Select the new disk to view the disk details.
   - If the **Array** field is populated in the disk details, this indicates that the storage array is under VMM management.

8. To configure additional disk settings, open Disk Management on the host. To open Disk Management, select **Start**, enter **diskmgmt.msc** in the search box, and then press ENTER. The new disk appears in the list of disks as a basic disk. If you chose

to format the disk, the disk is already formatted and online. You can right-click the disk to see the available options, such as **Format** and **Change Drive Letter and Paths**.

Configure storage for a Hyper-V cluster

1. Select **Fabric** > **Servers** > **All Hosts**. Right-click the cluster you want to configure > **Properties**. In **Host Cluster Name** > **Properties**, select a tab:

   - **Available Storage**: For adding available storage, converting available storage to shared storage (CSV), or removing available storage.

   - **Shared Volumes**: For adding cluster shared volumes (CSVs), converting CSVs to available storage, or removing CSVs. The cluster must run at least Windows Server 2016 to support CSVs.

2. Configure storage for the host cluster.

   - If you add available storage for CSVs, use only alphanumeric characters for a LUN. You can't change the partition style of a disk that has already been initialized.
   - If you're converting available storage to CSVs, ensure that there are no VMs on the cluster that have their associated .vhd or .vhdx files located on the storage that you want to convert.

     Convert volumes one at a time. After conversion, confirm that the logical unit appears on the **Shared Volumes** tab.

   > ⊗ **Caution**
   >
   > If you convert shared to available storage and the storage is being used by virtual machines, serious data loss can result.

   - You can only remove storage if there are no VMs in the cluster currently using the storage for their vhds.

3. When you're ready to commit the changes, select **OK**.

Create an iSCSI session

1. On the target host, in the Services snap-in, ensure that the Microsoft iSCSI Initiator Service is started and set to **Automatic**.
2. In **Fabric** > **Servers** > **All Hosts**, right-click the host that you want to configure > **Properties**.
3. Under **iSCSI Arrays**, see if the storage array is already listed. If it's not, on the toolbar, next to **iSCSI Array**, select **Add**.
4. In the **Create New iSCSI Session** > **Array**, select the storage array you want to use.
5. Select **Create** to create a new session. Select Use advanced settings if you want to modify customized settings, including target listener, name, or the host NIC that you want to use.
6. The array that you added appears under **iSCSI Arrays**. Select it to view more details.

Next steps

Set up networking for Hyper-V hosts and clusters.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage MPIO for Hyper-V hosts in the VMM fabric

Article • 08/09/2024

Read this article to learn how System Center Virtual Machine Manager (VMM) manages Multipath I/O (MPIO) on Hyper-V hosts.

When you add Fiber Channel or iSCSI storage to a Hyper-V host managed in the VMM fabric, the Multipath I/O (MPIO) feature must be enabled on each host.

- If MPIO is enabled on the host, VMM adds it for supported storage arrays using the Microsoft DSM. If you installed vendor-specific DSMs, the vendor-specific MPIO settings will be used to connect to the storage array.
- If you add a host and MPIO isn't enabled, VMM will show a warning message in the **Jobs** window.
- If you add a host to VMM and enable MPIO afterwards, you need to add the MPIO feature, and then manually configure MPIO to add the discovered device hardware IDs. Alternatively, you can install vendor-specific DSMs.

MPIO tracking in VMM

When Hyper-V hosts and clusters are added to the VMM fabric, VMM deploys an agent to connect between the host and the VMM server. Additionally, VMM collects configuration information about the host or cluster and adds it to VMM. For MPIO, VMM adds two registry keys containing MPIO information.

- HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Control\MPDEV\MPIOSupportedDeviceList
- HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\msdsm\Parameters\DsmSupportedDeviceList

After supported storage devices are added to the device list, VMM makes a **claim** on them, and a restart is required on the host. If you've added the host to VMM before deploying workloads on it, then this probably isn't an issue, but if workloads are already running on the host, this could cause interruptions. To avoid potential outages, you can run a PowerShell script to prepopulate the MPIO registry keys on a host, before adding it to the VMM fabric. Learn more about this script.

Prevent VMM from claiming device IDs

If you don't want VMM to claim any storage device IDs for MPIO purposes, do the following:

1. Open registry location **HKLM\Software\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings**.
2. In this location, create a registry key **RemoveMPIOHardwareIds** with type multi-string.
3. Add the device IDs from the default list. Ensure that you use the same spacing.
4. Restart the VMM service.
5. Add the Hyper-V host in the VMM.

Next steps

Provision a VM

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage port ACLs in VMM

Article • 09/10/2024

In System Center Virtual Machine Manager (VMM), you can centrally configure and manage Hyper-V port access control lists (ACLs). Port ACLs can be configured for both a Network Controller-managed fabric and for networks that aren't managed by Network Controller.

- A port ACL is a set of rules that filter traffic at the layer 2 port level. A port ACL in VMM filters access to a particular VMM object. A network object can have no more than one port ACL attached.
- An ACL contains rules and can be attached to any number of network objects. You can create an ACL without rules, and then add rules later. Each ACL rule corresponds to only one port ACL.
- If an ACL has multiple rules, they're applied based on priority. After a rule matches criteria and is applied, no other rules are processed.
- A global settings port ACL is applied to all VM virtual network adapters in an infrastructure. There's no separate object type for global settings. Instead, the global settings port ACL is attached to the VMM management server.
- Port ACL settings are exposed only through PowerShell cmdlets in VMM and can't be configured in the VMM console.
- Port ACLs can be applied to:
  - Virtual subnets and adapters in a Network Controller deployment.
  - Virtual subnets, network adapters, VM networks, and the VMM management server in networks that aren't managed by Network Controller.

Before you start

- To apply an ACL to objects managed by Network Controller, you use the **ManagedByNC** flag, and set it to **True**. If it isn't set to **True**, the ACL only applies to network objects that aren't managed by Network Controller.
- ACL types aren't interchangeable. You can’t apply an ACL with **ManagedByNC** set to **false**, to objects managed by Network Controller and vice versa.
- The key difference between these two kinds of ACLs is that you need to remediate each network adapter after applying ACL on objects that aren't managed by Network Controller.
- There's also a difference in priority ranges:
  - **Hyper-V port ACLs (not managed by Network Controller)**: 1 - 65535
  - **SDN port ACLs (managed by Network Controller)**: 1 - 64500

- You need full VMM admin permissions to attach a port ACL to global settings. To attach the ACL to VMM objects (VM networks, subnets, virtual network adapters), you need to be a VMM admin or tenant admin or a self-service user.

Unsupported scenarios

Here's a list of unsupported scenarios:

- Manage individual rules for a single instance when the ACL is shared with multiple instances. All rules are managed centrally within their parent ACLs and apply wherever the ACL is attached.
- Attach more than one ACL to an entity.
- Apply port ACLs to virtual network adapters in the Hyper-V parent partition (management operating system).
- Create port ACL rules in VMM that include IP-level protocols (other than TCP or UDP). Other protocols are still supported natively by Hyper-V.
- Apply port ACLs to logical networks, network sites (logical network definitions), subnet VLANs, and other VMM networking objects that aren't mentioned as supported.

Deployment steps

Use the VMM PowerShell interface to do the following:

1. Define port ACLs and rules.

   - The rules are applied to virtual switch ports on Hyper-V servers as "extended port ACLs" (VMNetworkAdapterExtendedAcl). This means that they can apply only to hosts running Windows Server 2016 or later because VMM doesn't create legacy Hyper-V port ACLs (VMNetworkAdapterAcl) for earlier versions.

   - All port ACL rules defined in VMM are stateful for TCP. You can't create stateless TCP ACL rules.

2. Attach a port ACL to global settings. This applies the ACL to all VM virtual network adapters.

3. Attach the port ACLs to VM networks, VM subnets, or VM virtual network adapters.

4. Manage port ACL rules.

Create port ACLs

1. Open PowerShell in VMM.

2. Create a port ACL with the New-SCPortACL cmdlet.

```
New-SCPortACL [-Name] <String> [-Description <String>] [-JobVariable
<String>] [-ManagedByNC] [-OnBehalfOfUser <String>] [-
OnBehalfOfUserRole <UserRole>] [-Owner <String>] [-PROTipID <Guid>] [-
RunAsynchronously] [-UserRole <UserRole>] [-VMMServer
<ServerConnection>] [<CommonParameters>]
```

Parameters

Expand table

Parameter	Details
Name; Description	Port ACL name and description
JobVariable	Stores job progress
ManagedByNC	Specifies whether objects are managed by Network Controller
OnBehalfOfUser/OnBehalfOfRole	Run job with username or role
Owner	Specifies the owner of a VMM object in the form of a valid domain user account. Example: Contoso\PattiFuller or PattiFuller@Contoso
ProTipID	ID of ProTip that triggered action
RunAsychronously	Indicates whether job runs asynchronously
UserRole	Specifies user role
VMMServer	Specifies VMM server
CommonParameters	Learn more

Examples

Create a port ACL for objects managed by Network Controller "DemoACLManagedByNC":

```
PS: C:\> New-SCPortACL -Name "DemoACLManagedByNC" -Description "PortACL
Example Managed by NC" -ManagedByN
```

Create a port ACL for objects not managed by Network Controller "DemPortACL":

```
PS: C:\> New-SCPortACL -Name "DemoPortACL" -Description "Port ACL Example
Non Managed by NC"
```

Define port ACL rules for a port ACL

1. Open PowerShell in VMM.

2. Create one or more rules with the New-SCPortACLRule cmdlet.

```
New-SCPortACLrule -PortACL <PortACL> -Name <string> [-Description
<string>] -Type <Inbound | Outbound> -Action <Allow | Deny> -Priority
<uint16> -Protocol <Tcp | Udp | Any> [-LocalAddressPrefix <string:
IPAddress | IPSubnet>] [-LocalPortRange <string:X|X-Y|Any>] [-
RemoteAddressPrefix <string: IPAddress | IPSubnet>] [-RemotePortRange
<string:X|X-Y|Any>]
```

Parameters

Expand table

Parameter	Details
Name, Description	Rule name and description
Type	Specifies the traffic direction for which the ACL is applied (Inbound or Outbound)
Action	Specifies whether the ACL allows or blocks traffic (Allow or Deny)
LocalAddressPrefix	Specifies the source IP address or subnet that's used to identify traffic that must be filtered
LocalPortRange	Specifies the source port range that's used to identify traffic
RemoteAddressPrefix	Specifies the destination IP address or subnet that's used to identify traffic for filtering

Parameter	Details
RemotePortRange	Specifies the destination port range that's used to identify traffic.
Protocol	Specifies the protocol for which the rule is applied
Priority	Specify the priority of the rule in port ACL. Rules are applied according to order. Set a priority between 1 and 65535, where the lowest number has highest priority. Port ACLs rules for objects managed by Network Controller must be set equal to or greater than 100. Network Controller doesn't support priority below 100.

Examples

Create a port ACL and store the object in $portACL:

```
PS: C:\> $portACL = New-SCPortACL -Name "RDP ACL" -Description "Acl on RDP
access"
```

Create a port ACL rule to allow RDP access from a remote subnet:

```
PS: C:\> New-SCPortACLRule -Name "AllowRDPAccess" -PortACL $portACL -
Description "Allow RDP Rule from a subnet" -Action Allow -Type Inbound -
Priority 110 -Protocol Tcp -LocalPortRange 3389 -RemoteAddressPrefix
10.184.20.0/24
```

Modify the priority of an ACL rule:

```
PS: C:\> $portACLRule = Get-SCPortACLRule -Name "AllowRDPAccess" `` <br/>
<br/> `` PS: C:\> Set-SCPortACLRule -PortACLRule $portACLRule -Priority 220
```

The first command gets the port ACL rule "AllowRDPAccess". The second command changes the priority of the rule to 220.

Modify the port ACL rule for the destination address range and protocol for a rule:

```
PS: C:\> $portACLRule = Get-SCPortACLRule -Name "AllowRDPAccess" `` <br/>
<br/> `` PS: C:\> Set-SCPortACLRule -PortACLRule $portACLRule -
```

```
RemoteAddressPrefix 172.185.21.0/24 -Protocol Udp
```

The first command retrieves rule **AllowRDPAccess**. The second changes the protocol to UDP and sets the destination to subnet 172.185.21.0/24.

Attach and detach port ACLs

A port ACL can be attached to global settings, VM networks, VM subnets, and virtual network adapters. A port ACL attached to global settings applies by default to all VM virtual network adapters.

1. Open PowerShell in VMM.

2. Attach a portal ACL using the Set-SCVMMServer cmdlet.

   ```
   Set-SCVMMServer -VMMServer <VMMServer> [-PortACL
   <NetworkAccessControlList> | -RemovePortACL ]
   ```

Parameters

Expand table

Parameter	Details
VMM server	Name of the VMM server on which the port ACL is applied
PortACL	Optionally attaches the specified port ACL to global settings

Examples

Attach an ACL to global settings:

```
Set-SCVMMServer -VMMServer "VMM.Contoso.Local" -PortACL $acl`` <br/><br/>
ExampleL: `` Set-SCVMMServer -VMMServer "VMM.Contoso.Local" -PortACL $acl
```

Detach an ACL from global settings:

```
Set-SCVMMServer -VMMServer "VMM.Contoso.Local" -RemovePortACL
```

Attach an ACL to a VM network during creation:

```
New-SCVMNetwork [-PortACL <NetworkAccessControlList>] [rest of the
parameters]
```

Attach an ACL to an existing VM network:

```
Set-SCVMNetwork -PortACL $acl`
```

Attach an ACL to a VM subnet during creation:

```
New-SCVMSubnet [-PortACL <NetworkAccessControlList>] [rest of the
parameters]
```

Attach an ACL to an existing VM subnet:

```
Set-SCVMSubnet [-PortACL <NetworkAccessControlList> | -RemovePortACL] [rest
of the parameters]
```

Retrieve and view port ACLs and rules

1. Open PowerShell in VMM.

2. Run the Get-SCPortACL cmdlet to retrieve and view a port ACL:

   ```
   Get-SCPortACL [[-Name] <String> ] [-ID <Guid> ] [-OnBehalfOfUser
   <String> ] [-OnBehalfOfUserRole <UserRole> ] [-VMMServer
   <ServerConnection> ] [ <CommonParameters>]
   ```

3. Run the Get-SCPortACLRule to retrieve and view a rule:

```
Get-SCPortACLRule [-Name <String> ] [-ID <Guid> ] [-OnBehalfOfUser
<String> ] [-OnBehalfOfUserRole <UserRole> ] [-PortACL <PortACL> ] [-
VMMServer <ServerConnection> ] [ <CommonParameters>]
```

Parameters

Expand table

Parameter	Details
No parameters	Retrieves all ACLs
Name/ID	Retrieve by name or GUID
OnBehalfOfUser/OnBehalfOfUserRole	Run with username or role
VMMServer	Retrieve ACLs on specific VMM server
CommonParameters	Learn more

Examples

Retrieve a specific ACL:

```
PS: C:> $portACL = Get-SCPortACL -Name "DemoPortACL"
```

Get rules for a specific ACL:

```
PS: C:> Get-SCPortACLRule -Name "AllowRDPAccess"
```

Get all rules for ACL:

```
PS: C:> Get-SCPortACLRule -PortACL $portACL
```

Modify port ACLs and rules

1. Open PowerShell in VMM.

2. Run the Set-SCPortACL cmdlet to modify a port ACL:

```
Set-SCPortACL [-PortACL] <PortACL> [[-Description] <String>] [-
JobVariable <String>] [-Name <String>] [-OnBehalfOfUser <String>] [-
OnBehalfOfUserRole <UserRole>] [-PROTipID <Guid>] [-RunAsynchronously]
[-VMMServer <ServerConnection>] [<CommonParameters>]
```

3. Run the Remove-SCPortACL to remove an ACL:

```
Remove-SCPortACL [-PortACL] <PortACL> [-Confirm] [-JobVariable
<String>] [-OnBehalfOfUser <String>] [-OnBehalfOfUserRole <UserRole>]
[-PROTipID <Guid>] [-RunAsynchronously] [-VMMServer <ServerConnection>]
[-WhatIf] [<CommonParameters>]
```

Parameters

Expand table

Parameter	Details
Name/Description	Name and description of port ACL
JobVariable	Stores job progress
OnBehalfOfUser/OnBehalfOfUserRole	Run with username or role
ProTipID	ID of ProTip that triggered action
RunAsynchronously	Indicates whether job runs asynchronously
Confirm	Prompts before running job
WhatIf	Shows what happens without running command

Examples

Set an ACL description:

```
PS: C:> $portACL = Get-SCPortACL -Name "DemoPortACL"
```

```
PS: C:> Set-SCPortACL -PortACL $portACL -Description "Port ACL Example Non
Managed by Network Controller"
```

The first cmdlet retrieves the ACL; the second sets the description on the ACL.

Remove an ACL:

```
PS: C:> $portACL = Get-SCPortACL -Name "DemoPortACL"
```

```
PS: C:> Remove-SCPortACL -PortACL $portACL
```

The first cmdlet retrieves the ACL; the second removes it.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage Hyper-V clusters in the VMM fabric

Article • 08/09/2024

Use this article to manage Hyper-V host clusters in the System Center Virtual Machine Manager (VMM) fabric. You can configure cluster properties and manage cluster nodes.

Configure cluster properties

1. In **Fabric**, right-click the cluster > **Properties**.
2. Configure the settings summarized in the table.

Expand table

Tab	Settings
General	View the name, host group, and description. You can also configure the **Cluster reserve (nodes)** setting and view the cluster reserve state. The **Cluster reserve (nodes)** setting specifies the number of node failures a cluster must be able to sustain while supporting all virtual machines deployed on the host cluster. If the cluster can't withstand the specified number of node failures and still keep all the virtual machines running, the cluster is placed in an over-committed state. When over-committed, the clustered hosts receive a zero rating during virtual machine placement. An administrator can override the rating and place a highly-available virtual machine on an over-committed cluster during a manual placement.
Status	View detailed status information for the host cluster: Cluster validation test runs and succeeds. Includes a link to the latest validation report (if available). Accessing the report requires administrative permissions on the cluster node where the report is located. For host clusters, you can perform an on-demand cluster validation through VMM. To do this, in the **Fabric** workspace, locate, and select the host cluster. Then, on the **Host Cluster** tab, select **Validate Cluster**. Cluster validation begins immediately. Online elements in the cluster: cluster core resources, disk witness in quorum, and the cluster service on each node.
Available Storage	Shows available storage, that is, storage logical units that are assigned to the host cluster but aren't Cluster Shared Volumes (CSVs). You can also do the following: Add and remove storage logical units that are managed by VMM.

Tab	Settings
	Convert available storage to shared storage (CSV).
Shared Volumes	Shows the shared volumes (CSVs) that are allocated to the host cluster. You can also do the following: Add and remove CSVs that are managed by VMM. Convert CSVs to available (non-CSV) storage.
Custom Properties	Custom properties that you manage.

Add a node to the cluster

1. If you already used Failover Cluster Manager to add the node, then in **Fabric** > **Servers** > **All Hosts**, right-click the host with a **Pending** status and select **Add to Host Cluster**.
2. If you didn't add the node with the Failover Cluster Manager, you can add hosts that are already managed by VMM. In **Fabric** > **Servers** > **All Hosts**, right-click the cluster > **Add Cluster Node**. In the Add Nodes Wizard > **Resource Type**, select the Run As account that will be used to add the nodes. Ensure **Existing servers running a Windows Server operating system** is selected. In **Select Hosts**, select the Hyper-V host server that you want to add. Finish the wizard and verify the settings.

Remove a node from the cluster

1. Select **Fabric** > **Servers** > **All Hosts**.
2. Locate the cluster node you want to remove and view the status in the **Hosts** pane.
3. If the node isn't in maintenance mode, select **Start Maintenance Mode**. Select **Move all virtual machines to other hosts in the cluster** and verify the status.
4. Right-click the host > **Remove Cluster Node** > **Yes**. During the job to remove the node any shared storage is unregistered from the node. If you manage storage outside VMM, then you must unregister the storage from the node.

Uncluster a cluster

Remove a host cluster as follows:

1. Select **Fabric** > **Servers** > **All Hosts**. Ensure the cluster isn't supporting any highly available VMs or clustered services/apps.
2. Right-click the host cluster > **Uncluster**. Select **Yes** to continue. During the job to remove the cluster, any shared storage is unregistered from the cluster nodes. If you manage storage outside VMM, then you must unregister the storage.

Feedback

Update Hyper-V hosts and clusters

Article • 08/09/2024

Read this article to learn about keeping Hyper-V hosts and clusters updated in the System Center Virtual Machine Manager (VMM) fabric.

Before you start

You'll need to set up an update (WSUS server) in the VMM fabric and configure update baselines.

Update a host or cluster

1. In **Fabric** > **Servers** > **Show** > **Compliance**, select the computers you want to update. All the baselines for the computer will be displayed. The computer could be compliant for some baselines and not for others.
2. Select **Remediate**. You'll see this option only if the selected objects aren't compliant.
3. In **Update Remediation**, select or clear update baselines or individual updates to determine which updates to install. When you select a computer, all updates are initially selected. If you're running a Hyper-V cluster, ensure that:

    - To update all cluster nodes, select the host cluster by its cluster name.
    - To update single nodes, select the individual hosts in the cluster. With this setting, VMM doesn't display cluster remediation options but treats each node as a standalone Hyper-V host.

4. If you prefer to restart the computers manually after remediation completes, select **Do not restart the servers after remediation**. By default, the computer restarts if any updates require it. If you choose not to restart and updates need it, the computer status will be **Pending Machine Reboot** after the remediation. The updates won't be activated until you restart. With this status, VMM won't scan the machines for compliance during refreshes.
5. If you're running a cluster:

    - If cluster node is already in maintenance mode, select **Allow remediation of clusters with nodes already in maintenance mode**. In maintenance mode, VMs can't be created or moved to the host. The host has a zero rating and is excluded from dynamic optimization.

- Select **Live migration** to remove virtual machines from a host before performing update remediation so that they remain online. If you don't need to keep them online and want to perform a quicker update, select **Save state** to shut down virtual machines and proceed with remediation.

6. Select **Remediate** to start updating. After remediation, if no reboot is pending, the server or cluster will show as **Compliant**.

Next steps

Learn about VMM updates.

Perform a rolling upgrade of a Hyper-V host cluster to Windows Server in VMM

Article • 08/09/2024

Cluster rolling upgrade feature enables you to upgrade the operating system of cluster nodes without stopping Hyper-V workloads running on the nodes. Read more about rolling upgrade requirements and architecture.

> ⓘ Note
>
> System Center 2022 Virtual Machine Manager (VMM) supports rolling upgrade of a Hyper-V host cluster from Windows Server 2019 to Windows Server 2022. Use the following procedures as applicable for the version of VMM you're using and the upgrade version it supports.

Cluster rolling upgrade in VMM

System Center Virtual Machine Manager (VMM) supports using the rolling upgrade feature to upgrade Hyper-V clusters in the VMM fabric. You can upgrade an entire cluster or specific cluster nodes. Here's what the upgrade does:

- **Creates a template**: Creates a template of the node configuration by combining the appropriate physical computer profile with the node configuration settings detailed in the upgrade wizard.
- **Migrates workloads**: Migrates workloads off the node, so workload operations aren't interrupted.
- **Removes node**: Puts the node into maintenance mode and then removes it from the cluster. This removes all VMM agents, virtual switch extensions, and so forth, from the node.
- **Provisions the node**: Provisions the node running Windows Server 2016/2019, and configures it according to the saved template.
- **Returns the node to VMM**: Brings the node back under VMM management and installs the VMM agent.
- **Returns the node to the cluster**: Adds the node back into the cluster, brings it out of the maintenance mode, and returns virtual machine workloads to it.

> ⓘ Note

Ensure to install the latest updates on the VHD that you want to use as a physical computer profile.

Prerequisites

Review the platform restrictions and limitations before you start cluster rolling upgrade.

- The cluster must be managed by VMM.
- The cluster must be running Windows Server 2016 or 2019.
- The cluster must meet the requirements for bare metal deployment. The only exception is that the physical computer profile doesn't need to include network or disk configuration details. During the upgrade, VMM records the node's network and disk configuration and uses that information instead of the computer profile.
- You can upgrade nodes that weren't originally provisioned using bare metal as long as those nodes meet bare metal requirements such as BMC. You'll need to provide this information in the upgrade wizard.
- The VMM library needs a virtual hard disk configured with Windows Server 2016 or 2019.

Run the upgrade

1. Select **Fabric** > **Servers** > **All Hosts**. Right-click the host cluster > **Upgrade Cluster**.
2. In the Upgrade Wizard > **Nodes**, select the nodes you want to upgrade or **Select All**. Then select **Physical computer profile** and select the profile for the nodes.
3. In **BMC Configuration**, select the Run As account with permissions to access the BMC or create a new one. In **Out-of-band management protocol**, select the protocol that the BMCs use. To use DCMI, select IPMI. DCMI is supported even though it's not listed. Ensure the correct port is listed.
4. In **Deployment Customization**, review the nodes to upgrade. If the wizard couldn't figure out all the settings, it displays a **Missing Settings** alert for the node. For example, if the node wasn't provisioned by bare metal, BMC settings might not be complete. Fill in the missing information.

    - Enter the BMC IP address if required. You can also change the node name. Don't clear **Skip Active Directory check for this computer name** unless you're changing the node name and you want to ensure the new name isn't in use.
    - In the network adapter configuration, you can specify the MAC address. Do this if you're configuring the management adapter for the cluster, and you want to configure it as a virtual network adapter. It's not the MAC address of

the BMC. If you choose to specify static IP settings for the adapter, select a logical network and an IP subnet, if applicable. If the subnet contains an address pool, you can select **Obtain an IP address corresponding to the selected subnet**. Otherwise, enter an IP address within the logical network.

5. In **Summary**, select **Finish** to begin the upgrade. If the wizard finishes the nodes upgrade successfully, the wizard upgrades the cluster functional level to Windows Server 2019/2022.

If for some reason you need to update the cluster functional level of a cluster that was upgraded outside VMM, right-click the **Cluster** > **Update Version**. This could happen if you upgrade the cluster nodes before adding the cluster to the VMM fabric, but the cluster is still functioning as a Windows Server 2016/2019 cluster.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Service hosts and virtual machines in the VMM compute fabric

Article • 08/09/2024

Read this article to learn about service Hyper-V hosts and virtual machines in the System Center Virtual Machine Manager (VMM) fabric.

Before you start

We recommend you keep hosts in a Hyper-V host cluster up-to-date with the same updates to avoid VMM operations issues.

You can service hosts and VMs by:

- **Setting up servicing windows**: Servicing windows provide a method for scheduling servicing outside VMM. You can associate a servicing window with individual hosts, virtual machines, or services. Before using other applications to schedule maintenance tasks, you can use Windows PowerShell scripts or custom applications to query the object and determine if it's currently in a servicing window. Servicing windows don't interfere with the regular use and functionality of VMM.
- **Placing hosts in maintenance mode**: You can start the maintenance mode for a virtual machine host whenever you need to perform maintenance tasks on the physical host, such as applying security updates or replacing hardware on the physical host computer. You can place Hyper-V hosts and VMware ESX hosts in the VMM fabric into maintenance mode.

> ⓘ **Note**
>
> - When a host is in maintenance mode, the following restrictions apply:
>   - VMs can't be created on the host.
>   - VMs can't be moved to the host.
>   - The host has a zero rating and can't be selected for placement.
>   - The host is excluded from dynamic optimization.
> - For ESX hosts, if the VMware Distributed Resources Scheduler is not configured, all virtual machines on the host must be either manually shut down or moved to another host to successfully start maintenance mode on an ESX host.

- If you're monitoring with the Operations Manager and you've maintenance mode enabled for monitoring, the Operations Manager agent suppresses alerts, notifications, rules, monitors, automatic responses, state changes, and new alerts for hosts that are placed in maintenance mode.

Set up a servicing window

1. In the VMM console, select **Settings** > **Create** > **Create Servicing Window**.
2. In **New Servicing Window**, specify a name and optional description for the window.
3. In **Category**, enter or select the category of servicing window.
4. In **Start time**, enter the date, time of day, and time zone for the maintenance window.
5. In **Duration**, specify the number of hours or minutes in the servicing window.
6. Under **Recurrence pattern**, select the frequency (Daily, Weekly, or Monthly), and then schedule the occurrences within that frequency.
7. After the window is set up, you can assign it to a host or VM. To assign to a host, select the host properties > **Servicing Window** > **Manage**, and select the window you want to add to the host.

Put hosts in maintenance mode

1. In the VMM console, select **Fabric** > **Fabric Resources** > **Servers** > **All Hosts**.
2. Select the host to place in maintenance mode, and in the **Host** group, select **Start Maintenance Mode**.
   - You can select **Move all virtual machines to other hosts in the cluster** if you want to move all highly available VMs to other hosts in the cluster (the host must be in a cluster that's capable of live migration).
   - Otherwise, select **Place all running virtual machines into a saved state**. Note that list causes a loss of service for users currently using the VM.
3. You can verify if the host is in maintenance mode by checking its status in **Fabric** > **Hosts**.

To bring a host out of maintenance node, select it and select **Stop Maintenance Mode**.

ⓘ **Note**

VMM doesn't automatically restart the VM and doesn't automatically migrate VMs back to the host.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Set up VMware servers in the VMM compute fabric

Article • 08/09/2024

Read this article to learn about managing VMware servers and VMs in the System Center Virtual Machine Manager (VMM) fabric.

VMM enables you to deploy and manage virtual machines and services across multiple hypervisor platforms, including VMware vSphere hosts and vCenter servers.

- You can add vCenter and vSphere hosts to the VMM fabric.
- VMM integrates directly with VMware vCenter Server. Through the VMM console, you can manage the day-to-day operations of VMware vSphere hosts and clusters, such as the discovery and management of hosts.
- VMM provides the ability to create, manage, store, place, and deploy virtual machines on vSphere hosts. You can import VMware templates.
- You can associate host adapters with VMM logical networks. More advanced management takes place on the vCenter Server, for example, configuring port groups, standard and distributed virtual switches (or **vSwitches**), vMotion, and Storage vMotion.
- You can convert VMware VMs to Hyper-V.

Before you start

- VMM supports the management of hosts and clusters running VMware. Learn more for supported versions of VMware.

- You need a vCenter server in your deployment. vSphere hosts and host clusters must be managed by a vCenter server, which, in turn, is managed by VMM.

- The following features are supported by VMM when hosts and clusters are managed with a vCenter server:

- VMM command shell (same shell across all hypervisors).

- VM placement based on host ratings when you create, deploy, or migrate VMware VMs. Includes concurrent VM deployment during service deployment.

- You can deploy VMM services to vSphere hosts. You can't deploy vApps.

- You can make vSphere host resources available to a VMM cloud by creating clouds from host groups in which vSphere hosts are located or by creating a cloud from a VMware resource pool.

  > ⓘ **Note**
  >
  > VMM doesn't integrate with VMware vCloud.

- You can use dynamic optimization and power optimization for vSphere hosts. VMM can load balance virtual machines on vSphere clusters using live migration. With power optimization, you can configure VMM to turn vSphere hosts on and off for power management.

- You can transfer VMware resources using live migrating between hosts in a cluster (uses vMotion) and live storage migration (uses storage vMotion). Resources supported for transfer include network migration to and from the library and between hosts.

  > ⓘ **Note**
  >
  > VMware thin provision disks become thick when you migrate a disk to the VMM library.

- You can place vSphere hosts managed by VMM into and out of maintenance mode.

- You can organize and store VMware VMs, VMDK files, and VMware templates in the VMM library. You can create new VMs from templates.

  > ⓘ **Note**
  >
  > VMM doesn't support older VMDK disk types. These disk types are supported:
  > - Regular VMDK files (VMFS and monolithic flat)
  > - VMDK files that are used to access physical disks (vmfsPassthroughRawDeviceMap)
  > - Snapshots (vmfssparse)

- You can create templates using .vmdk files stored in the library. You can also import templates stored on vSphere hosts (only template metadata is imported to VMM).

- VMM supports existing standard and distributed vSwitches and port groups. vSwitches and port groups must be configured with the vCenter server.
- You can do regular VMM networking tasks, including assigning logical networks, static IP address, and MAC address to Windows-based VMs running on VMware.
- VMM supports and recognizes VMware Paravirtual SCSI (PVSCSI) storage adapters.
- VMM doesn't support VMware VM with virtual hard disks connected to an IDE bus.
- VMM supports VMware thin provision hard disk through the dynamic disk type.

  > ⓘ **Note**
  >
  > If you create and deploy a VM to a vSphere host configured to use a dynamic disk, the disk will be thin provisioned. If a VM was created as a thin provisioned disk, out-of-band VM will display it as dynamic. If you save a thin provisioned disk to the library, VMM will save it as thick. It remains thick if you create a VM from it.

- All storage must be added to vSphere hosts outside VMM.
- Communication between VMM and the vCenter server is SSL encrypted. You'll need a certificate to identify the vCenter server. You can use a self-signed certificate for a vCenter server or a non-Microsoft verified certificate.
- If you're using a self-signed certificate for authenticating the vCenter server to VMM, you can manually import the certificate to the Trusted People certificate store on the VMM management server before adding the vCenter server. If you don't, you'll be prompted to do this during deployment.
- You'll need an account with admin permissions for the vCenter server (local or Active Directory account) and an account with admin permissions for the vSphere hosts. You can create Run As accounts before you begin. If you don't, you'll need to create accounts during the deployment procedure.
- You can decide whether you want VMM to communicate with the vSphere hosts managed by the vCenter server over a secure connection. If so, you'll need a certificate to authenticate communications on each vSphere host or cluster. You can either use the self-signed certificate that VMware created when vSphere was installed on the host, or a certificate from a trusted CA. If you're using a self-signed certificate, you can import it from each vSphere host to the VMM management server before you begin deployment

- Before you configure network settings for vSphere hosts, ensure that you've created logical networks that you want to associate with the physical network adapters on the hosts.

Add a vCenter server

1. Select **Fabric** > **Servers** > **vCenter servers** > **Add** > **Add Resources** > **VMware vCenter Server**.
2. In **Add VMware vCenter Server**, specify the name (FQDN, NetBIOS, or IP address) of the vCenter server. Add the port needed to connect to the vCenter server (443 by default).
3. In **Run As account**, select the Run As account with admin permissions for the vCenter server. Select **Create Run As Account** if you don't have one.
4. In **Security**, select or clear **Communicate with VMware ESX hosts in secure mode**. We recommend you keep the setting checked. If selected, you'll need a certificate and public key for each vSphere host managed by the vCenter server.
5. If you're using a self-signed certificate to communicate with the vCenter server and you haven't manually copied it to the Trusted People certificate store, the **Import Certificate** dialog will appear. Select **Import** to add the certificate to the store.
6. In **Jobs**, wait until the job has a Completed status and then check that the server appears in **Fabric** > **Servers** > **vCenter Server** with a **Responding** status.

Add an ESX/ESXi host

1. Ensure that the vCenter server is managed by VMM before you start. When you add the vCenter server, vSphere hosts for the server are discovered automatically.
2. Select **Fabric** > **Add Resources** > **VMware ESX Hosts and Clusters**.
3. In the **Add Resource Wizard** > **Credentials**, select the Run As account that has admin permissions on the vSphere hosts you want to add. Create a Run As account if you don't have one.
4. In **Target Resources**, select the vCenter server. If the hosts are clustered, they'll be listed together with the cluster nodes.
5. In **Computer Name**, select the hosts or clusters you want to add or **Select All**.
6. In **Host Settings**, select the host group to which you want to assign the host or cluster. You don't need to add VM placement paths.
7. In **Summary**, verify the settings and select **Finish**. Wait until the Jobs dialog shows a **Completed** status.
8. Select **Fabric** > **Servers**> **All Hosts** and in the host group, check the status of each host or cluster. Either select **OK** or **OK (limited)**.

9. If the status is limited, it means you've enabled the setting **Communicate with VMware ESX hosts in secure mode** but haven't yet imported a certificate from each vSphere host. To modify the security setting, right-click the vCenter server > **Properties** > **Security**.
10. To import the certificate, select each relevant host name > **Properties** > **Management** > **Retrieve** > **OK**. The host status must be **OK** after the import.

Associate host adapters with logical networks

By default, when you added vSphere hosts to VMM, VMM automatically created logical networks that match the virtual network switch name.

> ⓘ **Note**
>
> VMM doesn't automatically create port groups, so you'll need to configure port groups with the necessary VLANs that correspond to network sites on the vCenter server.

Associate the logical network with the physical network adapter (for an external virtual network) as follows:

1. Select **Fabric** > **Servers** > **All Hosts** > vSphere host > **Host** > **Properties** > **Hardware**.

2. In **Network Adapters**, select the physical network adapter on the host. In **Logical network connectivity**, select the logical networks you want to associate with the adapter.

   > ⓘ **Note**
   >
   > Only logical networks available to the host group are available.

3. Select **Advanced** > **Advanced Network Adapter Properties** to see IP subnets and VLANs available for a logical network. By default, for a logical network, the subnets and VLANs are scope to the host group or inherited via a parent host group. If none appears, it indicates that no network site exists for the logical network. If **Unassigned** is available, select it to view VLANS to which the physical adapter is connected but that isn't included in a network site.

4. View virtual network settings in the host properties > **Virtual Networks**. View compliance information in **Fabric** > **Networking** > **Logical Networks** > **Hosts** >

Logical Network Information for Hosts > **Compliance**. A status of **Fully compliant** indicates that all subnets and VLAN that are in the network site are assigned to the network adapter.

Import templates from vCenter

You can import VMware templates from the vCenter server to the VMM library. VMM copies only the metadata associated with the template and not the .vmdk file. This means that VMM is dependent on the vCenter server to use the template.

1. Select **Library** > **Home** > **Import** > **Import VMware template**.
2. In **Import VMware Templates**, select each template you want to import and select **OK**.
3. Verify the templates in **Library** > **Templates** > **VM Templates**.

Set up a servicing window for a VMware host

Servicing windows provide a method for scheduling servicing outside VMM. You can associate a servicing window with individual hosts, virtual machines, or services. Before using other applications to schedule the maintenance tasks, you can use Windows PowerShell scripts or custom applications to query the object and determine if it's currently in a servicing window. Servicing windows don't interfere with the regular use and functionality of VMM. Set up a servicing window as follows:

1. In the VMM console, select **Settings** > **Create** > **Create Servicing Window**.
2. In **New Servicing Window**, specify a name and optional description for the window.
3. In **Category**, enter or select the category of servicing window.
4. In **Start time**, enter the date, time of day, and time zone for the maintenance window.
5. In **Duration**, specify the number of hours or minutes in the servicing window.
6. Under **Recurrence pattern**, select the frequency (Daily, Weekly, or Monthly), and then schedule the occurrences within that frequency.
7. After the window is set up, you can assign it to a host or VM. To assign to a host, select the host properties > **Servicing Window** > **Manage**, and select the window you want to add to the host.

Feedback

Set up infrastructure servers in the VMM compute fabric

Article • 08/09/2024

Read this article to learn about adding and managing infrastructure servers in the System Center Virtual Machine Manager (VMM) fabric.

In addition to the infrastructure servers used by the VMM fabric (library server, PXE servers, and IPAM servers), you can add other infrastructure servers such as Active Directory, DNS, DHCP, and System Center to the VMM fabric. This allows you to manage and update all these servers in the same location.

The **Infrastructure** node in the VMM console shows the infrastructure servers you add. It also shows the VMM management servers, vCenter servers, VMM library servers, IPAM servers, and PXE servers if you add them.

Add an infrastructure server

1. Select **Fabric** > **Servers** > **Infrastructure** > **Add Resources** > **Infrastructure Server**.
2. In **Add Infrastructure Server Wizard** specify the FQDN of the server you want to add an account with permissions for the server. Then select **Add**.

Update infrastructure servers

In order to update infrastructure servers, you'll need to set up a WSUS server and configure update baselines.

After the WSUS server is in place, you can update infrastructure servers as follows:

1. In **Fabric** > **Servers** > **Home** > **Show** > **Compliance**, select the server you want to update. All the baselines for the server will be displayed. The server could be compliant for some baselines and not for others.
2. Select **Remediate**. You'll see this option if the selected objects aren't compliant.
3. In **Update Remediation**, select or clear update baselines or individual updates to determine which updates to install. When you select a computer, all updates are initially selected.
4. If you prefer to restart the server manually after remediation completes, select **Do not restart the servers after remediation**. By default, the server restarts if any updates require it. If you choose not to restart and updates need it, the computer status will be **Pending Machine Reboot** after the remediation. The updates won't

be activated until you restart. With this status, VMM won't scan the machines for compliance during refreshes.

5. Select **Remediate** to start updating.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up update servers in the VMM compute fabric

Article • 08/09/2024

Learn about deploying update servers in the System Center Virtual Machine Manager (VMM) fabric.

You deploy update servers in the VMM fabric to manage compliance and remediation for virtualization hosts, library servers, the VMM management server, PXE servers, the WSUS server itself, and any infrastructure servers. Learn more.

This article explains the prerequisites, information about how to add a WSUS server to the fabric, set up update baselines, run a scan, and create update exemptions.

Before you start

- The WSUS server must be running Windows Server Update Service (WSUS) 4.0 or later and supported versions of Windows Server, as detailed in system requirements.
- The WSUS server must be in the same domain as the VMM server, or in a domain with full trust.
- VMM can use a WSUS root server or downstream WSUS server. You can't use a WSUS replica server.
- The WSUS server can be dedicated to VMM or an existing server.
- The WSUS server can be installed on the VMM management server, but if you'll be processing a large number of updates, we recommend a separate server.
- VMM can work with System Center Updates Publisher, but only full content updates are supported. Metadata-only updates can't be added to a baseline.
- After you add a WSUS server to VMM, you must manage it in the VMM console and not in the WSUS console. In VMM, you update the properties of the update server to configure a proxy server for synchronizations and to change the update categories, products, and supported languages that are synchronized by the WSUS server.
- In VMM, administrators and delegated administrators manage fabric updates. Only administrators can manage the update server and synchronize updates. Delegated administrators can scan and remediate updates on computers that are within the scope of their user roles. Delegated administrators can use baselines created by administrators and other delegated administrators. But delegated administrators can't modify or delete baselines created by others.

Add a WSUS server to the VMM fabric

1. Ensure that the server is running the WSUS role.
2. Select **Fabric** > **Home** > **Add** > **Add Resources** > **Update Server**.
3. In **Add Windows Server Update Services Server**, specify the name, port, and credentials of the WSUS server. The account needs admin rights on the server. Use an existing Run As account or create a new one. Specify whether you want to use SSL for connections.
4. The WSUS server will be added to the fabric, followed by initial synchronization of the updates catalog. This could take a while. Monitor status in the **Add Update Server** and **Synchronize Update Server** jobs.
5. After the server is added, you can update its properties to configure a proxy server for synchronization. In **Fabric** > **Servers** > **Update Server** > **Properties**, select the **Proxy Server** tab. Configure WSUS to use a proxy server when configuring updates, or update the port for an existing proxy server.
6. In addition, you can select **Update Classification** to select the update classification that you want to synchronize, select **Product** to select the products that you want to include when synchronizing, and **Language** to select the supported synchronization languages.

After you've added the server, you can update the WSUS settings and perform manual synchronization in **Servers** > WSUS server name > **Update Server**.

Add WSUS servers that are managed in Configuration Manager

If you want to add an existing WSUS server from a Configuration Manager environment to the VMM fabric, you'll need to do the following:

1. Create a collection in Configuration Manager and add any servers that you'd like to add to the VMM fabric.
2. Exclude this collection from any software update deployments delivered by Configuration Manager. This ensures that VMM controls update management for the servers. You'll still be able to view compliance information for the collection in Configuration Manager reports.
3. If you want to include VMM compliance information in Configuration Manager, create an update group in Configuration Manager that contains all the updates for which you want to measure compliance for the machines that will be in the VMM fabric. This update group is only for reporting. Don't deploy it to the machines managed by VMM.

4. Now add the WSUS server as described above.
5. After adding the server, select **Update Server** > **Properties** > **General** > **Allow Update Server configuration changes**.

Create and assign update baselines

After you've added the WSUS server to the fabric, you can configure update baselines. An update baseline contains a set of required updates scoped to an object such as a host group, a standalone host, a host cluster, a VMM management server, or an infrastructure server.

- Update baselines can be assigned to host groups and to individual computers based on their role in VMM.
- Update baselines that are assigned to a host group are applied to all standalone hosts and host clusters in the host group, as well as the standalone hosts and host clusters in child host groups.
- During a compliance scan, computers that are assigned to a baseline are graded for compliance with their assigned baselines. After a computer is found noncompliant, an administrator brings the computer into compliance through update remediation.
- If a host is moved from one host group to another, the baselines for the new host group are applied to the host, and the baselines for the preceding host group no longer apply - that is, unless the baseline is assigned to both host groups. Explicit baseline assignments to a managed host stay with the host when it's moved from one host group to another. It's only when the baseline is assigned to a host group that baseline assignments get revoked during the move.
- You can use two methods to prepare update baselines for remediation:
  - A VMM built-in update baseline: Sample Baseline for Critical Updates and Sample Baseline for Security Updates.
  - A custom update baseline.

Assign servers to a built-in baseline

1. Select **Library** > **Update Catalog and Baselines** > **Update Baselines**.
2. In **Baselines**, select the baseline you want to use.
3. Select **Home** > **Properties** > **Updates** for the baseline. In **Updates**, add or remove baselines as required. To ensure all security updates are remediated, don't remove anything.
4. Select **Assignment Scope**, and select the host groups, clusters, standalone servers, and infrastructure servers to add to the baseline. Or select **All Hosts** to add all.

Assign servers to a custom baseline

1. Select **Library** > **Update Catalog and Baselines** > **Update Baselines**.
2. Select **Home** > **Create** > **Baseline** for the baseline.
3. In **Update Baseline Wizard** > **General**, specify a name and description.
4. In **Update**, add the updates you want to include.
5. In **Assignment Scope**, expand **Host Groups** and **Infrastructure**. Select the groups and servers you want to add.
6. In **Summary**, select **Finish**, and accept the **Microsoft License Terms** if needed to install any of the updates. Verify the baseline in **Library** > **Update Catalog and Baselines** > **Baselines**.

Scan for update compliance

After you assign computers to an update baseline, you can scan them to determine their compliance status for the baselines. When a computer is scanned for compliance:

- WSUS checks each update in the assigned update baselines to determine whether the update is applicable, and if the update is applicable, whether it has been installed.
- After a compliance scan, for every computer, each update has a compliance status of **Compliant**, **Non-Compliant**, **Error**, **Pending Reboot**, or **Unknown**. You can view compliance properties for additional information.
- The compliance scan focuses only on the updates that the administrator has identified as important by adding them to a baseline. That enables organizations to monitor for compliance for what is deemed important for their organization.
- The following changes can cause an Unknown update status for a computer and must be followed by a scan operation to access the computer's compliance status:
  - A host is moved from one host group to another host group.
  - An update is added to or removed from a baseline that is assigned to a computer.
  - The computer is added to the scope of a baseline.

To check compliance:

1. Select **Fabric** > **Servers**
2. In **Home** > **Show**, select **Compliance**.
3. Since you haven't yet scanned computers, the compliance status will show as **Unknown**, with an operational status **Pending Compliance Scan**.
4. Select the computers you want to check and select **Scan**.

5. While the scan is in progress, status will be Unknown. After it's finished, compliance status for each update will be **Compliant**, **Non-Compliant**, or **Error**.

Manage update exemptions

You can create update exemptions for specific machines. For example, if an update has caused the machine to be in an unhealthy state, you could uninstall the update out-of-band and then exempt the machine from the update until the issue is resolved. When the compliance scan runs next, the machine will show as **Non-Compliant**.

1. Select **Fabric** > **Home** > **Show** > **Compliance**. Then on the **Fabric** node, select **Servers** and navigate to the server you want to exempt.
2. In the result pane, expand the update baselines for the machine and select the update.
3. Select **Compliance** > **Compliance Properties**.
4. In **Compliance Properties**, select the update > **Create**.
5. In **Create Exemption**, add notes about the reason and the expected exemption data. Change the update status to **Exempt**.
6. After you've resolved the issue and you want to cancel the exemption so that the machine is compliant again, select the exemption > **Delete** > **Yes** in **Compliance Properties**.
7. To return the server to a compliant state, select the noncompliant server and select **Remediate** on the **Compliance** tab.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up the VMM networking fabric

Article • 08/22/2024

This article provides an overview of setting up the System Center Virtual Machine Manager (VMM) networking fabric.

Here's what you'll typically do to set up networking in the VMM fabric:

1. Set up logical networks: Create logical networks that map to your physical networks. You can create network sites that map to network sites in your physical network. For example, IP subnets, VLNS, or subnet/VLAN pairs. Then if you're not using DHCP, you create IP address pools for the network sites that exist within your physical networks.
2. Create VM networks: Create VM networks that map to network sites that exist within your physical networks.
3. Set up IP address pools: Create address pool to allocate static IP addresses. You'll need to configure pools for logical networks, and in some circumstances for VM networks too.
4. Add a gateway: You might need to set up network virtualization gateways in the VMM networking fabric. By default, if you're using isolated VM networks in your VMM fabric, VMs associated with a network can only connect to machines in the same subnet. If you want to connect VMs further than the subnet, you'll need a gateway.
5. Create port profiles: Create uplink port profiles that indicate to VMM which networks a host can connect to on a specific network adapter. If necessary, create virtual port profiles to specify settings that must be applied to virtual network adapters. You can create custom port classifications to abstract virtual port profiles.
6. Configure logical switches: Create a logical switch, apply it to a host, and select the network adapters on the host that you want to bind to the switch. When you apply the switch, networking settings will be applied to the host.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up logical networks in the VMM fabric

Article • 08/21/2024

Read this article to learn how to create logical networks in System Center Virtual Machine Manager (VMM)

You have different types of networks in your organization, including corporate networks, management networks, and others. In VMM, each of these networks is defined as a logical network. Logical networks are logical objects that mirror your physicals networks.

When you create logical networks, you assign them properties that match your physical environment. You specify the type of network, the associated network sites associated, and the static address pools if you're not using DCHP to assign IP addresses to VMs you create in the network sites. You also specify whether networks are isolated physically or virtually, using network virtualization and virtual LANs (VLANs).

You use logical networks when you provision virtualization hosts in the VMM fabric. You associate physical adapters on hosts with logical networks.

