Hyper-V Planning and Deployment Guide

Microsoft Corporation
Published: March 2009

Abstract
This guide describes the considerations you should take into account when planning to deploy the Hyper-V™ technology, and provides installation and configuration details that will help you deploy Hyper-V.
Copyright information

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Microsoft Corporation. All rights reserved.

Active Directory, Hyper-V, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.
All other trademarks are property of their respective owners.
# Contents

Hyper-V Planning and Deployment Guide ................................................................. 7  
  About this guide ................................................................................................. 7

Overview of Hyper-V .......................................................................................... 7  
  What does Hyper-V do? .................................................................................. 7  
  Who will be interested in this role? ................................................................. 8  
  What are the key features of Hyper-V? ......................................................... 8

Before You Install Hyper-V ................................................................................ 8

Hardware Considerations .................................................................................. 9  
  Hardware requirements ................................................................................ 9  
  Memory ........................................................................................................ 10  
  Processors .................................................................................................... 10  
  Networking .................................................................................................... 10  
  Storage ......................................................................................................... 11  
  Other hardware components ........................................................................ 12

About Virtual Machines and Guest Operating Systems .................................. 13  
  Running multiple virtual machines ............................................................... 13  
  Supported guest operating systems ............................................................... 13  
  Integration services ...................................................................................... 14  
  Additional considerations ............................................................................ 16

Planning for Hyper-V Security ......................................................................... 16  
  Hyper-V security best practices .................................................................. 17  
  Additional resources .................................................................................... 20

Using Authorization Manager for Hyper-V Security ....................................... 20

Configure Hyper-V for Role-based Access Control ....................................... 21  
  Configuring role-based access control ......................................................... 22  
  Additional resources .................................................................................... 23

Planning for Backup ......................................................................................... 24  
  Understanding backup options and considerations ..................................... 24  
    Storage considerations .............................................................................. 25  
  Understanding online and offline backups ............................................... 25  
  Understanding the restore process ............................................................ 26  
  Considerations about clustered virtual machines ....................................... 27

Installing Hyper-V ............................................................................................ 28
Modify virtual machine settings (reconfigure a virtual machine) ........................................ 54
Pass CTRL + ALT + DELETE (send control signals to a virtual machine) ................................. 54
Pause a virtual machine ........................................................................................................ 55
Remove external network from server .................................................................................. 55
Remove internal network adapter from a virtual machine .................................................... 55
Remove internal network from server .................................................................................. 56
Remove private network from server .................................................................................. 56
Rename a snapshot .................................................................................................................. 56
Rename a virtual machine ....................................................................................................... 56
Resume a virtual machine ........................................................................................................ 56
Save a virtual machine and start a virtual machine .............................................................. 57
Start a virtual machine ........................................................................................................... 57
Turn off a virtual machine ...................................................................................................... 57
View Hyper-V server settings .............................................................................................. 57
View network management ................................................................................................... 57
View virtual machines ............................................................................................................ 57

Appendix B: Authorization Manager Terminology .................................................................. 58
Terminology .............................................................................................................................. 58
Hyper-V Planning and Deployment Guide

About this guide
The Hyper-V Planning and Deployment Guide is intended to help you understand the considerations you should take into account when planning to deploy Hyper-V™, and to provide installation and configuration details that will help you deploy Hyper-V.

- Overview of Hyper-V
- Before You Install Hyper-V
- Installing Hyper-V
- Configuring Virtual Networks
- Implementing Disks and Storage
- Appendix A: Example Authorization Manager Tasks and Operations
- Appendix B: Authorization Manager Terminology

Overview of Hyper-V
Hyper-V enables you to create a virtualized server computing environment using a technology that is part of Windows Server® 2008. You can use a virtualized computing environment to improve the efficiency of your computing resources by utilizing more of your hardware resources. This is possible because you use Hyper-V to create and manage virtual machines and their resources. Each virtual machine is a virtualized computer system that operates in an isolated execution environment. This allows you to run multiple operating systems simultaneously on one physical computer.

Note
Hyper-V is a hypervisor-based virtualization technology that requires specific hardware. For more information about the requirements and other considerations about hardware, see Hardware Considerations.