VMM virtual machine (VM) networks are based on logical networks. VM networks provide an interface through which VMs connect to a logical network. A logical network can have a single or multiple VM networks mapped to it.

Before you start

Before you start, it's important to understand how logical networks work in VMM.

- **Automatic logical networks**: By default, VMM creates logical networks automatically. When you provision a host in the VMM fabric and there's no VMM logical network associated with a physical network adapter on that host, VMM automatically creates a logical network and associates it with an adapter. By default, for the logical network VMM assigns the first DNS suffix label of the connection-specific DNS suffix. By default, VMM also creates a VM network configured with **No isolation**.
- **Manual logical networks**: When you create a logical network manually, you specify:
- **Network type**: You specify whether the network is isolated or not, and if it's how it's isolated. Then when you create VM networks based on the logical network, they'll be created with the type of network you specified.

  - **No isolation**: This is the simplest type of network model that specifies there's just a single network within which machines can connect to each other with no need to isolate these machines from each other. VM networks in VMM provide an interface through which VMs connect to a logical network, and in a no isolation model you'll have a single VM network mapped to a logical network.
  - **Isolation**: More often you'll want to isolate networks from each other. For example, you might want to isolate networks that have different purposes, or you might be a provider who wants to host workloads for multiple tenants on a single logical network, with isolation for each tenant. In this case, you'll have multiple VM networks mapped to a logical network. VM networks mapped to a logical network can be isolated using VLANs/private VLANs or network virtualization.

> ⓘ Note
>
> - A typical setup might be an infrastructure network with no isolation or VLAN isolation, a load balancer backend and internet facing network with PVLAN, and tenant networks with isolation using network virtualization.
> - You can only use one type of isolation on a single logical network. If you do need this, you'll need multiple logical networks.
> - There's a practical limit of ~2000 tenants and ~4000 VM networks for a single VMM server.

- **Network sites**: If your organization has different locations and datacenters, you can include information about those sites in your logical network settings. For example, you could specify a New York site with an IP subnet and/or VLAN settings and then a London site with different IP/VLAN settings. You can then assign IP addresses to VMs based on network, location, and VLAN settings.

> ⓘ Note
>
> - You need to assign an IP subnet to a site if VMM is going to distribute static IP addresses to VMs in the site. If you're using DHCP, you don't need a subnet.
> - You need to configure a VLAN if one is used in your physical site. If you're not using VLANs and you're using DHCP, you don't need to define network sites in your logical network.

Create logical networks automatically

If you want VMM to automatically create logical networks (and VM networks), you can specify how VMM determines the logical network name.

1. Select **Settings** > **General**. Double-click **Network Settings**.
2. Configure the **Logical network matching** setting.

> ⓘ **Note**
>
> - For Hyper-V hosts, you can use the entire DNS suffix label or the first one. For example, if the DNS suffix is corp.contoso.com the logical network will be corp-contoso.com or just corp. This isn't supported for VMware hosts.
> - For Hyper-V and VMware hosts, you can select the network connection name or the virtual network switch name (the name of the virtual network switch to which the physical adapter of the host is bound).
> - By default, VMware hosts use the virtual network switch option.
> - You can also specify a fallback option if the first logical matching fails.

If you don't want VMM to create logical and VM networks automatically, you can disable the global setting.

1. Select **Settings** > **General** and double-click **Network Settings**.
2. Clear **Create logical networks automatically**.

Create logical networks manually

1. **Fabric** > **Home** > **Show** > **Fabric Resources**. In **Fabric**, expand **Networking** > **Logical Networks** > **Home** > **Create** > **Create Logical Network**.
2. In **Create Logical Network Wizard** > **Name**, specify a name and description.
3. Specify how you want to isolate VM networks associated with this logical network:

- If you want to have multiple VM networks associated with the logical network and isolate them using network virtualization, select **One connected network** > **Allow new VM networks created on this logical network to use network virtualization**.
- If you want to have multiple VM networks associated with the logical network and isolate them using a VLAN/PVLAN, select **VLAN-based independent networks** or **Private VLAN (PVLAN) networks**.
- If you don't want to isolate networks in the logical network, select **One connected network** > **Create a VM network with the same name to allow virtual machines to access this logical network directly**. With this setting, you'll have a single VM network associated with your logical network.

- If you've deployed a Microsoft Network Controller in the VMM fabric, you can select to have the logical network managed by the network controller.

4. In **Network Site**, add network sites to the logical network. If you don't need to create network sites, select **Next**.

- **DHCP no VLAN**: If you're using DHCP to allocate IP addresses and you don't have VLANs, you don't need a network site.

> ⓘ **Note**
>
> VMM automatically suggests a site name. Any network name must not be longer than 64 characters.

- **Static IP**: If you're using static IP addresses, create at least one network site and associate at least one IP subnet with it.
- **VLAN**: If you're using VLANs with static IP addressing, create a corresponding network site for the VLAN and subnet pairs. If you're using DHCP, create corresponding network sites for VLAN information only.
- **Network virtualization**: If you're using network virtualization, create at least one network site with an associated IP subnet so that the logical network has an IP address pool.
- **Load balancer**: If the logical network will contain a load balancer, create at least one network site with an associated IP subnet.

5. If you're using an external network managed by a vendor network management console or virtual switch extension manager outside VMM, you can configure settings in the vendor console and import them into VMM.
6. In **Host groups that can use this network site**, select each host group to which you want to make the logical network available.
7. In **Associated VLANs and IP subnets**, select **Insert Row** to specify the settings that you want to assign to the network site. If you're selecting PVLAN, you'll need to add a **SecondaryVLAN** for each VLAN. Ensure that the VLANs and subnets are available in your physical network. If you leave the VLAN field empty, VMM assigns a value of 0 to indicate that VLANs aren't used. In trunk mode, 0 indicates native VLAN.
8. In **Summary**, review the settings and select **Finish**. When the job shows as **Completed**, verify the logical network in **Logical Networks and IP Pools**.

Next steps

If you created network sites and associated one or more IP subnets with them (you're not using DHCP), you can create static IP address pools from those subnets. Then VMM can automatically allocate IP addresses to VMs in the network site. Set up IP address pools.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up logical networks in the VMM 2022 fabric

Article • 08/21/2024

This article describes how to create logical networks in System Center 2022 Virtual Machine Manager (VMM). VMM offers a simplified flow of logical network creation. It supports network types and illustrations in the product based on use cases.

You have different types of networks in your organization, such as corporate networks and management networks. In VMM, each of these networks is defined as a logical network. Logical networks are logical objects that mirror your physical networks.

When you create logical networks, you assign them properties that match your physical environment. You specify the type of logical network and the associated network sites. You specify static address pools if you don't use DHCP to assign IP addresses to VMs that you create in the network site. You also specify whether networks are isolated physically or virtually by using network virtualization and virtual LANs (VLANs).

You use logical networks when you provision virtualization hosts in the VMM fabric. You associate physical adapters on hosts with logical networks.

VMM virtual machine (VM) networks are based on logical networks. VM networks provide an interface through which VMs connect to a logical network. A logical network can have a single VM network or multiple VM networks mapped to it.

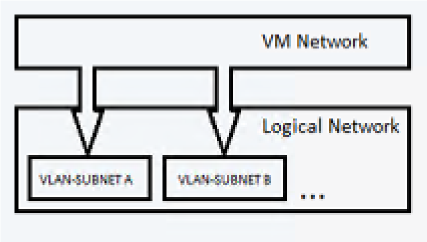
Before you start

Before you start, it's important to understand how logical networks work in VMM.

- **Automatic logical networks**: By default, VMM creates logical networks automatically. When you provision a host in the VMM fabric and there's no VMM logical network associated with a physical network adapter on that host, VMM automatically creates a logical network and associates it with an adapter. By default, for the logical network, VMM assigns the first DNS suffix label of the connection-specific DNS suffix. By default, VMM also creates a connected VM network.

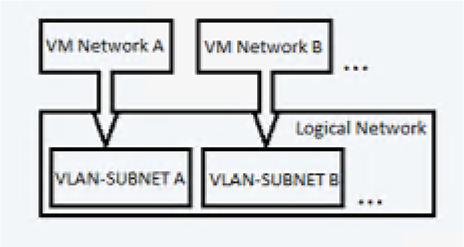
- **Manual logical networks**: When you create a logical network manually, you specify:

- **Network type**: Specify whether the network is a connected network or an independent network and the type of connected network. Then when you create VM networks based on the logical network, they're created with the type of network you specified.
  - **Connected network**: The VLAN and subnet pairs of the underlying physical networks are logically equivalent. A single VM network is created on top of this logical network, and this VM network provides access to all the underlying VLAN-subnet pairs. This network type was earlier known as *One Connected Network*.

    Example scenario: Enterprise Contoso needs a network to host their DevTest workloads. This network might have multiple VLANs or subnets. Contoso creates a logical network of the type *Connected network*. VMM is responsible for assigning the VLAN or subnet to the VMs based on the host group on which the VM is placed.

  - **Independent network**: Multiple VM networks can be created on top of this logical network. Each VM network created provides access to a specific VLAN-subnet pair. The VM networks are independent of each other.

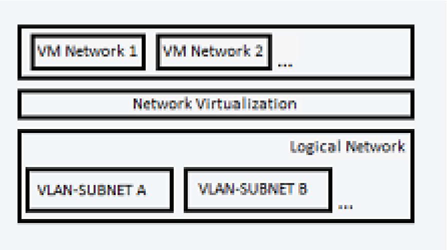
    

    There are two types of independent networks:
    - VLAN-based independent networks
    - PVLAN-based independent networks

    Example scenario: Woodgrove IT is a host. Woodgrove IT has Contoso and Fabrikam as its tenants. Both Contoso and Fabrikam need a DevTest network. Contoso's network must be isolated from that of Fabrikam. All VMs of Contoso must be connected to the *Contoso-DevTest* VM network. The VMs of Fabrikam must be connected to the *Fabrikam-DevTest* VM network.

Woodgrove IT creates a logical network of the *Independent network* type and names it *DevTest*. This logical network has two VLAN-subnet pairs. Two VM networks are created on top of this logical network, and each VM network gets access to a specific VLAN-subnet. One VM network is named *Contoso-DevTest* and is provided for Contoso's use. The other VM network is named *Fabrikam-DevTest* and is provided for Fabrikam's use.

- **Virtualized network**: This is the fabric network. Multiple virtualized VM networks can be created on top of this logical network. Each VM network has its own virtualized address space.



> ⓘ **Note**
>
> - A typical setup might be an infrastructure network with no isolation or VLAN isolation, a load balancer back end and internet-facing network with PVLAN, and tenant networks with isolation using network virtualization.
> - You can use only one type of isolation on a single logical network. If you do need isolation, you need multiple logical networks.
> - There's a practical limit of approximately 2,000 tenants and approximately 4,000 VM networks for a single VMM server.

- **Network sites**: If your organization has different locations and datacenters, you can include information about those sites in your logical network settings. For example, you can specify a New York site with an IP subnet and VLAN settings. You can specify a London site with different IP or VLAN settings. You can then assign an IP address to VMs based on network, location, and VLAN settings.

> ⓘ **Note**
>
> - Assign an IP subnet to a site if VMM is going to distribute static IP addresses to VMs in the site. If you use DHCP, you don't need a subnet.
> - Configure a VLAN if one is used in your physical site. If you don't use VLANs and you use DHCP, you don't need to define network sites in your logical network.

Create logical networks automatically

If you want VMM to automatically create logical networks (and VM networks), you can specify how VMM determines the logical network name.

1. Select **Settings** > **General**. Double-click **Network Settings**.

2. Configure the **Logical network matching** setting.

   > ⓘ **Note**
   >
   > - For Hyper-V hosts, you can use the entire DNS suffix label or the first one. For example, if the DNS suffix is corp.contoso.com, the logical network is corp-contoso.com or just corp. This capability isn't supported for VMware hosts.
   > - For Hyper-V and VMware hosts, you can select the network connection name or the virtual network switch name. The switch name is the name of the virtual network switch to which the physical adapter of the host is bound.
   > - By default, VMware hosts use the virtual network switch option.
   > - You can also specify a fallback option if the first logical matching fails.

If you don't want VMM to create logical and VM networks automatically, you can disable the global setting.

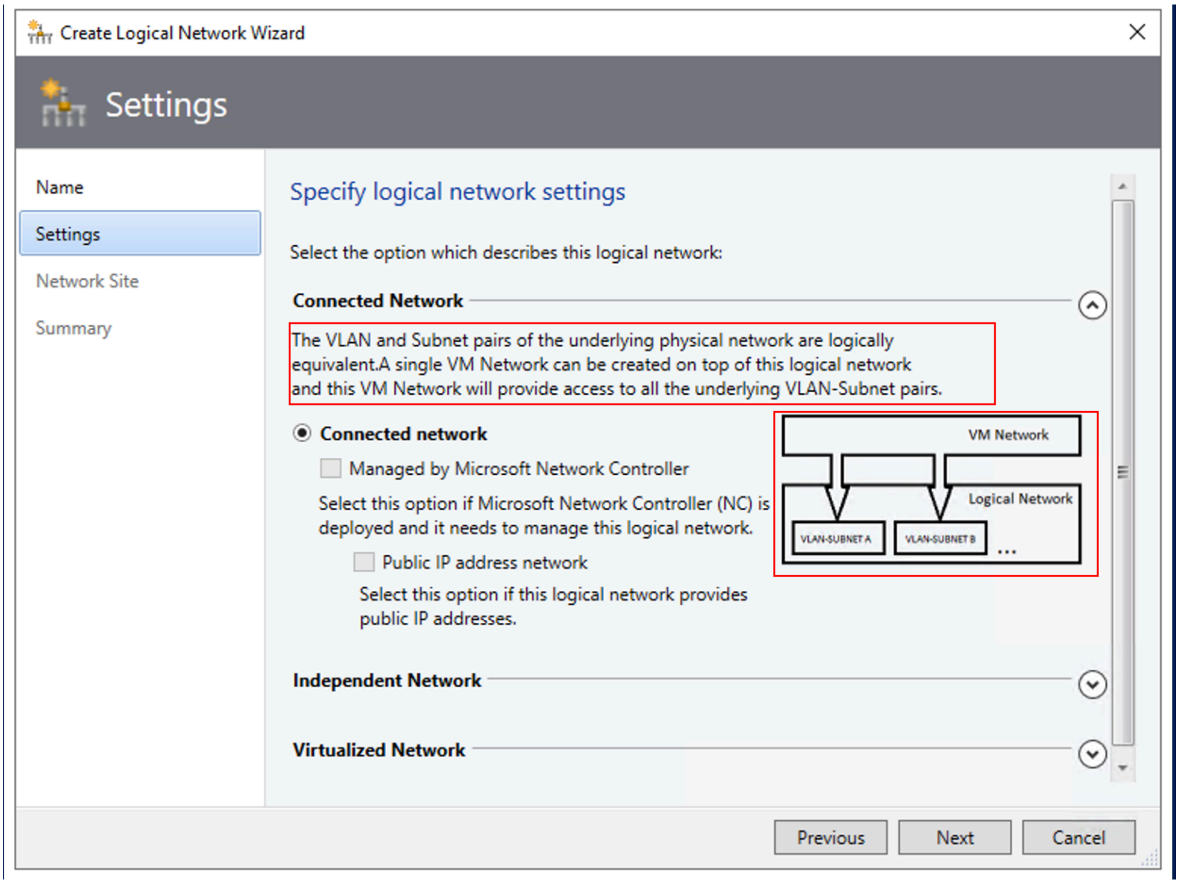
1. Select **Settings** > **General**. Double-click **Network Settings**.
2. Clear **Create logical networks automatically**.

Create logical networks manually

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. Specify how you want to isolate VM networks associated with this logical network.



Specify logical network settings

Select the option which describes this logical network:

Connected Network

The VLAN and Subnet pairs of the underlying physical network are logically equivalent.A single VM Network can be created on top of this logical network and this VM Network will provide access to all the underlying VLAN-Subnet pairs.

● Connected network

□ Managed by Microsoft Network Controller

Select this option if Microsoft Network Controller (NC) is deployed and it needs to manage this logical network.

□ Public IP address network

Select this option if this logical network provides public IP addresses.

Independent Network

Virtualized Network

To simplify logical network creation, descriptions and illustrations of the logical network types are available in VMM. Each type of logical network has an in-product description and an illustration that describes the use case.

- If you want to create a single VM network that has access to all the underlying VLAN-subnet pairs, choose **Connected network**. Here, the VLAN and IP subnet pairs of the underlying physical network are logically equivalent.
  - To allow Microsoft Network Controller to manage the logical network, choose **Managed by Microsoft Network controller**.
  - If the logical network provides public IP addresses, choose **IP address network**.
- To create multiple VM networks that are independent of each other, choose **Independent Network**. Each VM network will have access to a specific VLAN subnet pair or a PVLAN subnet pair.
- To create a multiple virtualized VM network that has its own virtualized address space, choose **Virtualized network**.

4. In **Network Site**, add network sites to the logical network. If you don't need to create network sites, select **Next**.

   IP pools can be created when you add network sites in the **Create Logical Network Wizard**.

- **DHCP no VLAN**: If you use DHCP to allocate IP addresses and you don't have VLANs, you don't need a network site.

  > ⓘ Note
  >
  > VMM automatically suggests a site name. A network name is limited to a length of 64 characters.

- **Static IP**: If you use static IP addresses, create at least one network site and associate at least one IP subnet with it.

- **VLAN**: If you use VLANs with static IP addressing, create corresponding network sites for the VLAN and subnet pairs. If you use DHCP, create corresponding network sites for VLAN information only.

- **Network virtualization**: If you use network virtualization, create at least one network site with an associated IP subnet so that the logical network has an IP address pool.

- **Load balancer**: If the logical network will contain a load balancer, create at least one network site with an associated IP subnet.

5. If you use an external network managed by a vendor network management console or virtual switch extension manager outside VMM, you can configure settings in the vendor console and import them into VMM.

6. In **Host groups that can use this network site**, select each host group to which you want to make the logical network available.

7. In **Associated VLANs and IP subnets**, select **Insert Row** to specify the settings that you want to assign to the network site. If you select **PVLAN**, you need to add a **Secondary VLAN** for each VLAN. Ensure that the VLANs and subnets are available in your physical network. If you leave the **VLAN** field empty, VMM assigns a value of 0 to indicate that VLANs aren't used. In trunk mode, 0 indicates a native VLAN.

8. If you created network sites and associated one or more IP subnets with them (when you're not using DHCP), you can create static IP address pools from those subnets. Then VMM can automatically allocate IP addresses to VMs in the network site. IP pools can be created within the **Create Logical Network Wizard**.

To set up an IP address pool on a logical network, follow these steps.

Next steps

- Create a VM network.
- Set up static IP address pools in the VMM fabric.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Set up VM networks in the VMM fabric

Article • 08/21/2024

This article describes how to create VM networks based on System Center Virtual Machine Manager (VMM) logical networks.

In a virtualized network environment, we want to abstract virtual machines from the underlying logical network. VM networks help you do this. VM networks are abstract objects that act as an interface to logical networks.

- A logical network can have one or more associated VM networks.
- If a logical network isn't isolated, then a single VM network will be associated with it.
- If a logical network is isolated, then multiple VM networks can be associated with it. These multiple VM networks allow us to use networks for different purposes. For example, as a provider you might want to host workload for multiple tenants on a single logical network, using a separate VM network for each tenant. The type of VM network you set up depends on the isolation settings for the logical network:
  - **Network virtualization**: If the logical network is isolated using network virtualization, you can create multiple VM networks for a logical network. Within a VM network, tenants can use any IP addresses they want for their VMs regardless of the IP addresses used on other VM networks. Tenants can also configure some network settings.
  - **VLAN**: If the logical network is isolated using VLAN or PVLAN, you'll create on VM network for each network site and VLAN in the logical network.
  - **No isolation**: If the logical network is configured without isolation, you'll create a single VM network linked to a logical network.

Before you start

- In some circumstances, you'll need to create a static IP address pool on the VM network after you've created it. Learn more.
- By default, machines within a specific VM network can connect to each other. If your VM network will connect to other networks, you can configure it with a gateway (network service). If you want to add a gateway to the VM network, you'll need to create it. Learn more.

Create a VM network (network virtualization)

1. Select **VMs and Services** > **VM Networks** > **Home** > **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. In **Isolation**, select **Isolate using Hyper-V network virtualization** and verify the IP address protocols.
4. In **VM Subnets**, select **Add** and specify subnets for the VM network using CIDR notation. You can add multiple subnets.
5. In **Connectivity**, if you see the message **No network service**, it specifies a gateway has been added to VMM and you can select **Next**. If you don't see the message, specify the gateway (network service) options:
   - **No connectivity**: Leave all checkboxes cleared if the virtual machines on this VM network will communicate only with other virtual machines on this VM network. You can also leave clear if you plan to configure the gateway later.
   - **Connect to another network through a VPN tunnel**: Select this option if the virtual machines on this VM network will communicate with other networks over VPN. If the device will use the Border Gateway Protocol, enable this protocol. Select the VPN gateway device that you want to use. Confirm the settings. If the **VPN Connections** or Border Gateway Protocol pages appear, complete the settings based on information from the VPN admin. If you selected the checkbox for Border Gateway Protocol, the Border Gateway Protocol page also appears.
   - **Connect directly to an additional logical network**: Select this option if the virtual machines on this VM network will communicate with other networks in this data center. Select either direct routing or NAT. Select the gateway device you want to use and confirm the settings.
6. In **Summary**, verify settings and select **Finish**. Verify the network in **VM Networks and IP Pools**.

Create a VM network (VLAN/PVLAN)

1. Select **VMs and Services** > **VM Networks** > **Home** > **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. In **Isolation Options**:

   - Select **Automatic** if you want VMM to automatically configure the isolation settings for the VM network. VMM will select a network site and subnet VLAN based on those available in the logical network.
   - Select **Specify a VLAN** to configure isolation manually.

   > ⓘ Note
   >
   > - Tenant administrators can only select the **Automatic** option.

4. In **Summary**, verify settings and select **Finish**. Verify the network in **VM Networks and IP Pools**.

Create a VM network (no isolation)

1. Select **VMs and Services** > **VM Networks** > **Home** > **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. In **VM Networks and IP Pools**, check for a VM network with the same name as the logical network you want to give direct access to. If one exists, it probably indicates that the VM network was created automatically when you created the logical network. You can check whether the VM network provides direct access by selecting its properties. If **Name** and **Access** are the only tabs, it provides direct access.
4. If there's no existing VM network, select **Home** > **Create** > **Create VM Network**.
5. In **Summary**, verify settings and select **Finish**. Verify the network in **VM Networks and IP Pools**.

Set up static IP address pools in the VMM fabric

Article • 08/21/2024

This article describes how to set up static IP address pools for logical and VM networks in the System Center Virtual Machine Manager (VMM) networking fabric.

> ⓘ **Note**
>
> While creating a static IP address pool in VMM, don't use the IP address range (that is managed by the pool) outside of VMM, in the same environment.

When you set up the logical network, you'll need to configure a static IP address pool if you're not using DHCP. In some circumstances you'll need to create IP address pools on the logical network only, and in others you'll need to create the pool on both the logical and VM networks:

- **Pool on logical and VM network**: If you configure your logical network for network virtualization, you'll need to create IP address pools on the logical network and the VM network.
- **Pool on logical network only**: If you're using VLAN or no isolation, you can use DHCP or create IP address pools on the logical network only. They'll automatically become available on the VM network.
- **Imported address pools**: If you're using external networks through a vendor console, your IP address pools will be imported from the vendor, and you don't need to create them in VMM.

Create a static address pool for a logical network

1. In **Logical Networks and IP Pools**, select the logical network > **Home** > **Create** > **Create IP Pool**.

2. In **Create Static IP Address Pool Wizard** > **Name**, specify a name and description. Ensure that the correct logical network is indicated.

3. In **Network Site**, select to use an existing site and select the IP subnet or create a new site.

- For an existing site, select the site and IP subnet from which to create the pool.
- For a new site, specify the site name, IP subnet to assign to the site, and VLAN information if relevant. Select the host groups that can access this site and the logical network.

4. If you're using network virtualization, you can use the pool to support multicasting or broadcasting. To do this, select **Create a multicast IP address pool** and select the IP subnet you want to use. To use multicasting or broadcasting, ensure that:

   - The logical network must have network virtualization enabled.
   - The IP protocol setting for the VM network must match the IP protocol settings for the underlying logical network. You can't view the protocol setting in the VMM console after you've created it. You'll need to run **Get-SCVMMNEtwork -Name <VM network name> | Format -List Name, Isolation Type, PoolType** to see it.
   - After you've configured this feature, multicast and broadcast packets on the VM network will use the IP addresses from the multicast IP address pool. Each subnet in the VM network will consume one IP address from the multicast pool.

5. In **IP address range**, enter the start and end address for the pool. They must be contained within the subnet. In **VIPs and reserved IP addresses**, specify the IP address range you want to reserve for VIPs. VIPS are used during the deployment of a service in a load-balanced service tier. VMM automatically assigns a VIP to the load balancer from the reserved VIP address range.

6. In **Gateway**, select **Insert** if you want to specify one or more default gateways and the metric. The default gateway address must be in the same subnet range as the IP address pool but doesn't need to be part of the pool.

7. In **DNS**, specify DNS information, including DNS servers, the default DNS suffix for the connection, and the list of DNS search suffixes.

8. In **WINS**, select **Insert** if you want to enter the IP address of a WINS server. You can also select whether to enable NetBIOS over TCP/IP. This isn't recommended if the address range is made up of public addresses.

9. In **Summary**, verify the settings and select **Finish**. When the job shows as **Completed**, verify the pool in **Logical Networks and IP Pools**.

Set up an IP address pool on a VM network

1. Select **VMs and Services** > **VM Networks** > **Home** > **Show** > **VM Networks** > **VM Network**.
2. In **VM Networks and IP Pools**, select the VM network > **Create** > **Create IP Pool**.
3. In **Create Static IP Address Pool Wizard** > **Name**, specify a name and description. Ensure that the correct logical network is indicated. Ensure the correct VM network and subnet is selected.
4. In **IP address range**, enter the start and end addresses for the pool. You can create multiple IP address pools in a subnet but the ranges mustn't overlap. In **Reserved IP addresses**, specify any range you want to reserve for other purposes.
5. In **Gateway**, select **Insert** if you want to specify one or more default gateways and the metric. The default gateway address must be in the same subnet range as the IP address pool but doesn't need to be part of the pool.
6. In **DNS**, specify DNS information, including DNS servers, the default DNS suffix for the connection, and the list of DNS search suffixes. For virtual machines that will join an Active Directory domain, we recommend that you use Group Policy to set the primary DNS suffix. This will ensure that when a Windows-based virtual machine is set to register its IP addresses with the primary DNS suffix, a Windows-based DNS server will register the IP address dynamically. Additionally, the use of Group Policy enables you to have an IP address pool that spans multiple domains. In this case, you would not want to specify a single primary DNS suffix.
7. In **WINS**, select **Insert** if you want to enter the IP address of a WINS server. You can also select whether to enable NetBIOS over TCP/IP. This isn't recommended if the address range is made up of public addresses.
8. In **Summary**, verify the settings and select **Finish**. When the job shows as **Completed**, verify the pool in **Logical Networks and IP Pools**.

Release inactive addresses from the static address pool

You can release inactive addresses. When you do, VMM returns the address to the static IP pool, or MAC address pool and considers it available for reassignment. An address is considered inactive if:

- A host that was assigned a static IP address through the bare-metal deployment process is removed from VMM management. When you remove the host, any IP and MAC addresses that were statically assigned to virtual machines on the host are also marked as inactive.
- A virtual machine goes into a missing state because it was removed outside VMM.

1. Release the IP addresses:

   - To release addresses in a pool in a logical network, select **Logical Networks and IP Pools**, expand the logical network, and select the IP address pool.

- To release addresses in a pool in a VM network, select **Logical Networks and IP Pools**, expand the VM network, and select the IP address pool.

2. Select **Home** > **Properties** > **Inactive addresses**, and select the inactive IP addresses that you want to release.

Next steps

Add a network virtualization gateway to the VMM fabric.

Add a network virtualization gateway to the VMM fabric

Article • 08/21/2024

Read this article to learn about setting up network virtualization gateways in the System Center Virtual Machine Manager (VMM) networking fabric.

By default, if you're using isolated VM networks in your VMM fabric, VMs associated with a network can only connect to machines in the same subnet. If you want to connect VMs further than the subnet, you'll need a gateway.

Network virtualization

You set up network virtualization so that multiple VM networks are overload on the VMM logical networks that model your physical network topology and thus decouple the VM networks from the physical network infrastructure. Network virtualization uses NVGRE (Network Virtualization using Generic Routing Encapsulation) to virtualize IP addresses. Review the following to learn more about NVGRE.

To figure out whether you need a network virtualization gateway in your network, consider:

- Do you need to connect from VMs in isolated VM networks to other on-premises apps?
- Do you need to connect from isolated VMs to the Internet?
- Do you need to connect from isolated VM networks to shared services such as DNS?

You can set up your gateway in many ways depending on your requirements:

- Connectivity to a public network can be achieved through NAT.
- Connectivity to an on-premises network is over a VPN tunnel (with or without Border Gateway Protocol (BGP))
- Direct routing without NAT can be used for connectivity between different VM networks.

Prerequisites

- **Provider software**: If you want to use a non-Windows gateway device, you'll need the provider and an account with permissions to configure the gateway. You install the provider on the VMM server. If certificates are required (for example, if the gateway is in an untrusted domain), you'll need to be able to view thumbprint information for those certificates.

- **Windows Server gateway**: If you want to configure a gateway running Windows Server, you can use a predefined template available from the Microsoft Download Center.

- **Logical networks**: You need logical networks (you'll need more than one if you want the gateway to connect from VM networks in one logical network to VM networks in another).
- **Remote VPN settings**: If you want to connect the gateway to a remote VPN server, you'll need:
  - The remote server IP address and information about on-premises subnets or the BGP address, if relevant.
  - You'll need to identify how you'll authenticate with the remote VPN server. If it uses a preshared key, you can authenticate with a Run As account and specify the shared key as the password. Or you can authenticate with a certificate. The certificate can be either a certificate that the remote VPN server selects automatically or a certificate that you've obtained and placed on your network.
  - Check whether you need specific VPN connection settings (encryption, integrity checks, cipher transforms, authentication transforms, Perfect Forward Secrecy (PFS) group, Diffie-Hellman group, and VPN protocol) or you can use the default settings.

Add a Windows Server Gateway

The service template provides a highly available Windows Server Gateway deployment in active-standby mode.

1. You'll need to download the template from the Download Center.

2. The download is a compressed zip file. You'll need to extract the file. Files include a user guide, two service templates, and a custom resource folder (a folder with a .cr extension) that contains files required for the service templates.
3. You'll need to decide which template to use, and then follow the instructions in the Quick Start Guide. The guide includes prerequisites for the template deployment, and instructions for setting up logical networks, creating a scale-out file server, preparing virtual hard disks for the gateway VM, and copying the custom resource file to the library. After you've set up the infrastructure, it describes how to import and customize the template and how to deploy it. There's also troubleshooting information if issues arise.

Add a non-Windows gateway

> ⓘ **Note**
>
> You'll need to install the provider software on the VMM management server and add the gateway to the fabric. Obtain the provider software. You can review a list of supported providers in **Settings** > **Configuration Providers**.

Use the following procedure to add the non-Windows gateway:

1. Select **Fabric** > **Network Service**. Right-click and select **Add Network Service** to open the Network Service wizard. Network services include gateways, virtual switch extensions, network managers, and top-of-rack (TOR) switches. Or on Home, select **Add Resources** > **Network Service**.
2. In **Add Network Service Wizard** > **Name**, specify a name and description for the gateway.
3. In **Manufacturer and Model**, select the required settings.
4. In **Credentials**, specify a Run As account with permissions in the domain to which the gateway is connected.
5. In **Connection String**, enter the string that the gateway must use. The string syntax is defined by the gateway vendor.
6. In **Certificates**, if listed, verify the thumbprints of the certificates match those installed on the gateway. Select to confirm that the certificates can be imported. If none is listed, the gateway probably doesn't need certificate authentication. If they're needed, ensure that they're installed correctly on the gateway.
7. In **Gather Information**, select **Scan Provider** to run the basic validation test against the gateway.
8. In **Host Group**, select one or more host groups to which the gateway will be available.
9. In **Summary**, review the settings and select **Finish**.
10. After the gateway is added, find its listing in **Network Services**, and right-click > **Properties** > **Connectivity**.
11. Select **Enable front end connection**, and select the gateway network adapter and network site that provides connectivity outside the enterprise datacenter or hosting provider. Select **Enable back end connection**, and select a gateway network adapter and network site in a logical network within the enterprise. The network must have network virtualization enabled, and the network site must have a static IP address.
12. When you create a VM network, you can assign the gateway to it and select the required connectivity options.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Set up port profiles in the VMM fabric

Article • 08/21/2024

Use this article to learn about and set up uplink port profiles and virtual network adapter port profiles in the System Center Virtual Machine Manager (VMM) networking fabric.

- **Uplink port profiles**: You can create uplink port profiles and then apply them to physical network adapters when you deploy switches. Uplink port profiles define the load balancing algorithm for an adapter and specify how to team multiple network adapters on a host that uses the same uplink port profile. This profile is used with the logical network that you associated with the adapter.
- **Virtual network adapter port profiles**. You apply virtual network adapter port profiles to virtual network adapters. These profiles define specific capabilities, such as bandwidth limitations and priority. VMM includes many built-in profiles.
- **Port classifications**: After creating a virtual network adapter port profile, you can create port classifications. Port classifications are abstractions that identify different types of virtual network adapter port profiles. For example, you could create a classification called FAST to identify ports that are configured to have more bandwidth and another one called SLOW with less bandwidth. Classifications are included in logical switches. Administrators and tenants can choose a classification for their VM virtual machine adapters. By default, VMM includes built-in classifications that map to the built-in virtual network adapter port profiles

Define uplink port profiles

Some guidelines for creating uplink port profiles:

- You need at least one uplink port profile for each physical network in your environment. If you do have a simple environment with a single physical network and all hosts are configured the same way with the same protocols for network adapter teaming, then you might only need a single uplink port profile. This is rare though. You'll probably need to scope or restrict certain logical networks to a specific group of hosts computer, and this need makes it useful to create multiple uplink port profiles.
- You need to define uplinks for each physical location that has its own VLAN and IP subnets.
- If you plan to restrict or otherwise scope logical networks to a specific set of host computers, you'll need to create uplinks for each group of computers.
- You need separate uplink port profiles for groups of computers (in each physical location) that have different connectivity requirements or use different teaming

protocols.

- You might consider creating separate uplinks for networks that don't or won't support network virtualization.
- Network sites that will be included in a profile must be scoped to the same group of host computers. If they aren't, you'll receive an out-of-scope error when you try to apply it to a computer that isn't a member of the host groups defines in every one of the network sites included in the uplink profile.
- You must try to ensure that each of the network sites that you add to an uplink port profile refers to a different logical network. If you do otherwise, all the VLANs and IP subnets defined in those network sites will be associated with the logical network on any host computer on which the uplink port profile is applied. If you're not using VLAN isolation, the host computer has no way of establishing which of the range of possible VLANs and IP subnets will be needed to allow VMs connected to the logical network.
- You can create an uplink port profile that contains references to multiple network sites (and hence logical networks). You must ensure that the VLANs and IP addresses in each of the selected sites must be valid (routable) from the physical network adapter to which the port profile has been applied.
- When you apply the profile to a physical network adapter, these network sites determine the set of logical networks that must be associated with the physical adapter, and the VLANs and IP subnets that will be allocated to VMs and services that connect to those logical networks.

Create an uplink 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 load balancing and teaming settings:

    - **Load balancing**: **Host Default** is the default setting and this will either distribute network traffic based on the Hyper-V switch port identifier of the source VM or use a **Dynamic** loading balancing algorithm, depending on what the Hyper-V host supports. You can also select:
        - **Hyper-V port**: Distributes network traffic according to the Hyper-V switch port identifier of the source VM.
        - **Transport ports**: Uses the source and destination TCP ports and the IP addresses to create a hash and then assigns the packets that have the hash value to one of the available network adapters.

    - **IP addresses**: Uses the source and destination IP addresses to create a hash and then assigns the packets that have the hash value to one of the available network adapters.
    - **MAC addresses**: Uses the source and destination MAC addresses to create a hash and then assigns the packets that have the hash value to one of the available network adapters.

  - **Teaming**: **Switch Independent** is the default setting, and this specifies that physical network switch configuration isn't needed for the NIC team. The network switch isn't configured and so allows network adapters within the team to be connected to multiple (non-=trunked) physical switches. You can also select:
    - **LACP**: Use the LACP protocol to dynamically identify links that are connected between the host and a given switch.
    - **Static teaming**: Configure both the switch and host to identify which links form the team.

3. In **Network Configuration**, select one or more network sites for this uplink port profile to support. Uplink port profiles contain a list of network sites with each network site representing a link to a different logical network. Select **Enable Hyper-V Network Virtualization** if you want to enable network virtualization to deploy multiple VM networks on a single physical network. You must only do this if the logical network is configured for network virtualization with **Allow new VM networks created on this logical network to use network virtualization** enabled.

4. In **Summary**, review the settings and select **Finish**.

After you create an uplink port profile, the next step is to add it to a logical switch, which places it in a list of profiles that're available through that logical switch. When you apply the logical switch to a network adapter in a host, the uplink port profile is available in the list of profiles, but it isn't applied to that network adapter until you select it from the list. This not only helps you to create consistency in the configurations of network adapters across multiple hosts but also enables you to configure each network adapter according to your specific requirements.

Create a virtual network adapter port profile

1. Select **Fabric** > **Home** > **Show** > **Fabric Resources**. Select **Fabric** tab > **Networking** > **Port Profiles** > **Home** > **Create** > **Hyper-V Port Profile**.

2. In **Create Hyper-V Port Profile Wizard** > **General** enter a name and description and select **Uplink Port Profile**.

3. In **Offload Setting**, specify a setting for offloading traffic:

   - **Enable virtual machine queue (VMQ)**: Packets destined for a virtual network adapter are delivered directly to a queue for that adapter, and they don't have to be copied from the management operating system to the virtual machine. The physical network adapter must support VMQ.
   - **Enable IPsec task offloading**: Some or all of the IPsec computational work is shifted from the computer's CPU to a dedicated processor on the network adapter. The physical network adapter and the guest operating system must support it.
   - **Enable single-root I/O virtualization**: A network adapter can be assigned directly to a virtual machine. This maximizes network throughput while minimizing network latency and minimizing the CPU overhead that is required to process network traffic. The physical network adapter and drivers in the management operating system and guest operating system must support it. If you want to use SR-IOV, you'll need to enable it in the port profile (in **Offload** settings) and in the logical switch (**General** settings) that includes the port profile. It must be configured correctly on the host when you create the virtual switch that brings port settings and the logical switch you want to use on the host together. In the virtual switch, you attach the port profile to the virtual switch using a port classification (either the default SR-IOV classification provided by VMM or a custom one)

4. In **Security Settings**, specify:

   - **Allow MAC spoofing**: Allows a virtual machine to change the source MAC address in outgoing packets to an address that isn't assigned to that virtual machine. For example, a load-balancer virtual appliance might require this setting to be enabled.
   - **Enable DHCP guard**: Helps protect against a malicious virtual machine that represents itself as a DHCP server for man-in-the-middle attacks.
   - **Allow router guard**: Helps protect against advertisement and redirection messages that are sent by an unauthorized virtual machine that represents itself as a router.
   - **Allow guest teaming**: Allows you to team the virtual network adapter with other network adapters that are connected to the same switch.
   - **Allow IEEE priority tagging**: Allows you to tag outgoing packets from the virtual network adapter with IEEE 802.1p priority. These priority tags can be used by Quality of Service (QoS) to prioritize traffic. If IEEE priority tagging isn't allowed, the priority value in the packet is reset to 0.
   - **Allow guest specified IP addresses**: Affects VM networks using network virtualization. The VM (guest) can add and remove IP addresses on this virtual

network adapter. This can simplify the process of managing virtual machine settings. Guest-specified IP addresses are required for virtual machines that use guest clustering with network virtualization. The IP address that a guest adds must be within an existing IP subnet in the VM network.

5. In **Bandwidth Settings**, specify the minimum and maximum bandwidths that are available to the adapter. The minimum bandwidth can be expressed as megabits per second (Mbps) or as a weighted value (from 0 to 100) that controls how much bandwidth the virtual network adapter can use in relation to other virtual network adapters.

> ⓘ **Note**
>
> If bandwidth settings aren't used, SR-IOV is enabled on the port profile and the logical switch that contains the port profile.

6. In **Summary**, review the settings and select **Finish**.

After creating a port profile, you can create a port classification.

Create port classifications for virtual network adapter port profiles

1. Select **Fabric** > **Home** > **Show** > **Fabric Resources**. Select the **Fabric** tab > **Networking** > **Port Classifications** > **Home** > **Create** > **Port Classification**.
2. In **Create Port Classification Wizard** > **Name**, specify a classification name.

Next steps

Set up logical switches.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up logical switches

Article • 08/21/2024

This article describes how to create logical switches in the System Center Virtual Machine Manager (VMM) fabric.

How to create logical switches

This article describes how to create logical switches in the System Center Virtual Machine Manager (VMM) fabric, convert a host virtual switch to a logical switch, and set up virtual switch extensions if you need them.

A logical switch brings virtual switch extensions, port profiles, and port classifications together so that you can configure each network adapter with the settings you need and have consistent settings on network adapters across multiple hosts. You can team multiple network adapters by applying the same logical switch and uplink port profile to them.

Set up virtual switch extensions

You install switch extensions on the VMM server and then include them in a logical switch. There are a few types of switch extensions:

- **Monitoring extensions** can be used to monitor and report on network traffic, but they can't modify packets.
- **Capturing extensions** can be used to inspect and sample traffic, but they can't modify packets.
- **Filtering extensions** can be used to block, modify, or defragment packets. They can also block ports.
- **Forwarding extensions** can be used to direct traffic by defining destinations, and they can also capture and filter traffic. To avoid conflicts, only one forwarding extension can be active on a logical switch.

You can set up a virtual switch extension manager (network manager) if you want to manage extensions using a vendor management console and the VMM console together.

Set up a virtual switch extension manager

1. Obtain the provider software from your vendor and install the provider on the VMM management server. If you have a cluster, install it on all the nodes.
2. Select **Fabric** > **Home** > **Show** > **Fabric Resources** > **Networking** > **Switch Extension Managers**.
3. In **Add Virtual Switch Extension Manager Wizard** > **General**, specify the manufacturer and enter the connection string. For example, myextmanager1.contoso.com:443. The exact syntax is defined by the vendor. Specify the account you want to use to connect to the resource.
4. In **Host Groups**, specify the host groups for which you want to use the extension manager.
5. In **Summary**, review settings and select **Finish**. Check that the extension appears in the **Virtual Switch Extension Managers** pane.

Set up a logical switch

> ⓘ **Note**
>
> Ensure you've at least one uplink port profile before you begin.

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
   - Provide a description (optional).

5. In **Uplink Mode**, select:

   - **Embedded Team** - if you're using Windows Server 2016 or later
   - **Team** - if you're using Windows Server 2012 and want to use NIC teaming
   - **No Uplink Team** - if you're not using any teaming.

   Embedded Team is the default Uplink mode.

6. In **Settings**, select the minimum bandwidth mode. If you've deployed Microsoft network controller, you can specify that it must manage the switch. If you enable this setting, you won't be able to add extensions to the switch.

- **Weight** - Weight is the default minimum bandwidth mode. Weight specifies a percentage of bandwidth rather than a specific number of bits per second. Minimum bandwidth is a value ranging from 1 to 100.
- **Default** - The system sets the mode to **Weight** if the switch isn't IOV enabled, or **None** if the switch is IOV enabled.
- **Absolute** - Minimum bandwidth will be in bits per second.
- **None** - Minimum bandwidth is disabled on the switch. Users can't configure it on any network adapter that is connected to the switch.

7. Enable SR-IOV if you need to. SR-IOV enables virtual machines to bypass the switch and directly address the physical network adapter. If you want to enable:

   - Ensure you've SR-IOV support in the host hardware and firmware, the physical network adapter, and drivers in the management operating system and in the guest operating system.
   - Create a native port profile for virtual network adapters that is SR-IOV enabled.
   - When you configure networking settings on the host (in the host property called Virtual switches), attach the native port profile for virtual network adapters to the virtual switch by using a port classification. You can use the SR-IOV port classification that is provided in VMM or create your own port classification.

8. In **Extensions**, if you're using virtual switch extensions, select them and arrange the order. Extensions process network traffic through the switch in the order you specify.

> ⓘ **Note**
>
> Only one forwarding extension can be enabled. None of the extensions are enabled by default.

9. In **Virtual Port**, add one or more port classifications and virtual network adapter port profiles. Every Port Classification must be mapped to a Port Profile. You can view Port Classification to Port Profile mapping on the **Virtual Port** screen.

10. In **Uplink**, add an uplink port profile, or create a new one. When you add an uplink port profile, it's placed in a list of profiles that are available through that logical switch. However, when you apply the logical switch to a network adapter in a host, the uplink port profile is applied to that network adapter only if you select it from the list of available profiles.

If *Uplink* is chosen as Embedded Team (Switch Embedded Team or SET), then only Hyper-V Port and Dynamic load balancing algorithms are supported. Hyper-V Port is the default load balancing algorithm. If *Uplink* mode is chosen as Embedded Team, then Hyper-V Port is the recommended load balancing algorithm; Dynamic isn't recommended.

11. In **Summary**, review the settings and select **Finish**. Verify if the switch created appears in **Logical Switches**.

Convert virtual switch to logical switch

If a host in the VMM fabric has a standard virtual switch with or without SET, you can convert it to use as a logical switch.

> ⓘ **Note**
>
> - Before you can convert, you need a logical switch in place with specific settings.
> - You must be a member of the Administrator user role, or a member of the Delegated Administrator user role, where the management scope includes the host group in which the Hyper-V host is located.

Compare switch settings

1. Record if NIC Teaming (LBFO) or SET is being used on the host.

2. If you're using NIC teaming on the host, record teaming and load balancing settings by running the PowerShell commandlet *Get-NetLbfoTeam*.

3. In **Hyper-V Manager**, right-click the host > **Virtual Switch Manager**. Select the virtual switch and verify whether **Enable single-root I/O virtualization (SR-IOV)** is selected. Close Hyper-V Manager.

4. In the VMM console > **Fabric** > **Servers** > **All Hosts**, right-click the host > **Properties**.

5. In **Virtual Switches**, note the properties, including logical network and minimum bandwidth mode.

6. In **Fabric** > **Networking** > **Logical Switches**, right-click the logical switch that you want to convert the host configuration to and select **Properties**.

7. In **Logical Switches**, record the information:

    - In **General**, record the uplink mode, whether SR-IOV is enabled, and minimum bandwidth mode.
    - In **Extensions**, note whether any forwarding extensions have been added to the logical switch.
    - In **Virtual port**, record the names of the port profiles that are listed. Ensure to note if one of them has SR-IOV in the name.
    - In **Uplinks**, record the network sites, whether uplink mode is teamed, the load balancing algorithm, and teaming mode.

8. In **Fabric** > **Networking**, select **Port Profiles**. For any relevant port profiles, select **Properties**. In **Offload Settings**, see if **Enable Single-root I/O virtualization** is checked.

9. Now compare the recorded information that you recorded for the logical switch and port profiles, with the virtual switch information.

10. Review the following table to see whether you can convert the host to use the logical switch.

Expand table

Item	Conversion
SR-IOV	The SR-IOV setting (enabled or disabled) must be the same in the logical switch as it's in the virtual switch. If SR-IOV is enabled, it must be enabled in the logical switch itself, and in at least one virtual network adapter port profile within the logical switch.
Uplink mode **Load balancing algorithm** **Teaming mode**	The **Uplink mode** setting must match. If the uplink mode is **Team**, then the **Load balancing algorithm** and **Teaming mode** must also match.
Minimum bandwidth mode	Must match.
Network sites	The logical switch must be configured for the correct network sites (in the correct logical network) for this host.

11. If the settings in the logical switch don't match as described in the table, you need to find or create a logical switch that does match.

Convert a host to use a logical switch

> ⓘ **Note**
>
> - The conversion will not interrupt network traffic.
> - If any operation in the conversion fails, no settings will be changed and the switch will not be converted.

1. In VMM, select **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 to which you want to convert the host. Select the uplink port profile to use and select **Convert**.
4. The **Jobs** dialog box might appear, depending on your settings. 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.

Next steps

Apply network settings on a host with a logical switch.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up MAC address pools in the VMM fabric

Article • 08/21/2024

This article provides information about System Center Virtual Machine Manager (VMM) default MAC addresses and describes how to create and manage a custom MAC address pool.

VMM uses static MAC address pools to automatically generate and assign MAC address to VMs. This article describes default MAC address pools in the VMM fabric and explains how to create custom pools.

Default MAC address pool settings:

Expand table

MAC pool name	Environment	Default range
Default MAC address pool	Hyper-V	00:1D:D8:B7:1C:00 – 00:1D:D8:F4:1F:FF
Default VMware MAC address pool	ESX/ESXi	00:50:56:00:00:00 – 00:50:56:3F:FF:FF

Before you start

Before you create a custom MAC pool, ensure that:

- If you want to divide one of the default pools into smaller custom pools, you must first delete the default MAC address pool or the default VMware MAC address pool. You must delete the default pool to avoid duplicate MAC address assignments.
- The first three octets of the beginning and ending MAC address must be the same.
- You must enter a valid hexadecimal value between 00 and FF.
- The ranges that you specify can't overlap.
- The address range must not have the multi-cast bit set to 1. For example, you can't use addresses that start with X1, X3, X5, X7, X9, XB, XD, or XF, where X is any value.
- To avoid conflicts with addresses reserved by Microsoft, VMware, and Citrix, don't use the following prefixes:
  - Reserved for Microsoft: 00:03:FF; 00:0D:3A; 00:12:5A; 00:15:5D; 00:17:FA; 00:50:F2; 00:1D:D8 (except for the 00:1D:D8:B7:1C:00 – 00:1D:D8:F4:1F:FF range that is reserved for VMM)

- Reserved for VMware: 00:05:69; 00:0C:29; 00:1C:14; 00:50:56 (except for the 00:50:56:00:00:00 – 00:50:56:3F:FF:FF range that is reserved as the default VMware static range)

Create a custom pool

1. Select **Fabric** > **Networking** > **MAC Address Pools** > **Home** > **Show** > **Fabric Resources** > **Create** > **Create MAC Pool**.
2. In **Create MAC Address Pool Wizard** > **Name and Host Group**, specify a name and description. In **Host Group**, select the host groups that must use the pool.
3. In **MAC Address Range**, specify the start and end addresses.
4. In **Summary**, review the settings and select **Finish**. When the job shows as **Completed**, verify pool in **MAC Pools**.

Release IP addresses

In some circumstances, you might want to remove addresses from the MAC pool. For example, if a host that was assigned an IP address during bare metal deployment is removed from VMM management or if a VM goes into a missing state because it was removed outside VMM.

1. Select **Fabric** > **Networking** > **MAC Address Pools** > **Home** > **Show** > **Fabric Resources**.
2. In **MAC Pools**, select the pool you want to modify > **Properties**.
3. In **Inactive addresses**, select the addresses you want to release.

Next steps

Learn about creating an IP address pool.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Integrate load balancing with VMM service templates

Article • 08/22/2024

Read this article to learn about integrating Windows network load balancing (NLB) and hardware load balancers with System Center Virtual Machine Manager (VMM) service templates.

Service templates group VMs together to provide an app. They contain information about a service, including the VMs that are deployed as part of the service, the applications installed on VMs, and the network settings that must be used. You can add VM templates, network settings, applications, and storage to a service template.

Service templates can be single or multi-tier. A single tier service contains one VM used as a specific app. A multi-tier service contains multiple VMs. Learn more.

Set up load balancing for a service tier

You can add a load balancer to load balance requests to VMs in a service tier. You can use a hardware load balancer or NLB for round robin balancing.

To add a load balancer, you'll need to do the following:

- Ensure you have logical networks configured. The logical networks must have associated network sites. Those network sites must have one or more associated subnets from which you can create static IP address pools. In addition, associate each network site with the host group where the service will be deployed.
- Create an IP address pool for the logical networks. The IP pool must contain a reserved range of virtual IP addresses that can be assigned to the load balancer. You must set up the static IP address pools for the load balancer and for the virtual machines behind the load balancer. These can be from the same pool or from different pools, but you'll need both VIPs and IP addresses for the virtual machines.
- Create VM networks on top of logical networks.
- Create VIP templates: A virtual IP (VIP) template contains load balanced settings for a specific type of network traffic. After you create a VIP template, you can specify it when you set up load balancing in a service template.
- Set up a hardware load balancer: If you want to enable hardware load balancing in a service template, there are many prerequisites you'll need to prepare.
- Set up NLB: If you don't want to use a hardware load balancer, you can use NLB. There are some requirements and limitations.

Create VIP templates

1. In the VMM console, select **Fabric** > **Networking** > **VIP Templates**.

2. Select **Home** > **Show** > **Fabric Resources** > **Create** > **Create VIP Template**.

3. In the **Load Balancer VIP Template Wizard** > **Name**, specify the template name and description. In **VIP port**, specify the port that will be used for the type of network traffic you want to balance. For example, 443 for HTTPS traffic. In **Backend port**, specify the portal on which the backend server is listening for requests.

4. In **Type**, do the following:

   - To use NLB, select **Microsoft** in the manufacturer list and **Microsoft network controller** in **Model**.
   - To use a hardware load balancer, select **Generic** to create a template for any supported hardware load balancer. Select **Specific** to create a template for a specific load balancer and specify the manufacturer and model.

5. In **Protocol**, select the protocol for which you want to create the VIP template.

   - If you select **HTTPS**, you'll need to specify where the traffic terminates.
   - Select **HTTPS passthrough** to pass the traffic to the VM without decrypting it.
   - Select **HTTPS terminate** to terminate and decrypt the HTTPS traffic at the load balancer. This option gives the load balancer more information, such as cookies and headers. To use this option, specify the subject name of a certificate on the load balancer that can be used for HTTPS authentication. With this option, you can enable **Re-Encrypt** to re-encrypt the HTTPS traffic from the load balancer to the VM.
   - Select **Custom** to specify **TCP**, **UDP**, or both.

6. In **Persistence**, select **Enable persistence** to make the client session sticky (affinity). This setting means that the load balancer will always try to direct the same client to the same VM. It's based on the specified source IP address and subnet mask, the destination IP address, and other parameters that vary depending on the protocol.

7. In **Health Monitors**, you can optionally specify that a verification must run against the load balancer at regular intervals. To add a health monitor, specify the protocol and the request. For example, entering the command GET? makes an HTTP GET request for the home page of the load balancer and checks for a header response. You can also modify the response type, monitoring interval, timeout, and retries.

ⓘ **Note**

The timeout must be less than the interval.

8. In **Load Balancing**, select which load balancing method you want to use. You can configure new connections to be directed based on the least connections or the fastest response time, using round robin, or using a custom method supported by the load balancer. If you're enabling NLB, select **Round Robin**.
9. On the **Summary** page, review the settings and select **Finish**. The **Jobs** dialog appears. Wait for a **Completed** status. Then verify that the template appears in the **VIP Templates** pane.

Set up a hardware load balancer

Set up a hardware load balancer as follows:

- **Get a configuration provider**: To add a supported hardware load balancer, you'll need to download and install a configuration provider available from the load balancer manufacturer. VMM currently supports Brocade ServerIron ADX load balancer provider and Citrix NetScaler load balancer provider. The provider is a VMM plug-in that translates VMM PowerShell commands to the load balancer API. After you've installed the provider, you must restart the VMM service (**net stop scwmmservice** > **net start scvmmservice**).
- **Set up an account**: Create a VMM Run As account with a username and password with permissions to configure the downloaded load balancer.
- **Add the load balancer to VMM**: Add a hardware load balancer to VMM using the Add Load Balancer Wizard.

Add the hardware load balancer to VMM

During the wizard, select the host groups for which the load balancer is available, specify the load balancer model, specify the address and port used to manage the load balancer, specify affinity to VMM logical network, select the configuration provider, and test the connection. You'll need to configure the hardware load balancer before you deploy a service. After the service is deployed, a load balancer can't be added.

1. Select **Fabric** > **Networking** > **Load Balancers** > **Fabric Resources** > **Home** > **Add** > **Add Resources** > **Load Balancer**.
2. In **Add Load Balancer Wizard** > **Credentials**, select the Run As account with the load balancer credentials.
3. In **Host Group**, select each host group where the service will be deployed. Hosts must be able to access the load balancer. In addition, a physical network adapter on the host must be configured to use the same logical network as the service tier.

4. In **Manufacturer and Model**, select the appropriate entries.
5. In **Address**, specify the **IP address** and **FQDN** or **NetBIOS** names of the load balancer. Specify the port on which the load balancer listens for requests.
6. In **Logical Network Affinity**, specify the affinity to logical networks.

> ⓘ Note
>
> - For frontend affinity, you'll select the logical network from which the load balancer obtains its VIP. The VIP is the IP address that's assigned to the load balancer when you deploy it in a service template.
> - For frontend affinity, based on the logical networks, VMM determines the static IP address pools that are accessible from both the load balancer and from the relevant host group.
> - When selecting logical networks for frontend affinity, the associated network site with the reserved VIP address range must be available to the host groups associated with the load balancer.
> - For backend affinity, you'll select the logical networks to which you want to make the load balancer available for connections from the VMs in a service tier.

7. In **Provider**, select the load balancer provider. Select **Test** to check the configuration.
8. In **Summary**, verify the settings and select **Finish**. The **Job** dialog box appears. Wait for a **Completed** status and check in the **Provider** column that the provider is active.

Set up NLB

NLB is automatically included as a load balancer in VMM. As long as you've set up an NLB VIP template, no other action is required, but note that:

- NLB can't be used if VM networks are configured with network virtualization.
- NLB can't be used in service tiers running Linux VMs.

Enable load balancing

1. If the service template isn't open, select **Library** > **Templates** > **Service Templates** and open it.
2. Select **Actions** > **Open Designer**.

3. In the Service Template Designer, select the **Service Template Components** group > **Add Load Balancer**.
4. Select the load balancer object. You'll identify it with the VIP template name.
5. Select **Tool** > **Connector**. Select the **Server connection** associated with template and then select a **NIC** object to connect the load balancer to the adapter. In the NIC properties, check the address types and that the MAC address is static.
6. With the **Connector** enabled, select the **Client connection** associated with the load balance and then select a logical network object.
7. Save the service template in **Service Template** > **Save and Validate**.

Set up the hardware VIP for user access

When the service is deployed, VMM automatically selects a VIP from the reserved range in the static IP address pool and assigns it to the load-balanced service tier. To enable users to connect to the service, after the service is deployed, you need to determine the VIP and configure a DNS entry for it.

1. After the service is deployed, select **Fabric** > **Networking** > **Load Balancers**.
2. Select **Show** > **Service** > **Load Balancer Information for Services** and expand the service to see which VIP is assigned.
3. Request that the DNS administrator manually create a DNS entry for the VIP. The entry must be the name that users will specify to connect to the service. For example, servicename.contosol.com.

Next steps

You can also set up a software load balancer in a software defined networking (SDN) infrastructure in the VMM fabric.

Set up an IPAM server in the VMM fabric

Article • 08/21/2024

This article explains how to add an IP Address Management (IPAM) server to the System Center Virtual Machine Manager (VMM) networking fabric.

An IPAM server helps you to plan, track, and manage the IP address space used in your networks.

- With an IPAM server in the VMM fabric, the IP address settings that are associated with logical networks and VM networks in VMM are synchronized using settings stored on the IPAM server.
- As an administrator, you can use the IPAM server to configure and monitor logical networks and their associated network sites and IP address pools. You can also use the IPAM server to monitor the usage of VM networks that you've configured or changed in VMM.
- Tenants must continue to use the VMM server (not IPAM) to configure VM networks that use network virtualization. In other words, to control the address space that is typically controlled by tenants rather than by VMM administrators.

Before you start

- Ensure that you have an IPAM server. Learn more. The IPAM server can be running these versions of Windows Servers.
- Create or identify a domain account and set it to never expire. On the IPAM server, add the account to these groups:
- **IPAM ASM Administrators**: A local group that exists on all IPAM servers and provides permissions for IP address space management (ASM). For more information, see Assign Administrator Roles.
- **Remote Management Users**: A built-in group that provides access to WMI resources through management protocols, such as WS-Management through the Windows Remote Management service.
- Check that the time is synchronized on the IPAM and VMM servers. This depends on settings for the Windows Time Service. If you can't synchronize them, you'll need to update permissions on the IPAM software so that VMM can query the current time setting on the server. To do this, on the IPAM server, run **mimgmt.msc** to open the WMI Control (Local) snap-in. Right-click **WMI Control (Local)** >

Properties > **Security**. Navigate to **Root\CIMV2**, select the Security button Security and select the account you configured. For **Remote Enable**, select **Allow**.

- Verify the FQDN of the IPAM server to use as a connection string.
- Verify the names of the VMM host groups for which you want to use the IPAM server.
- The provider software for an IPAM server is included in VMM. You don't need to install it. You can review settings in **Settings** > **Configuration Providers**.
- If you want to use the IPAM server to delete a logical network, delete the IP address subnets assigned to that logical network, and don't delete the name associated with the **VMM Logical Network** field on the IPAM server. The two servers will then be able to synchronize correctly, and the logical network will be deleted. If you do delete the name associated with the **VMM Logical Network** field on the IPAM server, you must go to the VMM server and delete the network sites and the logical network. Then, after the two servers synchronize, the deletion will be complete.

Add an IPAM server to the fabric

1. Select **Fabric** > **Home** > **Show** > **Fabric Resources** > **Fabric** > **Networking** > **Network Service**. Network services include gateways, virtual switch extensions, network managers (which include IPAM servers), and top-of-rack (TOR) switches.
2. Select **Home** >**Add** > **Add Resources** > **Network Service**.
3. In **Add Network Service Wizard** > **Name**, specify a name and optional description.
4. In **Manufacturer and Model** > **Manufacturer**, select **Microsoft**, and select **Model** > **Microsoft Windows Server IP Address Management**.
5. In the **Credentials** page, specify the account you created.
6. In the **Connection String** page, in the **Connection string** box, enter the FQDN of the IPAM server. If you've configured a specific port on the IPAM server, end the string with the port number (for example, **:443**). If a port number isn't specified, the default port for the IPAM server is used.
7. In **Provider** > **Configuration provider** > **Microsoft IP Address Management Provider**, select **Test** to run basic validation tests with the provider. Results that say **Passed** or **Failed** indicate whether the provider works as expected. One possible cause of failure is insufficient permissions in the Run As account. Results that say **Implemented** and **Not implemented** are informational only, and indicate whether the provider supports a particular API.
8. In **Host Group**, select one or more host groups for which you want integration between the IPAM server and the VMM server.
9. In **Summary**, review the settings and select **Finish**. Check that the IPAM server is listed under **Network Services**. Right-click the server > **Refresh** to get the latest

settings.

10. On the IPAM server, to view the logical networks and related settings that were configured in VMM, navigate to **VIRTUALIZED IP ADDRESS SPACE**, and then to **Provider IP Address Space**. For each logical network, the IPAM server will have an address space (an overarching category that is found in IPAM, but not in VMM) with a name that is based on the name of the logical network. The logical network will be contained within the address space, with the name of the logical network displayed under the heading **VMM Logical Network**. To see the types of information that are stored in IPAM, expand the address space and select different views.

The following table can help you interpret some of the information that you see on the IPAM server:

Expand table

VMM name	IPAM name
Logical network	VIRTUALIZED IP ADDRESS SPACE Provider IP Address Space: **VMM Logical Network** column
Network site	VIRTUALIZED IP ADDRESS SPACE Provider IP Address Space: **Network Site** column
IP address subnet	IP Address Subnet (same name in IPAM as in VMM)
IP address pool	IP Address Range
VM network	VIRTUALIZED IP ADDRESS SPACE Customer IP Address Space: **VM Network** column

IP address reservation

IP reservation in IPAM is honored by VMM. Follow the steps below for reserving IP addresses.

1. In IPAM, right-click **IP Address Range** for IP address reservation.
2. Select **Edit IP Address Range** and a window opens.
3. In the opened window, there's a **Reservations** tab on the left.
4. In the **Reservations** tab, you can reserve IP addresses for reservation or whether to use them as VIPs.
5. Go to VMM console. Refresh the IPAM service in the network service section.
6. Now, you can see the reserved IP addresses reflected in the pool section of the logical network.

Next steps

Set up logical networks.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Set up the VMM storage fabric

Article • 08/22/2024

You can use System Center Virtual Machine Manager (VMM) to manage your physical and virtualized infrastructure. As part of that management, VMM can manage storage that you assign to virtual hosts and clusters and VMs.

- **Local and remote**: VMM recognizes both local and remote storage. Local is storage located on the VMM server or directly attached to it, commonly a disk drive on the server that's connected with inbuilt RAID or SAS JBOD connectivity. This type of dedicated host storage isn't shared and doesn't provide resilience or high availability.
- **Block and file-based**: VMM can manage block storage devices and file-based storage.

Block storage

Expand table

Feature	Details
Connection	VMM can manage block storage devices that connect using Fibre Channel, Serial Attached SCSI (SAS), or iSCSI (Internet SCSI). VMM can discover and manage iSCSI arrays with static, dynamic, or manual targets. You can use a Microsoft iSCSI target server as a storage device by installing its provider.
Protocols	VMM provides support for storage devices that use the SMI-S and SMP protocols. VMM uses Window Storage Management API (SMAPI) to manage block-based storage devices compliant with SMI-S or SMP specifications. VMM combines SMAPI and SMP to manage directly attached storage and external storage arrays. VMM combines SMAPI and the Storage Management service (which functions as an SMI-S client) to manage SMI-S storage devices. Vendors of storage devices with the SMI-S standard create SMI-S provides for their devices.

Feature	Details
Virtualization hosts	Storage configured in VMM can only be used for Hyper-V hosts and clusters.
Supported storage arrays	Specific storage arrays are supported in VMM. You can use other arrays, but there's no guarantee that you'll be able to manage all storage tasks in VMM. We recommend that you chat with your storage provider to determine VMM support.
Virtual fibre channel	If you want to use virtual Fibre Channel to give VMs direct access to Fibre Channel storage, you can manage this storage with VMM in these configurations. Single storage array connected to a single fabric (comprised of single or multiple switches) connected to a single vSAN. Single storage array connected to multiple fabrics (comprised of single or multiple switches per fabric) connected to a single vSAN. Multiple storage arrays connected to a single fabric (comprised of single or multiple switches) connected to a single vSAN. Multiple storage arrays connected to multiple fabrics (comprised of single or multiple switches per fabric) connected to multiple vSANs. This configuration provides dual-redundant paths to storage arrays. A vSAN can only include HBAs from a single fabric.

Set up block storage

The general process for setting up block-based storage in the VMM fabric is as follows:

1. Create storage classifications: You create storage classifications to group storage based on shared characteristics, often performance, and availability. Then instead of assigning specific storage devices to them, you assign storage to VMM host groups you assign a specific classification so that host groups can use any available storage device with the assigned classification. You don't have to create classifications before you add storage devices. You can create them during storage device discovery.
2. Add the storage: You add the storage as a resource in the VMM fabric. When you add the device, VMM automatically discovers any existing storage pools and logical units on the device. You can classify storage as you add it.
3. Configure storage and allocate capacity: After a storage array is managed by VMM, you can configure settings. You can specify how you want to use rapid provisioning

on the device (snapshots or cloning). You can add and modify storage pools and storage logical units (LUNs) in the pools. You can allocate capacity (either entire storage pools) or specific LUNs to one or more host groups.

4. Use the storage: After storage is allocated to a host group, you can use the storage for a specific host or cluster. When you add a host or cluster to a host group, the host and cluster can use storage associated with the group.

File storage

VMM can manage file storage that supports the SMB 3.0 protocol. SMB is supported by file shares on computers running Windows Server 2016 or later, and by non-Microsoft vendors of network-attached storage (NAS) devices.

- **Windows file server**: You can add a remote file server as a storage device or you can scale file-based storage Scale-Out File Server (SOFS).
- **Scaled-out file server (SOFS)**: SOFS provides a file server cluster in which storage is shared between the cluster nodes. Storage for SOFS can be a SAN (SAS, iSCSI, Fibre Channel) or can integrate with Storage Spaces Direct.
- **Storage Spaces Direct (S2D)**: S2D virtualizes storage by grouping disks into storage pools and creating virtual disks (storage spaces) from the pool capacity. In S2D, you can build highly available storage using local storage. This removes the need for remote SAN storage devices and enables the use of storage devices that weren't previously available, such as SATA SSD or NVMe flash. Learn more.
- **Storage replication**: VMM supports Windows Storage Replica for protecting data in a primary storage volume and replicating it to a secondary volume. Learn more.
- **Storage resources**: You can control access to shared storage on a SOFS or VM by setting storage quality-of-service (QoS) policies. These policies set maximum and minimum bandwidth for storage resources.

Set up file storage

The general process for setting up file storage in the VMM fabric is as follows:

1. **Add and discover storage**: You add the file server as a resource in the VMM fabric. When you add the device, VMM automatically discovers any file shares on the device. You can classify storage as you add it.
2. **Create storage classifications**: You create storage classifications to group file shares based on shared characteristics, often performance and availability. Then instead of assigning specific storage devices to VMM host groups, you assign a specific classification so that host groups can use any available storage with the

assigned classification. You don't have to create classifications before you add storage devices. You can create them during storage device discovery.

3. **Provision storage**: After a file server is managed by VMM, you can configure settings. For example, you can modify storage pools on a SOFS or create a file share.
4. **Allocate capacity**: After you have the storage set up, you can allocate capacity from the array. You allocate capacity by assigning file shares to one or more host groups.
5. **Use the storage**: After storage is allocated to a host group, you can use the storage for a specific host or cluster. When you add a host or cluster to a host group, the host and cluster can use storage associated with the group.
6. **Decommission storage**: VMM can decommission the storage it manages.

Learn more about setting up file storage in VMM.

Storage classifications

Storage classifications provide a layer of abstraction over specific storage devices. You group storage devices together based on their characteristics. For example, you can create:

- Bldg1Gold: A set of solid-state drives (SSDs) that you'll make available to users in building 1.
- Bldg1Silver: A set of SSDs and hard disk drives (HDDs) that you'll make available to users in building 1.
- Bldg2Gold: A set of SSDs that you'll make available to users in building 2.
- Bldg2Silver: A set of SSDs and HDDs that you'll make available to users in building 2.

After you've created classifications, you assign them to storage pools that include block or file-based storage. You can tweak classification settings for file shares within pools as required.

Monitor storage health

This functionality helps you to monitor the health and operational status of a storage pool, LUNs, and physical disks in the VMM fabric.

You can monitor storage health from VMM console **Fabric** page.

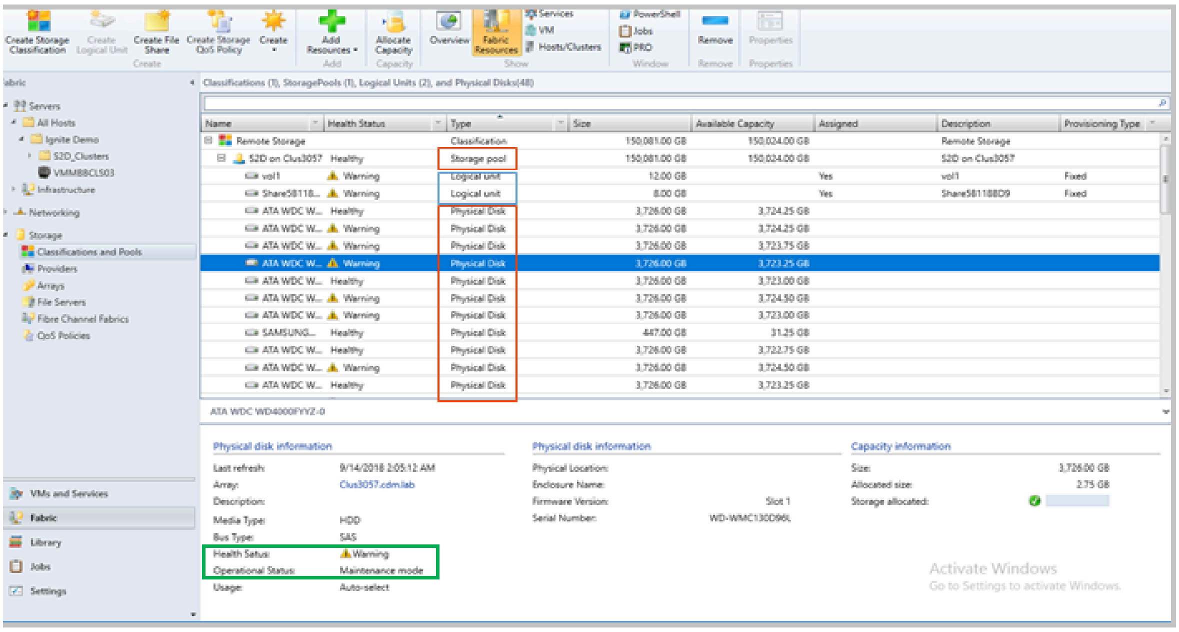
Follow these steps:

1. Go to VMM console, **Fabric** > **Storage** > **Classification and Pools**.

   The **Health Status** column displays the status of the storage pool, LUN, and physical disks.

2. To check the operational status, select a storage item.

   The information pane for the selected storage item displays the operational status as shown in the sample below:



Classifications (1), StoragePools (1), Logical Units (2), and Physical Disks(48)

Name	Health Status	Type	Size	Available Capacity	Assigned	Description	Provisioning Type
Remote Storage		Classification	150,081.00 GB	150,024.00 GB		Remote Storage	
S2D on Clus3057	Healthy	Storage pool	150,081.00 GB	150,024.00 GB		S2D on Clus3057	
vol1	⚠ Warning	Logical unit	12.00 GB		Yes	vol1	Fixed
Share58118...	⚠ Warning	Logical unit	8.00 GB		Yes	Share581188D9	Fixed
ATA WDC W...	Healthy	Physical Disk	3,726.00 GB	3,724.25 GB			
ATA WDC W...	⚠ Warning	Physical Disk	3,726.00 GB	3,724.25 GB			
ATA WDC W...	⚠ Warning	Physical Disk	3,726.00 GB	3,723.75 GB			
ATA WDC W...	⚠ Warning	Physical Disk	3,726.00 GB	3,723.25 GB			
ATA WDC W...	Healthy	Physical Disk	3,726.00 GB	3,723.00 GB			
ATA WDC W...	⚠ Warning	Physical Disk	3,726.00 GB	3,724.50 GB			
ATA WDC W...	⚠ Warning	Physical Disk	3,726.00 GB	3,723.00 GB			
SAMSUNG...	Healthy	Physical Disk	447.00 GB	31.25 GB			
ATA WDC W...	Healthy	Physical Disk	3,726.00 GB	3,722.75 GB			
ATA WDC W...	⚠ Warning	Physical Disk	3,726.00 GB	3,724.50 GB			
ATA WDC W...	Healthy	Physical Disk	3,726.00 GB	3,723.25 GB			

ATA WDC WD4000FYYZ-0

Physical disk information

Last refresh: 9/14/2018 2:05:12 AM
Array: Clus3057.cdm.lab
Description:
Media Type: HDD
Bus Type: SAS
Health Satus: ⚠ Warning
Operational Status: Maintenance mode
Usage: Auto-select

Physical disk information

Physical Location:
Enclosure Name:
Firmware Version: Slot 1
Serial Number: WD-WMC130D96L

Capacity information

Size: 3,726.00 GB
Allocated size: 2.75 GB
Storage allocated: ✓

Next steps

Set up storage classifications in the VMM fabric.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up storage classifications in the VMM fabric

Article • 08/22/2024

Use storage classifications to abstract storage devices in the System Center Virtual Machine Manager (VMM) fabric. You can classify storage devices with similar characteristics and assign these classifications, rather than specific storage devices, to hosts and clusters. The host and cluster can then use any available storage n the classification.

Classifications are often based on storage types or performance characteristics. For example, you could create:

⛶ Expand table

Name	Description
GOLD	Storage pool based on solid-state drives (SSDs) that delivers high performance for I/O intensive applications
SILVER	Fibre Channel Serial Attached SCSI (SAS) storage (RAID 5)
BRONZE	iSCSI Serial ATA (SATA) storage (RAID 5)

Create classifications:

1. Select **Fabric** > **Storage**, right-click **Classification and Pools** > **Create Classification**.
2. In **New Classification**, enter a name and description > **Add**.

Next steps

Add storage devices to the VMM fabric.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Add storage devices to the VMM fabric

Article • 08/22/2024

To manage storage in System Center Virtual Machine Manager (VMM), you discover and add it to the VMM storage fabric.

Before you start

Ensure that the storage device is supported before you add it.

Add a storage device

1. Select **Fabric** > **Storage** > **Add Resources** >**Storage Devices**.
2. In **Add Storage Devices Wizard** > **Select Provider Type**, select to add a storage device with SMI-S or SMP according to the device you're using.
3. In **Specify Discovery Scope**:

   - If you're using SMI-S, specify whether the provider uses **SMI-S CIMXML** or **SMI-S WMI WMI**, add the IP address/FQDN and add the port used to connect to the provider on the remote server. You can enable SSL if you're using CIMXML. Specify an account for connecting to the provider.
   - If you're using SMP, select the provider from the list. If it isn't in the list, select **Import** to refresh it.

4. In **Gather Information**, VMM automatically tries to discover and import the storage device information. To retry, select **Scan Provider**.
5. If you selected the option to use an SSL connection for an SMI-S provider, you observe that:

   - During discovery, the **Import Certificate** dialog appears. Check settings and select **Import**. By default, the certificate common name (CN) will be verified. This might cause storage discovery to fail if there's no CN or if it doesn't match.
   - If discovery fails because of the CN, disable CN verification in the registry on the VMM server. In the registry, go to **HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Storage Management/** and create a new DWORD value - **DisableHttpsCommonNameCheck**. Set the value to 1.

6. If the discovery process succeeds, the discovered storage arrays, storage pools, manufacturer, model, and capacity are listed on the page. When the process finishes, select **Next**.
7. In **Select Storage Devices**, you can specify a classification for each storage pool. Storage classifications group storage pools with similar characteristics together so that you can assign a classification as storage for a host or cluster rather than a specific storage device. Learn more about setting up classifications.
8. On the **Summary** page, confirm the settings, and then select **Finish**. The **Jobs** dialog appears. When the status is **Completed**, you can verify the storage in **Fabric** > **Storage**.

Next steps

Allocate storage to host groups.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Allocate storage to host groups

Article • 08/22/2024

After block storage has been discovered and classified in the System Center Virtual Machine Manager (VMM) fabric, you can allocate it to host groups. You can allocate an entire storage pool or a specific logical unit (LUN).

- **Allocate storage pools**: You can optionally allocate storage pools to host groups. If you do, you can:
    - Create and assign LUNs directly from Hyper-V hosts in the host group.
    - Use the storage pool for rapid provisioning using SAN cloning or snapshots. During this process, you don't need to create LUNs because VMM requests a copy of an existing LUN during provisioning.

- **Allocate LUNs**:
    - You can assign LUNs for storage pools that are managed in the VMM fabric.
        - To allocate LUNs to host groups, there must be unassigned LUNs in the managed storage pools.
        - If you need additional LUNs, you can create them outside of VMM in your storage management tool, or you can provision them directly in VMM if the storage pool is allocated to a host group.

Allocate a storage pool to a host group

1. Select **Fabric** > **Storage** > **Allocate Capacity**, and select the host group. If you're a delegate admin with scope restricted to host groups, right-click the host group > **Properties** > **Storage**.
2. The total and available storage capacity information is displayed for the host group. The storage capacity information includes the total and available capacity for both local and remote storage, and total and available allocated storage. Select **Allocate Storage Pools**.
3. Select a storage pool > **Add**.

Create a LUN in VMM

1. Ensure that you've allocated the storage pool to the host group, and select **Fabric** > **Storage** > **Create Logical Unit**.
2. Specify the storage pool, a name and description for the LUN, and the size. Select **OK** to create the LUN.

3. Verify that the LUN was created in **Fabric Resources** > **Classifications, Storage Pools, and Logical Units**.

Allocate a LUN to a host group

1. Select **Fabric** > **Storage** > **Allocate Capacity** > **Allocate Storage Capacity**, and select the host group.
2. Select **Allocate Logical Units**, and select a unit > **Add**.

After LUNs are allocated to host groups, you can assign them to Hyper-V hosts and clusters.

Next steps

After you set up Hyper-V hosts and clusters, learn about provisioning VMs.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up a Microsoft iSCSI Target Server in the VMM storage fabric

Article • 08/22/2024

Microsoft iSCSI Target Server is a server role that enables a Windows server machine to function as a storage device. This article explains how to set up a Microsoft iSCSI Target Server in System Center Virtual Machine Manager (VMM) storage.

Here's what you need to do:

1. **Install the role**: Install the iSCSI Target Server role (**Server Roles** > **File and Storage Services** > **File and iSCSI Services**) on a server that you want to add as a block storage device.
2. **Set up virtual iSCSI disks**: After installing the role, you'll need to set up virtual iSCSI disks and connect to the servers you want. Learn more.

4. **Add account**: Add the VMM admin account as an administrator on the server.
5. **Discover in VMM**: Add the storage device to VMM. Select **SAN and NAS devices discovered and managed by a SMI-S provider** as the provider type and specify the IP address or FQDN as the server. Select the account with permissions to the server as the Run As account. Add it to the required storage classification and complete the **Add Storage Devices Wizard**.

After adding the server as a storage device under VMM management, you can allocate the storage pools and LUNs to a host group and provision storage to hosts and clusters.

PowerShell example

You can use VMM to configure the iSCSI Target Server through Windows PowerShell. This section lists some common tasks with examples of Windows PowerShell commands that you can use for those tasks. The SMI-S provider supports all management tasks through VMM.

Manage storage on an iSCSI target server

Open PowerShell and use the cmdlets described below to manage iSCSI target server resources in VMM.

Add a storage provider

Expand table

Command	Purpose
`$Cred = Get-Credential`	Obtain the iSCSI Target Server local administrative credentials that are based on username and password. Any account that is part of the Local Administrators group is sufficient.
`$Runas = New-SCRunAsAccount -Name "iSCSIRunas" -Credential $Cred`	Create a Run As account in VMM.
`Add-SCStorageProvider -Name "Microsoft iSCSI Target Provider" -RunAsAccount $Runas -ComputerName "<computername>" -AddSmisWmiProvider`	Add the storage provider.

View storage properties

Expand table

Command	Purpose
`$array = Get-SCStorageArray -Name “<computername>”`	Review the storage array attributes.
`$array.StoragePools`	View available storage pools.

Add pools from iSCSI Target Server to VMM management

Expand table

Command	Purpose
`$pool = Get-SCStoragePool -Name "MS iSCSITarget Concrete: D:"`	Get the specific storage pool to add.
`$class = New-SCStorageClassification -Name “gold”`	Create a storage classification if none exists.
`Set-SCStorageArray -AddStoragePoolToManagement $pool -StorageArray $pool.StorageArray -StorageClassification $class`	Add the storage pool to VMM.
`Set-SCStoragePool -StoragePool $pool -AddVMHostGroup (Get-SCVMHostGroup -Name "All Hosts")`	Allocate the storage pool to a virtualization server group.

Create a LUN

⛶ Expand table

Command	Purpose
`$LUN = New-SCStorageLogicalUnit -Name "iSCSI1" -StoragePool $pool -DiskSizeMB 1000`	Create an iSCSI logical unit number (LUN).
`Set-SCStorageLogicalUnit -StorageLogicalUnit $LUN -VMHostGroup (Get-SCVMHostGroup -Name "All Hosts")`	Allocate the LUN to the host group.
`$host = Get-SCVMhost -ComputerName <host name>`	Retrieve the properties of a host.
`Register-SCStorageLogicalUnit -StorageLogicalUnit $LUN -VMHost $host`	Assign the LUN to the host.

Decommission resources

⛶ Expand table

Command	Purpose
`Remove-SCStorageLogicalUnit -StorageLogicalUnit $LUN`	Delete a LUN.
`Remove-SCStorageProvider -StorageProvider (Get-SCStorageProvider -Name "Microsoft iSCSI Target Provider")`	Remove a storage provider.

Next Steps

Learn about provisioning storage for Hyper-V hosts and clusters.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up Hyper-V virtual Fibre Channel in the VMM storage fabric

Article • 08/22/2024

Read this article to set up Hyper-V virtual Fibre Channel in the System Center Virtual Machine Manager (VMM) storage fabric.

Virtual Fibre Channel provides Hyper-V VMs with direct connectivity to Fibre Channel-based storage. Hyper-V provides Fibre Channel ports within guest operating systems so that you can virtualize applications and workloads that have dependencies on Fibre Channel storage. You can also cluster guest operating systems over Fibre Channel.

Before you start

- VMM supports the following virtual Fibre Channel deployments:
  - Single storage array connected to a single fabric (comprised of single or multiple switches) connected to a single virtual SAN (vSAN). A vSAN is a named group of physical Fibre Channel Host Bus Adapter (HBA) ports on a host computer that VMs connect to access Fibre Channel storage devices.
  - Single storage array connected to multiple fabrics (comprised of single or multiple switches per fabric) that are connected to a single vSAN.
  - Multiple storage arrays connected to a single fabric (comprised of single or multiple switches) that is connected to a single vSAN.
  - Multiple storage arrays connected to multiple fabrics (comprised of single or multiple switches per fabric) that are connected to multiple vSANs. This configuration provides dual-redundant paths to storage arrays.

Here's what you need:

- One or more vSANs can be created for each host computer. A vSAN can only contain HBAs from a single fabric.
- Storage arrays, switches, and HBAs must have the latest firmware and drivers installed.
- Ensure that storage arrays can present logical units (LUs).
- Enable NPIV on Fibre Channel switches and HBAs.

- Hyper-V hosts must be running Windows Server 2016 or later.

- Ensure that an SMI-S provider is installed. VMM manages Fibre Channel fabrics and SAN devices using the SMI-S provider. Remember not to install the SMI-S provider on the VMM server, but on a server that the VMM server can connect to with an FQDN or IP address.

Deploy virtual Fibre Channel

To deploy virtual Fibre Channel, follow these steps:

1. Discover and classify Fibre Channel fabrics.
2. Create vSANs for each host computer by grouping host HBA ports.
3. Create a VM that can access the virtual Fibre Channel storage.
4. Create zones that connect each host or VM vHBA to a storage array. Zones are used to connect a Fibre Channel array to a host computer VM.
5. Create LUNs and register them for a host, VM, or service tier.
6. Create a service template and add VM templates to it. For each vHBA, specify dynamic or static WWN assignments and select the classification. Create and deploy a service tier based on the service template to access Virtual Fibre Channel storage. Zone a Fibre Channel array to the tier, add a disk, create a LUN, and register the LUN to the tier.

Discover and classify Fibre Channel fabrics

1. Select **Fabric** > **Storage** > **Add Resources** > **Storage Devices**.
2. In **Add Storage Devices Wizard** > **Select Provider Type**, select **Fibre Channel fabric discovered and managed by an SMI-S provider**.
3. In **Specify Discovery Scope**, specify the IP address or FQDN and the port number of the provider.
4. If you're using SMI-S, specify whether the provider uses **SMI-S CIMXML** or **SMI-S WMI**, and add the IP address/FQDN and port used to connect to the provider on the remote server. If you're using CIMXML, you can enable SSL.
5. Specify an account for connecting to the provider.
6. In **Gather Information**, VMM automatically discovers and imports the Fibre Channel fabric information. If the discovery process succeeds, the discovered fabric name, switches, and fabric World Wide Node Names (WWNN) are listed on the page. When the process successfully completes, select **Next**. To retry the discovery process for an unsuccessful attempt, select **Scan Provider**.
7. If you selected the option to use an SSL connection for an SMI-S provider, ensure that:

    - During discovery, the **Import Certificate** dialog appears. Check settings and select **Import**. By default, the certificate's common name (CN) is verified. Storage discovery can fail if there's no CN or it doesn't match.

- If discovery fails because the CN disables CN verification in the registry on the VMM server, in the registry, go to **HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Storage Management/** and create a new DWORD value - **DisableHttpsCommonNameCheck**. Set the value to 1.

8. On the **Fibre Channel Fabrics** page, do the following for each storage fabric that requires a classification:
   a. In the **Storage Device** column, select the checkbox next to a Fibre Channel fabric that you want VMM to manage.
   b. In the **Classification** column, select the classification that you want to assign to the fabric. The fabric classification task is separate from that for storage classification, although the concept is similar.
9. On the **Summary** page, confirm the settings and select **Finish**.

Create vSANs and assign HBAs

You can create vSANs and assign HBAs to it. One or more vSANs can be created for each host computer. Each vSAN can only contain HBAs that are from the same fabric.

Virtual Host Bus Adapters (vHBAs) represent the virtualization of Fibre Channel HBAs and are used by VMs to connect with vSANs. Each vHBA has a World Wide Node Name (WWNN), which is different from the host HBA WWNN. Using N_Port ID Virtualization (NPIV), a host computer HBA can map to multiple vHBAs. HBA ports assigned to a vSAN can be added or removed as needed.

1. Select **Fabric** and right-click the applicable host > **Properties** > **Hardware** > **New Virtual SAN**.

2. In **New Virtual SAN**, specify a name and optional description. In **Fibre Channel adapters**, select the checkboxes next to the Fibre Channel HBAs that you want to assign to the vSAN. Select **OK**.

3. If you want to edit vSAN port assignments, in **Properties** > **Hardware** > **FC Virtual SAN** > **Fibre Channel adapter details**, select or unselect the HBA ports.

4. If you want to add a new vHBA and assign it to a vSAN, select **Properties** > **Hardware Configuration** > **New** > **Fibre Channel Adapter**. In **Virtual SAN name**, select a vSAN to assign it. Specify whether you want to assign port settings for the vHBA statically or dynamically.

5. If you want to change the global default port settings for vHBA, select **Properties** > **Hardware** > **Global Settings** and modify settings in **Fibre Channel adapter details**.

> ⓘ Note
>
> Changing these settings does not affect vHBA ports that have already been created. To apply a new setting to an existing vHBA port, recreate the port by removing it and then adding it again.

Create a VM template

vHBAs are used by VMs to connect with vSANs. For vHBAs to connect to vSANs, they must be first added to the hardware profile of a VM template.

1. Use the **Create Virtual Machine Wizard** to create a new VM, and then add a new Fibre Channel adapter (vHBA) to the **Configure Hardware** page of the VM template. For each vHBA that you create, specify dynamic or static WWPN assignments and select the fabric classification.
2. Still using the **Create Virtual Machine Wizard**, place and deploy the VM to a destination host. Ensure that the host contains a virtual SAN that matches the storage fabric.

After you deploy the VM to a host, you can zone a virtual Fibre Channel storage array to the VM. Then you create a LUN and register (unmask) it to the VM.

Create zones

Zones are used to connect a Fibre Channel array to a host or virtual machine (VM). The storage array target ports are mapped to the HBA ports on the host or to the virtual HBA (vHBA) ports for the VM. You can create zones for a host, a VM, or both. For Hyper-V failover clusters, a zone is needed for each host in the cluster. Ensure that:

- Zones are grouped into zonesets, which use common Fibre Channel fabric devices. When all zones in a zoneset have been added, modified, or removed as needed, the zoneset must be activated. Zoneset activation pushes information for each zone down to the Fibre Channel switches in the selected fabric.
- Only members of the same zone can communicate with each other.
- You'll need to create new zones and then activate the zoneset. Activating a zoneset can cause some downtime in the fabric as information is propagated to all the switches.
- If you want to add a storage array to a Hyper-V cluster, you need to zone the array to each host computer first. Similarly, if you want to add an array to a guest cluster, you need to zone the array to each VM first.

Set up zones as follows:

1. Select **VMs and Services** > **Services**, right-click the applicable VM, > **Properties** > **Storage** > **Add** > **Add Fibre Channel Array**.
2. In **Add Fibre Channel Array** > **Properties** page > **Create New Zone**, specify a zone name, select a storage array, and in **Fabric**, select a switch. In **Storage array target ports**, select the applicable WWPM port or ports. In **Virtual machine initiator**, select the applicable WWPM port or ports. Select **Create**. Select **Show aliases** to view the available zone aliases.
3. To activate the zoneset, select **Fabric** > **Name**, and select the inactive zoneset > **Activate Zoneset**.
4. You can view the zonesets for a fabric in **Fabric** > **Fibre Channel Fabric** > **Name**; right-click the applicable fabric > **Properties** > **Zonesets**.
5. If you want to modify zoning for a storage array, select **VMs and Services** > applicable host > **Properties** > **Storage** > **Fibre Channel Arrays** > **Edit** > applicable array and modify the zoning settings.

Create and register LUNs

For a host computer, VM, or computer service tier to access storage array resources, LUNs must be created and then registered (unmasked) to the host, VM, or tier.

1. Select **Fabric** > **Storage** > **Classifications and Pools**. Under **Name**, select the applicable storage device > **Create Logical Unit**.
2. In the **Create Logical Unit**, select a storage pool, and specify a name and description and LUN size. Specify whether you want to create a thin or fixed size LUN.
3. To register the LUN, in **VMs and Services** pane, right-click the applicable VM > **Properties** > **Add** > **Add Disk**.
4. In **Create Logical Unit**, select a storage pool, name, and size. Select **OK** to register the LUN.

Create and deploy a service tier

1. Using the **Service Template Designer**, create a service template and add the applicable VM templates you previously created to the service template.
2. Add a new virtual Fibre Channel Adapter (vHBA) to the **Configure Hardware** page of the service template. For each vHBA that you create, specify dynamic or static WWPN port assignments and select the fabric classification.
3. Create service tier from the service template and assign the service tier to a computer tier.

4. Deploy the tier.
5. After you deploy it, you can zone a virtual Fibre Channel storage array to the service tier. Then create a LUN for the array and register (unmask) it to the tier.

Next steps

Set up storage for Hyper-V hosts and clusters.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Set up file storage in the VMM fabric

Article • 08/22/2024

You can manage file storage that supports SMB 3.0 in the System Center Virtual Machine Manager (VMM) storage fabric. This includes Windows file servers, scale-out file servers (SOFS), and network-attached storage (NAS) devices from non-Microsoft vendors such as EMC and NetApp.

This article describes how to add file storage to the VMM fabric. After file shares are available in the fabric, you can assign them to Hyper-V hosts and clusters.

Add a file share to the VMM fabric

When you add a file server, VMM automatically discovers all the shares that are currently present on the server.

1. Select **Fabric** > **Storage** > **Add Resources** > **Storage Devices**.
2. In **Add Storage Devices Wizard** > **Select Provider Type**, select **Add a Windows-based file server as managed storage device** to manage a single or clustered file server in the VMM console.
3. In **Specify Discovery Scope**, specify the address or the name of the file server. If the file server resides in a domain that isn't trusted by the domain in which the virtual machine hosts are located, select **This computer is in an untrusted Active Directory domain**. Select a Run As account that can access the file server.
4. In **Gather Information**, VMM automatically tries to discover and import information about the shares on the file server. If the discovery process succeeds, information about the file server is displayed. When the process finishes, select **Next**.
5. In **Select Storage Devices**, select the file shares that you want VMM to manage.
6. In **Summary**, review the settings and select **Finish**.

Create a file share

You need to create a file share on the file server. When you do this, VMM assigns permissions automatically.

1. Select **Fabric** > **Storage** > **Providers**.
2. Select the file server > **Create File Share**.
3. In **Create File Share**, specify the path on which you want to create the share. If it doesn't exist, VMM will create it.

Assign files shares

You can assign file shares on any host on which you want to create VMs that will use the file share as storage.

1. Select **Fabric** > **Servers** > **All Hosts** and select the host or cluster node you want to configure.

2. In **Host** > **Properties**, select **Properties** > **Host Access**. Specify a Run As account. By default, the Run As account that was used to add the host to VMM is listed. In the Run As account box, configure the account settings. You can't use the account that you use for the VMM service.

    - If you used a domain account for the VMM service account, add the domain account to the local Administrators group on the file server.
    - If you used the local system account for the VMM service account, add the computer account for the VMM management server to the local Administrators group on the file server. For example, for a VMM management server that is named VMMServer01, add the computer account VMMServer01$.
    - Any host or host cluster that accesses the SMB 3.0 file share must have been added to VMM using a Run As account. VMM automatically uses this Run As account to access the SMB 3.0 file share.
    - If you specified explicit user credentials when you added a host or host cluster, you can remove the host or cluster from VMM and then add it again using a Run As account.

3. Select **Host Name Properties** > **Storage** > **Add File Share**.

4. In **File share path**, select the required SMB 3.0 file share, and select **OK**. To confirm that the host has access, open the **Jobs** workspace to view the job status. Or open the host properties again and select the **Storage** tab. Under **File Shares**, select the SMB 3.0 file share. Verify that a green check mark appears next to **Access to file share**.

5. Repeat this procedure for any standalone host that you want to access the SMB 3.0 file share or for all nodes in a cluster.

Next steps

After you set up the Hyper-V host or cluster, learn about provisioning VMs.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Manage Storage Replica in VMM

Article • 08/27/2024

Storage Replica enables storage-agnostic, block-level, synchronous replication between clusters or servers for disaster preparedness and recovery and stretching of a failover cluster across sites for high availability. Synchronous replication enables mirroring of data in physical sites with crash-consistent volumes, ensuring zero data loss at the file system level. Asynchronous replication allows site extension beyond metropolitan ranges with the possibility of data loss.

Learn more and review the FAQs.

This article explains how Storage Replica integrates with System Center Virtual Machine Manager (VMM) and describes how to set up Storage Replica using PowerShell to replicate storage in the VMM fabric.

Storage Replica in VMM

You can use Storage Replica to replicate Hyper-V cluster data or file data. Using Storage Replica in VMM provides many business advantages:

- Eliminates the cost and complexity associated with synchronous replication solutions such as SAN.
- Synchronous replication minimizes downtime and data loss. It provides an RPO of 0 (zero data loss). RTO (data unavailability) only occurs during the time in which a primary site fails and a secondary site starts.
- Source and destination storage hardware don't need to be identical.

Before you start

- VMM must be running on Windows Server 2016 or later Datacenter Edition.
- Hyper-V must be running on Windows Server 2016 or later Datacenter, Server Core, or Nano.
- Only synchronous replication is supported. Asynchronous isn't supported.
- You need two sets of storage, either volume or file storage. Both the source and destination locations must have the same type of storage (file or volume) but the actual storage can be mixed. For example, you could have Fibre Channel SAN at one end and Spaces Direct (in hyper-converged or disaggregated mode) at the other.

- Each set of storage must be available in each of the clusters. Cluster storage must not be shared.
- Source and destination volumes (including log volumes) need to be identical in size and block size. This is because Storage Replica uses block replication.
- You need at least one 1-GbE connection on each storage server, preferably 10 GbE, iWARP, or InfiniBand.
- Each file server or cluster node needs firewall rules that allow ICMP, SMB (port 445, plus 5445 for SMB Direct), and WS-MAN (port 5985) bidirectional traffic between all nodes.
- You need to be a member of the Administrator group on each cluster node.
- Storage Replica can only be set up using Windows PowerShell at present.
- Source and destination storage must be managed by the same VMM server.
- Integrating VMM with Azure Site Recovery isn't supported.
- Setting write order and consistency groups isn't supported.

Deployment steps

1. **Identify storage**: Identify the source and destination storage you want to use.

2. **Discover and classify**: If your storage isn't currently in the VMM fabric, you need to discover it with VMM. Both the source and destination storage must be managed by the same VMM server. After discovery, create a storage pool and a storage classification for it. Learn more.

3. **Pair**: Pair the source and destination storage array.

4. **Provision**: After your storage is paired, you'll need to provision identical data and log volumes from the source and destination storage pools created on the respective storage arrays. In addition to provisioning a volume for data that will be replicated, you also need to provision a volume for replication transaction logs. As data is updated on source storage, the transaction log is appended, and delta changes are synchronized (using synchronous replication) with destination storage.

5. **Create replication groups**: After the volumes are in place, you create replication groups. Replication groups are logical groups containing multiple volumes. The replication groups need to be identical, containing the data and log volumes for the source and destination sites, respectively.

6. **Enable replication**: Now you can enable replication between the source and destination replication groups.

7. **Refresh**: To finalize the creation of replication groups and to trigger the initial data replication, you need to refresh the primary and secondary storage provider. Data replicates to destination storage.