What does Hyper-V do?
Hyper-V provides software infrastructure and basic management tools in Windows Server 2008 that you can use to create and manage a virtualized server computing environment. This virtualized environment can be used to address a variety of business goals aimed at improving efficiency and reducing costs. For example, a virtualized server environment can help you:

- Reduce the costs of operating and maintaining physical servers by increasing your hardware utilization. You can reduce the amount of hardware needed to run your server workloads.
Increase development and test efficiency by reducing the amount of time it takes to set up hardware and software and reproduce test environments.

Improve server availability without using as many physical computers as you would need in a failover configuration that uses only physical computers.

Who will be interested in this role?
Hyper-V can be useful to you if you are:
- An IT administrator, planner, or designer.
- An IT architect responsible for computer management and security throughout your organization.
- An IT operations manager who is looking for ways to reduce the total cost of ownership of their server infrastructure, in terms of both power costs and management costs.
- A software developer or tester who is looking for ways to increase productivity by reducing the time it takes to build and configure a server for development or test use.

What are the key features of Hyper-V?
The key features of Hyper-V are as follows:
- 64-bit native hypervisor-based virtualization.
- Ability to run 32-bit and 64-bit virtual machines concurrently.
- Uniprocessor and multiprocessor virtual machines.
- Virtual machine snapshots, which capture the state, data, and hardware configuration of a running virtual machine. Because snapshots record system states, you can revert the virtual machine to a previous state.
- Large virtual machine memory support.
- Virtual local area network (VLAN) support.
- Microsoft Management Console (MMC) management snap-in.
- Documented Windows Management Instrumentation (WMI) interfaces for scripting and management.

For more information about the WMI interfaces, see Virtualization WMI Provider (http://go.microsoft.com/fwlink/?LinkId=108564).

Before You Install Hyper-V

Hyper-V has specific hardware requirements and considerations that you should familiarize yourself with when planning to deploy this technology. Topics to review include the following:
- **Hardware Considerations**
- **About Virtual Machines and Guest Operating Systems**
Planning for Hyper-V Security
Planning for Backup

Hardware Considerations

To effectively plan for and deploy Hyper-V, you should understand the requirements and maximum configurations for the physical and virtual hardware that will comprise the virtualized server computing environment.

Hardware requirements

Hyper-V requires specific hardware. To install and use the Hyper-V role, you will need the following:

- **An x64-based processor.** Hyper-V is available in 64-bit editions of Windows Server 2008—specifically, the 64-bit editions of Windows Server 2008 Standard, Windows Server 2008 Enterprise, and Windows Server 2008 Datacenter. Hyper-V is not available for 32-bit (x86) editions or Windows Server 2008 for Itanium-Based Systems. However, the Hyper-V management tools are available for 32-bit editions. For more information about the tools, see Installing Hyper-V.

- **Hardware-assisted virtualization.** This is available in processors that include a virtualization option—specifically processors with Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) technology.

- **Hardware-enforced Data Execution Prevention (DEP) must be available and enabled.** Specifically, you must enable Intel XD bit (execute disable bit) or AMD NX bit (no execute bit).

You can identify systems that support the x64 architecture and Hyper-V by searching the Windows Server catalog for Hyper-V as an additional qualification (see [http://go.microsoft.com/fwlink/?LinkId=111228](http://go.microsoft.com/fwlink/?LinkId=111228)).

💡 Tip

The settings for hardware-assisted virtualization and hardware-enforced DEP are available in the BIOS. However, the names of the settings may differ from the names identified above. For more information about whether a specific processor model supports Hyper-V, check with the manufacturer of the computer. If you modify the settings for hardware-assisted virtualization or hardware-enforced DEP, we recommend that you turn off the power to the computer and then turn it back on. Restarting the computer may not apply the changes to the settings.
Memory
The maximum amount of memory that can be used is determined by the operating system, as follows:
- For Windows Server 2008 Enterprise and Windows Server 2008 Datacenter, the physical computer can be configured with up to 1 TB of physical memory, and virtual machines that run either of those editions can be configured with up to 64 GB of memory per virtual machine.
- For Windows Server 2008 Standard, the physical computer can be configured with up to 32 GB of physical memory, and virtual machines that run that edition can be configured with up to 31 GB of memory per virtual machine.