8. **Verify status**: Now you can check the status of the primary replication group. It must be in the Replicating state.

9. **Add VMs**: When delta replication is up and running, you can add VMs that use storage contained in the replication group. When you add the VMs, they'll be detected and will begin replicating automatically.

10. **Run failover**: After replication is in a Synchronizing state, you can run a failover to check if it's working as expected. There isn't a test failover mechanism, so you'll run a manual failover in response to planned or unplanned outages. After failover, you can delete the VM on the source site (if it still exists) and create a VM on the destination site using the replicated data.

11. **Run failback**: After failover is complete and replica VMs are up and running, you can fail back as you need to. Ensure that:

    - If you run an unplanned failover and your source location isn't available, you'll run a failover to fail back from the secondary to primary location, and then create the VM in the primary location.
    - If you run a planned failover and the source VM is still available, you need to stop replication, remove the source VM, create the VM in the secondary location, and then restart replication. Then at the primary site, you can create the VM with the same settings as the original VM.

Retrieve PowerShell objects

1. Before you start, retrieve the name of the PowerShell objects you want to use.

2. Get the name of the primary storage array and assign it to a variable.

   PowerShell

   ```
   $PriArray = Get-SCStorageArray -Name $PriArrayName
   ```

3. Get the name of the secondary storage array and assign it to a variable.

   PowerShell

   ```
   RecArray = Get-SCStorageArray -Name $RecArrayName
   ```

4. Get the name of the primary storage pool and assign it to a variable.

PowerShell

```
    $ $ PriPoolName $RecPool = Get-SCStoragePool -Name $
```

5. Get the name of the secondary storage pool and assign it to a variable.

PowerShell

```
    $ $PriPoolName $RecPool = Get-SCStoragePool -Name $
```

Pair the storage arrays

Pair the primary and secondary storage arrays using the variables for the storage array names.

> ⓘ Note
>
> The array name must be the same as the cluster name.

PowerShell

```
      Set-SCStorageArray -StorageArray $PriArray -PeerStorageArrayName
$RecArray.name
```

If you created the cluster outside the VMM and you do need to rename the array name to match the cluster name, use:

PowerShell

```
      Get-SCStorageArray -Name "existing-name" | Set-SCStorageArray -Name
"new-name"
```

Provision LUNs and create the storage groups

Provision a LUN from the storage pool for data and for the log. Then create replication groups.

1. Provision and create on the source.

PowerShell

```
    Set-SCStorageArray -StorageArray $PriArray -PeerStorageArrayName
$RecArray.name

    $PrimaryVol = New-SCStorageVolume -StorageArray $PriArray -
StoragePool $PriPool -Name PrimaryVol -SizeInBytes $VolSize -
RunAsynchronously -PhysicalDiskRedundancy "1" -FileSystem "CSVFS_NTFS"
-DedupMode "Disabled"

    $PrimaryLogVol = New-SCStorageVolume -StorageArray $PriArray -
StoragePool $PriPool -Name PrimaryLogVol -SizeInBytes $LogVolSize -
GuidPartitionTable -RunAsynchronously -FileSystem "NTFS"

    $PriRG = New-SCReplicationGroup -Name PriRG -StorageVolume
$PrimaryVol -LogStorageVolume $PrimaryLogVol
```

2. Provision and create on the destination.

PowerShell

```
    $RecoveryVol = New-SCStorageVolume -StorageArray $RecArray -
StoragePool $RecPool -Name RecoveryVol -SizeInBytes $VolSize -
RunAsynchronously -PhysicalDiskRedundancy "1" -FileSystem "CSVFS_NTFS"
-DedupMode "Disabled"

    $RecoveryLogVol = New-SCStorageVolume -StorageArray $RecArray -
StoragePool $RecPool -Name RecoveryLogVol -SizeInBytes $LogVolSize -
GuidPartitionTable -RunAsynchronously -FileSystem "NTFS"

    $RecRG = New-SCReplicationGroup -Name RecRG -CreateOnArray -
ProtectionMode Synchronous -StorageVolume $RecoveryVol -
LogStorageVolume $RecoveryLogVol
```

Enable replication

Enable synchronous replication between the source and destination replication groups.

PowerShell

```
    Set-SCReplicationGroup -ReplicationGroup $PriRG -Operation
EnableProtection -TargetReplicationGroup $RecRG -EnableProtectionMode
Synchronous
```

Refresh the storage providers

1. Open the VMM console.

2. Select **Fabric Resources** > **Providers**. Right-click the provider > **Refresh**.

Verify replication status

Retrieve the replication status for the source replication group to ensure that replication is working as expected.

PowerShell

```powershell
    Get replication status Get-SCReplicationGroup | where
{($_.Name.EndsWith("PriRG")) -or ($_.Name.EndsWith("RecRG"))}  | fl Name,
IsPrimary, ReplicationState, ReplicationHealth
```

Create a VM

Create a VM using a LUN in the source replication group. Alternatively, you can create a VM in the VMM console.

PowerShell

```powershell
    New-SCVirtualMachine -Name "DemoVM" -VMHost <HostName> -Path $PrimaryVol
-VMTemplate <VMTemplate>
```

Run a failover

Run failover.

PowerShell

```powershell
    Set-SCReplicationGroup -ReplicationGroup $PriRG -Operation
PrepareForFailover

    Set-SCReplicationGroup -ReplicationGroup SRecRG -Operation Failover
```

Run failback

Before you fail back, in the VMM console, remove the source VMs if they're still available. You can't fail back to the same VM.

Run failback:

PowerShell

```
    Set-SCReplicationGroup -ReplicationGroup $PriRG -Operation ReverseRoles
-EnableProtectionMode Synchronous -TargetReplicationGroup $RecRG
```

After running failback, you can create VMs at the source site using the failed back VHD/configuration files.

Stop replication

If you want to stop replication, you'll need to run this cmdlet at the source and destination.

PowerShell

```
    Set-SCReplicationGroup -ReplicationGroup $RecRG -Operation TearDown
Tear down need to be done on both RGs
```

Next steps

- Learn more about Storage Replica.
- Learn about allocating storage to Hyper-V hosts and clusters.
- Learn more about Migrate storage.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage scale-out file server (SOFS) in the VMM fabric

Article • 08/22/2024

Scale-out file server (SOFS) is a file server deployed as an active/active cluster based on SMB 3.0. Using a SOFS cluster provides apps with the bandwidth of all nodes in the cluster. All nodes in the cluster accept SMB requests, providing continuous availability and transparent failover if a node goes down.

You can add and manage SOFS clusters in the System Center Virtual Machine Manager (VMM) fabric. There are many ways you can add a SOFS cluster. You can add an existing SOFS cluster to the fabric, provision a SOFS cluster from the existing Windows machines in the fabric, or provision a cluster from bare metal computers.

- Perform a rolling upgrade of an SOFS cluster.
- Add an existing SOFS to the VMM storage fabric.
- Create an SOFS cluster from standalone servers in the VMM fabric.
- Provision SOFS from bare-metal computers.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Run a rolling upgrade of a SOFS cluster to Windows Server 2016 in VMM

Article • 08/22/2024

Cluster rolling upgrade enables you to upgrade the operating system of cluster nodes in a scale-out file server (SOFS) cluster, or Hyper-V cluster, without stopping workloads running on the nodes. Read more about rolling upgrade requirements and architecture.

This article describes how to perform a cluster rolling upgrade of SOFS managed in the System Center Virtual Machine Manager (VMM) fabric. Here's what the upgrade does:

- **Creates a template**: Creates a template of the node configuration by combining the appropriate physical computer profile with the node configuration settings detailed in the upgrade wizard.
- **Migrates workloads**: Migrates workloads off the node so that workload operations aren't interrupted.
- **Removes node**: Puts the node into maintenance mode and then removes it from the cluster. This removes all VMM agents, virtual switch extensions, and so forth, from the node.
- **Provisions the node**: Provisions the node running Windows Server 2016, and configures it according to the saved template.
- **Returns the node to VMM**: Brings the node back under VMM management and installs the VMM agent.
- **Returns the node to the cluster**: Adds the node back into the SOFS cluster, brings it out of the maintenance mode, and returns virtual machine workloads to it.

Before you start

- The cluster must be managed by VMM.
- The cluster must be running Windows Server 2016 or later.
- The cluster must meet the requirements for bare metal deployment. The only exception is that the physical computer profile doesn't need to include network or disk configuration details. During the upgrade, VMM records the node's network and disk configuration and uses that information instead of the computer profile.
- You can upgrade nodes that weren't originally provisioned using bare metal as long as those nodes meet bare metal requirements such as BMC. You'll need to provide this information in the upgrade wizard.
- The VMM library needs a virtual hard disk configured with Windows Server 2016.

Run the upgrade

1. Select **Fabric** > **Storage** > **File Servers**. Right-click the SOFS > **Upgrade Cluster**.
2. In the Upgrade Wizard > **Nodes**, select the nodes you want to upgrade or **Select All**. Select **Physical computer profile**, and select the profile for the nodes.
3. In **BMC Configuration**, select the Run As account with permissions to access the BMC or create a new account. In **Out-of-band management protocol**, select the protocol that the BMCs use. To use DCMI, select **IPMI**. DCMI is supported even though it's not listed. Ensure that the correct port is listed.
4. In **Deployment Customization**, review the nodes to upgrade. If the wizard couldn't figure out all the settings, it displays a **Missing Settings** alert for the node. For example, if the node wasn't provisioned by bare metal, BMC settings might not be complete. Fill in the missing information.

   - Enter the BMC IP address if required. You can also change the node name. Don't clear **Skip Active Directory check for this computer name** unless you're changing the node name and you want to ensure the new name isn't in use.
   - In the network adapter configuration, you can specify the MAC address. Do this if you're configuring the management adapter for the cluster, and you want to configure it as a virtual network adapter. It's not the MAC address of the BMC. If you choose to specify static IP settings for the adapter, select a logical network and an IP subnet if applicable. If the subnet contains an address pool, you can select **Obtain an IP address corresponding to the selected subnet**. Otherwise, enter an IP address within the logical network.

5. In **Summary**, select **Finish** to begin the upgrade. If the wizard finishes, the node upgrades successfully so that all the SOFS nodes are running Windows Server 2016 or later. The wizard upgrades the cluster functional level to Windows Server 2016.

If you need to update the functional level of a SOFS that was upgraded outside VMM, you can do that by right-clicking the **Files Servers** > SOFS name > **Update Version**. This might be necessary if you upgraded the SOFS nodes before adding it to the VMM fabric, but SOFS is still functioning as a Windows Server 2016 or later cluster.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Add an existing SOFS to the VMM fabric

Article • 08/22/2024

You can add an existing scale-out file server (SOFS) to the System Center Virtual Machine Manager (VMM) storage fabric. When you add a file server, VMM automatically discovers all the file shares on it.

1. Select **Fabric** > **Storage** > **Home** > **Add Resource** > **Storage Devices** to open the **Add Storage Devices Wizard**.
2. If the file server is in a domain that's not trusted by the Hyper-V hosts for which it will provide storage, select **This computer is in an untrusted Active Directory domain**. Select **Browse** and select a Run As account with admin permissions on the SOFS. Or create a Run As account if you don't have one.
3. In **Select Provider type**, select **Windows-based file server**.
4. In **Specify Discovery Scope**, enter the FQDN or IP address of the SOFS (not of the underlying cluster)
5. In **Gather Information**, VMM discovers and imports information about the SOFS.
6. In **Select Storage Device**, select the file shares that you want VMM to manage. You can configure more settings on the file server after you finish the wizard.
7. On the **Summary** page, confirm the settings and then select **Finish**. You can monitor the cluster status on the **Jobs** page. After the job finishes, check the SOFS in **Fabric** > **Storage** > **File servers**.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Provision a scale-out file server (SOFS) from standalone file servers in the VMM fabric

Article • 08/22/2024

Use the instructions in this article if you want to use System Center Virtual Machine Manager (VMM) to create a scale-out-file server (SOFS) from standalone file servers that are managed in the VMM fabric.

1. In the VMM console, select **Fabric** > **Create** > **File Server Cluster**.

2. In the **Create Clustered File Server** wizard > **General**, specify a cluster name, a file server name, and IP addresses if required.

1. In **Resource Type**, select the option to provision computers on which Windows Server 2016 or later is installed and fill in the details.

1. In **Cluster Nodes**, define a list of computers to add to the cluster.

2. On the **Summary** page, confirm the settings and select **Finish**.

You can monitor the cluster status on the **Jobs** page. After the job finishes, check the cluster in **Fabric** > **Storage** > **File servers**.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Provision a scale-out file server (SOFS) cluster from bare metal computers in the VMM fabric

Article • 08/22/2024

In addition to adding existing file servers to an SOFS cluster in the System Center Virtual Machine Manager (VMM) fabric, VMM can discover provision bare metal machines as SOFS cluster nodes. This article includes the steps for setting up a bare metal SOFS cluster in VMM.

Before you start

Here's what you need for the deployment:

- **Physical computers** to deploy as SOFS cluster nodes. These computers must meet the prerequisites described in the table below. They can be running on operating system or an operating system that will be overwritten during the deployment process.
- **Virtual hard disk** with an appropriate operating system located on a VMM library share. When you create the virtual hard disk, you can create a virtual machine, install the guest operating system, and use Sysprep with the /generalize and the /oobe options.
  The operating system on the virtual hard disk that you deploy on the cluster nodes must support the boot from the virtual hard disk (VHD) option.
- **PXE server** configured with Windows Deployment Services is needed for bare metal deployment.

Physical computer requirements

Expand table

Prerequisite	Details
BMC	Each physical computer must have a baseboard management controller (BMC) installed that enables out-of-band management by VMM. Through a BMC, you can access the computer remotely, independent of the operating system and control system functions such as the ability to turn the computer off or on.

Prerequisite	Details
	The BMCs must use one of the supported out-of-band management protocols, and the management protocol must be enabled in the BMC settings. Supported protocols: Intelligent Platform Management Interface (IPMI) versions 1.5 or 2.0; Data Center Management Interface (DCMI) version 1.0; System Management Architecture for Server Hardware (SMASH) version 1.0 over WS-Management (WS-Man); custom protocols such as Integrated Lights-Out (iLO). The BMCs must use the latest version of firmware for the BMC model. The BMCs must be configured with sign-in credentials and must use either static IP addressing or DHCP. If you use DHCP, we recommend that you configure DHCP to assign a constant IP address to each BMC. For example, by using DHCP reservations. The VMM management server must be able to access the network segment on which the BMCs are configured.
Operating system	Physical computers must be running Windows Server 2012 R2 or later.
Accounts	You'll need two Run As accounts. A Run As account for joining computers to the domain, and an account for access to the BMC on each computer.

Expand table

Prerequisite	Details
BMC	Each physical computer must have a baseboard management controller (BMC) installed that enables out-of-band management by VMM. Through a BMC, you can access the computer remotely, independent of the operating system and control system functions such as the ability to turn the computer off or on. The BMCs must use one of the supported out-of-band management protocols, and the management protocol must be enabled in the BMC settings. Supported protocols: Intelligent Platform Management Interface (IPMI) versions 1.5 or 2.0; Data Center Management Interface (DCMI) version 1.0; System Management Architecture for Server Hardware (SMASH) version 1.0 over WS-Management (WS-Man); custom protocols such as Integrated Lights-Out (iLO). The BMCs must use the latest version of firmware for the BMC model.

Prerequisite	Details
	The BMCs must be configured with sign-in credentials and must use either static IP addressing or DHCP. If you use DHCP, we recommend that you configure DHCP to assign a constant IP address to each BMC. For example, by using DHCP reservations. The VMM management server must be able to access the network segment on which the BMCs are configured.
Operating system	Physical computers must be running Windows Server 2016 or later.
Accounts	You'll need two Run As accounts. A Run As account for joining computers to the domain, and an account for access to the BMC on each computer.

PFX server requirements

Expand table

Prerequisite	Details
Deployment requirements	You must have a PXE server configured with Windows Deployment Services. If you've an existing PXE server in your environment configured with Windows Deployment Services, you can add that server to VMM. Then you can use it for provisioning in VMM (and VMM will recognize only the resulting servers). All other requests will continue to be handled by the PXE server according to how it's configured. If you don't have an existing PXE server, you can deploy the Windows Deployment Services role on a server running a supported operating system (Windows Server 2016 or later).
Location	The PXE server must be in the same subnet as the physical computers that you want to provision.
Windows Deployment Services installation	When you install Windows Deployment Services, you must install both the Deployment server and Transport server options. You don't need to add images. During host deployment, VMM uses a virtual hard disk that you've created and stored in the library. You don't need to configure settings on the PXE response tab. VMM provides its own PXE provider.

Prerequisite	Details
Permissions	When you add a PXE server, you must specify account credentials for an account that has local administrator permissions on the PXE server. You can enter a user name and password or specify a Run As account. You can create the Run As account before you begin or during deployment.

Virtual disk and template requirements

Expand table

Prerequisite	Details
Virtual hard disk	Ensure that you've a generalized virtual hard disk in a VMM library share. It must be running Windows Server 2016 or later. We recommend that for production servers, you use a fixed disk (.vhd or .vhdx file format) to increase performance and to help protect user data. Ensure that you've a generalized virtual hard disk in a VMM library share. It must be running Windows Server 2016 or later.
Dynamic disk	When you create a physical computer profile, VMM converts a dynamic disk to a fixed disk.
Custom drivers	If you plan to assign custom drivers to a physical computer profile, you add them to a VMM library share in one or more folders with a .CR (custom resources) extension. VMM recognizes them as custom resources.
Answer file	Like custom resources, if you want a physical computer profile to include references to an answer file (Unattend.xml file), create the answer file and add it to a VMM library share before you start deployment. For example, you might want to create an answer file to enable Remote Desktop Services and place it on a library share. Then you can select that file when you configure a physical computer profile.
RDS	If you use Remote Desktop Services (RDS) to manage servers, we recommend that you enable the RDS connections in the image. You can also enable RDS using an answer file in the physical computer profile.
Logical networks	If you've already configured logical networks or logical switches in VMM, you can include those configurations in the physical computer profile. To include static IP addressing controlled through a logical network in a physical computer profile, configure the logical network. The logical network must include at least one network site and static IP address pool.

Prerequisite	Details
	The network site must also be available to the host group or to a parent host group where you want to assign the hosts that you'll be creating from bare metal.
Logical switch	To use a logical switch, install all the necessary virtual switch extensions and extension providers, and create the switch before you create the physical computer profile. In the logical switch, as a best practice, include one or more port classifications for the virtual ports. To apply a logical switch to physical adapters in a physical computer profile, ensure that you've installed the intended number of NICs on the physical computer.

Deployment steps

1. **Before you start**: Verify the prerequisites above before you start.
2. **Prepare physical computer**: Set up the BIOS on each physical computer to support virtualization.
3. **Prepare the PXE server environment**: Add the PXE server to the VMM fabric.
4. **Add driver files**: Add driver files to the VMM library if you want to use custom drivers.
5. **Create profile**: Create a profile for the physical computers.
6. **Create the cluster**: Run the Create Clustered File Server Wizard to discover the physical computers, configure the cluster, and start the cluster deployment. The physical computers boot from a customized Windows PE image on the PXE server. The Failover Cluster and File Server roles are enabled. After the cluster is created, the Scale-Out File Server role is enabled. The computer is then restarted.
7. **Add nodes to SOFS cluster**: After you've provisioned the nodes, you can create a new cluster with them or add them to an existing one.

Prepare physical computers

Prepare each computer to support virtualization, as follows:

1. Set the BIOS boot order to boot from a Pre-Boot Execution Environment (PXE)-enabled network adapter as the first device.
2. Configure the sign-in credentials and IP address settings for the BMC on each computer.

3. If your environment has multiple DNS servers, where replication can take some time, we strongly recommend that you create DNS entries for the computer names that will be assigned to the physical computers, and allow time for DNS replication to occur. Otherwise, the deployment of the computers can fail.

Add a PXE server to the VMM fabric

1. Select **Fabric** > **Servers** > **Home** > **Add** > **Add Resources** > **PXE Server**.
2. In **Computer name**, specify the PXE server name.
3. Add the credentials for an account that has local administrator permissions on the PXE server. You can specify an existing Run As account or create a new account. Manually enter user credentials in the format domain_name\user_name. Then select **Add**.
4. In **Jobs**, verify that the job status is **Completed**, and close the dialog. The job sets up the new PXE server, installs the VMM agent on the PXE server, imports a new Windows Preinstallation Environment (Windows PE) image, and adds the machine account to VMM for the PXE server.
5. Verify that the PXE server is added in **Fabric** > **Servers** > **PXE Servers**. The agent status must be **Responding**.

Add custom resources to the library

If you plan to assign custom drivers, the driver files must exist in the library. You can tag the drivers in the library so that you can later filter them by tag. After the files are added, when you configure a physical computer profile, you can specify the driver files. VMM installs the specified drivers when it installs the operating system on a physical computer.

In the physical computer profile, you can select to filter the drivers by tags, or you can select to filter drivers with matching Plug and Play (PnP) IDs on the physical computer. If you select to filter the drivers by tags, VMM determines the drivers to apply by matching the tags that you assign to the drivers in the library to the tags that you assign in the profile. If you select to filter drivers with matching PnP IDs, you don't need to assign custom tags.

1. Locate a driver package that you want to add to the library.
2. In the library share that is located on the library server associated with the group where you want to deploy the physical computers, create a folder to store the drivers and copy the driver package to the folder.
3. We strongly recommend that you create a separate folder for each driver package, and that you don't mix resources in the driver folders. If you include other library

resources such as .iso images, .vhd files, or scripts with an .inf file name extension in the same folder, the VMM library server won't discover those resources. Also, when you delete an .inf driver package from the library, VMM deletes the entire folder where the driver .inf file resides.

4. In the VMM console > **Library** > **Library Servers**, expand the library server where the share is located, right-click the share, and select **Refresh**. After the library refreshes, the folder must appear.
5. Assign tags if required. In **Library**, expand the folder that you created to store the drivers, and select the folder that contains the driver package.
6. In the **Physical Library Objects**, right-click the driver .inf file and select **Properties**.
7. In the **Driver File Name Properties** > **Custom tags**, enter custom tags separated by a semicolon, or select **Select** to assign available tags, or to create and assign new ones. If you select **Select** and then select **New Tag**, you can change the name of the tag after you select **OK**. For example, if you added a network adapter driver file, you could create a tag that is named ServerModel NetworkAdapterModel, where ServerModel is the server model and NetworkAdapterModel is the network adapter model.

Create a physical computer profile

Before you start, determine whether the physical computers use Extensible Firmware Interface (EFI) or BIOS. If you've both, create a separate profile for each type.

1. Select **Library** > **Home** > **Create** > **Physical Computer Profile**.
2. In the **New Physical Computer Profiles Wizard** > **Profile Description**, enter a name and description and select **VM host**.
3. In **OS Image** > **Virtual hard disk file** > **Browse**, select the generalized virtual hard disk that you added to the library share. By default, if the disk is dynamic, VMM converts it to a fixed disk during host deployment. We recommend that for production servers, you use a fixed disk to increase performance and help protect user data.
4. In **Hardware Configuration** > **Management NIC**, select the network adapter you'll use to communicate with VMM and whether to use DHCP or a static address. If you want to use Consistent Device Naming (CDN) for the adapter or configure logical switches and ports, select **Physical Properties**. Select **Add** to add the adapter.
5. In **Disk**, specify the partitioning scheme for the first disk. You can use GPT if the physical computer profile is EFI. In **Partition Information**, select the volume label, whether to use all the remaining free space or a specific size, and whether to designate the partition as the boot partition. You can also add a new disk or

partition. During deployment, VMM will copy the virtual hard disk file to the boot partition and automatically create a system partition on the same disk.

6. In **Driver filter**, filter the drivers that will be applied to the operating system during host deployment. You can filter by Plug and Play ID or by specific tags. If you select to filter drivers with matching tags, ensure that you've added driver files to the library and assigned the corresponding tags.
7. In **OS Configuration**, specify the domain that the Hyper-V host or cluster must join, and specify the local admin credentials and identity information. Add the product key for installation, and set the time zone. In GUIRunOnce, you can specify one or more commands that will run when the user signs in to the Hyper-V host for the first time.
8. In **Host Settings**, specify the path of the host to store the files that are associated with virtual machines placed on the host. Don't specify drive C because it's not available for placement. If you don't specify a path, VMM placement will determine the most suitable location.
9. In **Summary**, verify the settings. Wait until **Jobs** shows a status of completed, and verify the profile in **Library** > **Profiles** > **Physical Computer Profiles**.

Provision a Scale-Out File Server cluster from bare metal

The Create Clustered File Server Wizard does the following:

1. Discovers the physical computers through out-of-band management.
2. Deploys the Windows Server operating system image on the computers using the physical computer profile (if configured to do so).
3. Enables the file server role on the computers.
4. Enables the Scale-Out File Server role on the cluster.
5. Adds the provisioned computers as a Scale-Out File Server cluster under VMM management.

Run the wizard:

1. Select **Fabric** > **Servers** > **Home** > **Create** > **File Server Cluster**.

2. In the **Create Clustered File Server Wizard** > **General**, enter a cluster name, file server name, and cluster IP addresses if needed.

3. In **Resource Type**, select the option to provision bare-metal computers. Select the physical computer profile and select **Next**.

4. In **Credentials and Protocols**, select **Browse** next to the Run As account and choose the account with permissions to access the BMC. In the **Protocol** list, select the out-of-band management protocol you want to use for discovery. If you want to use DCMI, select **Intelligent Platform Management Interface (IPMI)**. DCMI 1.0 isn't listed, but it's supported. Ensure that you use the latest version of firmware for the BMC model.

5. In **Discovery Scope**, specify the IP address scope that includes the IP addresses of the BMCs. You can add a single address, a subnet, or range.

6. In **Target Resources**, select the computers you want to provision, allow time for deep discovery, and select items to review and modify information.

   > ⓘ **Note**
   >
   > If the number of physical network adapters doesn't match the number of physical adapters defined in the computer profile, you'll need to add the missing information. If you don't want to deploy a computer immediately, you can select its BMC IP address and select **Remove**.

7. In **Deployment Customization**, configure the settings and when there are no more warnings about missing information, select **Next**.

   - **DHCP**: If your physical computer profile uses DHCP, select a BMC IP address and enter a computer name. Decide whether to skip the AD check. If you do the check, deployment will continue if the computer account exists. Select the entry for each BMC IP address.
   - **Static**: If the profile uses static IP addresses for each BMC IP address, enter a MAC address of the computer's network adapter that's used to communicate with VMM. Select the logical network you want to use. The default logical network is the one indicated in the profile. Select the IP subnet you want to use. The subnet list is scope to what's defined for the logical network in the associated network sites. You must select the IP subnet that corresponds to the physical location in which you're deploying the server and the network to which the adapter is connected. You can automatically assign an IP address or assign a specific address.

8. In **Summary**, confirm the settings and select **Finish**. To confirm the cluster was added, select **Fabric** > **Storage** > **File Servers**.

Next steps

Manage SOFS settings in the VMM fabric.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Manage SOFS settings in the VMM fabric

Article • 08/22/2024

You can manage scale-out file server (SOFS) in the System Center Virtual Machine Manager (VMM) fabric as follows:

- **Create storage pools**: Create storage pools from physical disks on SOFS nodes and allocate them.
- **Create file shares**: You can create file shares on a SOFS in the VMM fabric. You can set the storage type for a share as a storage pool, local pool, or volume.
- **QoS**: Set up a quality-of-service (QoS) policy for SOFS to control resources allocated to VMs.
- **Set a disk witness for a storage pool**: From VMM 2016, you can specify that the disk witness for a SOFS cluster must come from a particular storage pool. To do this, VMM creates a three-way mirror space and configures it as the disk witness for the cluster. The storage pool must have at least five physical disks.

Create storage pools

1. Select **Fabric** > **Storage** > **File Servers**. Right-click the SOFS server (not the nodes) and select **Manage Pools**.

2. In **Manage Pools of File Server**, select **New** to create a new pool or modify an existing one.

3. In **General**, specify a name and select a storage classification.

4. In **Physical Disks**, select the disks you want to include in the pool. Disks will be displayed in accordance with the SOFS settings. For example, a file server with shared storage might show SAS storage disks, or a file server using Storage Spaces Direct would show local disks attached to each node.

5. In **Default Settings**, retain the default settings unless you need to change for a specific reason.

   - **Fault domain**: When you select a fault domain, you specify how many copies of your data will be distributed across a cluster.

   ⓘ **Note**

> Fault domain isn't displayed for clusters configured with Storage Spaces Direct. These clusters have a fault domain of **Node** to indicate that copies of data are stored on multiple nodes in the cluster and data is available even if a specific node isn't.

- **Interleave**: Interleave (along with the number of columns) specify the way in which data is written to physical disks.

6. Select **OK** to save the storage pool settings. After the job completes, verify the pools in **Fabric** > **Storage** > **Classifications and Pools**.

Create a file share

1. Select **Fabric** > **Storage** > **Home** > **Create File Share**.
2. In **Create File Share Wizard** > **Storage Type**, select the SOFS on which you want to create a share. Enter a name and description for the share and select the storage pool you want to use. If the CSV exists, select **Volume** and specify it. If the folder path exists, select **Local path** and specify it. The file share inherits the classification of the storage pool.
3. In **Capacity**, specify the file share size and type. Leave the default type unless the disk is used for backups or deduplication, in which case NTFS is recommended.
4. In **Capacity** > **Resiliency**, for ReFS, resilience must be mirror (two or three-way). For NTFS, it can be mirror or parity (single or dual). The default is a three-way mirror.
5. Enable deduplication if necessary. Change the unit size allocation if required, and optionally enable storage tiers.
6. In **Summary**, review the settings and select **Finish**. Verify the file share in **Fabric** > **Storage** > **File Servers** > **File Shares**.

Set a storage QoS for a SOFS

System Center VMM 2016 and later include storage QoS policies to solve the **noisy neighbor** problem. This problem is common in virtualized environments. When two virtual machines (VMs) share a resource, say a disk, there's always a chance that one VM's usage of the resource exceeds that of the other. This can affect the performance of an app running on the VM. Storage QoS ensures:

- **Mitigation of noisy neighbor issues**: Ensures that a single VM doesn't consume all the resources and starves the other VMs of storage bandwidth.
- **Monitor end-to-end storage performance**: When VMs are started on a SOFS, their performance is monitored.

- **Manage storage I/O in accordance with business needs**: Storage QoS policies define minimum and maximum limits for VMs and ensure they're met even in over-provisioned environments. If policies can't be met, alerts are issued.

Set a storage QoS policy as follows:

1. Select **Fabric** > **Storage** > **QoS Policies** > **Create Storage QoS Policy**.
2. In **Create Storage QoS Policy Wizard** > **General**, specify a name and description for the policy.
3. In **Policy Settings**, select whether you want all the virtual hard disks for VMs to share resources equally or allocate resources per VM. If you choose to allocate per instance, you'll need to set a minimum and maximum IOPS. Then a virtual disk to which the policy is applied will receive the minimum and maximum limits.
4. In **Scope**, specify the file servers on which to apply the policy. You can apply the policy to multiple servers, which is useful when you migrate VMs across servers so that QoS policy settings remain the same.
5. In **Summary**, review the settings and select **Finish**. Verify the policy in **Fabric** > **Storage** > **QoS Policies**.

Set a disk witness for the SOFS

1. Select **Fabric** > **Storage** > **File Servers**. Right-click the SOFS server (not the nodes) and select **Properties**.
2. In **General**, select **Use disk witness for this file server from the specified pool** to indicate that the disk witness for the SOFS must come from a specific storage pool. VMM creates a three-way mirror space, and configures it as the disk witness for the cluster.

Next steps

Set QoS for storage resources.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set QoS for storage resources

Article • 08/22/2024

This article describes how to set up quality-of-service (QoS) policies to control IOPS for a scale-out file server (SOFS) in the System Center Virtual Machine Manager (VMM) fabric.

Before you start

You can verify the status of currently defined QoS policies for a SOFS cluster by running the Get-StorageQoSPolicy PowerShell cmdlet on a cluster node.

Create a QoS policy

1. Select **Fabric** > **Storage** > **QoS Policies** > **Create Storage QoS Policy**.
2. In the wizard > **General**, specify a policy name.
3. In **Policy Settings**, specify how the policy must apply. Select **All virtual disk instances share resources** to specify that the policy must be applied to all the virtual disks on the file server (pooled, single instance). Select **Resources allocated to each virtual disk instance** to specify that the policy is applied separately to each specified virtual disk (multi-instance). Specify the minimum and maximum IOPS. A setting of 0 means that no policy is enforced.
4. In **Scope**, select the file servers to which the policy is applied. If you select multiple servers, each server will receive the same policy GUID. This ensures there won't be any issues if you migrate VM storage.
5. In **Summary**, verify settings and finish the wizard.

Next steps

When you deploy a virtual machine and place it on a host, you can select the storage QoS when you review VM settings in **Virtual Machine Settings** > **Machine Resources** > **Virtual Hard Disk**. Learn more about deploying VMs.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Provision virtual machines in the VMM fabric

Article • 08/30/2024

This article provides an overview of provisioning Virtual Machines (VMs) in the System Center Virtual Machine Manager (VMM) compute fabric. Learn about provisioning methods and the features provided by VMM during provisioning.

Provisioning

VMs can be provisioned using multiple methods:

- Create VMs from a blank virtual hard disk: Create a VM and install an operating system from an .iso image, removable media, or from a network boot with a PXE server.
- Create a VM from an existing virtual hard disk: Create a VM from a virtual hard disk in the VMM library. We recommend a VHD that's been generalized with Sysprep.
- Clone a VM from an existing VM: Clone an existing VM in the VMM library to create a new one. We recommend you clone a VM that's been generalized with Sysprep.
- Create a VM from a template: Create VMs with consistent settings configured in a VM template. VM templates are XML objects stored in the VMM library. They can be used to control and restrict VM settings available to self-service users. Template settings include the guest operating system profile, a hardware profile, and one or more VHDs that can be used to create a new VM.
- **Create a VM in a service deployment**: In VMM, you can create services that are logical grouping of VMs that are configured and deployed as s single entity. A single tier service includes a single VM. Multi-tier services have multiple VMs.
- Rapidly provision a VM using storage area network (SAN) copy: Deploy a VM using SAN copy abilities, such as snapshot and clone. You can rapidly provision standalone VMs or VMs that are provisioned in a service.

Deploying a VM guest cluster

On a Hyper-V cluster, you can deploy a guest failover cluster that consists of multiple VMs and uses shared .vhdx files. VMM supports the following:

You can deploy a guest failover cluster that uses shared .vhdx files on a Hyper-V failover cluster. In this scenario, if Hyper-V uses Cluster Shared Volumes (CSVs) on block-level storage, then the shared vhdx files are stored on a CSV that's configured as shared storage. Alternatively, Hyper-V can use SMB file-based storage deployed by Scale-Out File Server (SOFS), as the location of the shared .vhdx files. No other storage types are supported, and third-party SMB storage isn't supported.

VM placement

When you deploy or migrate a VM, VMM uses intelligent VM placement to evaluate available hosts.

- The placement algorithm analyzes performance data for the workload and the host and rates hosts on a scale of one to five stars to indicate the best placement choice.

- Placement includes a preferred and possible owners feature that allows to specify which hosts are preferred and possible if failover of VMs occurs.

- Placement considers storage classifications. Clouds can be scoped to limit VM placement to specific storage classifications only.

- Placement options can be selected as follows:
  - **Create a new VM**: The placement process offers a suggestion for the host. If a self-service user creates a VM, the host is automatically assigned by VMM based on the highest rating.
  - **Migrate a VM**: During migration, VMM provides host ratings to help you select a host.
  - **Convert a VM to Hyper-V**: The conversion wizard provides rating for hosts so that you can select the best one.

Host ratings

- VMM evaluates all hosts within a selected host group and any hosts contained in child host groups. Host ratings are calculated on a scale of 0 to 5 stars, where five stars indicate the highest rating. The ratings are based on default criteria that don't include all information. For example, network connection speed isn't considered.

- Ratings are based on individual hosts, and not on the relative suitability of all the available hosts. Ratings for one host don't change based on the ratings of the other hosts.

- VMM calculates host ratings according to specific formulas, as described in the following table.

  - **CPU rating**: [1 – (CPU Utilization / (100 – CPU Reserve))] x CPU Weight
  - **Memory (RAM) rating**: [1 – (Memory Used / (Total Memory – Memory Reserve))] x Memory Weight
  - **Disk I/O capacity rating**: [1 – (Disk IOPS / Maximum Disk IOPS)] x Disk Weight
  - **Network rating**: [1 – (Network Utilization / (100 – Network Reserve))] x Network Weight

- A host is rated only when a virtual machine needs to be placed.

- The information gathered about a host is compared to the information about the resources required by the VM, and a rating is assigned to the host.

- During automatic placement, VMM attempts to use the host assigned the highest rating. During manual placement, the host rating is displayed so that you can select the appropriate host.

- VMM measures CPU, memory, disk, and network usage approximately every 10 minutes to recalculate an average rating that is an average of all the measurements taken that the last action that reset the host rating. Host ratings are reset when the following happens:
  - A new virtual machine is created
  - A virtual machine is deployed, stored, migrated, or deleted
  - A virtual machine is turned on, off, or moved into a stopped, paused, or saved state.

Zero rating

A host might be assigned a zero rating if it doesn't meet conditions to receive a non-zero rating. To receive a non-zero rating, the following criteria are required:

- The host must have at least one hard disk with enough storage to hold the total hard disk space required by the virtual machine. With dynamic hard disks, the current hard disk size is used, not the maximum hard disk size.

- The memory required for the virtual machine must be less than the current amount of memory available on the host. A host must also have sufficient memory available to start the virtual machine.

  ⓘ **Note**

> VMM does offer the option of overcommitting cloud and host group capacity for replica VMs.

- If dynamic memory is enabled, ensure the following:
  - If the virtual machine (including any one of its checkpoints) is configured to use Dynamic Memory, the host must also have Dynamic Memory enabled. If it doesn't, the placement of the virtual machine will be blocked during creation or migration.
  - For placement of a new or stopped virtual machine, the host must meet at least the startup memory requirement for the virtual machine.
  - For placement of a running virtual machine, the host must meet at least the current memory requirement for the virtual machine.
  - For placement of a virtual machine in a saved state, the last known memory usage value of the virtual machine will be compared to the startup memory of the virtual machine.

- The host must contain all the virtual networks required for the virtual machine. If you use network tags, the network location tags for the virtual machine and host must be identical.

- A host in maintenance mode automatically receives a zero rating.

- If Microsoft RemoteFX 3D video adapter is enabled on the virtual machine, the host must support RemoteFX and have one or more RemoteFX-capable graphics processing units (GPUs) with sufficient available memory. If these conditions aren't available and the virtual machine is running, placement will be blocked. If it's stopped or in a saved state, a zero rating with a warning will be issued, but placement won't be blocked.

- Highly available virtual machines must be placed on clustered hosts. VMM assigns zero stars to hosts that aren't clustered but manual placement isn't blocked. If you migrate a highly available virtual machine to a non-clustered host, the virtual machine will no longer be highly available after the migration.

- VMM blocks migration of Hyper-V hosts to hosts running different virtualization software. Migration of a virtual machine with specific features not allowed by the virtualization software that is running on a host will be blocked. For example, Hyper-V hosts don't allow booting up from a SCSI hard disk.

Handling Generation 1 and 2 VMs

In VMM, you can create Generation 1 and Generation 2 VMs.

- You can add VM templates specifying either Generation 1 or Generation 2 to a service template. Properties will appear for the generation you choose.
- Generation 2 VMs can only run on a host with a host operating system that supports them - Windows Server 2012 R2 and later. For example, VMM won't place a Generation 2 VM on a host running Windows Server 2012.
- When you use a virtual hard disk in .vhd format for a VM or VM template, the VM is automatically Generation 1 because .vhd doesn't support Generation 2. If you use .vhdx, you can select which option you want to use.
- If you use an existing virtual machine or virtual machine template as the starting point for a new virtual machine or virtual machine template, the generation is determined by the existing virtual machine or virtual machine template.
- If you create a hardware profile, you can choose between Generation 1 and 2. When you incorporate the profile into a VM or VM template, you specify the generation you want to use.
- In all wizards and PowerShell cmdlets, you'll be offered configuration options in line with the generation of the VM.
- Generation 1 and 2 VMs don't handle boot order in the same way.
    - You can customize the start order for Generation 1 VMs in the VMM console in the hardware settings when you create a VM. You can also customize using the BootOrder PowerShell parameter.
    - To customize the start order for Generation 1 VMs, you need to use PowerShell using the FirstBootDevice parameter when you create a VM. For example, to set the first boot device as the network adapter type: **Set-SCVMTemplate -Template "Generation2template" –FirstBootDevice "NIC,0"**

Optimizing provisioning

Differencing disks

- A differencing disk is a VHD that stores changes made about another VHD or guest operating system by storing them in a separate file.
- When you create a differencing disk, you associate another VHD with it (the parent disk). The differencing disk stores all the changes that would otherwise be made to the parent disk if the differencing disk didn't exist.
- In essence, the differencing disk saves changes without altering the parent disk.
- Multiple differencing disks can use the same parent VHD.

VMM optimizes support for differencing disks to provide the following:

- Optimized migration of storage that utilizes differencing disks. During a migration, VMM doesn't migrate base disks unless it's necessary.
- Optimized virtual machine deployment time by utilizing differencing disks. VMM will attempt to identify and utilize differencing disks on the target computer.
- When differencing disks are utilized, deployment of the base virtual disk is optimized by taking advantage of the Windows Offloaded Data Transfers (ODX) capability to copy files to the guest machine during service deployment.
- Optimize time and storage of cloning of virtual machines by utilizing differencing disks. VMM provides the option to create and utilize differencing disks during a cloning operation.

  > ⓘ **Note**
  >
  > If the parent disks are lost or corrupted, all VHDs that depend on them are also lost. You must have a backup plan in place.

If you're using differencing disks, you must optimize management by ensuring that unused parent HDs are removed regularly.

Fast file copy

During virtual machine deployment, VMM needs to move and copy large files, such as VHDs, between two locations.

Fast file copy improves the performance of file transfers, mostly using Windows Offloaded Data Transfers (ODX). In VMM, background intelligent transfer (BITS) is still used as a mechanism for file transfers, but VMM uses ODX when possible (for example, when copying files to SANs that support ODX). This greatly improves the time performance of virtual machine deployments.

Provisioning VMware VMs

After you've set up a vCenter server and ESX/ESXi hosts, you can provision VMware VMs like any other VM. Note the following:

- You can organize and store VMware VMs in the VMM library.
- You can organize and store VMware virtual machines, .vmdk (VMDK) files, and VMware templates in the VMM library.

- You can create VMs from VMware templates stored in the library. You can also import templates stored on vSphere hosts (only template metadata is imported to VMM). VMM doesn't support older VMDK disk types. These disk types are supported:
  - Regular VMDK files (VMFS and monolithic flat)
  - VMDK files that are used to access physical disks (vmfsPassthroughRawDeviceMap)
  - Snapshots (vmfssparse)
- You can create new VMware VMs from VMDK templates.
- You can deploy VMM services to vSphere hosts but not vApps.
- You can place VMs on VMware hosts based on host ratings when you create, deploy, or migrate VMware VMs. This includes concurrent VM deployment when you're deploying a service.
- You can use dynamic optimization and power optimization for VMware VMs.
- You can do regular VMM networking tasks, including assigning logical networks, static IP address, and MAC address to Windows-based VMs running on VMware.
- VMM doesn't support VMware VMs with VHDs connected to an IDE bus.
- VMM supports VMware thin provision hard disk through the dynamic disk type.

  > ⓘ **Note**
  >
  > If you create and deploy a VM to a vSphere host configured to use a dynamic disk, the disk will be thin provisioned. If a VM was created as a thin provisioned disk, out-of-band VM will display it as dynamic. If you save a thin provision disk to the library, VMM will save it as thick. It remains thick if you create a VM from it.

Converting VMware VMs to Hyper-V

VMM can be used as a V2V conversion tool to convert VMware VMs to Hyper-V VMs.

- **Convert Virtual Machine Wizard**: In the VMM console, you can use this wizard. This method has a few minor limitations:
  - Not supported for vSphere versions earlier than 4.1.
  - You can't convert VMware workstations.
  - You can't convert VMs with virtual hard disks connected to an IDE bus.

- Online conversions aren't supported. You need to power off the VMware VMs.
- Anti-virus apps must be supported.
- VMware tools must be uninstalled from the guest operating system of the VM.

Static MAC address for VMs deployed on a VMM cloud

In earlier releases, VMM allowed the users to set a static MAC address on the VMs deployed on the hosts and didn't have an option to set static MAC address for the VMs deployed on the cloud.

VMM allows you to set a static MAC address for the VMs deployed on VMM Cloud.

Use the following steps:

> ⓘ **Note**
>
> MAC address that you wish to assign to the VM must be part of an accessible MAC pool. As self-service users don't have visibility into the fabric MAC pools, they would need to coordinate with admins to ensure that the MAC address is part of the accessible MAC pool.

You can set the static MAC address on the VM while:

- Deploying a new VM onto the cloud from VHD/VM Template. or
- Changing the MAC address on an existing VM deployed to the cloud.

Set static MAC while deploying a new VM onto the cloud from VHD/VM template

1. In VMM Console, navigate to **VMs and Services** > **Home** > **Clouds**.

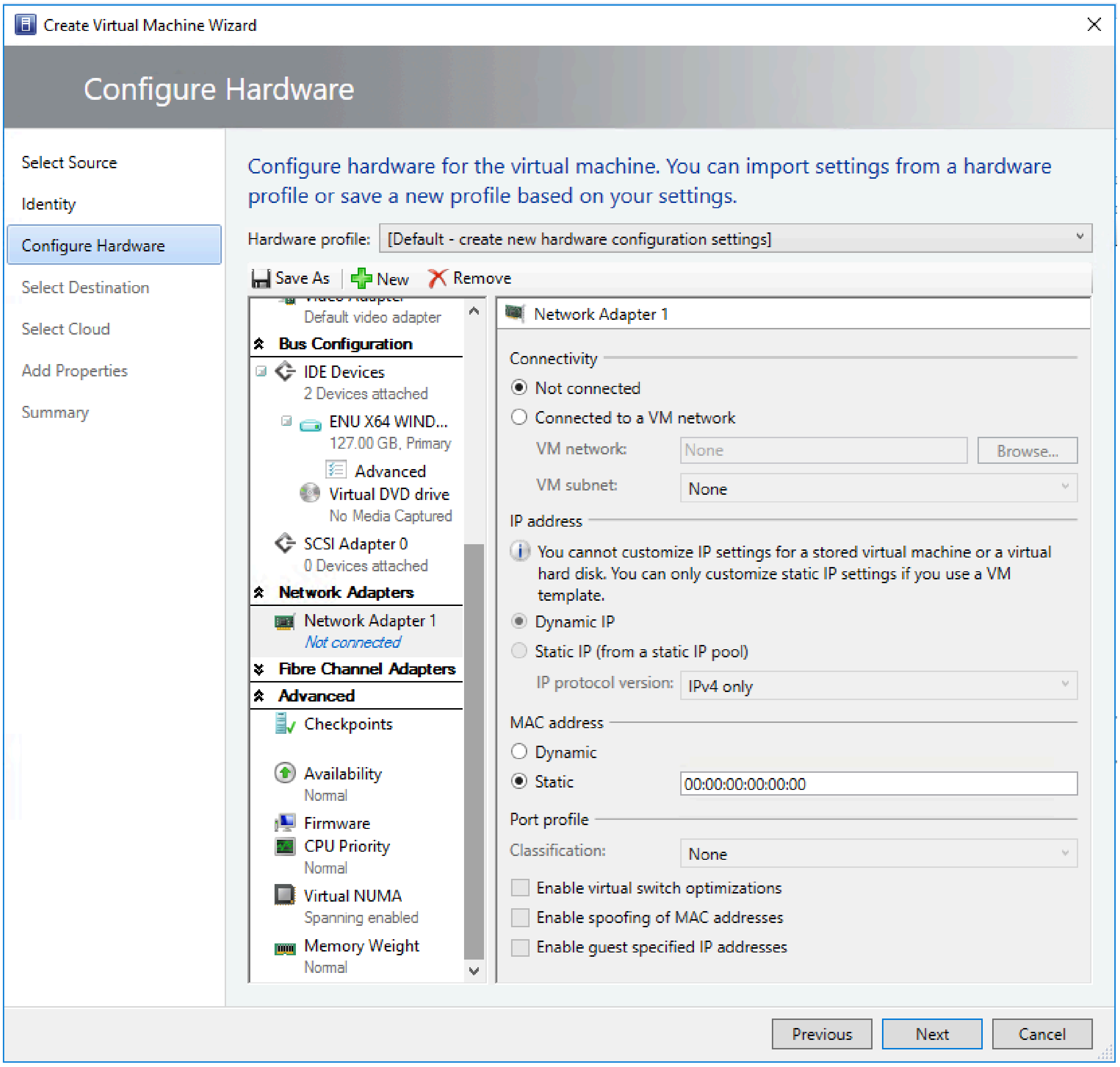
2. Select the cloud to deploy the VM.

3. Right-click > **Create Virtual Machine** to enter the Create Virtual Machine wizard and create the VM.

4. Right-click the VM and select **Properties**.

5. Navigate to the **Configure Hardware** page and select the network adapter to which you want to assign a static MAC address.

6. In the **MAC address** section, select **Static** and enter the MAC address in the text box.



Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings.

Hardware profile: [Default - create new hardware configuration settings]

Network Adapter 1

Connectivity

● Not connected

○ Connected to a VM network

VM network: None

VM subnet: None

IP address

You cannot customize IP settings for a stored virtual machine or a virtual hard disk. You can only customize static IP settings if you use a VM template.

● Dynamic IP

○ Static IP (from a static IP pool)

IP protocol version: IPv4 only

MAC address

○ Dynamic

● Static 00:00:00:00:00:00

Port profile

Classification: None

□ Enable virtual switch optimizations

□ Enable spoofing of MAC addresses

□ Enable guest specified IP addresses

Change the MAC address for a VM deployed on the cloud

1. Navigate to a VM deployed on the cloud for which you want to assign a static MAC address.
2. Follow the steps 4 to 6 from the above procedure.

Next steps

- Create VMs from a blank virtual hard disk.
- Create a VM from an existing virtual hard disk
- Clone a VM from an existing VM
- Create a VM from a template

Feedback

Was this page helpful? Yes No

Provide product feedback ↗ | Get help at Microsoft Q&A

Deploy VMs in the VMM fabric from a blank virtual hard disk

Article • 08/30/2024

This article describes how to create and deploy virtual machines in the System Center Virtual Machine Manager (VMM) fabric from a virtual hard disk (VHD).

Before you start

- To complete the steps, you must be an administrator or delegated administrator on the VMM server or a self-service user.
- If you're a self-service user, you need **Deploy** permissions with the **Store and re-deploy** action assigned. You must first deploy the VM to a private cloud and then store it in the library.
- You can only customize static IP address settings if you create a VM from a VM template.
- You can use VMM to configure the availability settings for the virtual machine. Learn more.

Create a VM

1. Select **VMs and Services** > **Create Virtual Machine** >**Create Virtual Machine**.

2. In **Create Virtual Machine Wizard** > **Select Source**, select **Create the new virtual machine with a blank virtual hard disk** > **Next**.

3. In **Identity**, specify the VM name and an optional description. In the **Generation** box, select **Generation 1** or **Generation 2**. And then select **Next**.

4. In **Configure Hardware** page, either select the profile that you want to use from the **Hardware profile** list or configure the hardware settings manually. The hardware setting displayed will differ depending on whether you're deploying a Generation 1 or Generation 2 machine. Select **Next**.

    - In **Compatibility**, if you want to deploy the virtual machine to a private cloud, select a capability profile that is available to the private cloud.

    - In **Bus Configuration**, if you want to install an operating system from a DVD or an .iso image, ensure there's a virtual DVD drive that is configured to use an available option, such as the **Existing ISO image file** option. If you want to use an ISO image file, the file must be present in the VMM library.

- If you want to store the virtual machine in the VMM library before you deploy it to a host, use of one of the blank virtual hard disks that are provided by default in the VMM library. Select the VHD in **Bus Configuration**. Select **Use an existing virtual hard disk** > **Browse**, and select a blank hard disk

- If the virtual machine is a generation 1 that boots from the network to install an operating system, in **Network Adapters**, use the legacy network adapter type.

5. In **Select Destination** page, specify how the virtual machine must be deployed - in a private cloud, on a host, or stored in the library.

Deploy the VM in a private cloud

1. In **Select Cloud**, select the private cloud on which you want to place the virtual machine. If you're connected as an Administrator, you can select the host on which the virtual machine must be deployed in the private cloud. Cloud suggestions are based on a 0-5 star rating. Learn more. Verify the settings and modify if required:

   - **Expected utilization**: Expected utilization for a VM created from a blank VHD is based on standard defaults. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.
   - **Make this VM highly available**: With this option selected, only hosts that are located in a cluster are available for selection.
   - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.
   - **Rating Explanation**: Provides an explanation if a host received a zero rating.
   - **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).
     The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded Data Transfers (ODX). Learn more.

2. In **Configure Settings**, review the VM settings. Either accept the default VM path on the host or specify a different location. You can optionally select to **Add this path to the list of default virtual machine paths on the host**. In **Machine Resources**, accept the default values for the VHD or modify as required. To prevent placement from choosing its own values, select the pin icon next to the setting. This option isn't available for self-service users.

3. In **Select Networks**, if it appears, optionally select the network settings, and select **Next**.

4. In **Add Properties**, configure the action to take when the host starts or stops, and the operating system that you'll install on the VM. Select **Next.**

5. In **Summary**, confirm the settings, and select **Create**. Confirm that the VM was created in **VMs and Services** > **Clouds** and select the cloud. The virtual machine appears in the **VMs** pane.

Deploy the VM on a host

1. In **Select Host**, view the ratings, select the host on which you want to deploy the VM, and select **Next**. The host suggestions are based on a 0-5 star rating. Learn more. Verify the settings and modify if required:

    - **Expected utilization**: Expected utilization for a VM created from a blank VHD is based on standard defaults. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.
    - **Make this VM highly available**: With this option selected, only hosts that are located in a cluster are available for selection.
    - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.
    - **Rating Explanation**: Provides an explanation if a host received a zero rating.
    - **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't recognize a virtual machine that is stored on a SAN as available for deployment by using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).
      The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded Data Transfers (ODX). Learn more.

2. In **Configure Settings**, review the VM settings. Either accept the default VM path on the host or specify a different location. You can optionally select to **Add this path to the list of default virtual machine paths on the host**. In **Machine Resources**, accept the default values for the VHD, or modify as required. To prevent placement from choosing its own values, select the pin icon next to the setting. This option isn't available for self-service users.

3. In **Select Networks**, if it appears, optionally select the network settings, and select **Next**.

4. In **Add Properties**, configure the action to take when the host starts or stops, and the operating system that you'll install on the VM. Select **Next.**

5. On the **Summary** page, confirm the settings and select **Create**.

Store the VM in the library

1. In **Select Library Server**, select the library server that you want to use and select **Next**.
2. In **Select Path**, specify the library share location to store the virtual machine. Select **Browse** to select a library share and an optional folder location, select **OK**, and select **Next**.
3. In **Summary**, confirm the settings and select **Create**.
4. To confirm that the virtual machine was created, in the **Library** workspace, in the **Library** pane, expand **Library Servers**, expand the library server where you stored the virtual machine, and select **Stored Virtual Machines and Services**. The stored virtual machine appears in the **Physical Library Objects** pane.

Next steps

After you create the virtual machine, you can install an operating system from an .iso image, from a CD or DVD or from a network boot if a Pre-Boot Execution Environment (PXE) server is available.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Deploy VMs in the VMM fabric from an existing virtual hard disk

Article • 08/30/2024

This article describes how to create and deploy virtual machines in the System Center Virtual Machine Manager (VMM) fabric from an existing virtual hard disk (VHD).

Before you start

- To complete the steps, you must be an administrator or delegated administrator on the VMM server or a self-service user.
- If you're a self-service user, you need **Deploy** permissions with the **Store and re-deploy** action assigned. You must first deploy the VM to a private cloud and then store it in the library.
- The VHD you want to use must be stored in the VMM library. Learn more
- Use a VHD that has been generalized using Sysprep. If you don't, then the identity of the cloned VM will be the same as the source VM, and issues might occur if you turn them on together.

Create a VM

1. Select **VMs and Services** > **Create Virtual Machine** > **Create Virtual Machine**.

2. In **Create Virtual Machine Wizard** > **Select Source**, select **Use an existing virtual machine, VM template, or virtual hard disk** > **Browse**. Select an existing VHD.

3. In **Identity**, specify the VM name and an optional description. If the VHD you choose is in the .vhdx format, in the **Generation** box, select **Generation 1** or **Generation 2**. Select **Next**.

4. In **Configure Hardware**, either select the profile that you want to use from the **Hardware profile** list or configure the hardware settings manually. The hardware setting displayed will differ depending on whether you're deploying a Generation 1 or Generation 2 machine. Select **Next**.

   - In **Compatibility**, if you want to deploy the virtual machine to a private cloud, select a capability profile that is available to the private cloud.
   - In **Bus Configuration**, if you want to install an operating system from a DVD or an .iso image, ensure there's a virtual DVD drive that is configured to use

an available option, such as the **Existing ISO image file** option. If you want to use an ISO image file, the file must be present in the VMM library.
- If you want to store the virtual machine in the VMM library before you deploy it to a host, use one of the blank virtual hard disks that are provided by default in the VMM library. Select the VHD in **Bus Configuration**. Select **Use an existing virtual hard disk** > **Browse**, and select a blank hard disk
- If the virtual machine is a Generation 1 that boots from the network to install an operating system, in **Network Adapters**, use the legacy network adapter type.

5. In **Select Destination** page, specify how the virtual machine must be deployed - in a private cloud, on a host, or stored in the library.

Deploy the VM in a private cloud

1. In **Select Cloud**, select the private cloud on which you want to place the virtual machine. If you're connected as an Administrator, you can select the host on which the virtual machine must be deployed in the private cloud. Cloud suggestions are based on a 0-5 star rating. Learn more. Verify the settings and modify if required:

   - **Expected utilization**: Expected utilization for a VM created from a blank VHD is based on standard defaults. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.

   - **Make this VM highly available**: With this option selected, only hosts that are located in a cluster are available for selection.

   - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.

   - **Rating Explanation**: Provides an explanation if a host received a zero rating.

   - **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

     The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded

Data Transfers (ODX). Learn more.

2. In **Configure Settings**, review the VM settings. Either accept the default VM path on the host or specify a different location. You can optionally select to **Add this path to the list of default virtual machine paths on the host**. In **Machine Resources**, accept the default values for the VHD or modify as required. To prevent placement from choosing its own values, select the pin icon next to the setting. This option isn't available for self-service users.

3. In **Select Networks**, if it appears, optionally select the network settings, and select **Next**.

4. In **Add Properties**, configure the action to take when the host starts or stops and the operating system that you'll install on the VM. Select **Next.**

5. In **Summary**, confirm the settings and select **Create**. Confirm that the VM was created in **VMs and Services** > **Clouds** and select the cloud. The virtual machine appears in the **VMs** pane.

Deploy the VM on a host

1. In **Select Host**, view the ratings, select the host on which you want to deploy the VM, and select **Next**. The host suggestions are based on a 0-5 star rating. Learn more. Verify the settings and modify if required:

   - **Expected utilization**: Expected utilization for a VM created from a blank VHD is based on standard defaults. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.

   - **Make this VM highly available**: With this option selected, only hosts that are located in a cluster are available for selection.

   - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.

   - **Rating Explanation**: Provides an explanation if a host received a zero rating.

   - **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded Data Transfers (ODX). Learn more.

2. In **Configure Settings**, review the VM settings. Either accept the default VM path on the host or specify a different location. You can optionally select to **Add this path to the list of default virtual machine paths on the host**. In **Machine Resources**, accept the default values for the VHD or modify as required. To prevent placement from choosing its own values, select the pin icon next to the setting. This option isn't available for self-service users.

3. In **Select Networks**, if it appears, optionally select the network settings, and select **Next**.

4. In **Add Properties**, configure the action to take when the host starts or stops and the operating system that you'll install on the VM. Select **Next.**

5. In **Summary**, confirm the settings and select **Create**.

Store the VM in the library

1. In **Select Library Server**, select the library server that you want to use and select **Next**.
2. In **Select Path**, specify the library share location to store the virtual machine. Select **Browse** to select a library share and an optional folder location, select **OK**, and select **Next**.
3. In **Summary**, confirm the settings and select **Create**.
4. To confirm that the virtual machine was created, in the **Library** workspace, in the **Library** pane, expand **Library Servers**, expand the library server where you stored the virtual machine, and select **Stored Virtual Machines and Services**. The stored virtual machine appears in the **Physical Library Objects** pane.

Next steps

Manage the VM settings.

Feedback

Clone VMs from another VM in the VMM fabric

Article • 08/30/2024

This article describes how to create and deploy virtual machines by cloning existing VMs in the System Center Virtual Machine Manager (VMM) fabric.

Before you start

- To complete the steps, you must be an administrator or delegated administrator on the VMM server or a self-service user.
- When you clone a virtual machine, the existing virtual machine source isn't deleted. We recommend that you clone a virtual machine that has been prepared and generalized with the Sysprep tool. If you don't use a generalized virtual hard disk, the identity of the new virtual machine will be the same as the source. Issues might occur if you turn on two virtual machines with the same identity at the same time.
- You can clone a virtual machine that is deployed on a host. The machine can be online, stopped, or in a saved state.
- You can clone a VM that is stored in the VMM library.
- The option to use differencing disk optimizations is automatically applied when you deploy the virtual machine on a host if a base disk exists on that host.
- If you're a self-service user, you need **Deploy** permissions with the **Store and re-deploy** action assigned. You must first deploy the VM to a private cloud and then store it in the library.

Create a VM

1. Select **VMs and Services** > **Create Virtual Machine** > **Create Virtual Machine**.
2. In **Create Virtual Machine Wizard** > **Select Source**, select **Use an existing virtual machine, VM template, or virtual hard disk** > **Browse**. Select an existing VM.
3. In **Select Source**, select **Next**.
4. In **Configure Hardware**, optionally configure any available settings. Select **Next**.
5. In the **Select Destination** page, specify how the virtual machine must be deployed - in a private cloud, on a host, or stored in the library.

Deploy the VM in a private cloud

1. In **Select Cloud**, select the private cloud on which you want to place the virtual machine. If you're connected as an Administrator, you can select the host on which the virtual machine must be deployed in the private cloud. Cloud suggestions are based on a 0-5 star rating. Learn more. Verify the settings and modify if required:

   - **Expected utilization**: Expected utilization for a VM created from a blank VHD is based on standard defaults. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.

   - **Make this VM highly available**: If this option is selected, only hosts that are located in a cluster are available for selection.

   - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.

   - **Rating Explanation**: Provides an explanation why a host received a zero rating.

   - **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

     The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded Data Transfers (ODX). Learn more.

2. In **Configure Settings**, review the VM settings. Either accept the default VM path on the host or specify a different location. You can optionally select to **Add this path to the list of default virtual machine paths on the host**. In **Machine Resources**, accept the default values for the VHD or modify as required. To prevent placement from choosing its own values, select the pin icon next to the setting. This option isn't available for self-service users.

3. In **Select Networks**, if it appears, optionally select the network settings and select **Next**.

4. In **Add Properties**, configure the action to take when the host starts or stops, and the operating system that you'll install on the VM. Select **Next.**

5. In **Summary**, confirm the settings, and select **Create**. Confirm that the VM was created in **VMs and Services** > **Clouds** and select the cloud. The virtual machine appears in the **VMs** pane.

Deploy the VM on a host

1. In **Select Host**, view the ratings, select the host on which you want to deploy the VM, and select **Next**. The host suggestions are based on a 0-5 star rating. Learn more. Verify the settings and modify if required:

    - **Expected utilization**: Expected utilization for a VM created from a blank VHD is based on standard defaults. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.

    - **Make this VM highly available**: With this option selected, only hosts that are located in a cluster are available for selection.

    - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.

    - **Rating Explanation**: Provides an explanation if a host received a zero rating.

    - **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

      The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded Data Transfers (ODX). Learn more.

2. In **Configure Settings**, review the VM settings. Either accept the default VM path on the host or specify a different location. You can optionally select to **Add this path to the list of default virtual machine paths on the host**. In **Machine Resources**, accept the default values for the VHD or modify as required. To prevent placement from choosing its own values, select the pin icon next to the setting. This option isn't available for self-service users.

3. In **Select Networks**, if it appears, optionally select the network settings, and select **Next**.

4. In **Add Properties**, configure the action to take when the host starts or stops, and the operating system that you'll install on the VM. Select **Next.**

5. On the **Summary** page, confirm the settings and select **Create**.

Store the VM in the library

1. In **Select Library Server**, select the library server that you want to use, and select **Next**.
2. In **Select Path**, specify the library share location to store the virtual machine. Select **Browse** to select a library share and an optional folder location, select **OK**, and select **Next**.
3. In **Summary**, confirm the settings and select **Create**.
4. To confirm that the virtual machine was created, in the **Library** workspace, in the **Library** pane, expand **Library Servers**, expand the library server where you stored the virtual machine, and select **Stored Virtual Machines and Services**. The stored virtual machine appears in the **Physical Library Objects** pane.

Next steps

- Manage the VM settings.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Deploy VMs with rapid provisioning using SAN copy in the VMM fabric

Article • 08/30/2024

This article describes how to rapidly provision VMs in the System Center Virtual Machine Manager (VMM) fabric using SAN copy.

Rapid provisioning provides a method for deploying new virtual machines to storage arrays without needing to copy VMs over the network. VMM uses the SAN infrastructure for cloning VMs, with a VM template to customize the guest operating system.

- You can use rapid provisioning to deploy standalone VMs and VMs that are deployed as part of a service.
- You create a SAN copy-capable template from a virtual hard disk (VHD) that resides on a storage logical unit that supports SAN copy through cloning or snapshots.
- When you create a VM using the SAN copy-capable template, VMM quickly creates a read-write copy of the logical unit that contains the VHD and places the virtual machine files on the new logical unit. When VMM deploys a virtual machine using rapid provisioning through SAN copy, VMM uses a SAN transfer instead of a network transfer. During a SAN transfer, a SAN copy of the logical unit that contains the virtual machine is created and is assigned to the destination host or host cluster. Because the files for a virtual machine aren't moved over the network when you transfer a virtual machine over a SAN, it's much faster than a transfer over a standard network.
- You can use either of the following methods to create a SAN copy-capable template.
  - Create a SAN-copy capable template from a new VM
  - Create a SAN-copy capable template from an existing VM

Before you start

- Any storage that is accessible by the provisioned computer can be partitioned during the provisioning process even if a specific disk is selected to be used as the operating system disk. In this case, data will be lost. To guarantee the use of a specific boot volume, use deep discovery and don't restart the computer before the deployment of the operating system completes.

- The storage array must support the new storage management features in VMM.

- The storage array must support cloning or snapshots, and the cloning or snapshots feature must be enabled. This might require additional licensing from your storage vendor.

- The storage pool that you want to use for rapid provisioning must be under VMM management. To meet this requirement, you must add the Storage Management Initiative Specification (SMI-S) provider for the array, discover storage pools, classify the storage, and set the preferred allocation method for the storage array to either snapshot or cloning.

- The storage pool that you want to use for rapid provisioning must be allocated to the host group where you want to use rapid provisioning of virtual machines.

- The Hyper-V hosts that you want to use as placement destinations must be members of the host group. Additionally, the following prerequisites must be met:

  - If you want to create a SAN-copy capable template from a new virtual machine, the host where you create the virtual machine must also be a member of this host group.

  - If you want to create a SAN-copy capable template from an existing virtual machine, and want to create and assign the logical unit from the library server, the library server must be a member of this host group. Therefore, the library server must be a Hyper-V host. (If you don't want to add the library server as a host, you can assign the logical unit out-of-band using your storage array vendor's management tools.)
  - All Hyper-V hosts that you want to use for rapid provisioning and the library server must have access to the storage array. Also, they must use the same type of SAN connectivity. For SAN migrations to succeed, you can't have some hosts that connect to the array through Fibre Channel and others that connect through iSCSI. Configuration varies, depending on your storage hardware.

- You must get specific configuration information from the storage vendor, but configuration typically requires:
  - The Multipath I/O (MPIO) feature must be added on each host that will access the Fibre Channel or iSCSI storage array. You can add the MPIO feature through Server Manager.
    - If the MPIO feature is already enabled before you add a host to VMM management, VMM will automatically enable MPIO for supported storage arrays using the Microsoft provided Device Specific Module (DSM). If you already installed vendor-specific DSMs for supported storage arrays and then add the host to VMM management, the vendor-specific MPIO settings will be used to communicate with those arrays.

    - If you add a host to VMM before you add the MPIO feature, you must manually configure MPIO to add the discovered device hardware IDs. Alternatively, you can install vendor-specific DSMs.
    - If you're using a Fibre Channel storage area network (SAN), each host that will access the storage array must have a host bus adapter (HBA) installed. Additionally, ensure that the hosts are zoned accordingly so that they can access the storage array.
    - If you use an iSCSI SAN, ensure that iSCSI portals have been added and that the iSCSI initiator is logged into the array. Additionally, ensure that the Microsoft iSCSI Initiator Service on each host is started and set to Automatic. For information on how to create an iSCSI session on a host through VMM, see How to Configure Storage on a Hyper-V Host in VMM.

Create a SAN copy-capable template from a new virtual machine

Create a new VM on a logical unit assigned to a Hyper-V host. On the library server, create a SAN-copy capable template from the VM.

> ⓘ Note
>
> - The library server doesn't need to be a managed Hyper-V host, but it must be able to access the storage pool in which the logical unit resides.
> - When you create the template, the logical unit is automatically unregistered from the host and registered to the library server.

1. Create a logical unit in the VMM storage fabric from the managed storage pool you want to use for rapid provisioning. Alternatively, you can create and assign the logical unit in your storage array management tool.

2. Allocate the logical unit to the host group where the target host resides. Then assign to logical unit to the host. When you assign the LUN, you can format it and assign a drive letter. Ensure that the logical unit you want to assign must be empty.

3. Create a virtual machine with a blank virtual hard disk file on the logical unit.

    - In **Select Source**, select **Create the new virtual machine with a blank virtual hard disk**.
    - In **Configure Hardware**, configure the required settings. Ensure that **Create a new virtual hard disk** is selected.

- In **Select Destination**, accept the default setting to **Place the virtual machine on a host**.
- In **Configure Settings**, in **Select Destination Folder**, select the drive that you created from the assigned logical unit. Verify that **SAN (Migration Capable)** appears next to the drive information. For example: **(L:) [9.92 GB free of 10.00 GB, SAN (Migration Capable)]**.
- In **Machine Resources**, select **Virtual Hard Disk**. In **Browse** > **Select Destination Folder**, select the drive you created from the assigned logical unit.
- In **Select Network** and **Add Properties**, select the required settings. In **Summary**, review the settings and select **Create**. Verify that the VM is listed in **VMs and Services** > **All Hosts** > **VMs**.

4. On the new VM, install and customize the guest operating system and the applications that you want. Generalize the image using Sysprep.exe with the **/generalize** and the **/oobe** options to generalize the associated virtual hard disk. Learn more. When you're finished, ensure there are no .iso image files attached to the virtual DVD drive.

Create a SAN copy-capable template from an existing VM

Create a template from an existing VM.

- If you want to perform this procedure in VMM, the library server must be added as a managed Hyper-V host. This enables you to assign the logical unit to the library server through VMM. If you don't want to make the library a managed Hyper-V host, you can use your array vendor’s management tools to assign the logical unit to the library server.
- You must have an existing virtual hard disk (that was generalized using Sysprep) that you want to use as a base image for rapid provisioning.
- Create a folder in the library share that you'll use to mount the logical unit to and to store the virtual hard disk. For example, create a folder in the SEALibrary library share that is named Rapid Provision VHD.

1. Create a logical unit in the VMM storage fabric from the managed storage pool you want to use for rapid provisioning.

2. Format the logical unit and mount it to the folder path you created.

3. Assign the logical unit to the library server. If the library server is a managed Hyper-V host, you can create and assign the logical unit from the library server.

You can also format the disk with NTFS and mount the logical unit to the folder path in the library share at the same time.

- When you create the logical unit, select the option **Mount in the following empty NTFS folder** > **Browse**, and then select the folder that you created.
- Don't assign a drive letter. Also, don't ever create multiple mount points to the folder.

4. If the library server isn't a managed Hyper-V host, use your array vendor’s management tools to create the logical unit and to unmask the logical unit to the library server. Then do the following:

   - Don't assign a drive letter.
   - Use Disk Management (diskmgmt.msc) to rescan the disk, initialize the disk, and format it.
   - In Disk Management, mount the logical unit to the folder path you created in the library share (**Change Drive Letter and Paths** > **Add** > **Mount in the following empty NTFS folder**, and select the empty library folder).

5. Copy the virtual hard disk you want to use to the new folder in the library share.

   > ⓘ **Note**
   >
   > The virtual hard disk must be the only file on the logical unit.

6. The new folder that you created appears in the library share. To verify the virtual hard disk SAN copy-capable, select the new folder, and in **Physical Library Objects**, select the VHD file. **SAN copy capable** must indicate **Yes**.

Create a SAN-copy capable template

1. Select **Library** > **Create** > **Create VM Template**.
2. In **Create VM Template Wizard** > **Select Source**, select **From an existing virtual machine that is deployed on a host** > **Browse**. Select the VM on the logical unit. Select **Yes** on the warning message.
3. In **Identity**, enter a template name and description.
4. In **Configure Hardware**, select **Next**. The classification that appears matches what you assigned to the storage pool from which you created the logical unit.
5. In **Configure Operating System**, select **Next**.
6. In **Select Library Server**, select the library server where you want to create the template. Verify that the **Transfer Type** is **SAN** and select **Next**. The library server

must have access to the same storage pool as the host.

7. In **Select Path**, select **Browse**, and select a location on the library server to store the VM files.
8. In **Summary**, review the settings and select **Create**. In **Jobs**, you can track the template being created. Wait for the **Completed** status. Verify the template in **Library** > **Templates** > **VM Templates**.

Deploy a VM from the template

Now deploy a VM from the SAN-copy capable template. This procedure explains how to deploy a standalone VM. Alternatively, you can select the template when you create a service. Ensure that:

- The hosts where you want to place the VMs must have access to the managed storage pool where the logical unit that is associated with the template resides.
- If you want to deploy the virtual machines to a private cloud, the storage classification that is assigned to the logical unit that was used to create the SAN clone-capable template must be available to the private cloud.
- For cloud deployment, the host groups that are used to provide resources for the private cloud must contain the hosts that have access to the managed storage pool where the logical unit that is associated with the template resides.

1. Select **VMs and Services** > **Create** > **Create Virtual Machine**.

2. In the Create Virtual Machine Wizard > **Select Source**, select **Use an existing virtual machine, VM template or virtual hard disk** > **Browse**. Select type **VM Template**, and select the template you created for rapid provisioning. The template must indicate **Yes** in the **SAN Copy Capable** column.

3. In **Select Source**, select **Next**.

4. Complete the rest of the steps wizard to create and deploy the virtual machine.

> ⓘ Note
>
> - In **Configure Hardware** > **Bus Configuration**, leave the **Classification** list empty or select the storage classification that
> - In **Select Host** or **Select Cloud**, ensure the **Transfer Type** column indicates **SAN**.
> - If you selected to place the virtual machine on a host, in **Configure Settings** > **Machine Resources**, select the virtual hard disk to verify the

deployment options. For rapid provisioning through SAN copy, ensure that the method to deploy the virtual hard disk to the host list is **Transfer the virtual disk by using the SAN**.

5. After you complete the wizard, open **Jobs** > **Create virtual machine job** to view the job status.

6. When you create a virtual machine from the SAN copy-capable template, a new logical unit is automatically provisioned from the same storage pool where the virtual hard disk that was used to create the SAN copy-capable template from resides. The logical unit is automatically registered and mounted on the target host.

7. To verify that the virtual machine was created, open the VMs and Services workspace. Expand **All Hosts** or **Clouds** and locate and select the destination host or private cloud. In **VMs**, verify that the new virtual machine appears. If you open Disk Management (Diskmgmt.msc) on the destination host, you can see the new disk that is assigned and registered to the host.

Next steps

Manage the VM settings.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Create and deploy VMs in the VMM fabric from a VM template

Article • 08/30/2024

This article describes how to create VMs in the System Center Virtual Machine Manager (VMM) fabric from a VMM virtual machine (VM) template. You can use a VM template to create standalone VMs or to create VMs in tiers in a service template.

Before you start

- Some settings, including server roles and features, application installation, and SQL Server settings, apply only when a VM template is used for service deployments. For standalone virtual machine creation, these settings aren't used and won't appear when you create a standalone VM.
- The ability to configure a VM to use static IP addresses from an IP address pool managed by VMM is only available when you deploy a VM using a VM template.
- To complete the steps, you must be an administrator or delegated administrator on the VMM server or a self-service user.
- If you're a self-service user, you need **Deploy** permissions with the **Store and re-deploy** action assigned. You must first deploy the VM to a private cloud and then store it in the library.
- You can only customize static IP address settings if you create a VM from a VM template.
- You can use VMM to configure the availability settings for the virtual machine. Learn more.

Create a VM

1. Select **VMs and Services** > **Create Virtual Machine** > **Create Virtual Machine**.

2. In **Create Virtual Machine Wizard** > **Select Source**, select **Use an existing virtual machine, VM template, or virtual hard disk** > **Browse**.

3. In **Select Virtual Machine Source**, select the template > **OK**. Select **OK** if a message appears that some deployment settings will be ignored.

4. In **Select Source**, select **Next**.

5. In **Identity**, specify the VM name and an optional description. Select **Next**.

6. In **Configure Hardware** page, either select the profile that you want to use from the **Hardware profile** list, or configure the hardware settings manually. The hardware setting displayed will differ depending on whether you're deploying a generation 1 or generation 2 machine. Select **Next**.

   - In **Compatibility**, if you want to deploy the virtual machine to a private cloud, select a capability profile that is available to the private cloud.
   - In **Network Adapters**:
     - If you want to use static IP addresses, set the MAC address to static.
     - If the VM uses a VHD in VMware .vmdk format, include a legacy network adapter in the template (**New** > **Network Adapter** > **Legacy Network Adapter**). If you don't, the VM might not be able to start in a domain, although it's OK in a workgroup.
   - In **Configure Operating System**, specify the guest operating system settings. If you have an existing profile, select in the **Guest OS profile** list.

7. In the **Select Destination** page, specify how the virtual machine must be deployed - in a private cloud, on a host, or stored in the library.

Deploy the VM in a private cloud

1. In **Select Cloud**, select the private cloud on which you want to place the virtual machine. If you're connected as an Administrator, you can select the host on which the virtual machine must be deployed in the private cloud. Cloud suggestions are based on a 0-5 star rating. Learn more. Verify the settings and modify if required:

   - **Expected utilization**: Expected utilization for a VM created from a blank VHD is based on standard defaults. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.

   - **Make this VM highly available**: With this option selected, only hosts that are located in a cluster are available for selection.

   - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.

   - **Rating Explanation**: Provides an explanation if a host received a zero rating.

   - **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded Data Transfers (ODX). Learn more.

2. In **Configure Settings**, review the VM settings. Either accept the default VM path on the host or specify a different location. You can optionally select to **Add this path to the list of default virtual machine paths on the host**. In **Machine Resources**, accept the default values for the VHD or modify as required. To prevent placement from choosing its own values, select the pin icon next to the setting. This option isn't available for self-service users.

3. In **Select Networks**, if it appears, optionally select the network settings, and select **Next**.

4. In **Add Properties**, configure the action to take when the host starts or stops and the operating system that you'll install on the VM. Select **Next.**

5. In **Summary**, confirm the settings, and select **Create**. Confirm that the VM was created in **VMs and Services** > **Clouds** and select the cloud. The virtual machine appears in the **VMs** pane.

Deploy the VM on a host

1. In **Select Host**, view the ratings, select the host on which you want to deploy the VM, and select **Next**. The host suggestions are based on a 0-5 star rating. Learn more. Verify the settings and modify if required:

   - **Expected utilization**: Expected utilization for a VM created from a blank VHD is based on standard defaults. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.

   - **Make this VM highly available**: With this option selected, only hosts that are located in a cluster are available for selection.

   - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.

   - **Rating Explanation**: Provides an explanation if a host received a zero rating.

- **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

  The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded Data Transfers (ODX). Learn more.

2. In **Configure Settings**, review the VM settings. Either accept the default VM path on the host or specify a different location. You can optionally select **Add this path to the list of default virtual machine paths on the host**. In **Machine Resources**, accept the default values for the VHD or modify as required. To prevent placement from choosing its own values, select the pin icon next to the setting. This option isn't available for self-service users.

3. In **Select Networks**, if it appears, optionally select the network settings, and select **Next**.

4. In **Add Properties**, configure the action to take when the host starts or stops, and the operating system that you'll install on the VM. Select **Next.**

5. On the **Summary** page, confirm the settings and select **Create**.

Store the VM in the library

1. In **Select Library Server**, select the library server that you want to use, and select **Next**.
2. In **Select Path**, specify the library share location to store the virtual machine. Select **Browse** to select a library share and an optional folder location, select **OK**, and select **Next**.
3. In **Summary**, confirm the settings and select **Create**.
4. To confirm that the virtual machine was created, in the **Library** workspace, in the **Library** pane, expand **Library Servers**, expand the library server where you stored the virtual machine, and select **Stored Virtual Machines and Services**. The stored virtual machine appears in the **Physical Library Objects** pane.

Next steps

Manage the VM settings

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Deploy a virtual machine from the VMM library

Article • 08/30/2024

This article describes how to deploy a virtual machine that's stored in the System Center Virtual Machine Manager (VMM) library.

Before you start

- You need one or more VMs stored in the VMM library. To store a VM in the library, the VM must be stopped, shut down, or saved. You can't store a VM while it's running.
- To store a VM in the library, select the VM > **Actions** > **Store in Library**. In the Select Library Server Wizard, specify where you want to store the VM. Select **Store** to move the VM to the library. Review progress on the **Jobs** tab.

Deploy a VM

1. In the **Library** workspace, navigate to the library server on which the VM is stored, and then select **Stored Virtual Machines and Services**.

2. Select the VM on the **Virtual Machines** tab > **Actions**, select **Deploy**.

3. In Deploy Virtual Machine Wizard > **Select Host**, select a host on which to deploy the VM. All available hosts are given a rating of 0–5 stars based on their suitability to host the virtual machine. You can select any host that has the required disk space, even if the host has a zero host rating. To learn more, review VM placement.

   - In **Network optimization**, if a host has network optimization enabled, a green check mark appears.
   - In **Highly available virtual machines**, to make a VM highly available, you can migrate it to a host in a cluster, even if the VM hasn't been configured as highly available. Conversely, you can migrate a highly available VM to a standalone host.
   - **Details**: Indicates the status of the host, the operating system, and the type and status of the virtualization software.
   - **Rating Explanation**: Provides an explanation if a host received a zero rating.
   - **SAN Explanation** or **Deployment and Transfer Explanation**: Lists any factors that make a storage area network (SAN) transfer unavailable. VMM doesn't

recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

- The **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is based on the Windows Offloaded Data Transfers (ODX). To learn more, review overview of Windows ODX.

4. In **Select Path**, specify where you want to store the configuration files for the VM.

    - If you didn't select the default path, and you want to store other VMs on the path, select **Add this path to the list of host default paths**.
    - If SAN transfers are enabled for this deployment, by default, the virtual machine is transferred to the host over the storage area network (SAN). If you don't want to perform a SAN transfer, select the **Transfer over the network even if a SAN transfer is available** checkbox. If SAN transfers aren't available for this deployment, this option isn't available.

5. In **Select Networks**, select the network settings the VM must use.

6. In **Summary**, review the settings, and select **Deploy**. You can select to start the VM after it's deployed.

Next steps

Manage the VM settings

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Create and deploy Linux virtual machines in the VMM fabric

Article • 08/30/2024

This article describes how to create and deploy Linux VMs in the System Center Virtual Machine Manager (VMM) fabric.

Before you start

VMM supports virtual machines that contain Linux as the guest operating system. Ensure that:

- Linux Integration Services (LIS) must be installed on the virtual machine.
- The VMM guest agent for Linux must be installed on the virtual machine. It's required for service template integration, and it allows you to modify properties on the Linux computer, such as the host name.

  > ⓘ **Note**
  >
  > The SCVMMLinuxGuestAgent (XPlat) cfghostdomain garbles the hosts file if hostname is already set to localhost. We recommend you not to set the hostname as localhost when deploying Linux VMs through VMM.

- VMM doesn't verify that the VM meets these requirements. However, if it doesn't, VM deployment will fail.

Create the VM

Create a VM running Linux using any of the available methods in the VMM fabric. Learn more.

Install LIS on the VM

By default, LIS is included with some distributions of Linux. If LIS isn't included in the distribution of Linux that you're using for the virtual machine, install it manually. Learn more.

Install the VMM guest agent

1. Open an elevated command prompt on the VMM server.
2. Go to the **c:\Program Files\Microsoft System Center\Virtual Machine Manager\agents\Linux** folder.
3. Copy all the agent installation files from that folder to a new folder on the VM.
4. Open the new folder on the VM and run the following command: **chmod +x install**.
5. Run either of these commands depending on the operating system.

   PowerShell

   ```
   ./install scvmmguestagent.1.0.0.544.x64.tar
   ```

   PowerShell

   ```
   ./install scvmmguestagent.1.0.0.544.x86.tar
   ```

When the agent installs on the VM, the following files and folders will be created on the VHD:

- A default installation folder (/opt/microsoft/scvmmguestagent), and an installation log file (scvmm-install.log)
- A default log files folder - /var/opt/microsoft/scvmmagent/log
- A specialization log file (scvmm.log). This file is created when the virtual machine is deployed and specialized.
- A configuration file (scvmm.conf). This file contains the location of the log file and is used to control logging during deployment and specialization.

Next steps

Manage the VM settings.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Configure a nested VM as a host

Article • 08/30/2024

Nested virtualization allows you to run Hyper-V inside a Hyper-V virtual machine. In other words, with nested virtualization, a Hyper-V host itself can be virtualized. Nested virtualization can be enabled out-of-band using PowerShell and Hyper-V host configuration.

You can use this functionality to reduce your infrastructure expense for development and test scenarios without the need for individual hardware.

With System Center Virtual Machine Manager (VMM), you can enable and disable the nested virtualization feature through VMM console. You can configure the nested Virtual Machine (VM) as a host in VMM and perform host operations from VMM on this VM. For example, VMM dynamic optimization will consider a nested VM host for placement.

Enable the nested virtualization on a VM and then configure it as a host.

> ⓘ **Note**
>
> Virtualization applications other than Hyper-V aren't supported in Hyper-V virtual machines and are likely to fail. This includes any software that requires hardware virtualization extensions.

Before you start

Ensure the following prerequisites are met:

- A Hyper-V host running Windows Server 2019, Windows Server 2022.
- A Hyper-V VM running Windows Server 2019, Windows Server 2022.
- A Hyper-V VM with configuration version 8.0 or greater.
- An Intel processor with VT-x and EPT technology.

Enable network virtualization

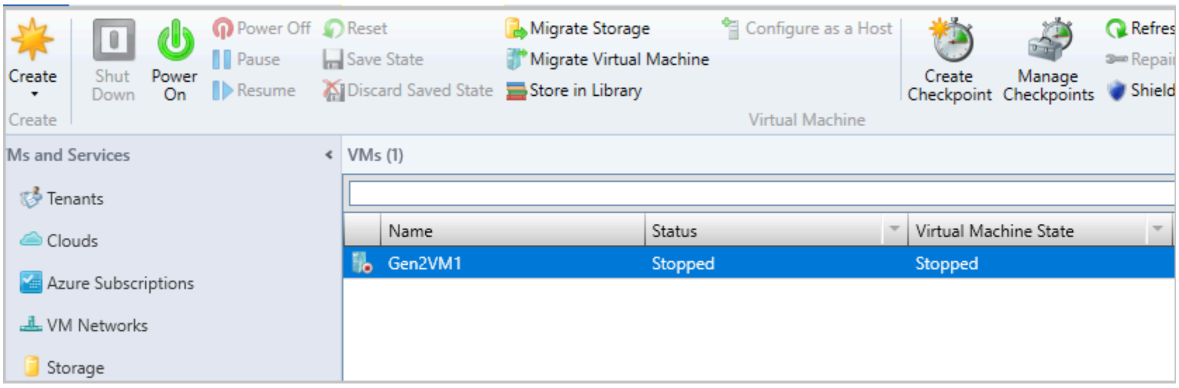
Administrators/delegated administrators can configure nested virtualization using VMM. Use the following procedures:

- Enable nested virtualization
- Configure the VM as a host in VMM

Enable nested virtualization on an existing virtual machine

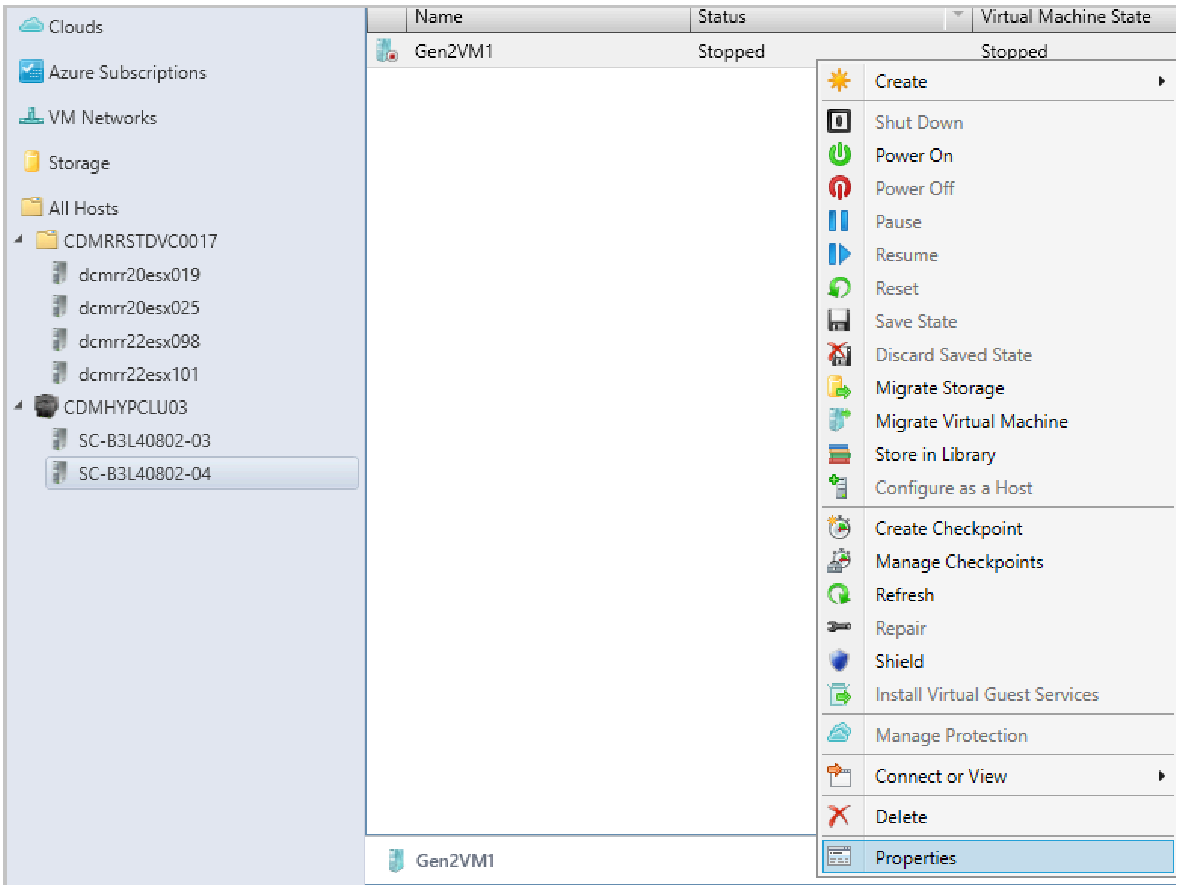
1. Identify the VM that meets the above prerequisites.

2. Ensure the VM is in **Stopped** state.



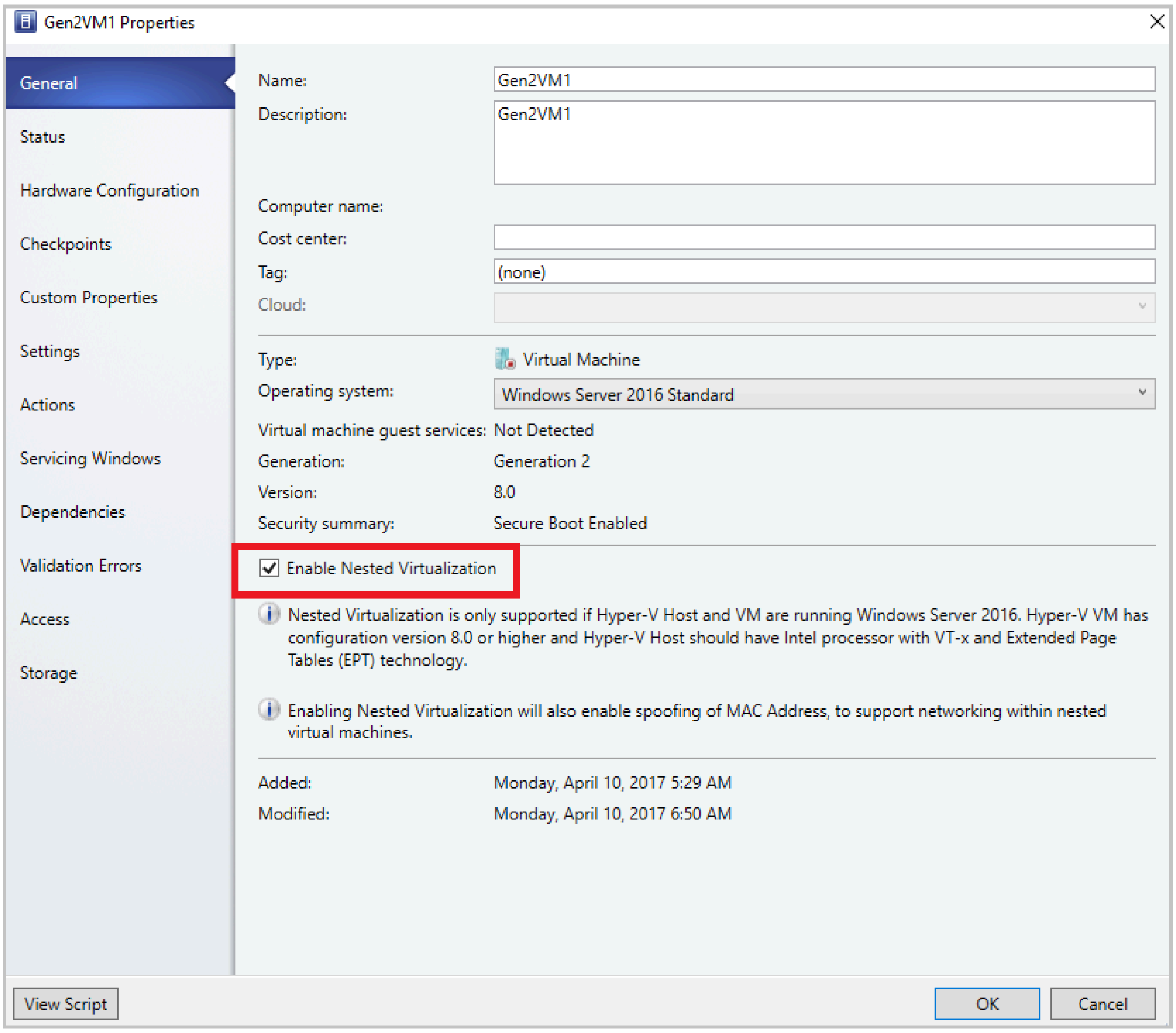
Name	Status	Virtual Machine State
Gen2VM1	Stopped	Stopped

3. Right-click the VM to browse its **Properties**.



Name	Status	Virtual Machine State
Gen2VM1	Stopped	Stopped

4. On **General**, select **Enable Nested Virtualization**.



Name: Gen2VM1

Description: Gen2VM1

Computer name:

Cost center:

Tag: (none)

Cloud:

Type: Virtual Machine

Operating system: Windows Server 2016 Standard

Virtual machine guest services: Not Detected

Generation: Generation 2

Version: 8.0

Security summary: Secure Boot Enabled

☑ Enable Nested Virtualization

Nested Virtualization is only supported if Hyper-V Host and VM are running Windows Server 2016. Hyper-V VM has configuration version 8.0 or higher and Hyper-V Host should have Intel processor with VT-x and Extended Page Tables (EPT) technology.

Enabling Nested Virtualization will also enable spoofing of MAC Address, to support networking within nested virtual machines.