Processors
The release version of Hyper-V is supported on physical computers with up to 16 logical processors. However, a hotfix (KB956710) is available that increases the maximum number of virtual processors to 24. For more information and links to the updates, see Hyper-V Update List.
A logical processor can be a single core or multi-core processor. You can configure up to 4 virtual processors on a virtual machine. Note that the number of virtual processors supported by a guest operating system might be lower. For more information, see About Virtual Machines and Guest Operating Systems. The following are some examples of supported systems and the number of logical processors they provide:
- A single-processor/dual-core system provides 2 logical processors.
- A single-processor/quad-core system provides 4 logical processors.
- A dual-processor/dual-core system provides 4 logical processors.
- A dual-processor/quad-core system provides 8 logical processors.
- A quad-processor/dual-core system provides 8 logical processors.
- A quad-processor/dual-core, hyper-threaded system provides 16 logical processors.
- A quad-processor/quad-core system provides 16 logical processors.

Networking
Hyper-V provides a variety of networking options and configurations to meet different networking requirements. For more information about different types of virtual networks and virtual network adapters, see Configuring Virtual Networks.
Hyper-V networking includes the following support:
- Each virtual machine can be configured with up to 12 virtual network adapters—8 can be the “network adapter” type and 4 can be the “legacy network adapter” type. The network adapter type provides better performance and requires a virtual machine driver that is included in the integration services packages.
- Each virtual network adapter can be configured with either a static or dynamic MAC address.
• Each virtual network adapter offers integrated virtual local area network (VLAN) support and can be assigned a unique VLAN channel.
• You can have an unlimited number of virtual networks with up to 512 virtual machines per virtual network.

**Note**
You cannot connect a virtual network to a wireless network adapter. As a result, you cannot provide wireless networking capabilities to virtual machines.

## Storage

Hyper-V supports a variety of storage options. For more information about the storage options, see [Implementing Disks and Storage](#).

You can use the following types of physical storage with a server that runs Hyper-V:

• **Direct-attached storage:** You can use Serial Advanced Technology Attachment (SATA), external Serial Advanced Technology Attachment (eSATA), Parallel Advanced Technology Attachment (PATA), Serial Attached SCSI (SAS), SCSI, USB, and Firewire.

• **Storage area networks (SANs):** You can use Internet SCSI (iSCSI), Fibre Channel, and SAS technologies.

**Important**
Microsoft does not support network-attached storage (NAS) for Hyper-V.

You can configure a virtual machine to use the following types of storage:

• **Virtual IDE devices.** Each virtual machine supports up to 4 IDE devices. The startup disk (sometimes referred to as the boot disk) must be attached to one of the IDE devices. The startup disk can be either a virtual hard disk or a physical disk. Although a virtual machine must use a virtual IDE device as the startup disk to start the guest operating system, you have many options to choose from when selecting the physical device that will provide the storage for the virtual IDE device. For example, you can use any of the types of physical storage identified in the preceding list.

• **Virtual SCSI devices.** Each virtual machine supports up to 4 virtual SCSI controllers, and each controller supports up to 64 disks. This means that each virtual machine can be configured with as many as 256 virtual SCSI disks. Use of virtual SCSI devices requires integration services to be installed in the guest operating system. For a list of the guest operating systems for which integration services are available, see [About Virtual Machines and Guest Operating Systems](#).

• **Virtual hard disks of up to 2040 GB.** You can use fixed virtual hard disks, dynamically expanding virtual hard disks, and differencing disks.

• **Physical disks.** Physical disks attached directly to a virtual machine have no size limitation other than what is supported by the guest operating system.
- **Virtual machine storage capacity.** Using virtual hard disks, each virtual machine supports up to 512 TB of storage. Using physical disks, this number is even greater depending on what is supported by the guest operating system.

- **Virtual machine snapshots.** Hyper-V supports up to 50 snapshots per virtual machine.