Added: Monday, April 10, 2017 5:29 AM

Modified: Monday, April 10, 2017 6:50 AM

Configure the nested VM as a host

1. Enable the following inbound and outbound firewall rules on the nested VM that you want to configure as the host.

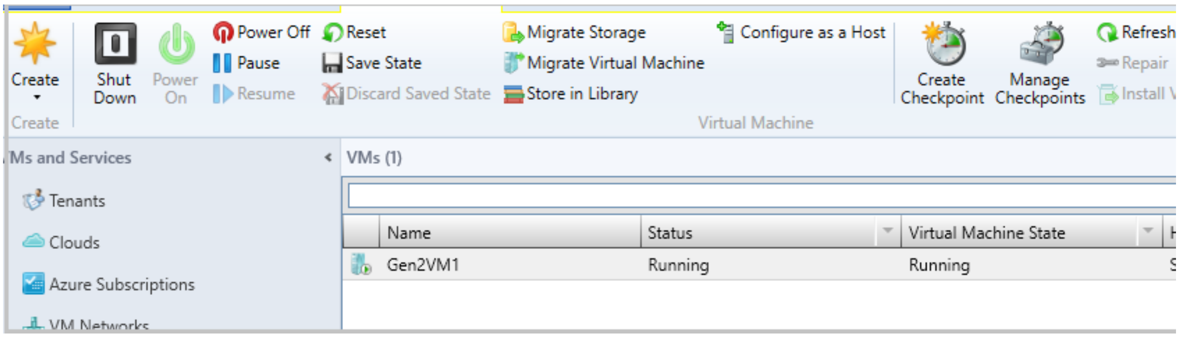
   Inbound Firewall rules

   - File and printer sharing
   - Windows remote management (HTTP-In)
   - Windows management instrumentation

   Outbound Firewall rules

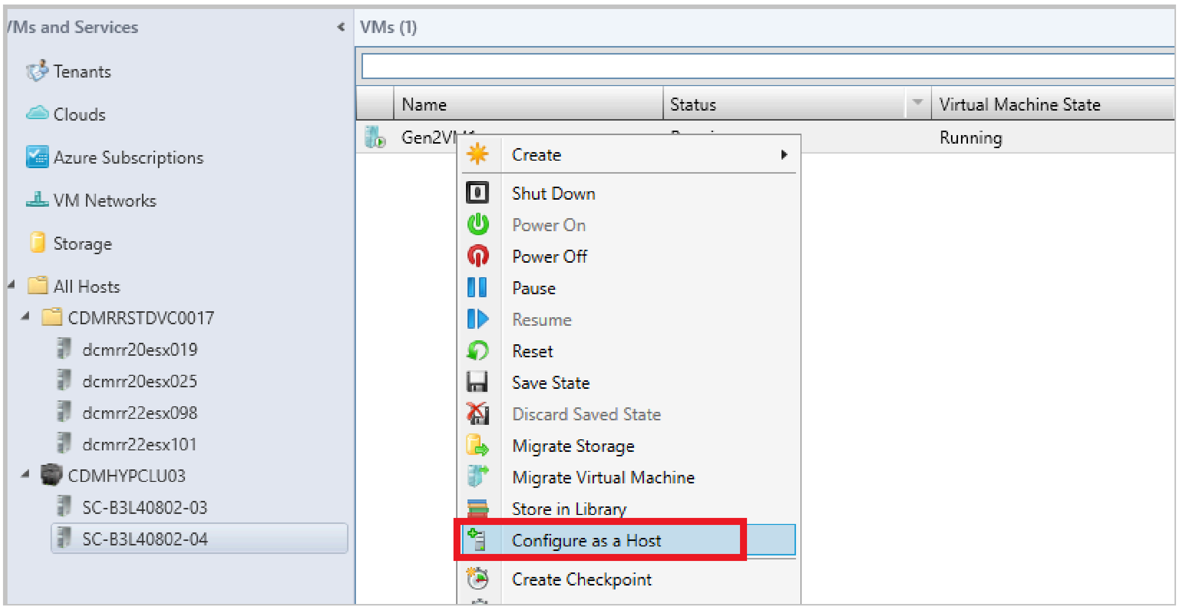
   - File and printer sharing
   - Windows management instrumentation (WMI-Out)

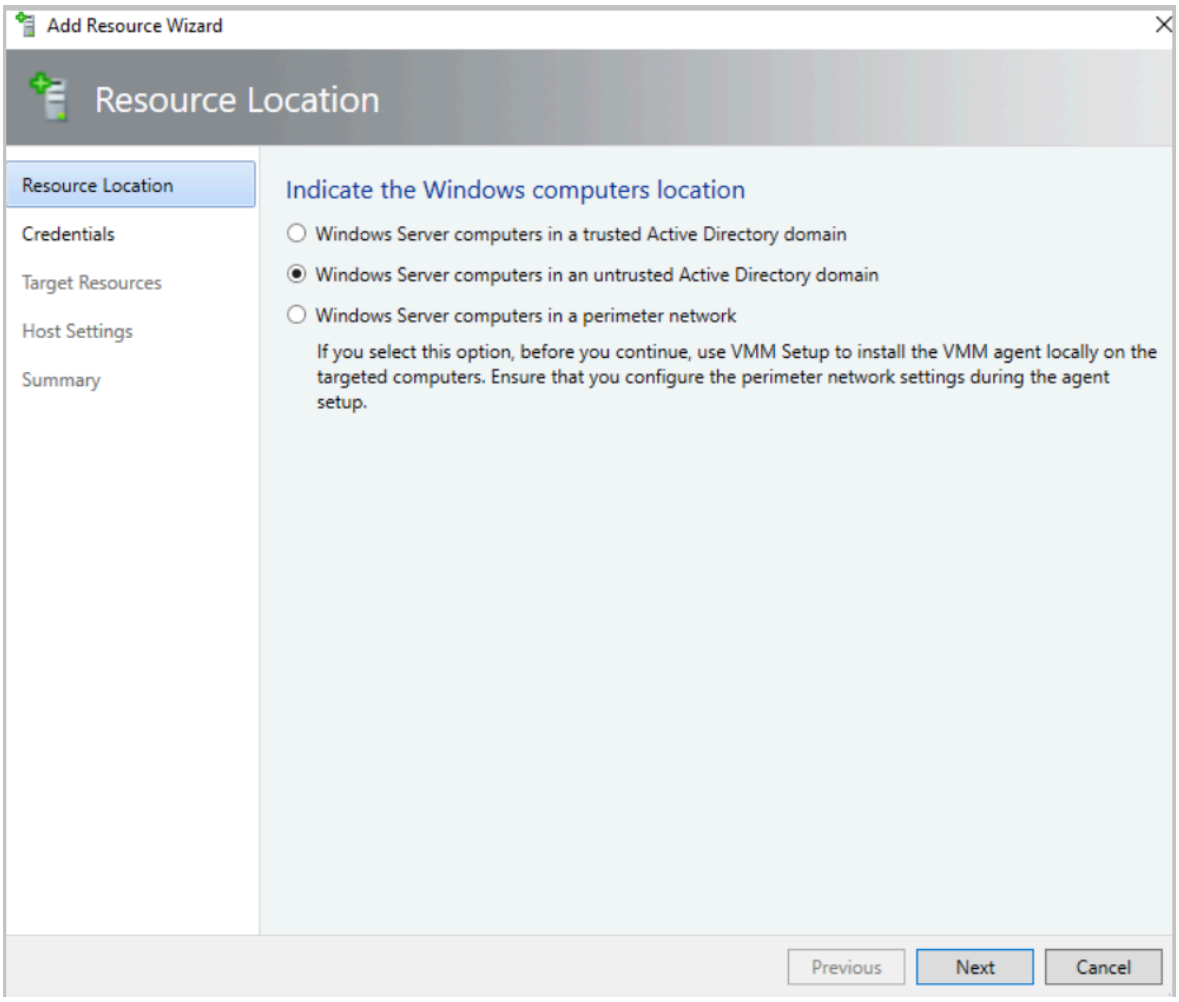
2. Ensure the VM is in **Running** state. Start the VM if it isn't running.



Name	Status	Virtual Machine State
Gen2VM1	Running	Running

3. Right-click the VM and select **Configure as a Host**. The **Add Resource** wizard appears.





Indicate the Windows computers location

○ Windows Server computers in a trusted Active Directory domain

● Windows Server computers in an untrusted Active Directory domain

○ Windows Server computers in a perimeter network

If you select this option, before you continue, use VMM Setup to install the VMM agent locally on the targeted computers. Ensure that you configure the perimeter network settings during the agent setup.

4. Run through the wizard, select the appropriate options, and complete the wizard.

Disable nested virtualization

1. Select the host or VM for which nested virtualization is enabled.

2. Ensure the VM is in **Stopped** state. Stop the VM if it's running.

3. Right-click the VM to browse its **Properties**.

4. On **General**, clear the **Enable Nested Virtualization** check box.

> ⓘ **Note**
>
> Check the note at the bottom of the wizard page before you disable nested virtualization.

Next steps

Run Hyper-V in a nested VM.

Convert a VMware VM to Hyper-V in the VMM fabric

Article • 08/30/2024

This article describes how to convert VMware VMs in the System Center Virtual Machine Manager (VMM) fabric to Hyper-V.

You can convert the VMs using the *Convert Virtual Machine* wizard. You can use this wizard from the VMM console.

> ⓘ **Important**
>
> - See system requirements for supported versions of vSphere (ESXi).
> - You can't convert VMware workstations.
> - You can't convert VMs with virtual hard disks connected to an IDE bus.
> - Anti-virus apps must be supported.
> - Online conversions aren't supported. You need to power off the VMware VMs.
> - VMware tools must be uninstalled from the guest operating system of the VM.
> - We recommend upgrading to VMM 2022 UR2 to convert your VMware VMs to Hyper-V four times faster.

> ⓘ **Note**
>
> We recommend that no more than ten conversions be triggered parallelly from the same ESXi source to the same Hyper-V destination. If the source-destination pair is different, VMM can support up to 100 VM conversions in parallel, with the remaining conversions queued. However, we recommend staging the VM conversions in smaller batches for higher efficiency.

> ⓘ **Note**
>
> After conversion, all VM disks except for the OS disk will be offline. This is because the `NewDiskPolicy` parameter is set to *offlineALL* on VMware VMs by default. To override this and to have the new disks brought online after conversion, you can make one of the following changes to your VMware VM disk policy before initiating the conversion:

- `Set-StorageSetting -NewDiskPolicy OfflineShared`: To have all the new shared bus disks offline and all the new local bus disks online
- `Set-StorageSetting -NewDiskPolicy OnlineAll`: To have all the new disks online, regardless of whether the disks are on a local or shared bus.

Convert using the wizard

1. Select **VMs and Services** > **Home** > **Create** > **Create Virtual Machines** > **Convert Virtual Machine**.
2. In **Convert Virtual Machine** wizard > **Select Source**, select **Browse** and in **Select Virtual Machine Source**, select the VMware VMs you want to convert.
3. In **Specify Virtual Machine Identity**, modify the machine name and description as required.
4. In **Virtual Machine Configuration**, specify the number of processors and memory settings.
5. In **Select Host**, select a Hyper-V host/Azure Stack HCI (applicable from VMM 2019 UR3 and later) for placement. In **Select Path**, configure the storage location on the host for the VM files. The default VM paths are listed.
6. In **Select Networks**, select the logical network, virtual network, and the VLAN as applicable.
7. In **Add Properties**, configure the required settings. In **Summary**, review the settings, and select **Start the virtual machine after deploying it** if necessary.
8. Select **Create** to start the conversion. Verify the VM's conversion in **VMs and Services** > **Home** > **Show** > **VMs**.

Convert EFI-based VM to Hyper-V Generation 2 VM

System Center VMM enables the migration of EFI-based VMware VMs to Hyper-V. VMware VMs that you migrate to Microsoft Hyper-V platform can now take advantage of Generation 2 features.

The **Convert Virtual Machine** wizard enables this migration. Based on the firmware type (BIOS or EFI), the wizard selects and defaults the Hyper-V VM generation appropriately.

- BIOS-based VMs are migrated to Hyper-V VM Generation 1.
- EFI-based VMs are migrated to Hyper-V VM Generation 2.

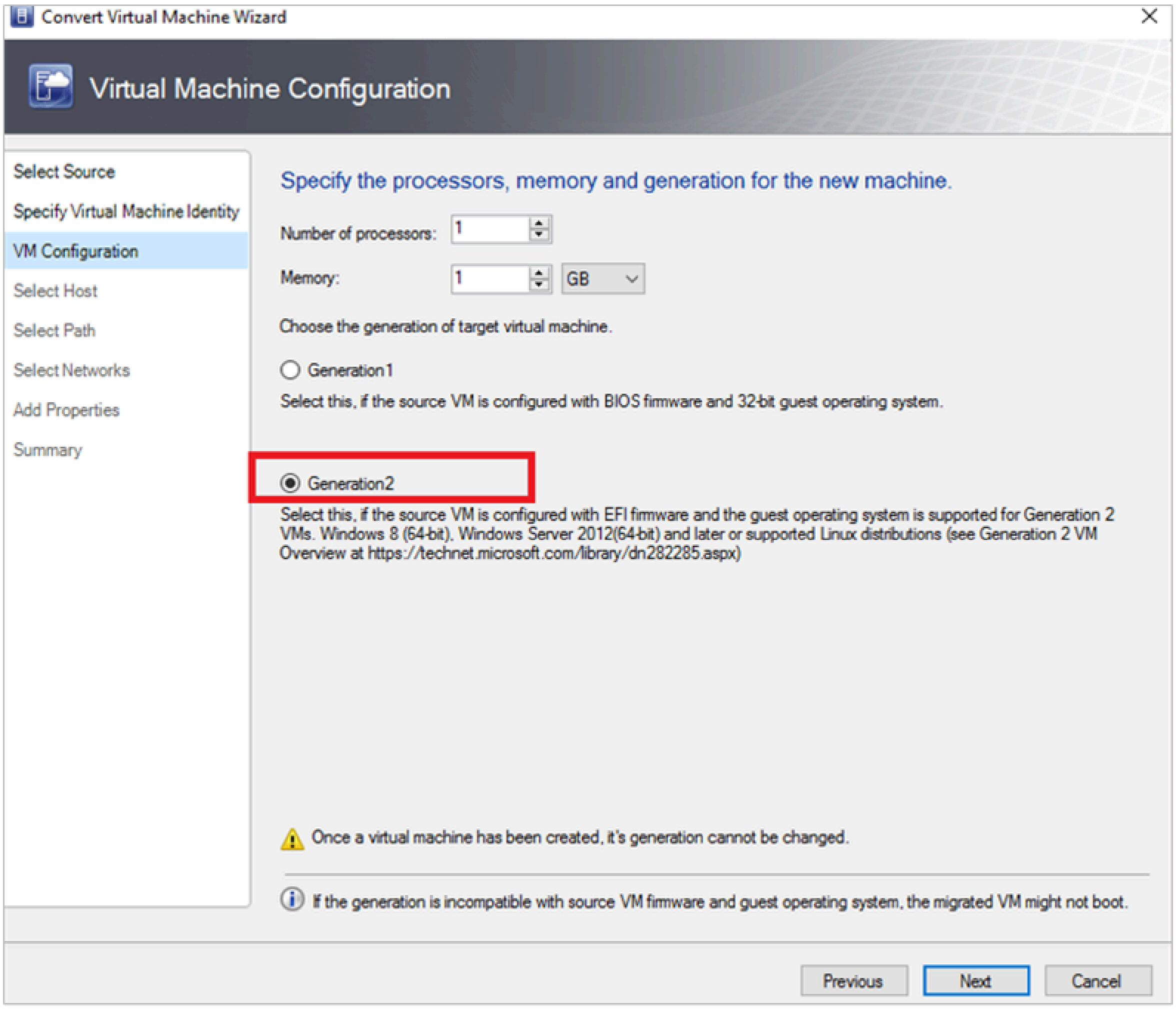
Before you start

Ensure the following prerequisites are met:

- VMware VMs with firmware type as EFI
- VMware ESXi Hosts added in System Center VMM

Conversion procedure

1. To convert, follow the above procedure and select **Generation 2** in step 4.



Specify the processors, memory and generation for the new machine.

Number of processors: 1

Memory: 1 GB

Choose the generation of target virtual machine.

○ Generation1

Select this, if the source VM is configured with BIOS firmware and 32-bit guest operating system.

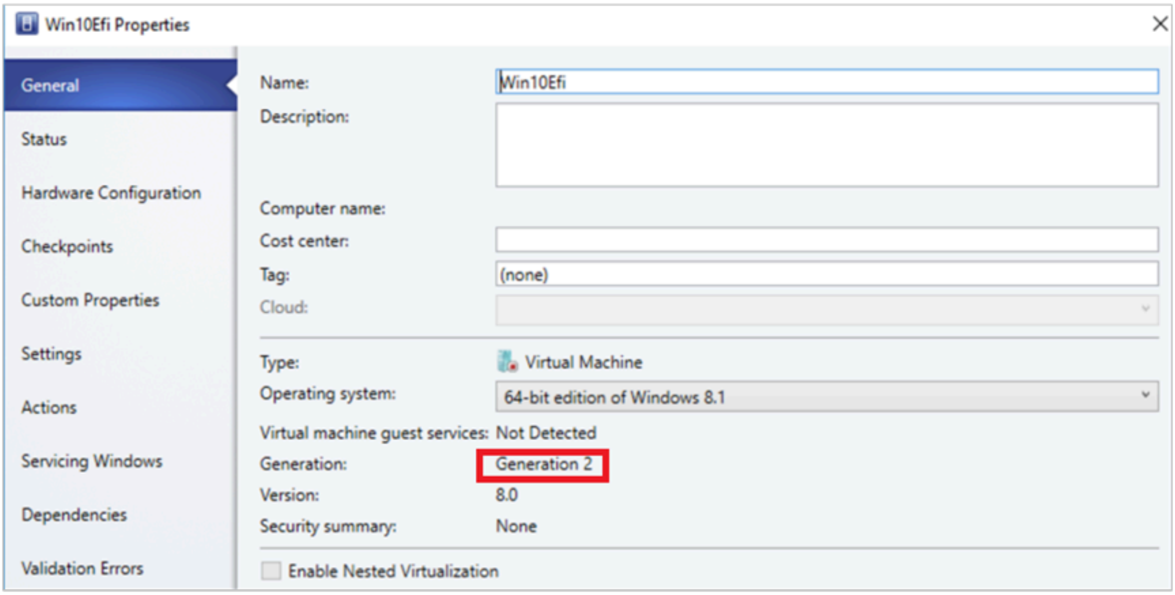
● Generation2

Select this, if the source VM is configured with EFI firmware and the guest operating system is supported for Generation 2 VMs. Windows 8 (64-bit), Windows Server 2012(64-bit) and later or supported Linux distributions (see Generation 2 VM Overview at https://technet.microsoft.com/library/dn282285.aspx)

⚠ Once a virtual machine has been created, it's generation cannot be changed.

ⓘ If the generation is incompatible with source VM firmware and guest operating system, the migrated VM might not boot.

2. Once the VM is converted, you can see the Generation 2 VM as shown in the image below:



Name: Win10Efi
Description:
Computer name:
Cost center:
Tag: (none)
Cloud:
Type: Virtual Machine
Operating system: 64-bit edition of Windows 8.1
Virtual machine guest services: Not Detected
Generation: Generation 2
Version: 8.0
Security summary: None
□ Enable Nested Virtualization

> ⓘ **Note**
>
> - PowerShell commands allow you to provide the disk type for the target Hyper-V VM, which will enable the VMware thick provisioned disk to be migrated as Hyper-V dynamic disk or vice versa, based on the requirements.

Convert using PowerShell cmdlets

Here are the sample cmdlets:

PowerShell

```
New-SCV2V -VMHost <Host> -VMXPath <string> [-EnableVMNetworkOptimization
<bool>] [-EnableMACAddressSpoofing
<bool>] [-VMMServer <ServerConnection>] [-LibraryServer <LibraryServer>] [-
JobGroup <guid>] [-Trigger] [-VhdType
{UnknownType | DynamicallyExpanding | FixedSize}] [-VhdFormat {VHD | VHDX}]
[-Description <string>] [-Name
<string>] [-Owner <string>] [-UserRole <UserRole>] [-Path <string>] [-
StartVM] [-CPUCount <byte>]
[-CPURelativeWeight <int>] [-CPUType <ProcessorType>] [-MemoryMB <int>] [-
Generation <int>] [-DelayStartSeconds
<int>] [-StartAction {NeverAutoTurnOnVM | AlwaysAutoTurnOnVM |
TurnOnVMIfRunningWhenVSStopped}] [-StopAction
{SaveVM | TurnOffVM | ShutdownGuestOS}] [-LogicalNetwork <LogicalNetwork>]
[-VMNetwork <VMNetwork>]
[-NoConnection] [-MACAddress <string>] [-MACAddressType <string>] [-
SourceNetworkConnectionID <string>]
[-VirtualNetwork <VirtualNetwork>] [-VirtualNetworkAdapter
<VirtualNetworkAdapter>] [-VLanEnabled <bool>] [-VLanID
<uint16>] [-OverridePatchPath <string>] [-
SkipInstallVirtualizationGuestServices] [-NetworkLocation <string>]
[-NetworkTag <string>] [-RunAsynchronously] [-PROTipID <guid>] [-JobVariable
<string>]  [<CommonParameters>]
```

Convert VMware VMs to Hyper-V faster

- As a prerequisite to start converting VMware VMs to Hyper-V four times faster, upgrade to SCVMM 2022 UR2 or later.
- As part of SCVMM 2022 UR2, a new registry named **V2VTransferChunkSizeBytes** is introduced at *HKLM:\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Agent* in the Hyper-V hosts managed by SCVMM.
- This registry of type REG_DWORD, with a value of *2147483648*, which is 2 GB in bytes has to be set on every Hyper-V host managed by VMM by running this script from the VMM Console.
- Alternatively, if you want to set this registry value in a single host and not on all the hosts, run this script from the VMM Console.
- After setting this registry value, if you remove any Hyper-V host(s) from SCVMM, stale entries for this registry might remain. If the same host(s) is re-added to SCVMM, the previous value of registry **V2VTransferChunkSizeBytes** will be honored.

Next steps

Manage the VM settings.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Install an operating system on a VM in the VMM fabric

Article • 08/30/2024

This article describes how to install an operating system on a VM in the System Center Virtual Machine Manager (VMM) fabric.

After you've deployed a VM in the VMM fabric, you can install an operating system on it. Review the supported operating systems.

You can install an operating system from a DVD, from an ISO image file in the VMM library, or from a network installation.

- For the system CD or ISO image, when you set up the VM, you need a virtual drive to attach to the physical drive or image file.
- To use an ISO image, it must be added to the VMM library.
- For a network installation, you configure a virtual network adapter.

Prepare to install from a system DVD

1. In **Virtual Machines**, right-click the VM > **Properties**.
2. In **Hardware Configuration**, select **DVD** on the **New** toolbar to add a virtual DVD drive to the IDE bus.
3. Select **Physical CD/DVD drive** and select the drive on the host.

Prepare to install from an ISO in the VMM library

1. Copy the image file to a share in the Virtual Machine Manager library. The file will be available when the library refreshes. Learn more about adding file-based resources to the library.
2. In the VM properties > **Hardware Configuration**, select **DVD** on the **New** toolbar to add a virtual DVD drive to the IDE bus.
3. Select **Known image file**, and select the file from the library resources in the list.

Enable shared ISOs

By default, when you create a VM, an ISO attached as a virtual DVD drive is copied into the VM folder. VMM does this so that you can easily migrate VMs from host to host. If you want to share the image from the VMM library, instead of copying it, you can do that as follows:

1. Specify an Active Directory domain account as the VMM service account on the VMM server.
2. Grant the VMM service account read access on the VMM library share that stores the ISO image files. Grant the Hyper-V host machine account read access for the shared ISO location.
3. Configure constrained delegation for each Hyper-V host. This ensures that each host presents delegated credentials for CIFS/SMB to the VMM server on which the library stores the ISO. To do this, in Active Directory, locate the host machine account and open the account properties. In the **Delegation** tab, select **Select this computer for delegation to specified services only** > **Use any authentication protocol** > **Add**. Add the VMM library server that contains the ISO you want to share. In **Add Services**, add **cifs**.
4. Now configure a virtual machine to share an ISO image.
   a. In the VM properties > **Hardware Configuration**, in **Capture** mode > select **Existing image file** and browse to select the ISO image file in the library.
   b. Select **Share image file instead of copying it**.

> ⓘ **Note**
>
> You must attach the shared ISO image file to the VM after you've created it. You cannot attach the file when you create the VM.

Prepare to install from the network

If the network adapter on the host computer supports network service boots, you can configure a virtual network adapter on the VM to enable this.

1. In **Virtual Machines**, right-click the VM > **Properties**.
2. In **Hardware Configuration**, configure a network connection.
3. On the **New** toolbar, select **Network Adapter** to add a virtual network adapter to the IDE bus.
4. In **Connect to**, select the external virtual network to use for the network service boot. The list contains all virtual networks that are configured on the host.
5. Under **Ethernet (MAC) address**, specify a dynamic or static IP address for the VM.

6. With the VM configured to provide access to the installation medium of choice, you can connect to the virtual machine to install the operating system. By default, VMM uses port 5900 to connect to VMRC. No configuration is required unless a firewall is blocking the port.

Install the operating system on the virtual machine

1. Right-click the VM > **Connect to virtual machine**. Select **Yes** to start the VM.
2. On the **Remote Control** menu, select **Special Keys** and then select **Send Ctrl+Alt+Delete**.
3. Install the operating system on the VM. The boot disk partition must be the Windows partition.
4. After completing the installation, end your session with the VM and stop the VM in VMM.

Next steps

Manage the VM settings.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Configure virtual machine settings in the VMM compute fabric

Article • 08/30/2024

This article describes how to configure performance and availability settings for VMs in the System Center Virtual Machine Manager (VMM) fabric.

Settings include changing VM properties and setting up performance options, such as quality-of-storage (QoS), availability options, resource throttling, and virtual NUMA.

Add a virtual adapter to a VM

You can add and remove virtual network adapters (vNICs) from VMs that are running. This reduces the workload downtime.

> ⓘ **Note**
>
> - You add new virtual network adapters by creating or modifying a VMM hardware profile.
> - This feature is only available for Generation 2 VMs.
> - By default, added virtual network adapters aren't connected to a virtual network. You can configure VMs assigned with the hardware profile to use one or more of the virtual network adapters after they're deployed on a host.

1. In the virtual machine properties > **Hardware Configuration**, select **Network Adapters**, and select the network adapter you want to add.

2. You can configure many properties for the network adapter, including:

   - **Connected to**: Select what the adapter is connected to.
   - **Not connected**: Select if you don't want to specify a network now.
   - **Internal network**: Select if you want to connect to an isolated internal network that enables communication among VMs on the same host. Virtual machines attached to the internal virtual network can't communicate with the host, with any other physical computers on the host's LAN, or with the Internet.
   - **External network**: Select to specify that a virtual machine created using this hardware profile will be connected to a physical network adapter on its host. Virtual machines attached to a physical network adapter can communicate

with any physical or virtual computer that the host can communicate with and with any resources available on the intranet and over the Internet that the host computer can access.

- **Ethernet (MAC) address**: A virtual MAC address on virtual machines uniquely identifies each computer on the same subnet. Select one of the following options:
  - **Dynamic**: Select this option if you want to enable a dynamic MAC address for a virtual machine.
  - **Static**: Select this option if you want to specify a static MAC address for a virtual machine. Enter a static MAC address in the field provided.
  - **Trunk Mode**: Select to enable Trunk mode.

Support for trunk mode

> ⓘ Note
>
> **Trunk mode** is supported only in VLAN-based independent networks.

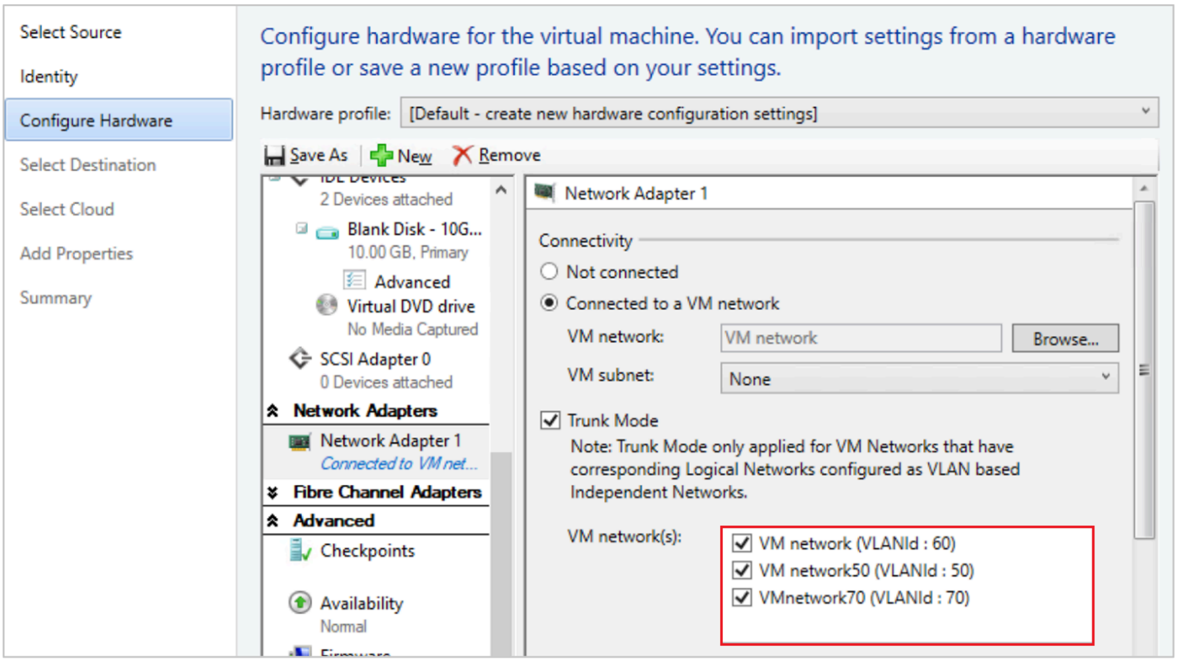
Trunk mode is used by NFV/VNF applications like virtual firewalls, software load balancers, and virtual gateways to send and receive traffic over multiple vLANs. You can enable trunk mode through console and PowerShell.

See the following section for enabling Trunk mode through console; see Set-SCVirtualNetworkAdapter and New-SCVirtualNetworkAdapter for enabling through PowerShell commandlets.

Configure trunk mode

To configure trunk mode in VMM, follow these steps:

1. Under VM **Properties**, navigate to **Configure Hardware Settings** > **Network Adapter**, and select **Trunk mode** to enable trunk mode for VM vNICs.
2. Select the VM networks (multiple vLANs) through which you want to direct the VM network traffic.



Select Source
Identity
Configure Hardware
Select Destination
Select Cloud
Add Properties
Summary

Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings.

Hardware profile: [Default - create new hardware configuration settings]

Save As | New | Remove

IDE Devices
2 Devices attached
Blank Disk - 10G...
10.00 GB, Primary
Advanced
Virtual DVD drive
No Media Captured
SCSI Adapter 0
0 Devices attached
Network Adapters
Network Adapter 1
Connected to VM net...
Fibre Channel Adapters
Advanced
Checkpoints
Availability
Normal
Firmware

Network Adapter 1

Connectivity

○ Not connected

● Connected to a VM network

VM network: VM network Browse...

VM subnet: None

☑ Trunk Mode

Note: Trunk Mode only applied for VM Networks that have corresponding Logical Networks configured as VLAN based Independent Networks.

VM network(s):
☑ VM network (VLANId : 60)
☑ VM network50 (VLANId : 50)
☑ VMnetwork70 (VLANId : 70)

3. The VM Network that is selected as part of *Connected to a VM Network* workflow must also be made the native VLAN. You can't change the native VLAN later, as this is based on the VM network that was selected as part of *Connected to a VM Network* workflow.

Add a virtual adapter with PowerShell

You can use PowerShell to add a virtual adapter.

Here are the sample cmdlets for setting this up. Select the required tab to view or copy the sample cmdlets:

Add a vNIC

Sample cmdlets for adding a vNIC:

- The first command gets the virtual machine object named VM01 and then stores the object in the $VM variable.
- The second command creates a virtual network adapter on VM01.

```
PS C:\> $VM = Get-SCVirtualMachine -Name "VM01"
PS C:\> New-SCVirtualNetworkAdapter -VM $VM -Synthetic
```

Manage static memory on a running VM

You can modify the memory configuration of a running VM that uses static memory. This feature helps in eliminating workload downtime due to reconfiguration. You can increase or decrease the memory allocation, or switch the virtual machine to dynamic memory. Users can already modify dynamic memory for a running VM from VMM, and this feature is about modifying the static memory.

Use the following PowerShell examples to modify the static memory setting.

Example 1

Change the static memory for a running virtual machine.

- The first command gets the virtual machine object named VM01, and then stores the object in the $VM variable.
- The second command changes the memory allocated to VM01 to 1024 MB.

```
PS C:\> $VM = Get-SCVirtualMachine -Name "VM01"
PS C:\> Set-SCVirtualMachine -VM $VM -MemoryMB 1024
```

Example 2

Enable dynamic memory for a running virtual machine.

- The first command gets the virtual machine object named VM02, and then stores the object in the $VM variable.
- The second command enables dynamic memory, sets the startup memory to 1024 MB, and sets the maximum memory to 2048 MB.

```
PS C:\> $VM = Get-SCVirtualMachine -Name "VM02"
PS C:\> Set-SCVirtualMachine -VM $VM -DynamicMemoryEnabled $True -MemoryMB
1024 -DynamicMemoryMaximumMB 2048
```

Add a servicing window to a VM

You can set up a servicing window for a VM or service so that you can maintain it outside the VMM console. You set up the window and assign it to the VM properties.

Create a production checkpoint for a VM

Production checkpoints allow you to easily create *point in time* images of a VM, which can then be restored later.

- Production checkpoints are achieved using backup technology inside the guest to create the checkpoint instead of using the saved state technology.
- On a virtual machine running a Windows operating system, production checkpoints are created with the Volume Snapshot Service (VSS).
- Linux virtual machines flush their file system buffers to create a file system consistent checkpoint.
- If you want to create checkpoints using saved state technology, you can still choose to use standard checkpoints for your virtual machine.
- You can set one of these checkpoint settings for a VM:
  - **Disabled**: No checkpoint taken.
  - **Production**: Production checkpoints are application consistent snapshots of a virtual machine. Hyper-V uses the guest VSS provider to create an image of the virtual machine where all its applications are in a consistent state. The production snapshot doesn't support the autorecovery phase during creation. Applying a production checkpoint requires the restored virtual machine to boot from an off-line state just like with a restored backup. This is always more suitable for production environments.
  - **ProductionOnly**: This option is the same as Production with one key difference: With ProductionOnly, if a production checkpoint fails, then no checkpoint will be taken. This is different from Production where if a production checkpoint fails, a standard checkpoint will be taken instead.
  - **Standard**: All the memory state of running applications gets stored so that when you apply the checkpoint, the application reverts to the previous state. For many applications this wouldn't be suitable for a production environment. Therefore, this type of checkpoint is typically more suitable for development and test environments for some applications.

Set the checkpoint with the following PowerShell command: `Set-SCVirtualMachine CheckpointType (Disabled, Production, ProductionOnly, Standard)`

Configure availability options for clustered VMs

You can configure many settings that help high availability and resilience for virtual machines in a cluster:

- **Storage QoS**: You can configure Hyper-V VM hard disks with quality-of-service (QoS) settings to control bandwidth. You use Hyper-V Manager to do this.
- **Virtual machine priority**: You can configure priority settings for VMs deployed in a host cluster. Based on VM priority, the host cluster starts or places high-priority virtual machines before medium-priority or low-priority virtual machines. This ensures that the high-priority virtual machines are allocated memory and other resources first for better performance. Also, after a node failure, if the high-priority virtual machines don't have the necessary memory and other resources to start, the lower priority virtual machines will be taken offline to free up resources for the high-priority virtual machines. Virtual machines that are preempted are restarted later in priority order.
- **Preferred and possible owners of virtual machines**: These settings influence the placement of virtual machines on the nodes of the host cluster. By default, there are no preferred owners (there's no preference), and the possible owners include all server nodes on the cluster.
- **Availability sets**: When you place multiple virtual machines in an availability set, VMM will attempt to keep those virtual machines on separate hosts and avoid placing them together on the same host whenever possible. This helps to improve continuity of service.

Select the required tab for steps to configure QoS, priority, preferred owners, or availability sets:

Configure QoS for a VM

Follow these steps to configure QoS for a VM:

1. Open **Hyper-V Manager** and select **Action** > **Settings**.
2. In **SCSI Controller**, select **Hard Drive**
3. In **Advanced Features**, select **Enable Quality of Service management**.
4. Specify minimum and maximum IOPS values.

Configure resource throttling

VMM includes resource throttling features, such as processor (CPU) and memory throttling, to control resource allocation and help virtual machines to run more effectively.

- **Processor throttling**: You can set the weight of a virtual processor to provide the processor with a larger or smaller share of CPU cycles. The properties ensure that VMs can be prioritized or deprioritized when CPU resources are overcommitted. For highly intensive workloads, more virtual processors can be added, especially when a physical CPU is close to its upper limit.
  - **High, Normal, Low, Custom**: Specifies how the CPU is distributed when contention occurs. Higher priority virtual machines will be allocated CPU first.
  - **Reserve CPU cycles (%)**: Specifies the percentage of CPU resources that are associated with one logical processor that must be reserved for the virtual machine. This is useful when a virtual machine runs applications that are particularly CPU-intensive and you want to ensure a minimal level of CPU resources. A zero setting indicates that no specific CPU percentage is reserved for the virtual machine.
  - **Limit CPU cycles (%)**: Specifies that the virtual machine must not consume more than the indicated percentage of one logical processor.

- **Memory throttling and weight**: Memory throttling helps to prioritize or deprioritize access to memory resources in scenarios where memory resources are constrained. When memory usage on a host is high, the virtual machines with a higher memory priority are allocated memory resources before the virtual machines with a lower priority. If you specify a lower priority, it might prevent a virtual machine from starting when other virtual machines are running, and the available memory is low. You can set the memory priority settings and thresholds as follows:
  - **Static**: The amount of static memory that is assigned to a specific virtual machine.
  - **Dynamic**: Dynamic memory settings include:
    - **Start-up memory**: The amount of memory that is allocated to the virtual machine when it starts up. It must at least be set to the minimum amount of memory that is required to run the operating system and applications on the virtual machine. Dynamic memory will adjust the memory amount as required.
    - **Minimum memory**: The minimum amount of memory that is required for the virtual machine. It allows an idle machine to scale back the memory consumption below the start-up memory requirement. The available memory can then be used by other virtual machines.
    - **Maximum memory**: The memory limit that is allocated to the virtual machine. The default value is 1 TB.
    - **Memory Buffer Percentage**: Dynamic memory adds memory to a virtual machine as required, but there's a chance that an application might demand memory more quickly than the dynamic memory allocates it. The memory

buffer percentage specifies the amount of available memory that will be assigned to the virtual machine if needed. The percentage is based on the amount of memory that is needed by the applications and services that run on the virtual machine. It's expressed as a percentage because it changes depending on the virtual machine requirements. The percentage is calculated as follows: Amount of memory buffer = memory needed by the virtual machine/(memory buffer value/100). For example, if the memory that is committed to the virtual machine is 1000 MB and the buffer is 20%, then an additional buffer of 20% (200 MB) will be allocated for a total of 1200 MB of physical memory allocated to the virtual machine.

- **Memory weight**: The priority that is allocated to a virtual machine when the memory resources are in full use. If you set a high priority value, it will prioritize a virtual machine when the memory resources are allocated. If you set a low priority, a virtual machine might be unable to start if memory resources are insufficient.

Select the required tab for steps to configure processor or memory throttling:

Processor throttling

Follow these steps to configure processor throttling:

1. In the virtual machine > **Properties** > **Advanced**, select **CPU Priority**.

2. Select a priority value for the virtual machine. These values specify how the CPU resources are balanced between virtual machines and correspond to the relative weight value in Hyper-V:

   - High - Relative weight value of 200
   - Normal - Relative weight value of 100
   - Low - Relative weight value of 50
   - Custom - Relative weight values that are supported are between 1 and 10000

3. In **Reserve CPU cycles (%)**, specify the percentage of the CPU resources on one logical processor that must be reserved for a virtual machine. This is useful when a virtual machine runs applications that are particularly CPU-intensive and you want to ensure a minimal level of CPU resources. A zero setting indicates that no specific CPU percentage is reserved.

4. In **Limit CPU cycles (%)**, specify the maximum percentage of the CPU resources on one logical processor that the virtual machine must consume. The virtual machine won't be allocated more than this percentage.

Configure virtual NUMA

You configure, deploy, and manage virtual Non-Uniform Memory Access (NUMA) in VMM. Virtual NUMA has the following properties:

- NUMA is a memory architecture that is used in multiprocessor systems, where the time that is required for a processor to access memory depends on the location of the memory relative to the processor. On a NUMA system, a processor can access the local memory (the memory that is directly attached to the processor) faster than the nonlocal memory (the memory that is attached to another processor). NUMA attempts to close the gap between the speed of processors and the memory they use. To do so, NUMA provides separate memory on a per-processor basis. Thus, this helps to avoid the performance degradation that occurs when multiple processors try to access the same memory. Each block of dedicated memory is known as a NUMA node.
- Virtual NUMA enables the deployment of larger and more mission-critical workloads that can be run without significant performance degradation in a virtualized environment, when compared to running nonvirtualized computers with physical NUMA hardware. When a new virtual machine is created, by default, Hyper-V uses values for the guest settings that are in sync with the Hyper-V host NUMA topology. For example, if a host has 16 cores and 64 GB divided evenly between two NUMA nodes with two NUMA nodes per physical processor socket, then a virtual machine that is created on the host with 16 virtual processors will have the maximum number of processors per node setting set to eight, maximum nodes per socket set to two, and the maximum memory per node set to 32 GB.
- NUMA spanning can be enabled or disabled. With spanning enabled, individual virtual NUMA nodes can allocate nonlocal memory, and an administrator can deploy a virtual machine that has more virtual processors per virtual NUMA node than the number of processors that are available on the underlying hardware NUMA node on the Hyper-V host. NUMA spanning for a virtual machine does incur a performance cost because virtual machines access memory on nonlocal NUMA nodes.

Set up virtual NUMA for VMs as follows:

1. In the virtual machine > **Properties** > **Advanced**, select **Virtual NUMA**.

2. In **Maximum processors per virtual NUMA node**, specify the maximum number of virtual processors that belong to the same virtual machine and that can be used concurrently on a virtual NUMA node. Configure this setting to ensure the maximum bandwidth. Different NUMA virtual machines use different NUMA nodes. The minimum limit is 1, and the maximum is 32.
3. In **Maximum memory per virtual NUMA node (MB)**, specify the maximum amount of memory (MB) that can be allocated to a single virtual NUMA node. The minimum limit is 8 MB, and the maximum is 256 GB.
4. In **Maximum virtual NUMA nodes per socket**, specify the maximum number of virtual NUMA nodes that are allowed on a single socket. The minimum number is 1, and the maximum is 64.
5. To enable spanning, select **Allow virtual machine to span hardware NUMA nodes**.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up dynamic and power optimization in VMM

Article • 08/30/2024

Read this article to learn about enabling dynamic optimization (DO) and power optimization for virtual machines (VMs) in System Center Virtual Machine Manager (VMM). The article includes features overview, instructions for setting up BMC for power optimization, and describes how to enable and run these features.

> ⓘ Note
>
> - VMM supports dynamic optimization for Compute and Storage. Use the following procedures, as applicable, for the version of VMM you are using.
> - VMM doesn’t support site aware clusters or stretched clusters. VMM doesn’t consider Hyper-V defined *site-specific fault domains* for dynamic optimization calculation.

- **Dynamic optimization**: Using dynamic optimization, VMM performs live migration of VMs and VHDs within a host cluster. The migration is based on the settings you specify to improve load balancing among hosts and cluster shared storage (cluster shared volumes (CSVs), file shares) and to correct the placement issues for VMs.
  - **Compute Dynamic optimization** (Optimization of hosts) can be performed on hosts in a cluster to optimize host performance by migrating VMs across hosts. You can set the host performance thresholds to **CPU** and **Memory**.

- **Storage Dynamic Optimization** (Optimization of disk space) can be performed on cluster shared storage (CSVs, file shares) to optimize storage space availability by migrating Virtual Hard Disks (VHDs) across shared storage. You can set free storage space threshold on cluster shared storage.

- **Power optimization**: Power optimization is a feature of dynamic optimization that saves energy by turning off hosts that aren't needed to meet resource requirements within a cluster, and turns them back on when they're needed.

VMM supports compute and storage dynamic optimization and power optimization on Hyper-V host clusters. Compute dynamic optimization and power optimization is also supported on VMware host clusters in the VMM fabric that support live migration.

Before you start

Note the following information before you start using DO.

Dynamic optimization

- Dynamic optimization and power optimization can be configured on host clusters that support live migration.
- Dynamic optimization can be configured on a host group to migrate virtual machines and virtual hard disks (VHDs) within host clusters with a specified frequency and aggressiveness. VM aggressiveness determines the amount of load imbalance that is required to initiate a migration during dynamic optimization.
- Disk space aggressiveness determines the amount of free storage space below disk space threshold that is required to migrate VHDs to other cluster shared storage during dynamic optimization.
- By default, virtual machines are migrated every 10 minutes with medium aggressiveness if automatic migration is enabled. When configuring frequency and aggressiveness for dynamic optimization, an administrator must factor in the resource cost of additional migrations against the advantages of balancing load among hosts/shared storage in a host cluster. By default, a host group inherits Dynamic Optimization settings from its parent host group.
- If you set up dynamic optimization on a host group without a cluster, it will have no effect.
- Dynamic optimization can be set up for clusters with two or more nodes. Storage dynamic optimization will need two or more shared storage files/volumes to be present in the cluster. If a host group contains standalone hosts or host clusters that don't support live migration, dynamic optimization isn't performed on those hosts. Any hosts that are in maintenance mode are also excluded from dynamic optimization. In addition, VMM only migrates highly available virtual machines that use shared storage. If a host cluster contains virtual machines that aren't highly available, those virtual machines aren't migrated during Dynamic Optimization.
- On-demand dynamic optimization is also available for individual host clusters using the Optimize Hosts/Optimize Disk space action in the VMs and Services workspace. It can be performed without configuring dynamic optimization on host groups. After dynamic optimization is requested for a host cluster, VMM lists the virtual machines/VHDs that will be migrated for the administrator's approval. Optimize Hosts performs VM load balancing across hosts in a cluster, while Optimize disk space migrates VHDs across Shared storage in a cluster.

Node fairness

It identifies cluster nodes with light loads, and distributes VMs to those nodes to balance load. This is similar to VMM's dynamic optimization. To avoid potential performance issues, dynamic optimization and node fairness must not work together. To ensure this doesn't happen, VMM disables node fairness in all clusters in a host group for which dynamic optimization is set to automatic. If you enable node fairness outside the VMM console, VMM will turn it off the next time that dynamic optimization refreshes. If you do want to use node fairness, disable dynamic optimization and then manually enable node fairness.

Power optimization

- For power optimization, the computers must have a baseboard management controller (BMC) that enables out-of-band management.
- Power optimization ensures that a cluster maintains a quorum if an active node fails. For clusters created outside VMM and added to VMM, Power Optimization requires more than four nodes. For each additional one or two nodes in a cluster, one node can be powered down. For instance:
  - One node can be powered down for a cluster of five or six nodes.
  - Two nodes can be powered down for a cluster of seven or eight nodes.
  - Three nodes can be powered down for a cluster of nine or ten nodes.
- When VMM creates a cluster, it creates a quorum disk and uses that disk as part of the quorum model. For clusters created by VMM, Power Optimization can be set up for clusters of more than three nodes. This means that the number of nodes that can be powered down is as follows:
  - One node can be powered down for a cluster of four or five nodes.
  - Two nodes can be powered down for a cluster of six or seven nodes.
  - Three nodes can be powered down for a cluster of eight or nine nodes.

Configure BMC

For hosts with BMC that support IMPI 1.5/2.0, DCMI 1.0, or SMASH 1.0 over WS-Management, you can configure BMC settings as follows:

1. Create a Run As account with permissions to access the BMC on a host.
2. Select **Fabric** > **Servers** > **All Hosts** > host > **Properties** > **Hardware** > **Advanced** > **BMC Setting**.
3. To enable VMM management, select **This physical machine is configured for OOB management**.

4. In **This computer supports the specified OOB power management configuration provider**, select the supported management protocol. Enter the IP address of the BMC, and accept the default port offered by VMM. Select the Run As account and select **OK**.

Enable dynamic and power optimization for a host group

1. Select **Fabric** > **Servers** > **All Hosts** and select the host group that you want to configure.

2. With the host group selected, select **Folder** > **Properties** group > **Properties**.

3. In the host group properties, select **Dynamic Optimization**.

4. In **Specify dynamic optimization settings**, clear the **Use Dynamic Optimization settings from the parent host group** checkbox.

5. In **Aggressiveness**, select a value on an integer scale of 1 to 5, where 1 is the lowest degree of aggressiveness and 5 is the highest.

VM aggressiveness determines the amount of load imbalance that is required to initiate a migration during dynamic optimization.

Disk space aggressiveness determines the amount of free storage space below disk space threshold that is required to migrate VHDs to other cluster shared storage during dynamic optimization.

When you configure frequency and aggressiveness for dynamic optimization, you must try to balance the resource cost of additional migrations against the advantages of balancing load among hosts in a host cluster. Initially, you might accept the default value of **3**. After you observe the effects of dynamic optimization in your environment, you can increase the aggressiveness.

6. To help conserve energy by having VMM turn off hosts when they aren't needed and turn them on again when they're needed, configure power optimization for the host group. Power optimization is only available when virtual machines are being migrated automatically to balance load.

7. To periodically run dynamic optimization on qualifying host clusters in the host group, enter the following settings:
   a. Select the **Automatically migrate virtual machines to balance load** checkbox to balance free storage space across shared storage.

b. In **Frequency**, specify how often to run dynamic Optimization. You can enter any value between 10 minutes and 1440 minutes (24 hours).

8. Set thresholds for each of the compute and storage resources listed. To change the units of the resources, go to **Host group**> **Properties** > **Host Reserves** and choose the unit from the dropdown menu.

9. To turn on power optimization on the host group, select the **Enable power optimization** checkbox. Select **OK** again to save your changes.

> ⓘ **Note**
>
> If there is a mismatch of disk space warning levels between host groups having the same file share, it can result in multiple migrations to and from that file share and can impact storage DO performance. We recommend you to not do a file share across different host groups where storage dynamic optimization is enabled.

Configure power optimization settings

1. In the **Fabric**, navigate to the host group and open **Properties**.
2. Select **Dynamic Optimization** > **Specify dynamic optimization settings** > **Settings**.
3. In **Customize Power Optimization Schedule**, change the settings for any of these resources: CPU, memory, disk I/O, or network I/O.
4. Under **Schedule**, select the hours when you want power optimization to be performed. Select a box to turn power optimization on or off for that hour. VMM applies the schedule according to the host time zone.

Run dynamic optimization on-demand in a host cluster

You can run dynamic optimization on demand on a host cluster. To do this, dynamic optimization doesn't need to be configured on the parent host group.

1. Open **Fabric** > **Servers** > **Host Groups** and navigate to the host cluster.

2. To perform compute resource load balancing, select **Optimize hosts**. To perform storage load balancing across cluster shared storage, select **Optimize disks**.

To Optimize hosts: VMM performs a dynamic optimization review to determine whether VHDs can be migrated to improve load balancing in the host cluster. If migration of VMs can improve load balancing, VMM displays a list of VMs that are recommended for migration, with the current and target hosts indicated. The list excludes any hosts that are in maintenance mode in VMM and any virtual machines that aren't highly available.

To Optimize Disk Space: VMM performs a dynamic optimization review to determine whether VHDs can be migrated to meet the free storage space threshold (disk space) while considering aggressiveness set in the Dynamic Optimization page. Dynamic Optimization will only be triggered when any cluster shared storage violates the disk space threshold set. If migration of VHDs can help free the storage space threshold in shared storage in the cluster, VMM displays a list of VHDs that are recommended for migration, with the current and target storage space indicated. VHDs will only migrate to another shared storage with the same storage classification.

3. Select **Migrate**.

> **Note**
>
> If VHDs are migrated between one storage type to another (for example, from a CSV to NAS file share), the storage migration will be slow. If the storage optimization does not return a list of VHDs to migrate even when the threshold and aggressiveness criteria are met:
>
> - Check the HostVolumeID using Get-SCStorageVolume Cmdlet. If the HostVolumeID returns Null for the volume, refresh the VM and perform Storage Dynamic Optimization again.
> - Check the DiskSpacePlacementLevel of the host group using the Get-SCHostReserve cmdlet. Set the DiskSpacePlacementLevel value equal to the value of Disk Space set in Host Reserve settings in the Dynamic Optimization wizard.

Power on/off a computer in VMM

1. Select **Fabric** > **Servers** > **All Hosts** > host name.
2. On the **Host** tab, in the **Host** group, select **Power On** or **Power Off**. You can view information about power on and off events in the BMC logs (select **Hardware** > **Advanced** > **BMC Logs**).

Next steps

Learn about provisioning VMs.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Configure VM failover between virtual networks

Article • 08/30/2024

This article describes how to handle replication and failover of VMs in System Center Virtual Machine Manager (VMM) between virtual networks when you're not using the Azure Site Recovery service to manage disaster recovery.

- Use Azure Site Recovery for replicating VMs. VMM doesn't manage Hyper-V Replica without Site Recovery, and you need to use Hyper-V Replica PowerShell cmdlets to automate Hyper-V Replica operations.
- For disaster recovery, we recommend that you use separate primary and secondary virtual networks. Primary VMs connect to the primary network, and replica VMs to the secondary network. This ensures that both VMs can be connected to a network at the same time.
- If you have a single virtual network, use Site Recovery to automate network management using the network mapping feature. If you don't use Site Recovery, you need to carefully check prerequisites, and the order in which VMs are attached to the network. In particular, the replica VM and primary VM mustn't be connected to the single virtual network at the same time. Otherwise, CA-PA records might get deleted in VMM and cause network connectivity loss.

Sample solution

This sample solution describes the following environment:

- A single VMM server manages both primary and secondary sites.
- Primary and replica VMs are hosted on a single Hyper-V virtual network.
- You want to run a planned failover and retain the IP address of the VM after the failover.
- VMs have IPv4 addresses.

Before you start

- Ensure that the virtual switch and logical switch settings are valid and match in the VMM fabric. If they don't, network attach operations might not succeed after failover.

- The primary VM must be connected to a virtual network

- The replica VM must not be connected to a network
- Only one IP address must be assigned to each network adapter of the primary VM. Run this command to ensure this. If there's more than one connected network adapter on the VM, run it for adapter by changing the array index.

  PowerShell

  ```
  $VMOnPD = Get-SCVirtualMachine -Name "VM Name" | where {$_.IsPrimaryVM
  -eq $true}
  Get-SCIPAddress -GrantToObjectId $VMOnPD.VirtualNetworkAdapters[0].ID``
  ```

- Ensure that the IP address assigned to the VM by the operating system is the same as the IP address displayed above. Sign in to the VM and run **ipconfig** to check this.
- Ensure that lookup tables are correctly set on the primary and replica. To do this, run the following command on each server, and ensure that there's an entry that corresponds to the IP address returned above: `Get-NetVirtualizationLookupRecord`
- Check that the IP address is IPv4, and not IPv6
- Ensure both VMs are turned off before you run the scripts.
- Ensure that the replication state is enabled on both VMs.

Run the planned failover script

Here's what this script does:

1. For each network adapter on a primary VM, it stores the IP address, VM network, and IP pool.
2. Revokes all the IP addresses for each network adapter on the primary and secondary VMs.
3. Disconnects all network adapters.
4. Fails over the primary and secondary VMs.
5. Optionally starts reverse replication.
6. Gives the same IP address (for each network adapter) to the replica VM.
7. Attaches each network adapter on the replicate VM to the VM networks that were stored in step 1.

Run the script

The script takes two arguments:

- $VMName – Name of the virtual machine
- $ReverseRep – Boolean argument to specify whether reverse replication must be performed or not
  - If $true is passed, then the reverse replication is started immediately, and you can't cancel failover later.
  - After this script is completed successfully with $ReverseRep as $true:
    - The primary VM must be in a **Prepared for planned failover** replication state.
    - The replica VM must be in a **Failover complete** replication state.
  - If $false is passed, then reverse replication isn't performed. ReverseRepORCancelFO.ps1 can be used to either perform reverse replication or cancel the failover.
  - After the script is completed successfully with $ReverseRep as $false:
    - The primary VM must be in a **Prepared for planned failover** replication state.
    - The replica VM must be in a **Failover complete** replication state.

If the script doesn't complete any of the steps, you need to manually complete the failed steps, and then return to the PowerShell window. The script steps include failover of the primary VM, failover of the replica VM, and optionally reverse replication.

Run the script:

PowerShell

```powershell
 Param(
 [Parameter(Mandatory=$True)]
   [string]$VMName,
 [Parameter(Mandatory=$true)]
   [boolean]$ReverseRep
)

# the script running on system with SCVMM Console/PowerShell installed.
Also, requires Hyper-V PowerShell module.``

Import-Module hyper-v

## Refresh VM configuration and initialize
Write-Host -ForegroundColor Green (Get-Date) ".....Refreshing the VMs..."
Get-SCVirtualMachine -Name $VMName | Read-SCVirtualMachine

$VMOnPD = Get-SCVirtualMachine -Name $VMName | where {$_.IsPrimaryVM -eq
$true}
$VMOnDR = Get-SCVirtualMachine -Name $VMName | where {$_.IsPrimaryVM -eq
$false}

if ($VMOnPD.StatusString -ne "Stopped")
{
    write-host -ForegroundColor Red (Get-Date) "....VM is not in stopped
state. Actual State " $VMOnPD.StatusString
    write-host -ForegroundColor Red (Get-Date) "....Exiting"
    exit 1
}

$error.Clear()
$VMRepConfig = Get-VMReplication -ComputerName $VMOnPD.HostName -VMName
$VMOnPD.Name
$VMRepConfig = Get-VMReplication -ComputerName $VMOnDR.HostName -VMName
$VMOnPD.Name

if ($error -ne 0)
{
    $temp = $VMOnPD.HostName.Split(".")
    $primaryHostName = $temp[0]

    $temp = $VMOnDR.HostName.Split(".")
    $recoveryHostName = $temp[0]

    write-host -ForegroundColor Red (Get-Date) "....Error in getting VM
Replication state using FQDN, switching to Hostname"
    write-host -ForegroundColor Yellow (Get-Date) "....Primary Hostname: "
$primaryHostName " Replica Hostname: " $recoveryHostName

    $error.Clear()
    $VMRepConfig = Get-VMReplication -ComputerName $primaryHostName -VMName
$VMOnPD.Name
    $VMRepConfig = Get-VMReplication -ComputerName $recoveryHostName -VMName
$VMOnPD.Name

    if ($error -ne 0)
    {
        write-host -ForegroundColor Red (Get-Date) "....Error in getting VM
Replication state using Hostname"
        write-host -ForegroundColor Red (Get-Date) "....Exiting"
        exit 1
    }

    write-host -ForegroundColor Green (Get-Date) "....Successful in getting
VM Replication state using Hostname"
}
else
{
    $primaryHostName = $VMOnPD.HostName
    $recoveryHostName = $VMOnDR.HostName
}

$VMOnPDAdapter = Get-SCVirtualNetworkAdapter -VM $VMonPD
$VMOnDRAdapter = Get-SCVirtualNetworkAdapter -VM $VMonDR

$fileName = $VMName + (Get-Date).ToString() + ".txt"
$fileName = $fileName.Replace("/","_")
$fileName = $fileName.Replace(":","_")
```

```
Write-Host -ForegroundColor Yellow (Get-Date) "....Dumping network
information for $VMName to file $fileName"
Write-Host -ForegroundColor Yellow (Get-Date) "....Number of Network
adapters found: " $VMOnPDAdapter.count

$VMNetwork = @()
$VMSubnet = @()
$Pools = @()

$counter = 0
foreach($vmAdapter in $VMOnPDAdapter)
{
    if ($vmAdapter.VMNetwork -eq $null)
    {
        $VMNetwork = $VMNetwork + $null
        $VMSubnet = $VMSubnet + $null
        $Pools = $Pools + $null
        $counter = $counter + 1
        continue
    }

    $VMNetwork = $VMNetwork + (Get-SCVMNetwork -Name
$vmAdapter.VMNetwork.Name -ID $vmAdapter.VMNetwork.ID)
    $VMSubnet = $VMSubnet + (Get-SCVMSubnet -Name $vmAdapter.VMSubnet.Name |
where {$_.VMNetwork.ID -eq $vmAdapter.VMNetwork.ID})
    #$PortClassification = Get-SCPortClassification | where {$_.Name -eq
"Guest Dynamic IP"}
    $Pools = $Pools + (Get-SCStaticIPAddressPool -IPv4 | where
{$_.VMsubnet.name -eq $vmAdapter.VMSubnet.Name})

    Out-File -FilePath $fileName -InputObject $VMNetwork[$counter] -Append
    Out-File -FilePath $fileName -InputObject $VMSubnet[$counter] -Append
    Out-File -FilePath $fileName -InputObject $Pools[$counter] -Append

    $counter = $counter + 1
}

if ($error.Count -ne 0)
{
    write-host -ForegroundColor Red (Get-Date) "....Error is gathering
information for $VMName. No changes made"
    write-host -ForegroundColor Red (Get-Date) "....Exiting"
    exit 1
}

$IP = @()
$counter = 0
foreach($vmAdapter in $VMOnPDAdapter)
{

    if ($VMNetwork[$counter] -eq $null)
    {
        Write-Host -ForegroundColor Yellow (Get-Date) ".....Network Adapter
'" $counter "' not connected"
        $IP = $IP + $null
        $counter = $counter + 1
        continue
    }

    ## Revoke IP
    $error.Clear()
    $IP = $IP +(Get-SCIPAddress –GrantToObjectId
$VMOnPD.VirtualNetworkAdapters[$counter].ID)
    Write-Host -ForegroundColor Yellow (Get-Date) "....Revoking IP "
$IP[$counter] "from Primary VM"
    Revoke-SCIPAddress $IP[$counter]
    if ($error.count -eq 0)
    {
        Write-Host -ForegroundColor Green (Get-Date) "....." $IP[$counter]
"revoke completed"
    }

    ## Disconnect Primary VM
    Write-Host -ForegroundColor Yellow (Get-Date) "....Disconnecting Primary
VM from Network " $VMNetwork[$counter]
    Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter
$VMOnPD.VirtualNetworkAdapters[$counter] -NoLogicalNetwork -NoConnection -
NoPortClassification
    Write-Host -ForegroundColor Green (Get-Date) "....Network Adapter '"
$counter "' of Primary VM Disconnected"

    $counter = $counter + 1
}

## Start failover
Write-Host -ForegroundColor Yellow (Get-Date) ".....We are going to Failover
" $VMName " from " $primaryHostName " to " $recoveryHostName

$error.Clear()
Start-VMFailover -ComputerName $primaryHostName -VMName $VMOnPD.Name -
Prepare -Confirm:$false

start-sleep 5

Write-Host -ForegroundColor Yellow (Get-Date) ".....Completing Failover on
Replica site..."
Start-VMFailover -ComputerName $recoveryHostName -VMName $VMOnDR.Name -
Confirm:$false
if ($ReverseRep)
{
    write-host -ForegroundColor Green (Get-Date) ".....Starting Reverse
Replication..."
    Set-VMReplication -ComputerName $recoveryHostName -reverse -VMName
$VMOnDR.Name
}

if ($error -ne 0)
{
    write-host -ForegroundColor Red (Get-Date) ".....Error occured during
Planned Failover for VM $VMName"
```

```
    write-host -ForegroundColor Red (Get-Date) ".....Please manually
complete Failover before continuing"
    Write-Host -ForegroundColor Red (Get-Date) ".....Press any key to
continue..."
    $ignoreKey = $host.UI.RawUI.ReadKey("NoEcho,IncludeKeyDown")
}

Write-Host -ForegroundColor Green (Get-Date) ".....Connecting Network(s) to
Failed-over VM"

$counter = 0
foreach($vmAdapter in $VMOnPDAdapter)
{

    if ($VMNetwork[$counter] -eq $null)
    {
        Write-Host -ForegroundColor Yellow (Get-Date) ".....Network Adapter
'" $counter "' not connected"
        $counter = $counter + 1
        continue
    }

    Write-Host -ForegroundColor Yellow (Get-Date) "Granting " $IP[$counter]
"to Failed-over VM"
    Grant-SCIPAddress -GrantToObjectType "VirtualNetworkAdapter" -
GrantToObjectID $VMOnDRAdapter[$counter].ID -StaticIPAddressPool
$Pools[$counter] -IPAddress $IP[$counter]
    Write-Host -ForegroundColor Green (Get-Date) "Granting IP completed"

    Write-Host -ForegroundColor Yellow (Get-Date) "Connecting Replica VM to
" $VMNetwork[$counter]
    Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter
$VMOnDRAdapter[$counter] -IPv4AddressType static -VMNetwork
$VMNetwork[$counter] -VMSubnet $VMSubnet[$counter]
    Write-Host -ForegroundColor Green (Get-Date) "Network Adapter '"
$counter "' of Failed-over VM connected to " $VMNetwork[$counter]

    $counter = $counter + 1
}
```

Run the reverse replication/cancel script

Here's what this script does:

1. If you didn't run reverse replication in the failover script, you can use this script for reverse replication, or to cancel the failover.
2. If you cancel, the script reverses the networking steps and restores the primary VM connections after disconnecting the replica VM networks.

Run the script

This script should be run for the failover script with $ReverseRep set to **$false**. This script takes three arguments:

- $VMName: VM name.
- $ReverseRep: Boolean argument to specify whether reverse replication should be performed. $true indicates that reverse replication runs.
- $CancelFO: Boolean argument to specify whether the failover is cancelled. $true indicates cancellation on primary and recovery sites.

One and only one of $ReverseRep and $CancelFO can be passed $true at a time. After the script runs successfully, the state on both VMs should be **Replication enabled**'.

Run the script:

PowerShell

```powershell
Param(
 [Parameter(Mandatory=$True)]
   [string]$VMName,
 [Parameter(Mandatory=$true)]
   [boolean]$ReverseRep,
 [Parameter(Mandatory=$true)]
   [boolean]$CancelFO
)

# the script running on system with SCVMM Console/PowerShell installed.
Also, requires Hyper-V PowerShell module.

Import-Module hyper-v

if ($ReverseRep -eq $CancelFO)
{
    write-host -ForegroundColor Red (Get-Date) "....Please ensure that one
and only one of the parameters -ReverseRep and -CancelFO is passed as $True"
    write-host -ForegroundColor Red (Get-Date) "....Exiting"
    exit 1
}

## Refresh VM configuration and initialize
Write-Host -ForegroundColor Green (Get-Date) ".....Refreshing the VMs..."
Get-SCVirtualMachine -Name $VMName | Read-SCVirtualMachine

$VMOnPD = Get-SCVirtualMachine -Name $VMName | where {$_.IsPrimaryVM -eq
$true}
$VMOnDR = Get-SCVirtualMachine -Name $VMName | where {$_.IsPrimaryVM -eq
$false}

$error.Clear()
$VMRepConfig = Get-VMReplication -ComputerName $VMOnPD.HostName -VMName
$VMOnPD.Name
$VMRepConfig = Get-VMReplication -ComputerName $VMOnDR.HostName -VMName
```

```
$VMOnPD.Name

if ($error -ne 0)
{
    $temp = $VMOnPD.HostName.Split(".")
    $primaryHostName = $temp[0]

    $temp = $VMOnDR.HostName.Split(".")
    $recoveryHostName = $temp[0]

    write-host -ForegroundColor Red (Get-Date) "....Error in getting VM
Replication state using FQDN, switching to Hostname"
    write-host -ForegroundColor Yellow (Get-Date) "....Primary Hostname: "
$primaryHostName " Replica Hostname: " $recoveryHostName

    $error.Clear()
    $VMRepConfig = Get-VMReplication -ComputerName $primaryHostName -VMName
$VMOnPD.Name
    $VMRepConfig = Get-VMReplication -ComputerName $recoveryHostName -VMName
$VMOnPD.Name

    if ($error -ne 0)
    {
        write-host -ForegroundColor Red (Get-Date) "....Error in getting VM
Replication state using Hostname"
        write-host -ForegroundColor Red (Get-Date) "....Exiting"
        exit 1
    }

    write-host -ForegroundColor Green (Get-Date) "....Successful in getting
VM Replication state using Hostname"
}
else
{
    $primaryHostName = $VMOnPD.HostName
    $recoveryHostName = $VMOnDR.HostName
}

if ($VMOnDR.ReplicationStatus.ReplicationState -ne "Recovered")
{
    write-host -ForegroundColor Red (Get-Date) "....Replica VM is not in
Failed over state. Actual State " $VMOnDR.ReplicationStatus.ReplicationState
    write-host -ForegroundColor Red (Get-Date) "....Exiting"
    exit 1
}

$error.Clear()

if ($ReverseRep -eq $true)
{
    write-host -ForegroundColor Green (Get-Date) ".....Starting Reverse
Replication..."
    Set-VMReplication -ComputerName $recoveryHostName -reverse -VMName
$VMOnDR.Name
```

```
    if ($error -ne 0)
    {
        write-host -ForegroundColor Red (Get-Date) ".....Error occured
during Reverse Replication for VM $VMName"
        write-host -ForegroundColor Red (Get-Date) ".....Please manually
complete Reverse replication"
        exit 1
    }

    write-host -ForegroundColor Green (Get-Date) ".....Reverse Replication
completed..."
    exit 0
}

if ($VMOnDR.StatusString -ne "Stopped")
{
    write-host -ForegroundColor Red (Get-Date) "....VM is not in stopped
state. Actual State " $VMOnDR.StatusString
    write-host -ForegroundColor Red (Get-Date) "....Exiting"
    exit 1
}

$VMOnPDAdapter = Get-SCVirtualNetworkAdapter -VM $VMonPD
$VMOnDRAdapter = Get-SCVirtualNetworkAdapter -VM $VMonDR

$fileName = $VMName + (Get-Date).ToString() + ".txt"
$fileName = $fileName.Replace("/","_")
$fileName = $fileName.Replace(":","_")

Write-Host -ForegroundColor Yellow (Get-Date) "....Dumping network
information for $VMName to file $fileName"
Write-Host -ForegroundColor Yellow (Get-Date) "....Number of Network
adapters found on Failed-over VM: " $VMOnDRAdapter.count

$VMNetwork = @()
$VMSubnet = @()
$Pools = @()

$counter = 0
foreach($vmAdapter in $VMOnDRAdapter)
{
    if ($vmAdapter.VMNetwork -eq $null)
    {
        $VMNetwork = $VMNetwork + $null
        $VMSubnet = $VMSubnet + $null
        $Pools = $Pools + $null
        $counter = $counter + 1
        continue
    }

    $VMNetwork = $VMNetwork + (Get-SCVMNetwork -Name
$vmAdapter.VMNetwork.Name -ID $vmAdapter.VMNetwork.ID)
    $VMSubnet = $VMSubnet + (Get-SCVMSubnet -Name $vmAdapter.VMSubnet.Name |
where {$_.VMNetwork.ID -eq $vmAdapter.VMNetwork.ID})
    #$PortClassification = Get-SCPortClassification | where {$_.Name -eq
"Guest Dynamic IP"}
    $Pools = $Pools + (Get-SCStaticIPAddressPool -IPv4 | where
{$_.VMsubnet.name -eq $vmAdapter.VMSubnet.Name})

    Out-File -FilePath $fileName -InputObject $VMNetwork[$counter] -Append
    Out-File -FilePath $fileName -InputObject $VMSubnet[$counter] -Append
    Out-File -FilePath $fileName -InputObject $Pools[$counter] -Append

    $counter = $counter + 1
}

if ($error.Count -ne 0)
{
    write-host -ForegroundColor Red (Get-Date) "....Error is gathering
information for $VMName. No changes made"
    write-host -ForegroundColor Red (Get-Date) "....Exiting"
    exit 1
}

$IP = @()
$counter = 0
foreach($vmAdapter in $VMOnDRAdapter)
{

    if ($VMNetwork[$counter] -eq $null)
    {
        Write-Host -ForegroundColor Yellow (Get-Date) ".....Network Adapter
'" $counter "' not connected"
        $IP = $IP + $null
        $counter = $counter + 1
        continue
    }

    ## Revoke IP
    $error.Clear()
    $IP = $IP +(Get-SCIPAddress –GrantToObjectId
$VMOnDR.VirtualNetworkAdapters[$counter].ID)
    Write-Host -ForegroundColor Yellow (Get-Date) "....Revoking IP "
$IP[$counter] "from Replica VM"
    Revoke-SCIPAddress $IP[$counter]
    if ($error.count -eq 0)
    {
        Write-Host -ForegroundColor Green (Get-Date) "....." $IP[$counter]
"revoke completed"
    }

    ## Disconnect Replica VM
    Write-Host -ForegroundColor Yellow (Get-Date) "....Disconnecting Replica
VM from Network " $VMNetwork[$counter]
    Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter
$VMOnDR.VirtualNetworkAdapters[$counter] -NoLogicalNetwork -NoConnection -
NoPortClassification
    Write-Host -ForegroundColor Green (Get-Date) "....Network Adapter '"
$counter "' of Replica VM Disconnected"
```

```
    $counter = $counter + 1
}

## Cancel failover
Write-Host -ForegroundColor Yellow (Get-Date) ".....We are going to Cancel
Failover " $VMName " on both " $primaryHostName " and " $recoveryHostName

$error.Clear()
Stop-VMFailover -ComputerName $recoveryHostName -VMName $VMName
Start-Sleep -Seconds 10
Stop-VMFailover -ComputerName $primaryHostName -VMName $VMName

if ($error -ne 0)
{
    write-host -ForegroundColor Red (Get-Date) ".....Error occured during
Cancel Failover for VM $VMName"
    write-host -ForegroundColor Red (Get-Date) ".....Please manually Cancel
Failover on both Primary and Recovery Server"
    Write-Host -ForegroundColor Red (Get-Date) ".....Press any key to
continue..."
    $ignoreKey = $host.UI.RawUI.ReadKey("NoEcho,IncludeKeyDown")
}

Write-Host -ForegroundColor Yellow (Get-Date) ".....Connecting Network(s)
back to the Primary VM"

$counter = 0
foreach($vmAdapter in $VMOnDRAdapter)
{

    if ($VMNetwork[$counter] -eq $null)
    {
        Write-Host -ForegroundColor Yellow (Get-Date) ".....Network Adapter
'" $counter "' not connected"
        $counter = $counter + 1
        continue
    }

    Write-Host -ForegroundColor Yellow (Get-Date) "Granting " $IP[$counter]
"to Primary VM"
    Grant-SCIPAddress -GrantToObjectType "VirtualNetworkAdapter" -
GrantToObjectID $VMOnPDAdapter[$counter].ID -StaticIPAddressPool
$Pools[$counter] –IPAddress $IP[$counter]
    Write-Host -ForegroundColor Green (Get-Date) "Granting IP completed"

    Write-Host -ForegroundColor Yellow (Get-Date) "Connecting Primary VM to
" $VMNetwork[$counter]
    Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter
$VMOnPDAdapter[$counter] -IPv4AddressType static -VMNetwork
$VMNetwork[$counter] -VMSubnet $VMSubnet[$counter]
    Write-Host -ForegroundColor Green (Get-Date) "Network Adapter '"
$counter "' of Primary VM connected to " $VMNetwork[$counter]

    $counter = $counter + 1
}
```

Migration of virtual machines – overview

Article • 08/30/2024

This article provides an overview of migrating virtual machines in the System Center Virtual Machine Manager (VMM) fabric.

You can migrate virtual machines and storage managed VMs in the VMM fabric. VMM automatically selects the type of transfer that will be used for migration. When you perform a migration in the VMM console using the Migrate VM Wizard, the migration type that will be used is displayed in the **Transfer Type** column. The types of migrations supported are summarized in the following table.

Expand table

Type	Use	Details
Network migration	Performs a network copy of the virtual machine data using BITS.	This is the slowest type of migration. The amount of downtime is in direct proportion to the size of the data transfer.
Quick migration	Also known as cluster transfer, it can be used to migrate a highly available virtual machine. It uses Windows Failover Cluster to migrate virtual machines between cluster nodes.	The running state of the virtual machine is saved to disk (the virtual machine is hibernated), the disk is failed over to the other cluster node, and then the saved state is loaded to wake up the virtual machine. Downtime is minimal because quick migration takes a snapshot of the virtual machine, and transfers data without requiring the virtual machine to be turned off.
Quick storage migration	Used to move VM storage from one location to another. For example, you can move the storage for a virtual machine from a Fibre Channel SAN to an iSCSI SAN.	The virtual disks of a running virtual machine can be migrated independent of the storage protocols (SCSI, Fibre Channel) or storage types (local, DAS, SAN). Downtime is minimal because quick storage migration takes a snapshot of the virtual machine and transfers data

Type	Use	Details
		without requiring the virtual machine to be turned off.
SAN migration	Uses SAN transfer to migrate virtual machines and highly available virtual machines in and out of a cluster. It can be used when both the source and destination hosts have access to the same storage infrastructure (LUN), and the storage can be transferred from one host to another.	For SAN migration, the files for a virtual machine aren't copied from one server to another and thus downtime is minimized. SAN migration can be used to copy a virtual machine from one host to another or copying a virtual machine to or from the library. When you migrate a virtual machine into a cluster using a SAN transfer, VMM checks that each node in the cluster can see the LUN, and automatically creates a cluster disk resource for the LUN. To migrate a virtual machine out of a cluster, the virtual machine must be on a dedicated LUN that isn't using CSV. These SAN infrastructures are supported for migration: Fiber Channel; iSCSI SANs; N_Port ID Virtualization (NPID).
Live migration	Moves a virtual machine running as part of a failover cluster from one cluster to another.	No noticeable downtime for users or network applications.

Live migration

Using live migration provides many benefits:

- **Increased flexibility**: Live migration features can help simplify the movement of virtual machines across hosts and clusters. Therefore, it becomes easier to manage a dynamic datacenter.
- **Ease-of-maintenance**: Live migration alleviates the need to take standalone hosts and cluster hosts offline for maintenance and migration purposes, which helps to avoid downtime. With the ability to perform concurrent migrations and maintenance, migration timeframes can become shorter, depending on the time that is required to perform the live migration. In addition, the planning process for Hyper-V mobility is simplified.

- **Better hardware utilization**: The distribution of virtual machines can be optimized across the infrastructure. Virtual machines and storage can be moved to standalone servers and clusters with spare capacity, without interrupting availability. Power consumption is reduced as virtual machines can be moved across hosts, and then hosts can be powered down to save energy.
- **Failover clustering features**: VMM takes advantage of failover clustering features that were introduced in Windows Server 2012. These features include additional APIs to migrate virtual machines across cluster nodes, and improved attach/detach functionality that enables migration of virtual machines in and out of failover clusters without downtime.

Live migration support

VMM supports the following types of live migration:

- **Live migration of standalone machines**: You can run live migration between two standalone machines that aren't in a cluster.
- **Live migration within a cluster**: You can run a live migration between nodes in the same cluster.
- **Live migration between nodes in different clusters**: You can migrate between nodes in different clusters.
- **Live migration of VM storage**: You can migrate storage to update the physical storage available in Hyper-V or to mitigate bottlenecks in storage performance. You can also use storage migration to move, service, or upgrade storage resources, or for migration of a standalone or cluster virtual machine. Storage can be added to either a standalone computer or to a Hyper-V cluster. VMs can be moved to the new storage while they continue to run.
- **Live Virtual machine and storage migration**: You can use live system migration (live VSM) to migrate virtual machines and their storage together in a single action.
- **Concurrent live migration**: You can perform multiple concurrent live migrations of virtual machines and storage. The concurrent limit can be configured manually. Any concurrent live migrations exceeding of the limit will be queued.

VMM inspects and validates the configuration settings of a destination host before migration from a source host begins.

Live VM migration support matrix

Expand table

Source	Destination: Standalone	Destination: Cluster
Standalone	Supported	Supported
Cluster	Supported	Supported Source and destination can be in the same or different clusters.

Live storage migration support matrix

Expand table

Source	Destination: Local disk (standalone)	Destination: SMB 3.0 share (standalone/cluster)	Destination: CSV (cluster)
Local disk	Supported	Supported. The virtual machine will be promoted to high availability.	Not supported.
SMB 3.0 share	Supported. In a cluster, the VM will be demoted and won't be highly available after migration.	Supported	Supported
Cluster	Supported In a cluster, the VM will be demoted and won't be highly available after migration.	Supported The SMB share must be available from the destination cluster node.	Supported The CSV must be available from the destination cluster node.

Live migration limitations

- Live migration requires two or more servers that run Hyper-V, that support hardware virtualization, and use processors from the same manufacturer, such as all AMD processors or all Intel processors.

- Virtual machines must be configured to use virtual hard disks or virtual Fibre Channel disks, not physical disks.

- For live migration network traffic, you must use a private network.

- Source and destination servers must belong to the same Active Directory domain or to different trusted domains.
- If the source or destination virtual machine VHD has a base disk, the base disk must be in a share that is accessible (registered) from the destination host. Generally, live migration doesn't move the base disk.
- Migration between clusters is only supported on hosts running in failover clusters. Cluster Shared Volume (CSV) storage must be enabled in the cluster.
- Live migration of a virtual machine doesn't migrate virtual machine storage, specifically meaning the location that stores the virtual machine images (VHD, ISO, VFD files). To handle storage requirements, you can use one of the following options:
    - Configure the virtual machine so that the storage files are available on a file share that is accessible by both the source and destination host of the migration.
    - Run a combined live virtual machine and storage migration (live VSM) in a single action.
    - Run a separate storage migration.
- If the source and destination hosts use shared storage, ensure the following:
    - All files that comprise a virtual machine, such as virtual hard disks, snapshots, and configuration, must be stored on an SMB share.
    - Permissions on the SMB share must be configured to grant access to the computer accounts of all servers that run Hyper-V.
- A storage migration moves virtual machine images (VHD, ISO, and VFD files), snapshot configurations, and data (saved state files).
- Storage migration is per virtual machine.
- Storage migration doesn't move base (parent) disks, except for snapshot disks.

Live Virtual machine and storage migration (Live VSM)

Live VSM migrates a VM and its machine storage in a single action.

- To use live VSM, the virtual machine LUN must be masked from the destination host.
- Live VSM is supported between two standalone hosts that run Hyper-V. The transfer can occur between local disks or SMB 3.0 file shares.

- Live VSM is supported between two host clusters that run Hyper-V. The virtual machine can be transferred to either a CSV or SMB 3.0 file share on the destination host cluster.

Next steps

- Migrate a virtual machine.
- Migrate storage.
- Run a live migration.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Migrate a virtual machine in the VMM fabric

Article • 08/30/2024

This article describes how to migrate a VM in System Center Virtual Machine Manager (VMM).

To perform a migration, you can do any of the following:

- **Run the Migrate VM Wizard**: Using this wizard, you can select a destination virtual machine host for the migration, specify the path that stores the virtual machine files, attach the virtual machine to any of the virtual networks that are found on the selected host, and, if a storage area network (SAN) transfer is available, select a network transfer instead.
- **Drag the virtual machine onto a host**: When you drag a virtual machine to a host, VMM uses automatic placement to place the virtual machine on the most suitable volume on the host. The placement is based on available space.
- **Drag the virtual machine onto a host group**: When you drag the virtual machine to a host group, VMM uses automatic placement to place the virtual machine on the most suitable host that is available in the host group, which is based on the virtual machine requirements and the host ratings. The virtual machine is placed on the most suitable volume on the host. The placement is based on available space. During automatic placement, the host rating process identifies the most suitable volume on each host.

Ensure the following before you begin the migration:

- If a correctly configured SAN is available, VMM automatically uses SAN to perform transfers. However, if you use the Migrate Virtual Machine Wizard to perform a transfer, you can override the SAN usage and perform a local area network (LAN) transfer.
- If you migrated a virtual machine that is connected to SAN storage, the virtual machine can't reconnect to the SAN unless the destination host also has access to that SAN. VMM can't detect if a virtual machine is connected to a SAN or if the destination host is connected to the same SAN, and therefore can't provide a warning. You must ensure that the new host is configured to enable the virtual machine to reconnect to the SAN before you migrate the virtual machine.
- To migrate VMs between the hosts with different processors, ensure that you make this exception in the VM **Properties** > **Processor** by selecting **Allow migration to a virtual machine host with a different processor version**. Else, the migration fails.

- If you change the permissions for a virtual machine through the file system and then migrate the virtual machine, VMM re-creates the access control list (ACL). All changes that were made outside VMM will be lost.
- If you attempt to migrate a virtual machine on a Hyper-V host soon after you've removed a checkpoint from the virtual machine, the migration might fail. If you attempt a migration before Hyper-V has finished deleting the checkpoint, the migration fails and you must repair the virtual machine using the **Undo** option. To avoid this issue, you can ensure that the checkpoint has been deleted, or you can wait for Hyper-V to delete it for you. Verify deletion as follows:

  1. In **Virtual Machines**, select the virtual machine > **Actions** > **Stop**.
  2. In Hyper-V Manage, **Status** > **Merge in progress** indicates that the checkpoint hasn't been deleted. Wait until this operation has finished before you migrate the virtual machine.

Migrate a virtual machine with the wizard

1. In the **Virtual Machines** view, browse to the host, select the VM, and in **Actions**, select **Migrate Virtual Machine**.

2. In **Select Host**, select the destination host. You can check the tabs for more details about the host.

   - **Details**: Indicates the status of the host, the operating system, and the type and status of virtualization software. Lists the virtual machines on the host.

   - **Rating Explanation**: Lists the factors that resulted in a zero star rating.

   - **SAN Explanation or Deployment and Transfer Explanation**: Lists the factors that make a SAN transfer unavailable. In addition, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy can't be used. Fast file copy is a feature in VMM that is based on the Windows Offloaded Data Transfers (ODX) feature. For information about ODX, see Windows Offloaded Data Transfers Overview.

   > ⓘ **Note**
   >
   > The Fast file copy feature isn't utilized when migrating a VM from Host to Library.

3. In **Select Path** page, accept the default path or select **Browse** and browse to the folder in which you want to store the configuration files for the virtual machine,

and select **OK**. Note the following:

- If the target host is a part of a failover cluster that has Cluster Shared Volumes (CSVs) enabled, you can store the virtual machine on a CSV Logical Units (LUs) and associated Number (LUN) that is already in use by other highly available virtual machines (HAVMs). With CSV, multiple HAVMs can share the same LUN. The migration of one HAVM doesn't affect others that are sharing the same LUN. VMM also supports multiple HAVMs per LUN for VMware environments that are configured with VMware VMFS LUNs.
- If you selected a path other than a default virtual machine path and want to store other virtual machines on that path, select the **Add this path to the list of host default paths** checkbox to add the path to the default paths on the host.
- If you use a network transfer, you have the option to specify separate storage locations for each virtual hard disk (.vhd or .vhdx) file for the virtual machine. By default, all .vhd or .vhdx files are stored in the same location that is specified for the virtual machine.
- If SAN transfers are enabled for this deployment, the virtual machine by default is transferred to the host over the SAN. If you don't want to perform a SAN transfer, select **Transfer over the network even if a SAN transfer is available**. If SAN transfers aren't available for this deployment, that option isn't available.

4. In **Select Networks**, modify the networks, and attach them to **None** or to any of the virtual networks that are found on the selected host. The networks area lists each of the virtual network adapters that are currently attached to the virtual machine. Network adapters default to **None** (if you selected **None** in the hardware configuration), or to the best matching virtual network according to the network matching rules.

5. In **Select Virtual SAN**, select the applicable virtual SANs from the dropdown list for each listed virtual HBA. Then select **Next**.

6. In **Summary**, review your settings. To start the VM after deployment, select **Start the virtual machine immediately after deploying it to the host**. Select **View Script** to view the Windows PowerShell cmdlets that perform the migration.

7. To start migration, select **Move**. Review progress in **Jobs**.

Migrate a VM with drag and drop

1. In **Virtual Machines**, browse to the virtual machine's current host in the navigation pane.
2. Select the VM, and, while you hold down the mouse button, drag the virtual machine to either the host of choice or to the host group of choice in the navigation pane.
3. When you release the mouse button, the system attempts to migrate the virtual machine using one of the following methods:

   - If you dragged the virtual machine to a host, the system evaluates the host's suitability for the virtual machine and attempts to migrate the virtual machine if the host is found suitable.
   - If you dragged the virtual machine to a host group, the system rates each host in the host group and attempts to migrate the virtual machine to the most suitable of those hosts. For the migration to succeed, a virtual machine path must be configured on the host for the recommended volume.

If you encounter difficulties using drag-and-drop, sign out of VMM, and then sign back in and try again. You can also try restarting the virtual machine, and then try again.

Next steps

- Migrate storage.
- Run a live migration.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Migrate storage in the VMM fabric

Article • 08/30/2024

This article describes how to migrate storage in the System Center Virtual Machine Manager (VMM) fabric.

Storage migration enables you to move VM files from one storage location to another on the same VM host. If the virtual machine is running, you can perform a quick storage migration, which results in little or no service outage for users of the virtual machine. If the virtual machine has more than one virtual hard disk, you can specify a separate location for each virtual hard disk (.vhd or .vhdx) file.

Read this article if you want to run a live migration of VM storage between two locations on a standalone host.

How to migrate storage

1. In **VM's and Services**, select **All Hosts**, and select the host on which the virtual machine is deployed.

2. Right-click the virtual machine > **Migrate Storage**.

   The Migrate Storage Wizard opens at the **Select Path** page. The current location of the VM configuration files is displayed in the **Storage location for VM configuration**, and the current location of each virtual hard disk (.vhd) is displayed in **Disks**.

3. On the **Select Path** page, do the following:
   a. In **Storage location for VM configuration**, select an existing default virtual machine path on the list. Browse to a location on the host. VMM automatically changes the paths for all virtual disks to the same path that you specified for the configuration files.
   b. Enter a path. When you enter a new path for the configuration files of the virtual machine, VMM doesn't automatically change the paths for the virtual disks until you right-click outside of the **Storage location for VM configuration** box.
   c. Select the **Add this path to the list of default storage locations on the host** checkbox if you selected a path other than an existing virtual machine path and you want to add the path to the default paths on the host.
   d. Specify the configuration file placement options, as follows:
      i. Select **Automatically place all VHDs with the configuration** to move all the virtual machine files to the same location.

ii. Select **Allow VHDs to be placed individually** to move one or more of the virtual machine files to a different location than the location of the configuration files. If you select this setting, in the **Disks** area, enter the new path in the **Location** box for each virtual hard disk, or select **Browse** to browse to the location where you want to store the file.

> ⓘ Note
>
> If the virtual machine is running and you change the path for any of the virtual hard drives, you must also specify a new path for the configuration files of the virtual machine, or the migration operation fails. You must enter the new path even if you want to leave the configuration files in their current location. In that case, you can create a new subfolder within the current location of the configuration files and then select that new location in the **Storage location for VM configuration** box.

4. On the **Summary** page, select **Move** to begin moving the virtual machine files. Review progress in **Jobs**.

Next steps

Run a live migration.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Run a live migration in the VMM fabric

Article • 08/30/2024

This article describes how to run a live migration of virtual machines (VMs) or VM storage in the System Center Virtual Machine Manager (VMM) fabric. VMM provides live migration support between standalone Hyper-V hosts or between cluster hosts that have live migration enabled. Learn more.

Migrate a VM between two standalone hosts

To migrate a virtual machine from one standalone Hyper-V host to another standalone Hyper-V host, the VM configuration files and virtual hard disk must be located on an SMB 3.0 file share.

1. In **VMs and Services** > **All Hosts**, select the standalone source host from which you want to migrate.
2. Select the host and in **VMs**, select the running VM that you want to migrate. Start the machine if it's not running.
3. In **Virtual Machine**, select **Migrate Virtual Machine** to start the Migrate Virtual Machine Wizard.
4. In **Select Host**, review the destination hosts and their associated transfer types. The **Live** transfer type appears if both hosts are configured to connect to the same SMB 3.0 file share.
5. Select the destination host where the transfer type is **Live** and select **Next**.
6. In **Summary**, select **Move**. To track the job status, open the **Jobs** workspace.
7. To verify that the virtual machine was migrated, check the **VMs** list on the destination host to ensure the VM is running.

Migrate a VM between clusters

You can migrate a VM between clusters using shared storage or with no shared infrastructure.

Select the required tab for steps for live migration with shared storage or with no shared infrastructure:

Live migration with shared storage

When you migrate a VM between clusters, note that the VM temporarily loses its high availability status. Therefore, a host failure during the migration causes the virtual machine to become unavailable. For live migration with shared storage, you must use SMB 3.0 file shares as the storage location. As the storage doesn't have to be migrated, the time in which high availability status can't be guaranteed is short.

1. In **VMs and Services** > **All Hosts**, select the cluster node from which you want to migrate.
2. In **VMs**, select the running VM that you want to migrate. Start the machine if it's not running.
3. In **Virtual Machine**, select **Migrate Virtual Machine** to start the Migrate Virtual Machine Wizard.
4. In **Select Host**, review the destination hosts and their associated transfer types. The **Live** transfer type is available for any destination cluster nodes that are configured to connect to the same SMB 3.0 file share on which the VM was originally created.
5. Select a node on a different cluster and select **Next**.
6. In **Summary**, select **Move**. To track the job status, open the **Jobs** workspace.
7. To verify that the virtual machine was migrated, check the **VMs** list on the destination node to ensure the VM is running.

> ⓘ **Note**
>
> When you run live migration on VMs from an older cluster version to a newer version, if the *Msvm_CompatibilityVector* value isn't updated, migration within the new cluster will be blocked.
>
> To fix this issue, restart the VM. VM restart updates the *Msvm_CompatibilityVector* values according to the new cluster version.

Migrate storage between two locations on a standalone host

> ⓘ **Note**
>
> You can't live migrate storage for a shared VHDX file. You can move the other VM files and perform normal live migration. To move the shared VHDX file to another location, you must shut down the VMs and then move the file.

You can run a live migration of VM storage between locations on standalone hosts. You can move the entire virtual machine, which includes virtual hard disks (VHDs) and configuration information, or move only specific VHDs to a different location.

1. In **VMs and Services** > **All Hosts**, select the standalone host where the VM is located.
2. In **VMs**, select the running VM for which you want to migrate storage. Start the machine if it's not running.
3. In **Virtual Machine**, select **Migrate Storage** to start the Migrate Virtual Machine Wizard.
4. In **Select Path** > **Storage location**, select one of the default storage locations on the host. Or select **Browse** to view all possible storage destinations. Select the destination SMB 3.0 file share or location on the local hard disk and select **OK**.

   If you specify an SMB 3.0 file share in the **Storage location** list, ensure that you use the fully qualified domain name (FQDN) of the destination server in the share path. For example, instead of \\fileserver1\smbshare, use \\fileserver1.contoso.com\smbshare.
5. Optionally, select **Add this path to the list of default storage locations on the host**, and select **Next**.
6. On the **Summary** page, select **Move**. Track the progress in **Jobs**.

Run live migrations concurrently

You can run live migration on multiple VMs so that two migrations occur at the same time on the same host. Note that:

- You can't select multiple VMs for a live migration. You need to manually start each migration.
- You can specify how many concurrent migrations to run. The default setting is two, which is the number of simultaneous live migrations and storage migrations that are enabled in Hyper-V. For example, a host can participate in one outgoing live migration plus one incoming, two outgoing live migrations, or two incoming live migrations.
- Live migrations and live storage migrations are independent. You can perform two live migrations and two live storage migrations simultaneously. VMM considers live virtual machine and storage migration (live VSM) as one live migration and one storage migration.
- You can view concurrent migrations in progress in Hyper-V Manager > **Actions** > **Hyper-V Settings** > **Server** > **Live Migrations** and **Storage Migrations**. In **Jobs**,

verify that the migrations occur simultaneously.

Improve live migration speed

On Hyper-V hosts, you can increase live migration speed using compression using SMB as the transport or both. The compression method uses algorithms that reduce the data that is transmitted over the wire. The SMB method can allow for faster data transfer.

By default, faster live migration is enabled to use the compression method. You can disable, enable, or change the method of faster live migration by changing the live storage migration settings, either at the Hyper-V host level or for each live migration instance.

Change live migration settings as follows:

1. In Hyper-V Manager, select **Actions** > **Hyper-V Settings** > **Server** > **Live Migration**, and select **Advanced Features**.

2. In **Migration settings** > **Live migration settings**, do one of the following:

   - To disable faster live migration, select **Standard live migration**.
   - To use compression for faster live migration, select **Use compression**.
   - To use SMB for faster live migration, select **Use SMB as Transport**.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage roles and permissions in VMM

Article • 09/02/2024

System Center Virtual Machine Manager (VMM) allows you to manage roles and permissions. VMM provides:

- **Role-based security**: Roles specify what users can do in the VMM environment. Roles consist of a profile that defines a set of available operations for the role, scope which defines the set of objects on which the role can operate, and a membership list that defines the Active Directory user accounts and security groups that are assigned to the role.
- **Run As accounts**: Run As accounts act as containers for stored credentials that you use to run VMM tasks and processes.

Role based security

The following table summarizes VMM user roles.

Expand table

VMM user role	Permissions	Details
Administrator role	Members of this role can perform all administrative actions on all objects that VMM manages.	Only administrators can add a WSUS server to VMM to enable updates of the VMM fabric through VMM.
Virtual machine administrator	Administrators can create the role.	Delegated administrator can create VM administrator role that includes entire scope or a subset of their scope, library servers, and Run-As accounts.
Fabric administrator (delegated administrator)	Members of this role can perform all administrative tasks within their assigned host groups, clouds, and library servers.	Delegated administrators can't modify VMM settings, add or remove members of the administrators user role, or add WSUS servers.
Read-Only administrator	Members of this role can view properties, status, and job status of objects within their assigned host groups, clouds, and library servers, but they can't modify the objects.	The read-only administrator can also view Run As accounts that administrators or delegated administrators have specified for that read-only administrator user role.

VMM user role	Permissions	Details
Tenant administrator	Members of this role can manage self-service users and VM networks.	Tenant administrators can create, deploy, and manage their own virtual machines and services using the VMM console or a web portal. Tenant administrators can also specify which tasks the self-service users can perform on their virtual machines and services. Tenant administrators can place quotas on computing resources and virtual machines.
Application administrator (Self-Service User)	Members of this role can create, deploy, and manage their own virtual machines and services.	They can manage VMM using the VMM console.

Run As accounts

There are different types of Run As accounts:

- **Host computer accounts** are used to interact with virtualization servers.
- **BMC accounts** are used to communicate with the BMC on hosts for out-of-band management or power optimization.
- **External accounts** are used to communicate with external apps such as Operations Manager.
- **Network device accounts** are used to connect with network load balancers.
- **Profile accounts** are used in Run As profiles when you're deploying a VMM service or creating profiles.

ⓘ Note

- VMM uses the Windows Data Protection API (DPAPI) to provide operating system level data protection services during storage and retrieval of the Run As account credentials. DPAPI is a password-based data protection service that uses cryptographic routines (the strong Triple-DES algorithm, with strong keys) to offset the risk posed by password-based data protection. Learn more.
- When you install VMM, you can configure VMM to use Distributed Key Management to store encryption keys in the Active Directory.

- You can set up Run As accounts before you start managing VMM, or you can set up Run As accounts if you need them for specific actions.

Next steps

- Set up user roles.
- Set up run as accounts.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Set up user roles in VMM

Article • 09/02/2024

This article describes how to set up System Center Virtual Machine Manager (VMM) user roles.

Before you start

- Learn more about user roles.
- Ensure you've the right permissions to create the role or to add users to it.
  - **Administrator role**: Administrators can add and remove users.
  - **Delegate Administrator role**: Administrators can create the role. Delegated administrators can create delegated administrator roles that include a subset of their scope, library servers, and Run As accounts.
  - **Read-only Administrator role**: Administrators can create the role. Delegated administrators can create Read-only Administrator roles that include a subset of their scope, library servers, and Run As accounts.
- **Virtual Machine Administrator role**: Administrators can create the role. Delegated administrator can create VM administrator role that includes entire scope or a subset of their scope, library servers, and Run As accounts.
- **Tenant Administrator role**: Administrators and Delegated administrators can create this role.
- The Administrator role is created by default when you install VMM. The user who performs the installation and all domain users in the local Administrators group on the server are added to the Administrator role. You can add or remove members in the role properties.

Create a role

1. Select **Settings** > **Create** > **Create User Role**.
2. In the **Create User Role Wizard**, enter a name and optional description for the role, and select **Next**.
3. In **Profile** page, select the role, and select **Next**.

4. In **Members**, select **Add** to add user accounts and Active Directory groups to the user role. Add the members in **Select Users, Computers, or Groups**, and select **Next**.

5. In **Scope**, select the private clouds or host groups that the members of the role can use. Select **Next**.

6. If one or more **Quotas** pages appear (based on whether you selected private clouds on the previous wizard page), review and specify quotas as needed for each private cloud. Otherwise, skip to the next step. Read-only Administrators can only view items in this defined scope.

   To set quotas for the combined use of all members of this user role, use the upper list. To set quotas for each individual member of this user role, use the lower list. By default, quotas are unlimited. To create a limit, clear the appropriate checkbox under **Use Maximum** and then, under **Assigned Quota**, select a limit. When you've completed all settings, select **Next**.

7. If the **Library servers** page appears, add one or more library servers.

8. In **Networking**, select **Add** to add the VM networks that the members of this role can use. Select **Next**.

9. In **Resources**, select **Add** to add resources. In **Specify user role data path**, select **Browse** to specify a library path that members of this user role can use to upload data. Select **Next**.

10. In **Permissions** page, select global actions, and any cloud-specific actions that you want to allow members of this role to perform. Select **Next**.

11. If the **Run As accounts** page appears, add Run As accounts that you want the members of this role to be able to use. Otherwise, skip to the next step.

12. If the **Quotas for VM networks** page appears, review and specify quotas to limit the number of VM networks that members of this user role can create. Otherwise, skip to the next step.

    To limit the combined number of VM networks that can be created by all members of this user role, use the upper setting. To limit the number of VM networks that can be created by each individual member of this user role, use the lower setting.

13. In **Summary** page, review the settings, and select **Finish** to create the role. Verify the role appears in **Settings** > **Security** > **User Roles**.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Create Run As accounts in VMM

Article • 09/02/2024

This article describes how to create and manage Run As accounts in System Center - Virtual Machine Manager (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. Learn more about different types of Run As accounts.

To create a Run As account, follow these steps:

1. Select **Settings**, and in **Create**, select **Create Run As Account**.
2. In **Create Run As Account**, specify name and optional description to identify the credentials in VMM.
3. In **User name** and **Password**, specify the credentials. The credentials can be a valid Active Directory user or group account or local credentials.
4. Clear **Validate domain credentials** if you don't need them and select **OK** to create the Run As account.

Next steps

Set up self-service in VMM.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Set up self-service in VMM

Article • 09/02/2024

This article describes how to set up self-service in System Center - Virtual Machine Manager (VMM).

VMM offers many options for self-service users:

- **Virtual machines/Services**: Users can deploy their virtual machines and services to private clouds. A private cloud can be assigned to multiple self-service user roles. Role-level quotas for each self-service user role with the private cloud in scope are used to allocate cloud compute and storage capacity. Member-level quotas set individual limits for members of the self-service user role.
- **Virtual hard disks**: Users can deploy VMs from VHDs and templates.
- **Templates/Profiles**: Users can create their own templates and profiles. The **Author** action for a self-service user role providing these authoring rights to create hardware profiles, guest operating system profiles, app profiles, SQL Server profiles, VM templates, and service templates.