  **Tip**

  Although the I/O performance of physical SCSI and IDE devices can differ significantly, this is not true for the virtualized SCSI and IDE devices in Hyper-V. Hyper-V IDE and SCSI storage devices both offer equally fast high I/O performance when integration services are installed in the guest operating system. For a list of the guest operating systems for which integration services are available, see About Virtual Machines and Guest Operating Systems.

### Other hardware components

The following is information about the other types of physical and virtual hardware components that you can use with Hyper-V.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **DVD drive** | A virtual machine has 1 virtual DVD drive by default when you create the virtual machine. Virtual machines can be configured with up to 3 DVD drives, connected to an IDE controller. (Virtual machines support up to 4 IDE devices, but one device must be the startup disk.)

A virtual DVD drive can access CDs and DVDs, either .iso files or physical media. However, only one virtual machine can be configured to access a physical CD/DVD drive at a time. |
| **Virtual COM port** | Each virtual machine is configured with 2 virtual serial (COM) ports that can be attached to a named pipe to communicate with a local or remote physical computer. |

  **Note**

  No access to a physical COM port is available from a virtual machine. |
| **Virtual floppy drive** | Each virtual machine is configured with 1 virtual floppy drive, which can access virtual floppy disk (.vfd) files. |

  **Note**

  No access to a physical floppy drive is
About Virtual Machines and Guest Operating Systems

Running multiple virtual machines
You can use Hyper-V to configure and use many virtual machines at the same time. The specific number depends on two factors. One factor is the available physical resources on the server running Hyper-V. For more information, see Hardware Considerations. The other factor is the maximum capacity of Hyper-V. You can configure as many as 512 virtual machines on a server running Hyper-V. With the appropriate physical resources, the release version of Hyper-V supports up to 128 virtual machines running at the same time. A hotfix (KB956710) is available that increases the maximum number of running virtual machines to 192. For more information and links to the updates, see Hyper-V Update List.

Supported guest operating systems
The following operating systems are supported for use on a virtual machine as a guest operating system. You can run 32-bit and 64-bit guest operating systems at the same time on one server running Hyper-V.

- You can use the following 32-bit and 64-bit editions of Windows Server 2008 as a supported guest operating system on a virtual machine configured with 1, 2, or 4 virtual processors:
  - Windows Server 2008 Enterprise and Windows Server 2008 Enterprise without Hyper-V
  - Windows Server 2008 Datacenter and Windows Server 2008 Datacenter without Hyper-V
  - Windows Web Server 2008
  - Windows Server 2008 HPC Edition

- You can use the following editions of Windows Server 2003 as a supported guest operating system on a virtual machine configured with 1 or 2 virtual processors:
  - Windows Server 2003 R2 Datacenter Edition with Service Pack 2
Windows Server 2003 R2 Standard x64 Edition with Service Pack 2
Windows Server 2003 R2 Enterprise x64 Edition with Service Pack 2
Windows Server 2003 R2 Datacenter x64 Edition with Service Pack 2
Windows Server 2003 Standard x64 Edition with Service Pack 2
Windows Server 2003 Enterprise x64 Edition with Service Pack 2
Windows Server 2003 Datacenter x64 Edition with Service Pack 2

You can run the following versions of Windows 2000 on a virtual machine configured with 1 virtual processor:

- Windows 2000 Server with Service Pack 4
- Windows 2000 Advanced Server with Service Pack 4

You can run the following Linux distributions on a virtual machine configured with 1 virtual processor:

- Suse Linux Enterprise Server 10 with Service Pack 2 (x86 edition or x64 edition)
- Suse Linux Enterprise Server 10 with Service Pack 1 (x86 edition or x64 edition)

You can run the following 32-bit and 64-bit versions of Windows Vista on a virtual machine configured with 1 or 2 virtual processors:

- Windows Vista Business with Service Pack 1
- Windows Vista Enterprise with Service Pack 1
- Windows Vista Ultimate with Service Pack 1

You can run the following versions of Windows XP on a virtual machine:

- Windows XP Professional with Service Pack 3 (configured with 1 or 2 virtual processors)
- Windows XP Professional with Service Pack 2 (configured with 1 virtual processor)
- Windows XP Professional x64 Edition with Service Pack 2 (configured with 1 or 2 virtual processors)

### Integration services

Integration services are available for supported guest operating systems as described in the following table.

<table>
<thead>
<tr>
<th>Guest operating system</th>
<th>Device and service support</th>
</tr>
</thead>
</table>

**Important**

When a service pack is listed, the service pack is required and the guest operating system is not supported without the listed service pack.

**Note**

Some guest operating systems do not support the Volume Shadow Copy Service. As a result, online backup service is not available and is not listed for those guest operating systems.
<table>
<thead>
<tr>
<th>Operating System</th>
<th>Drivers</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 (64-bit editions and x86 editions)</td>
<td>Drivers: IDE, SCSI, networking, video, and mouse</td>
<td>Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup</td>
</tr>
<tr>
<td>Windows Server 2003 (x64 editions) with Service Pack 2</td>
<td>Drivers: IDE, SCSI, networking, video, and mouse</td>
<td>Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This operating system does not support a legacy network adapter. For more information about virtual networking and network adapter types, see Configuring Virtual Networks.</td>
</tr>
<tr>
<td>Windows Server 2003 (x86 editions) with Service Pack 2</td>
<td>Drivers: IDE, SCSI, networking, video, and mouse</td>
<td>Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup</td>
</tr>
<tr>
<td>Windows 2000 Server with Service Pack 4</td>
<td>Drivers: IDE, networking, video, and mouse</td>
<td>Services: operating system shutdown, time synchronization, data exchange, and heartbeat</td>
</tr>
<tr>
<td>Windows 2000 Advanced Server with Service Pack 4</td>
<td>Drivers: IDE, networking, video, and mouse</td>
<td>Services: operating system shutdown, time synchronization, data exchange, and heartbeat</td>
</tr>
<tr>
<td>Suse Linux Enterprise Server 10 (x64 edition) with Service Pack 1 or 2</td>
<td>Drivers only: IDE, SCSI, and networking</td>
<td></td>
</tr>
<tr>
<td>Suse Linux Enterprise Server 10 (x86 edition) with Service Pack 1 or 2</td>
<td>Drivers only: IDE, SCSI, and networking</td>
<td></td>
</tr>
<tr>
<td>Windows Vista (64-bit editions) with Service Pack 1</td>
<td>Drivers: IDE, SCSI, networking, video, and mouse</td>
<td>Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup</td>
</tr>
<tr>
<td>Windows Vista (x86 editions) with Service Pack</td>
<td>Drivers: IDE, networking, video, and mouse</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| Windows XP Professional (x86 editions) with Service Pack 2 or 3 | Drivers: IDE, SCSI, networking, video, and mouse  
Services: operating system shutdown, time synchronization, data exchange, and heartbeat |
| Windows XP Professional x64 Edition with Service Pack 2          | Drivers: IDE, SCSI, networking, video, and mouse  
Services: operating system shutdown, time synchronization, data exchange, and heartbeat |

**Additional considerations**

- On Windows operating systems, you may need to close the Found New Hardware Wizard to start the installation of integration services.
- If you installed a prerelease version of integration services on a guest operating system, we recommend that you upgrade to the release version. For supported Windows operating systems, the release version of integration services is included in the update package for the Hyper-V role. For more information about the role update package, see [Installing Hyper-V](http://go.microsoft.com/fwlink/?LinkID=102024).
- Integration services for the supported versions of Linux distributions are distributed through the Microsoft Connect Web site and are identified as Linux Integration Components for Microsoft Hyper-V. For more information, see [http://go.microsoft.com/fwlink/?LinkID=102024](http://go.microsoft.com/fwlink/?LinkID=102024).

**Planning for Hyper-V Security**

You should secure your virtualization server using the same measures you would take to safeguard any server running Windows Server 2008. Additionally, you should use a few extra measures to help secure the virtual machines, configuration files, and data. For more information about how to secure Windows Server 2008 workloads, see the Windows Server 2008 Security Guide ([http://go.microsoft.com/fwlink/?LinkID=134200](http://go.microsoft.com/fwlink/?LinkID=134200)).