> ⓘ **Note**
>
> These resources can be created by a user with the self-service role and shared with other members of the self-service user role.

Self-service users use the VMM console (or PowerShell) to create and manage VMs, services, and so on. In the VMM console, self-service users can view status, resource usage, jobs, and PRO tips (if enabled) for their own VMs and services. They can view available capacity and quota usage in their private clouds. They can't see host groups, hosts, library servers and shares, or network and storage configuration settings.

You set up self-service in VMM as follows:

1. Create a self-service user role. Specify actions that the role can perform, assign resources to the role, and configure Run As accounts that self-service users can use when interacting with VMM.
2. Set up the VMM library. Assign a library share on which resources available to self-service users will reside. In addition, set up a share so that self-service users can share their resources with other users.

Set up a self-service user role

1. Select **Settings** > **Create** > **Create User Role**.

2. In the **Create User Role Wizard**, enter a name and optional description for the role, and select **Next**.

3. In **Profile** page, select **Self-Service User**, and select **Next**.

4. In **Members**, select **Add** to add user accounts and Active Directory groups to the role. Select **Next**.

5. In **Scope**, select at least one private cloud that members of the role will use. Select **Next**.

6. In **Quotas**, set a quota for each private cloud. Each quota sets an individual limit for each member of the user role. If you want all role members to share overall quotas, create a security group in Active Directory, and assign that group to the user role. Supported quota types include:

   - **Virtual CPUs**: Limits the total number of VM CPUs that can be consumed from the private cloud.
   - **Memory (MB)**: Limits the amount of VM memory that can be consumed from the private cloud.
   - **Storage (GB)**: Limits the amount of VM storage that can be consumed from the private cloud.
   - **Quota (points)**: Sets a quota on VMs deployed on the private cloud based on total quota points assigned to the VMs via their VM templates.
   - **Virtual machines**: Limits the total number of VMs that can be deployed on a private cloud.

7. In **Resources**, select **Add** to add resources that the role can use. You can assign hardware profiles, OS profiles, VM templates, app profiles, SQL Server profiles, and service templates that can be used when creating VMs and services.

8. In **Specify user role data path**, select **Browse** to specify a library path that members of this user role can use to upload and share their own data. Then select **Next**.

9. In **Actions**, select the actions that users are allowed to perform.

   - **Author**: Users can author templates and profiles, including hardware profiles, operating system profiles, application profiles, SQL Server profiles, virtual machine templates, and service templates.
   - **Checkpoint**: Users can create, edit, and delete checkpoints for their own VMs, and to restore a VM to a previous checkpoint. VMM doesn't support

checkpoint actions on services.

- **Checkpoint (Restore only)**: Users can restore their own VMs to a checkpoint but can't create, edit, and delete checkpoints.
- **Deploy**: Users can deploy virtual machines and services from templates and virtual hard disks that are assigned to their role. They can't author templates and profiles.
- **Deploy (from template only)**: Users can deploy VMs and services from templates only. They don't have authoring rights.
- **Local Administrator**: Users can be Local Admins on their own VMs. You must enable **Local Administrator** on any user role that has the **Deploy (From template)** enabled so that those users can set the Local Admin password during VM and service deployment. Users with the Deploy action don't need this to set credentials.
- **Pause and resume**: Users can pause and resume their own VMs and services.
- **Receive**: Users can use resources that are shared by members of other self-service user roles.
- **Remote connection**: Users can connect to their VMs from the VMM console or App Controller.
- **Remove/Save**: Users can remove or save their VMs.
- **Share**: Users can share resources that they own with other self-service user roles. Sharable resources include hardware profiles, operating system profiles, application profiles, SQL Server profiles, virtual machine templates, virtual machines, service templates, and services. A self-service user must be the owner of a resource to share it. For a user role to use the resources, it must have the **Receive** action.
- **Start/Stop**: Users can start and stop their own VMs and services.
- **Store and redeploy**: Users can store their own virtual machines in the VMM library and redeploy those virtual machines. Virtual machines stored in the library don't count against a user's virtual machine quota. VMM doesn't support storing services.

10. If the **Run As accounts** page appears, add Run As accounts that you want the members of this role to be able to use in the actions to create VMs and services. Then select **Next**.

11. In the **Summary** page, review the settings, and select **Finish** to create the role. Verify the role appears in **Settings** > **Security** > **User Roles**.

After you create the role, you can modify its settings on the properties page.

Prepare the VMM library for self-service

Self-service users with the required permissions can access the VMM library. Users with the Author action can create templates and profiles in the library. They can also share those templates and profiles with other self-service users. For self-service users to interact with the library, you need to prepare the following:

- **Read-only library shares**: To share physical resources, such as VHDs and ISO images with self-service users, you set up read-only library shares for private clouds, and add the resources to the path. The resources are then available for self-service users that have the private cloud in their scope. You can also store resources such as Application Frameworks on these shares to enable self-service users to configure templates and profiles with scripts.
- **Self-service user data paths**: Set up user data paths on self-service roles to provide a place where members of the role can upload and share their own resources. For example, a path might store app packages for services deployed by a self-service user role. Read and write permissions for the path are controlled through the file system. VMM discovers all paths that the current self-service user can access. These data paths must be on a library share.

Before you start

All these procedures must be performed by a VMM administrator. Delegated administrators can add library shares on library servers that are in the scope of their user role, can configure read-only library shares on private clouds that they created, and can configure user data paths on self-service user roles that they created. Only members of the local Administrators group can grant access permissions on their user data paths.

Create read-only library shares

1. Create a shared folder to store resources. The folder will include read-only library shares for private clouds, and user data paths for self-service user roles. We recommend that you create the folder near your default library share so that it's easy to access when you're managing the library. For example, C:\ApplicationData\Virtual Machine Manager Cloud Resources.
2. In the shared folder, create a folder to store the \ApplicationFrameworks resources in case you want to use them. For example, C:\ApplicationData\Virtual Machine Manager Cloud Resources\ApplicationFrameworks. Share the folder so that you can add it as a library share.

   > ⓘ Note

> The shared folder can't be in the default library share path. You can't add a library share that's in the path of an existing library share.

3. Copy the \ApplicationFrameworks folder from the default library share to the share you created for private cloud resources.
4. Add the share to the VMM library. In **Library** > **Library Server** > **Add Library Share**, select each shared folder you want to add to the library. Verify that the share is added in **Library Servers**.
5. To add the read-only share to a private cloud, open VMs and **Services** > **clouds**, and select the private cloud you want to update.
6. In the cloud, select **Folder** > **Properties** > **Library** > **Read-only library shares** > **Add**.

Enable self-service users to share resources

To enable self-service users with the Author action to share resources they create, you need to create a folder to store shared resources, and then enable resource sharing for the self-service user role.

Create a folder to share user resources

Configure a user data path for the self-service user role, and grant read/write permission on the folder.

1. Create a folder to store all resources that will be shared by self-service users. For example, C:\ProgramData\Virtual Machine Manager Cloud Resources\Self-Service User Data.

2. Within that folder, create a subfolder to store resources for the self-service user role. For example, C:\ProgramData\Virtual Machine Manager Cloud Resources\Self-Service User Data\Finance Service Managers.

3. Within that subfolder, create a third-level subfolder to store all the application packages for all releases of the virtual application that you'll use in this scenario. For example, C:\ProgramData\Virtual Machine Manager Cloud Resources\Self-Service User Data\Finance Service Managers<MyApplication>.

4. In that subfolder, create a fourth-level subfolder to store the application package for the first release of the service. For example, C:\ProgramData\Virtual Machine Manager Cloud Resources\Self-Service User Data\Finance Service Managers<MyApplication>\MyApplication v1>.

Each time you update and resequence an application using Server App-V, you'll need to store the new application package in a separate folder.

5. To enable members of the self-service user role to access the resources and upload their own resources to the folder, grant all members read/write permission on the folder.

6. If needed, share the folder that contains user data for all self-service user roles, and add the share to the VMM library. To be assigned to a self-service user role, a user data path must be on a library share.

7. Configure the path for a self-service user role as follows:
   a. In **Settings** > **Security** > **User Roles**, select the self-service user role.
   b. In the **User Role** group, select **Properties** > **Resource**.
   c. Browse and select the folder that will hold the shared resources. After you save the changes, the data path is added to the library. Verify the path in **Library** > **Self-Service User Content**.

Enable sharing for self-service users

To share a resource with a member of another self-service user role, you need the following:

- The self-service user who shares the resource must be the owner of the resource.
- The resource owner must belong to a self-service user role that has been assigned the Share action.
- The resource receiver must belong to a self-service user role that has been assigned the Receive action.

Enable resource sharing as follows:

1. Select **Settings** > **Security** > **User Roles**, and select the self-service user role for which you want to enable resource sharing.
2. In the **User Role** group, select **Properties**.
3. In **Actions**, select **Share**, and select **OK**. Members of this self-service user role can now share their own resources with members of any self-service user role that has the **Receive** action assigned to it.
4. To configure a user role with the **Receive** action, select the role > **Properties** > **Action**, and select **Receive**.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback ↗ | Get help at Microsoft Q&A

Work with VMM as a self-service user

Article • 09/02/2024

This article describes how to work with System Center Virtual Machine Manager (VMM) as a self-service user.

Self-service users can interact with VMM to deploy virtual machines and services to private clouds. Depending on your permissions, you can deploy VMs from VHDs and templates, and create and share your own templates and profiles. You interact with VMM using the VMM console (or PowerShell).

> ⓘ **Note**
>
> When the default language configured in the guest VM and the console differs, you may not be able to seamlessly copy text from the VMM console into the guest VM. This will primarily impact the login functionality when you are copying password from the VMM console and then pasting it in the Password textbox while logging into guest VM. You can circumvent this by changing the language using the keyboard language icon in the VM login page.

Create and deploy virtual machines

- Learn about creating a VM from an existing VHD.
- Learn about creating a VM from a blank VHD.
- Learn about cloning an existing VM.
- Learn about deploying VMs from VM templates.
- Learn about deploying VMs running Linux.

Create resources in the VMM library

The VMM library is a file share that includes a catalog of resources that are used to deploy virtual machines and services in the VMM fabric. The library stores:

- File-based resources such as virtual hard disks, ISO images, scripts, driver files, and application packages (SQL Server data-tier applications and Web Deploy).
- Non-file-based resources such as virtual machine templates and service templates that are used to create VMs and services.
- Offline virtual machines are stored in the library.

If you have Author permissions, you can create templates and profiles in the library. Learn more.

Share library resources

As a self-service user, you can share your library resources with the other members of your self-service user role when the following conditions are met:

- You must be the resource owner.
- You must belong to self-service user role that is assigned the Share action.
- To use the shared resource, the user must belong to a self-service user role that has been assigned the **Receive** action.

Share resources as follows:

1. Select **Library**, right-click the template or physical resource that you want to share > **Properties**.
2. In **Access** > **Users**, select **Add**.
3. In **Select Users**, in **User**, share the resource with another member of your role. In **User Role**, share the resource with other self-service user roles.

Import library resources

We recommend you to use the method described in this procedure to import and export file-based resources to and from the VMM library. Note the following:

- You can import resource to the user role data path in the Self Service User Content node in the library.
- You can export resources from your user role data path or private cloud library.
- To import and export, your self-service user role needs Author permissions.

Import resources as follows:

1. Select **Library** > **Import** > **Import Physical Resource**.

2. Select **Add custom resource** to import a folder with the .CR extension and its contents. Alternatively, you can select a folder without a .CR extension that contains one or more files of a supported file type.

   - If you select a folder without a .CR extension, only the files of a supported file type appear in the VMM library.
   - However, if you use Windows Explorer to access the library share, you can access all the files in the folder depending on the file and share permissions

that are configured outside VMM.
- If the folder with .CR extension contains more than 100 files to be imported, it's recommended that you zip the files before the import. This improves performance.

3. Select **Add resource** to import one or more files to another library location.

4. When you're finished, select **Import**. Check that the resources are listed under **Self Service User Content** > user role data path > **Self Service User Objects**.

Export library resources

1. Select **Library** > **Export** > **Export Physical Resource**.
2. Select **Add**, select the physical resources you want to export, and select **OK**.
3. In **Specify a destination for the export files**, select **Browse**, and select a destination folder. Then select **OK**.
4. When you're finished, select **Export**.

Next steps

Provision VMs.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Monitor VMM

Article • 09/02/2024

You configure monitoring and reporting in System Center Virtual Machine Manager (VMM) as follows:

- **VMM jobs**: In the VMM console, you can monitor the status of processes and operations with VMM jobs.
- **Monitoring in Operations Manager**: To monitor the health and status of VMM servers and the VMM fabric, you integrate VMM with System Center Operations Manager.
- **Reporting in Operations Manager**: After VMM is integrated with Operations Manager, you can create and view VMM reports.

Monitor with VMM jobs

A VMM job is created for any action that changes the status of a managed object.

- Jobs are composed of steps that are performed sequentially to complete an action. Simple jobs, such as stopping a virtual machine, contain only one step. More complex jobs, or running a wizard, can contain multiple jobs or job groups.
- Jobs are tracked in the **Jobs** view in the VMM console. The **Details** tab in the **Jobs** view shows the status of each step in a job.
- Each job is represented by one or more VMM PowerShell cmdlets. You can perform almost any VMM task with PowerShell. Each wizard includes a **View Script** button on the **Summary** page that displays the cmdlets that will perform the job that you just requested. You can save Windows PowerShell scripts to the VMM library, and view and run them in **Library** view.
- Each VMM job is independent and doesn't depend on the status of another job. For example, if you're running jobs to add multiple host servers, the failure to add one host doesn't affect the remaining jobs. When a job completes, an audit record is saved that lists the changes that the job made to the VMM object. You can view the audit record in **Jobs** > **Details** > **Change Tracking**.
- Jobs are started automatically when you perform tasks in the VMM console or using PowerShell. You can cancel some running jobs, but others, including adding hosts and system jobs, can't be canceled after they've started running.
- You can generally restart failed jobs, but note that:
  - If multiple jobs place a VM into a failed state, only the most recent job can be restarted.

- For jobs that run for a long time, such as virtual machine migration, intermediate results are stored periodically while the job is running, and the Restart action attempts to resume the job from the last known state. All other jobs start from the beginning.

Monitor with Operations Manager

You can monitor VMM health and status in Operations Manager by installing the VMM management pack, which provides many dashboards in the Operations Manager console.

Expand table

Dashboard	Details
Virtual Machine Dashboard	Monitors the health of virtual machines. It displays information about discovered VMs in the VMM fabric. You can view alerts, properties, host, and performance information for the VM.
VMM Host Dashboard	Monitors the health of virtualization hosts discovered in the VMM fabric. It displays information about the host properties, status, VMs, alerts, and performance.
Fabric Health Dashboard	Monitors the health of VMM private clouds. For each cloud, the dashboard monitors the state of host groups, the compute properties of the cloud (CPU, network adapters, and so on), and storage information such as pools, file share, LUNs, and network monitoring. A fabric monitoring dashboard diagram view shows the status for each piece of the fabric. The dashboard can be scoped to physical or virtual resources or to a particular cloud tenant.

Learn more about integrating VMM with Operations Manager.

Report with Operations Manager

After you've connected VMM to Operations Manager, you can view and create reports. VMM provides these default reports:

⛶ Expand table

Report	Details
Capacity Utilization	Details usage for VM hosts and other objects. Provides an overview of how capacity is being used in your datacenter and helps you make resources decisions for supporting your VMs.
Host Group Forecasting	Predicts host activity based on history of disk space, memory, disk IO, network IO, and CPU usage. To use the forecasting reports, SQL Server Analysis Services must be installed on the Operations Manager Reporting server.
Host Utilization	Shows the number of virtual machines that are running on each host and average usage, along with the total or maximum values for host processors, memory, and disk space.
Host Utilization Growth	Shows the percentage change in resource usage and the number of virtual machines that are running on selected hosts during a specified time period.
Power Savings	Shows how much power is saved through power optimization. You can view the total hours of processor power saved for a date range and host group, and the detailed information for each host in a host group.
SAN Usage Forecasting	Predicts SAN usage based on history.
Virtual Machine Allocation	Provides information about allocation of virtual machines.
Virtual Machine Utilization	Provides information about resource utilization by virtual machines, including average usage and total or maximum values for virtual machine processors, memory, and disk space.
Virtualization Candidates	Helps identify physical computers that are good candidates for conversion to virtual machines. You can use this report to identify little-used servers and display average values for a set of commonly requested performance counters for CPU, memory, and disk usage, along with hardware configurations, including processor speed, number of processors, and total RAM. You can limit the report to computers that meet specified CPU and RAM requirements, and you can sort the results by selected columns in the report.

View reports

You can view reports in the Reporting workspace in System Center Operations Manager, or by using a web browser and entering this address: `http://ReportingServerName:port/reports`. You can optionally specify **https** instead of http.

- `ReportingServerName` is the name of the Operations Manager reporting server.
- `port` is 80 for HTTP and 443 for HTTPS
- `reports` is the reporting server virtual directory, by default: **reports**

Integrate VMM with Operations Manager for monitoring and reporting

Article • 09/02/2024

This article describes how to integrate System Center Virtual Machine Manager (VMM) with System Center Operations Manager to monitor the health of virtualization hosts, virtual machines, and other resources in the VMM compute fabric.

- Operations Manager monitors the VMM server and all the hosts and virtual machines in the VMM fabric.
- An Operations Manager management group can monitor multiple VMM instances. The VMM fabric can only be monitored by a single Operations Manager management group.
- The Fabric Health Dashboard is imported to Operations Manager with the VMM management packs. It shows a detailed overview of the health of the VMM fabric and private clouds. You can link to other dashboards to drill into network and storage monitoring.

Deployment summary

You set up Operations Manager with VMM as follows:

1. Ensure the prerequisites are met.

2. Install the Operations Manager console on the VMM server so that you can monitor VMM from the server.

3. Install Operations Manager agents on the VMM management server and all hosts under management by VMM.

4. Locate the latest management pack.

5. Run the integration wizard to integrate VMM and Operations Manager. The wizard does the following:

   - Imports the VMM management packs into the Operations Manager.
   - Optionally enables Performance and Resource Optimization (PRO). PRO information is provided by the Operations Manager, and can be mapped to VMM to optimize performance. You can map specific Operations Manager alerts to remedial actions in VMM. For example, you could migrate VMs to a different host after a hardware issue. In addition, with PRO enabled,

Operations Manager can detect resource issues or hardware failures in the virtualization infrastructure.

- Optionally enables maintenance mode. VMM can place hosts in maintenance mode for servicing. When a host is in maintenance mode, VMM uses live migration to move VMs to another location and doesn't place new VMs on the host. If the maintenance mode is enabled for Operations Manager monitoring, when a host is placed into maintenance mode in VMM, Operations Manager also places it in the same mode. In the maintenance mode, the Operations Manager agent suppresses alerts, notifications, and state changes, so that the host isn't monitored while regular hardware and software maintenance activities are in progress.
- Enables support for SQL Server Analysis Services (SSAS) and the reporting capabilities provided by SSAS.

Before you start

> ⓘ **Note**
>
> Ensure that you're using a supported version of Operations Manager (running on System Center 2022).

- Operations Manager must use SQL Server 2016, SQL Server 2017, SQL Server 2019, or SQL Server 2022 with reporting services enabled. To use the forecasting reports, SQL Server Analysis Services must be installed on the Operations Manager reporting server. The SSAS instance name must match the SQL Server Reporting Services (MSSQLSERVER).

- The version of the Operations Manager operations console that is installed on the VMM management server must match the version of Operations Manager with which you intend to integrate. The Operations Manager agent version agent must be supported by the Operations Manager version.
- Ensure that the version of Windows PowerShell that's on all Operations Manager management servers is the most recent version supported by that version of Operations Manager. To determine which version of Windows PowerShell is on a server, run **Get-Host | Select-Object Version**
- Ensure that port 5724 is open between the VMM and Operations Manager servers.
- You need VMM admin permissions to run the integration wizard.
- VMM monitoring packs support up to 400 hosts, with up to 8000 virtual machines.

Install the Operations Manager console

1. Run Operations Manager Setup on each VMM management server.
2. In the wizard, select the **Operations** Console to install it.

Install the Operations Manager agent

1. Install the Operations Manager agent on each VMM server, and on each host managed in the VMM fabric.
2. You can install the agent from the Operations Manager Operations console, from Operations Manager setup, or from the command line. To understand the different methods for agent deployment, review the Managing discovery and agents section in Operations Manager documentation.

Locate the management packs

- The latest versions of management packs are coupled with every new release of VMM build.

- To locate the management packs, open the management packs folder on the VMM server. The default location is: `C:\Program Files\Microsoft System Center\Virtual Machine Manager\ManagementPacks`.

Run the integration wizard

Run the wizard to connect the VMM server to the Operations Manager server and import the VMM management pack to Operations Manager.

1. In the VMM console, select **Settings** > **System Center Settings** > **Operations Manager Server** > **Properties**.

   > ⓘ **Note**
   >
   > If the Operations Manager connection has already been established, selecting **Properties** opens the **Operation Manager Settings** dialog. If this dialog appears and doesn't describe the correct connection, remove the current connection before you enter the correct information.

2. In **Introduction**, select **Next**.

3. In **Connection to Operations Manager**, specify the Operations Manager server name, and select an account to use to connect to it. You can use the VMM server service account or specify a Run As account. This account must be a member of the Operations Manager Administrator role.

4. Select **Enable Performance and Resource Optimization (PRO)** if necessary.

5. Select **Enable maintenance mode integration with Operations Manager**, if desired. Select **Next**.

   When hosts are placed in maintenance mode using the VMM management server, Operations Manager places them in the maintenance mode as well. In this mode, the Operations Manager agent suppresses alerts, notifications, rules, monitors, automatic responses, state changes, and new alerts.

6. Enter credentials for Operations Manager to connect with the VMM management server and select **Next**. This account will be added to the Administrator user role in VMM.

7. Review the information in the **Summary** page and select **Finish**. You can view the status of the new connection in the **Jobs** workspace.

8. With **System Center Settings** still selected, in the results pane, right-click **Operations Manager Server**, and select **Properties**. In **Operation Manager Settings** > **Details** > **Connection Status**, confirm that the connection is **OK**.

If you later remove a connection to an Operations Manager server, this doesn't remove the VMM management packs from the server, but the connector is removed.

Monitor VMM in the Operations Manager console

You can monitor VMM processes and state in any of the VMM dashboards that appear in the Operations Manager console - the fabric dashboard, VM dashboard, or VMM host dashboard.

1. In the Operations console for Operations Manager, select **Monitoring**.
2. To monitor VMs, select **Virtual Machine Manager**. This dashboard includes health and performance information for virtual machines, hosts, and VMM servers.
3. To monitor VMM hosts, select **VMM Host Dashboard**. You can monitor the health of virtualization hosts discovered in the VMM fabric, and get information about the host properties, status, VMs, alerts, and performance.

4. To monitor a private cloud, select **Fabric Health Dashboard**. For each cloud, the dashboard monitors the state of host groups, the compute properties of the cloud (CPU, network adapters, and so on), and storage information such as pools, file share, LUNs, and network monitoring. You can scope the dashboard to physical or virtual resources or to a particular cloud tenant.
5. In **Virtual Machine Manager Views**, you can view graphic representations of managed systems. After you connect the VMM and Operation Manager servers for the first time, it can take several hours until the diagrams are available in the console.

Next steps

- Run VMM reports in Operations Manager.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Add an Azure subscription in VMM

Article • 09/03/2024

You can add Microsoft Azure subscriptions to System Center Virtual Machine Manager (VMM) by creating an Azure profile.

Using Azure profile, you can define the intended usage of the profile. Currently, Azure-VMM integration scenario supports the following:

- **Azure VM Management**: Perform basic actions on Azure VM instances without leaving the VMM console.
- **Azure Update Management**: Install the update on the VMs managed by VMM.

Before you start

Here's what you need to add an Azure profile for Azure VM management:

Expand table

Requirement	Details
Azure subscription	You need at least one Azure subscription to add it to the VMM console.
Internet connectivity	The computer on which you install the feature must be able to connect to the Azure subscription.
AD Authentication	To enable management of both Classic and Azure Resource Manager based VMs, the subscription must have Active Directory-based authentication associated with it. Create a Microsoft Entra ID application using Azure portal and make a note of the Directory ID, Application ID, and Key. Assign application to Classic VM contributor and VM contributor roles using *Subscription – Access Control (IAM) – Add*.

Here's what you need to create an Azure profile for Azure Update Management:

Expand table

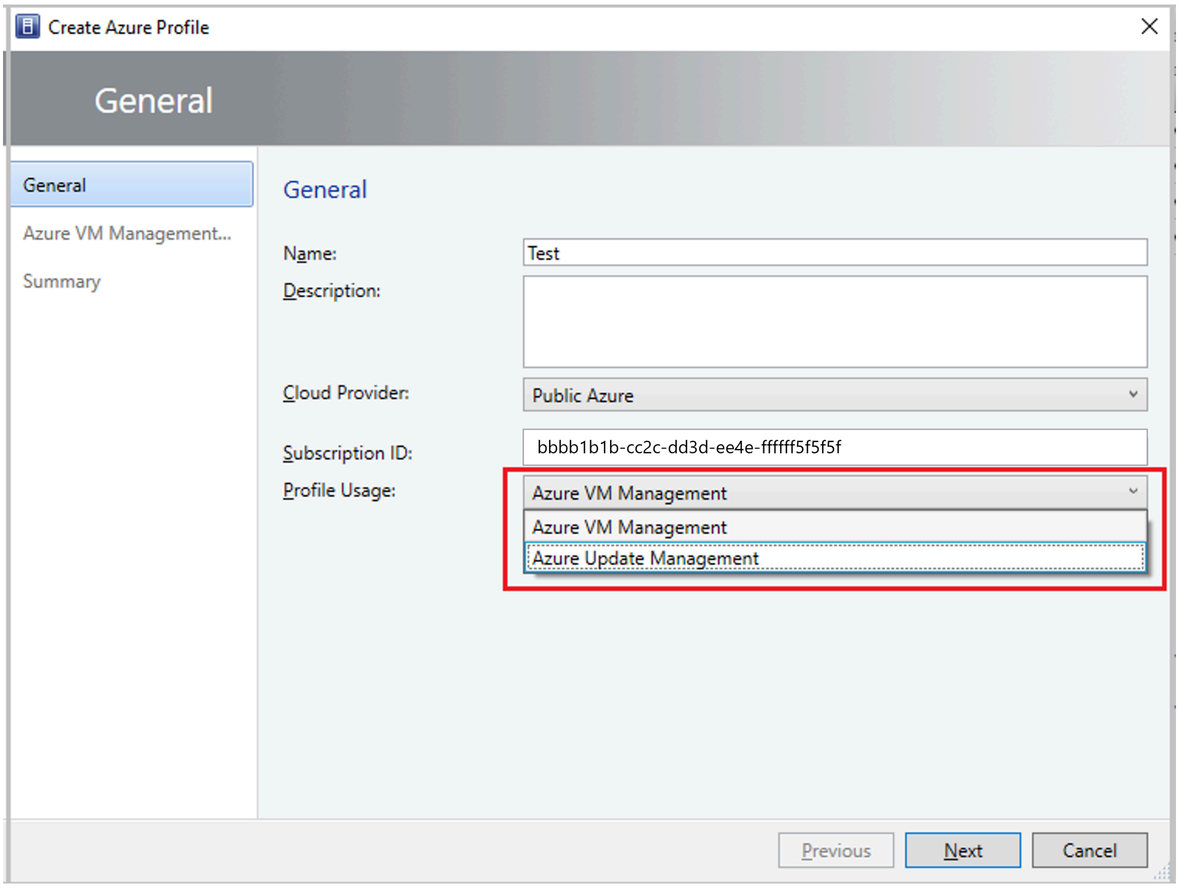
Requirement	Details
Azure subscription	You need Azure Automation Subscription with **Update Management** solution enabled.

Requirement	Details
	Create Automation Account and Enable Update Management Solution.
Internet connectivity	The computer on which you install the feature must be able to connect to the Azure subscription.

Create Azure Profile

Follow these steps:

1. In the VMM console, go to **Library** > **Create** > **Azure Profile**.


Create Azure Profile

General

General

Name: Test

Description:

Cloud Provider: Public Azure

Subscription ID: bbbb1b1b-cc2c-dd3d-ee4e-ffffff5f5f5f

Profile Usage: Azure VM Management

2. Under **Profile Usage** dropdown menu, select **Azure VM Management** or **Azure Update Management**. Based on the selection, the next page seeks authentication information for the subscription ID entered.

> ⓘ **Note**
>
> - You can share Azure profile with Self Service Users (SSUs) by adding them as members in the wizard.
> - You can view the list of all Azure profiles from **Library** > **Profiles** > **Azure Profiles**. Select an Azure profile from the list to view detailed information

of this profile under the **General Information** pane.

Next steps

- Manage Azure VMs.
- VM update management.

Feedback

Azure update management

Article • 09/02/2024

This article provides information about Azure update management feature in System Center Virtual Machine Manager (VMM).

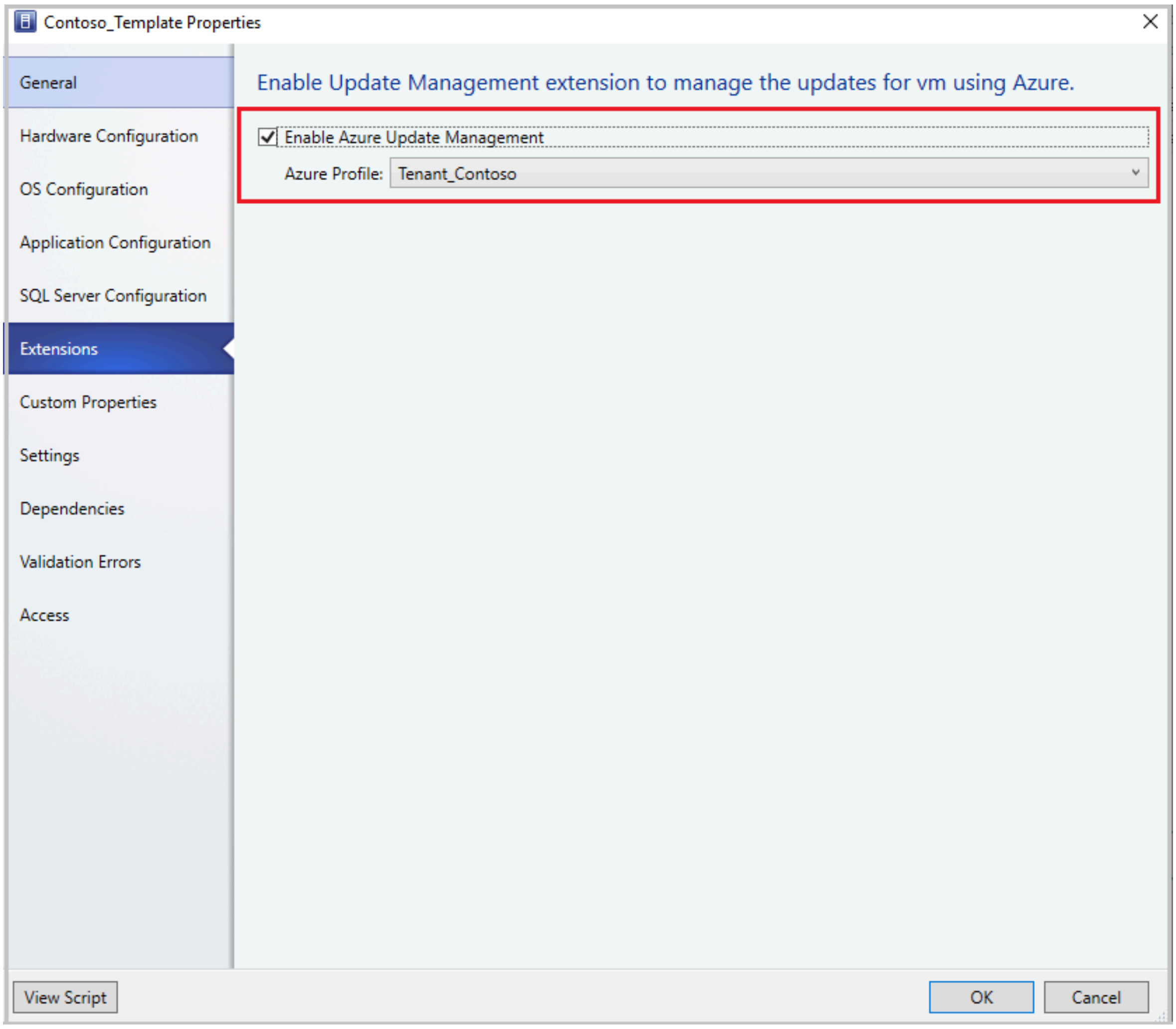
Using Azure update Management feature, you can manage updates for Virtual Machines (VMs) and Workloads running in a VMM.

Currently, VMM supports update management feature for all new VMs with Windows operating system and are deployed using a VM template with *Azure Update Management Extension* enabled.

Create a VM template linked to Azure profile

To create a VM template linked to Azure profile, follow these steps:

1. Create a profile for Azure Update management using steps detailed in Azure subscriptions article.
2. In the **Create VM Template** wizard, select **Source Page** > **Use an existing VM template or a virtual hard disk stored in the library**.
3. On the **Extensions** page, select **Enable Azure Update Management** and select your profile from the **Azure Profile** dropdown menu. Select **OK**.



Contoso_Template Properties

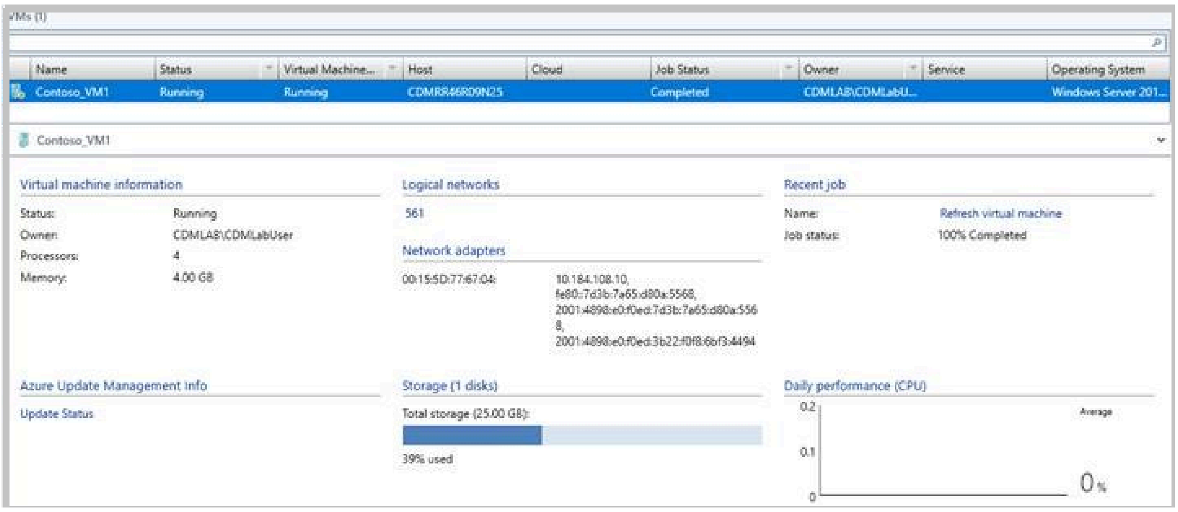
Enable Update Management extension to manage the updates for vm using Azure.

☑ Enable Azure Update Management

Azure Profile: Tenant_Contoso

4. Deploy the VMs from the VM template.

5. VMM onboards the VMs deployed through VM template to the *Azure Update Management* service and provides the link to the Azure console for managing the updates.



VMs (1)

Name	Status	Virtual Machine...	Host	Cloud	Job Status	Owner	Service	Operating System
Contoso_VM1	Running	Running	CDMRR46R09N25		Completed	CDMLAB\CDMLabU...		Windows Server 201...

Contoso_VM1

Virtual machine information

Status:	Running
Owner:	CDMLAB\CDMLabUser
Processors:	4
Memory:	4.00 GB

Logical networks

561

Network adapters

00:15:5D:77:67:04: 10.184.108.10, fe80::7d3b:7a65:d80a:5568, 2001:4898:e0:f0ed:7d3b:7a65:d80a:5568, 2001:4898:e0:f0ed:3b22:f0f8:6bf3:4494

Recent job

Name:	Refresh virtual machine
Job status:	100% Completed

Azure Update Management Info

Update Status

Storage (1 disks)

Total storage (25.00 GB):

39% used

Daily performance (CPU)

6. Select the **Update Status** link under **Azure Update Management info** to assess and deploy the updates for the VM.

ⓘ Note

> Azure update management capability also supports service deployments using service templates; the procedure is the same as above.

Next steps

Manage Azure VMs.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback | Get help at Microsoft Q&A

Manage Azure VMs

Article • 09/02/2024

This article provides information about the *Manage Azure Virtual Machines (VMs)* feature in System Center Virtual Machine Manager (VMM).

This feature allows you to perform basic actions on Azure instances attached to an Azure profile created for Azure VM management.

> ⓘ **Note**
>
> To perform these actions, you must create an Azure profile with **Profile Usage** selected as **Azure VM Management**. Once an Azure profile for Azure VM Management is created, the VMs deployed on Azure will be accessible on the **VMs and Services** page of VMM console and will be listed under **Azure Subscriptions**.

You can perform the following actions on Azure instances, without leaving the VMM console.

- Add and remove one or more Azure subscriptions using the VMM console.
- See a list view with details and status of all role instances in all deployments in that subscription.
- Refresh the list of instances manually
- Perform the following basic actions on the instances:
  - Start
  - Stop
  - Shutdown
  - Restart
  - Connect via RDP

What isn't supported?

This feature isn't intended to provide feature parity with the Microsoft Azure Management Portal. The functionality of this feature is a minor subset of the features at https://portal.azure.com, but you can view your Azure instances and do other basic actions to simplify everyday tasks and management.

With this feature, you can't:

- Manage your Azure subscription.
- Deploy instances to Azure.

- Migrate on-premises virtual machines to Azure.
- Manage Azure Storage.
- Manage Azure Networks.
- See the Dashboard Summary view.
- See the Performance Monitoring Summary.
- Manage more than 50 Azure VMs using Azure profile.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Manage VMs using Microsoft Entra ID-based authentication & authorization and region-specific Azure subscriptions

Article • 09/02/2024

This article provides information about how to manage the Azure Resource Manager-based and region-specific Azure subscriptions using System Center Virtual Machine Manager (VMM).

You can add Microsoft Azure subscriptions to System Center Virtual Machine Manager (VMM) and perform the required actions. Learn more. The VMM Azure plugin allows the management of Azure subscriptions through certificate-based authentication and authorization and VMs in global Azure region.

VMM also supports the management of Azure subscriptions through Microsoft Entra ID and region-specific Azure subscriptions. (namely, Germany, China, US Government Azure regions).

Management of Azure subscriptions through certificate-based authentication and authorization requires Management certificate. Learn More.

Management of VMs using Microsoft Entra ID-based authentication and authorization requires Microsoft Entra ID application.

> ⓘ **Note**
>
> Azure AD mentioned in this article refers to Microsoft Entra ID. Learn more.

Before you start

Ensure the following prerequisites are met:

- **Microsoft Entra ID application** - To manage VMs using VMM through AD authentication and authorization, you need to create a Microsoft Entra ID application and then provide the following details through VMM Azure plugin:
  - Azure Subscription ID
  - Microsoft Entra ID
  - Microsoft Entra ID - Application ID & Application Key

Learn more on how to create a Microsoft Entra ID app.

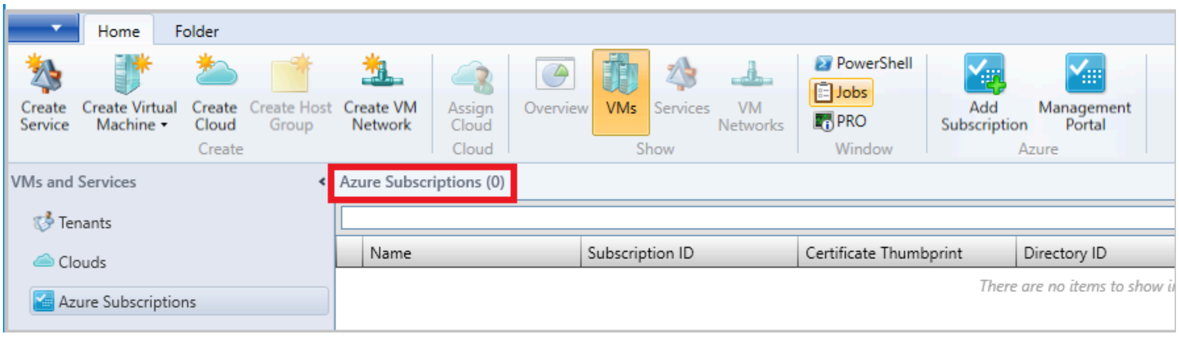
- **A management certificate** - Configured as described in this article.
  - The subscription must have a management certificate associated with it so that VMM can use the classic deployment model in Azure.
  - Make note of the subscription ID and the certificate thumbprint.
  - Certificates must be x509 v3 compliant.
  - The management certificate must be in the local certificate store on the computer on which you add the Azure subscription feature.
  - The certificate must also be in the Current User\Personal store of the computer running the VMM console.

    > ⓘ **Note**
    >
    > The certificate is required only if you choose to use certificate-based authentication to manage your Azure subscription.

Manage Microsoft Entra ID-based authentication & authorization and region-specific Azure subscriptions

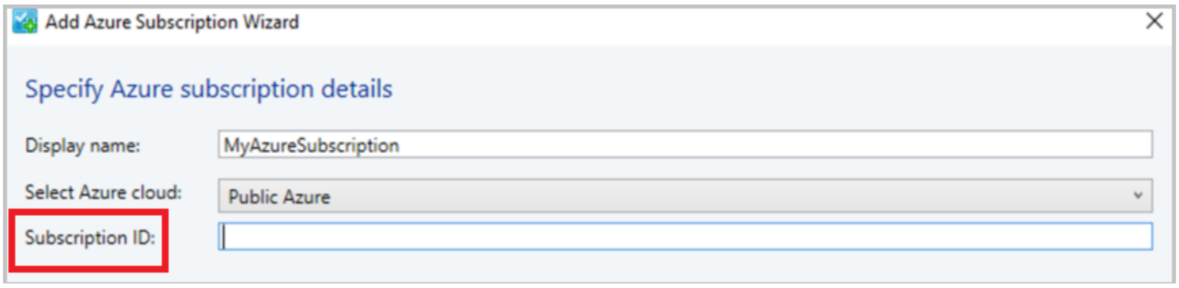
Use the following steps:

1. Browse to **Azure Subscriptions** and select **Add Subscription**.



2. Provide **Display Name**, **Azure cloud**, and **Subscription ID**.

   You can provide any friendly name as display name. Choose either global Azure or region-specific subscription as appropriate.



Add Azure Subscription Wizard

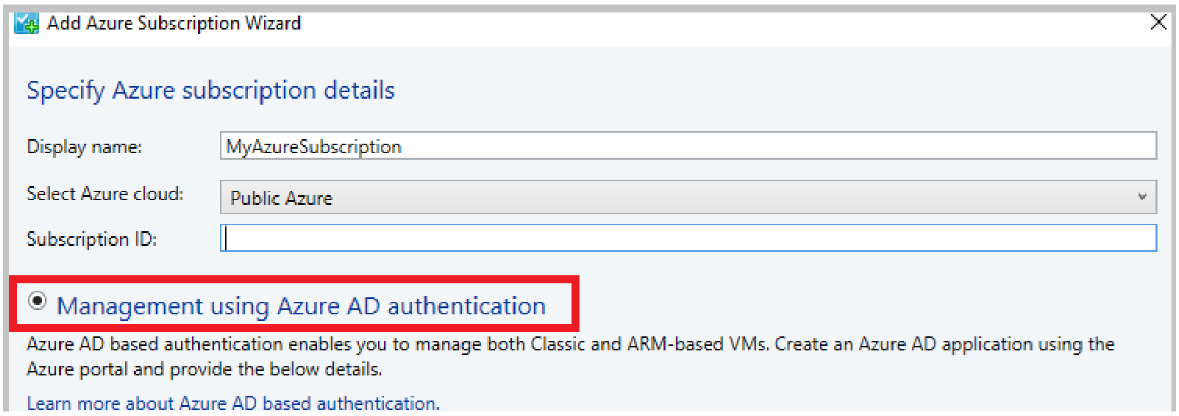
Specify Azure subscription details

Display name: MyAzureSubscription

Select Azure cloud: Public Azure

Subscription ID:

3. Select **Management using Azure AD authentication** (to use certificate-based management, go to step 5).



Add Azure Subscription Wizard

Specify Azure subscription details

Display name: MyAzureSubscription

Select Azure cloud: Public Azure

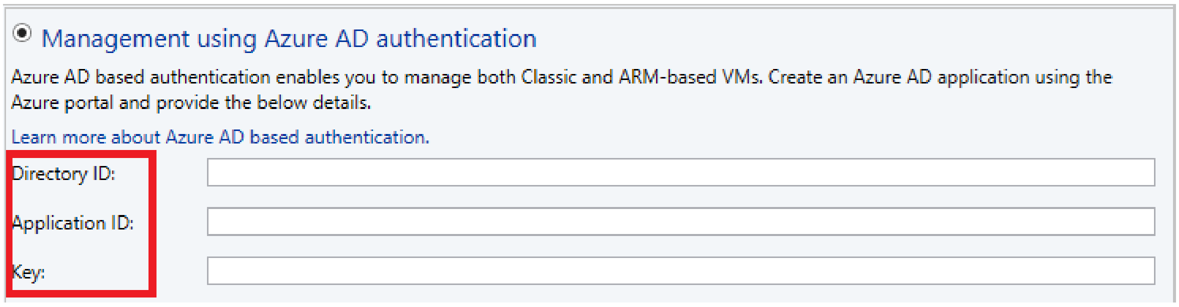
Subscription ID:

● Management using Azure AD authentication

Azure AD based authentication enables you to manage both Classic and ARM-based VMs. Create an Azure AD application using the Azure portal and provide the below details.

Learn more about Azure AD based authentication.

4. Provide **Directory ID**, **Application ID**, and **Key**, and select **Finish** (after this step, go to step 6 directly).



● Management using Azure AD authentication

Azure AD based authentication enables you to manage both Classic and ARM-based VMs. Create an Azure AD application using the Azure portal and provide the below details.

Learn more about Azure AD based authentication.

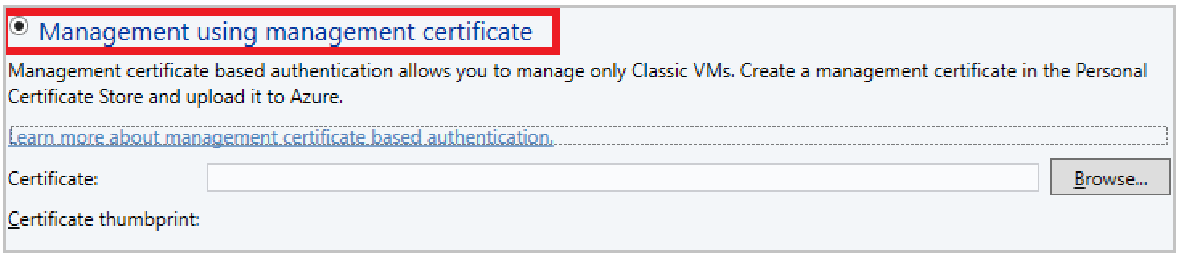
Directory ID:

Application ID:

Key:

5. To use management certificate, select **Management using management certificate** (not required if already performed step 3 and 4).

   If you want to continue using certificate-based authentication, then instead of selecting Microsoft Entra ID authentication, choose management certificate-based authentication and provide the management certificate from **Current User\Personal** certificate store and select **Finish**.



● Management using management certificate

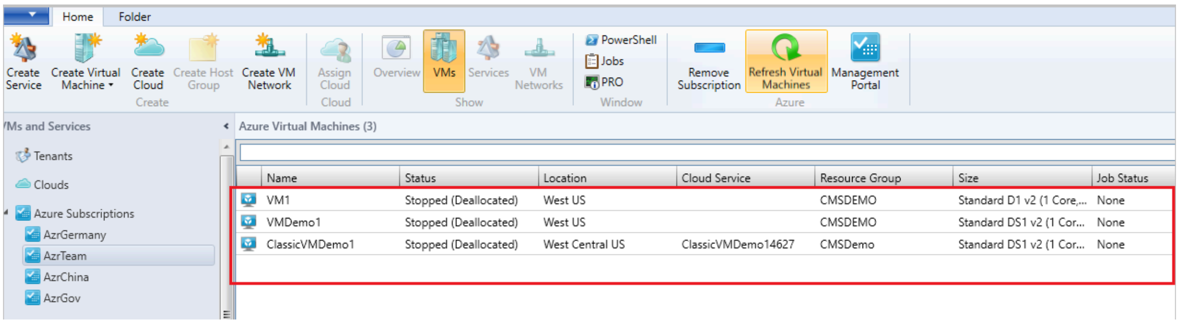
Management certificate based authentication allows you to manage only Classic VMs. Create a management certificate in the Personal Certificate Store and upload it to Azure.

Learn more about management certificate based authentication.

Certificate:

Certificate thumbprint:

6. Verify the Azure subscription and the VMs hosted on Azure.



Name	Status	Location	Cloud Service	Resource Group	Size	Job Status
VM1	Stopped (Deallocated)	West US		CMSDEMO	Standard D1 v2 (1 Core,...	None
VMDemo1	Stopped (Deallocated)	West US		CMSDEMO	Standard DS1 v2 (1 Cor...	None
ClassicVMDemo1	Stopped (Deallocated)	West Central US	ClassicVMDemo14627	CMSDemo	Standard DS1 v2 (1 Cor...	None

Next steps

- Create certificates.
- Create active directory.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Resources for troubleshooting

Article • 09/02/2024

Expand table

Resource	Description
Troubleshooting Guide	General information about troubleshooting VMM, such as collecting traces and logging information.
VMM Configuration Analyzer (VMMCA) in VMM Component Add-ons and Extensions on the Microsoft Download Center	A diagnostic tool that you can use to evaluate important post-installation configuration settings for computers that either might serve or are serving VMM roles or other VMM functions.
Microsoft Support Knowledge Base	Searchable articles describing issues and workarounds for VMM.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A