Additionally, see the following security-related topics in this guide:

- **Using Authorization Manager for Hyper-V Security**
- **Configure Hyper-V for Role-based Access Control**

You should secure the virtual machines running on the virtualization server according to your procedures for securing that kind of server or workload. There is nothing special or different you need to do to secure the virtual machine just because it is a virtual machine. For example, if your policies and procedures require that you run antivirus software, run it on the virtual machine. If
you have a policy requirement to segment the physical server to a particular network, follow the policy for the virtual machine as well.

We recommend the following best practices to improve the security of your servers running Hyper-V.

**Note**

You can use BitLocker Drive Encryption to help protect virtual machines and data, but it requires careful deployment and recovery planning. For more information, review the Windows BitLocker Drive Encryption Design and Deployment Guides ([http://go.microsoft.com/fwlink/?LinkId=134201](http://go.microsoft.com/fwlink/?LinkId=134201)).

## Hyper-V security best practices

- **Use a Server Core installation of Windows Server 2008 for the management operating system.** A Server Core installation provides the smallest attack surface and reduces the number of patches, updates, and restarts required for maintenance. For detailed information and installation guidance, see the Server Core Installation Option of Windows Server 2008 Step-By-Step Guide ([http://go.microsoft.com/fwlink/?LinkId=134202](http://go.microsoft.com/fwlink/?LinkId=134202)).

  For more information about enabling the Hyper-V role on a server running a Server Core installation, see [Install the Hyper-V Role on a Server Core Installation of Windows Server 2008](http://go.microsoft.com/fwlink/?LinkId=134202).

  **Notes**

  - There is no way to upgrade from a Server Core installation to a full installation of Windows Server 2008. If you need the Windows user interface or a server role that is not supported in a Server Core installation, install a full installation of Windows Server 2008.

  - To remotely manage Hyper-V on a Server Core installation, use the Hyper-V management tools for Windows Server 2008 and Windows Vista Service Pack 1 (SP1). For more information, see article 950050 ([http://go.microsoft.com/fwlink/?LinkId=122188](http://go.microsoft.com/fwlink/?LinkId=122188)) and article 952627 ([http://go.microsoft.com/fwlink/?LinkID=122189](http://go.microsoft.com/fwlink/?LinkID=122189)) in the Microsoft Knowledge Base. For more information about configuring tools for remote management of Hyper-V, see [Install and Configure Hyper-V Tools for Remote Administration](http://go.microsoft.com/fwlink/?LinkId=122189).

- **Do not run any applications in the management operating system—run all applications on virtual machines.** By keeping the management operating system free of applications and running a Windows Server 2008 core installation, you will need fewer updates to the management operating system because nothing requires software updates except the Server Core installation, the Hyper-V service components, and the hypervisor.

  **Notes**

  - If you run programs in the management operating system, you should run your antivirus solution there and add the following to the antivirus exclusions:

  - Virtual machine configuration files directory. By default, it is C:\ProgramData\Microsoft\Windows\Hyper-V.
- Virtual machine virtual hard disk files directory. By default, it is C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks.
- Snapshot files directory. By default, it is %systemdrive%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots.
- Vmms.exe
- Vmwp.exe

If you need to use the full version of Windows Server 2008 and run applications in the management operating system, then you should run an antivirus program there.

- **Use the security level of your virtual machines to determine the security level of your management operating system.** You should deploy virtual machines onto virtualization servers that have similar security requirements. For example, assume that you classify the level of risk and effort to secure your servers into three categories: “secure”, “more secure”, and “most secure”. You would put more compliance effort and control procedures into the most secure servers than on the secure servers. This would be true whether the server is physical or running on a virtual machine. If you deploy both secure and most secure virtual machines on the management operating system, then you should secure the virtualization server as a “most secure” server. Deploying virtual machines with similar security levels on a virtualization server can make management and movement of the virtual machines easier.

- **Do not give virtual machine administrators permissions on the management operating system.** According to the principle of least privilege, you should give administrators of a virtual machine (sometimes called department administrators or delegated administrators) the minimum permissions required. Managing the required permissions on all the objects associated with a virtual machine can be complex, and can lead to potential security issues if not handled properly. Role-based access control enables you to specify access control in terms of the organizational structure of a company—by creating a new object called a role. You assign a user to a role to perform a job function. Hyper-V uses Authorization Manager policies for role-based access control.

- **Ensure that virtual machines are fully updated before they are deployed in a production environment.** Because virtual machines are so much easier to move around and quicker to deploy than physical machines, there is a greater risk that a virtual machine that is not fully updated or patched might be deployed. To manage this risk effectively, use the same methods and procedures to update virtual machines as you use to update physical servers. For example, if you allow the use of automatic updates using Windows Update, Microsoft System Center Configuration Manager, or another software distribution method, ensure that virtual machines are updated and/or patched before they are deployed.

  You can use maintenance hosts and quick migration in Hyper-V to accomplish this. A maintenance host is a host computer that you can dedicate for patching stored resources and for staging virtual machines before you move them into your production environment. For more information about maintenance hosts, see Planning for Hosts ([http://go.microsoft.com/fwlink/?LinkId=134482](http://go.microsoft.com/fwlink/?LinkId=134482)). For information about using quick migration to move virtual machines to a maintenance host, see Hyper-V Step-by-Step Guide: Testing Hyper-V and Failover Clustering ([http://go.microsoft.com/fwlink/?LinkId=134481](http://go.microsoft.com/fwlink/?LinkId=134481)).
- **Ensure integration services are installed on virtual machines.** The accuracy of timestamps and audit log entries is important for computer forensics and compliance. Integration services ensure that time is synchronized between virtual machines and the management operating system. This synchronization makes sure that time is consistent with the physical location of the virtual machine in the event that virtual machines are migrated between data centers in different time zones or virtual machines are restored from previous snapshots.

- **Use a dedicated network adapter for the management operating system of the virtualization server.** By default, no virtual networking is configured for the management operating system. Use a dedicated network adapter for managing the server running Hyper-V and do not expose it to untrusted network traffic. Do not allow virtual machines to use this network adapter. Use one or more different dedicated network adapters for virtual machine networking. This allows you to apply different levels of networking security policy and configuration for your virtual machines. For example, you can configure networking so that the virtual machines have different networking access than your management operating system, including the use of virtual local area networks (VLANs), Internet Protocol Security (IPsec), Network Access Protection (NAP) and Microsoft Forefront Threat Management Gateway. For more information about configuring networking, see [Configuring Virtual Networks](http://go.microsoft.com/fwlink/?LinkId=134452).

For more information about NAP, see [http://go.microsoft.com/fwlink/?LinkId=117804](http://go.microsoft.com/fwlink/?LinkId=117804). For information about Microsoft Forefront Threat Management Gateway and Microsoft Forefront “Stirling”, see [http://go.microsoft.com/fwlink/?LinkId=134452](http://go.microsoft.com/fwlink/?LinkId=134452).

- **Use BitLocker Drive Encryption to protect resources.** BitLocker Drive Encryption works with features in server hardware and firmware to provide secure operating system boot and disk drive encryption, even when the server is not powered on. This helps protect data if a disk is stolen and mounted on another computer for data mining. BitLocker Drive Encryption also helps protect data if an attacker uses a different operating system or runs a software hacking tool to access a disk.

Losing a physical disk is a more significant risk in scenarios with small and medium businesses, as well as remote offices, where physical security of the server may not be as rigorous as in an enterprise data center. However, using BitLocker Drive Encryption makes sense for all computers. You should use BitLocker Drive Encryption on all volumes that store virtual machine files too. This includes the virtual hard disks, configuration files, snapshots, and any virtual machine resources, such as ISO images and virtual floppy disks. For a higher level of security that includes secure startup, BitLocker Drive Encryption requires Trusted Platform Module (TPM) hardware. For more information about TPM management, see the [Windows Trusted Platform Module Management Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=134227).

For more information on how to configure BitLocker Drive Encryption to help protect your server and the virtual machines running on it, see [Windows Server 2008 Hyper-V and BitLocker Drive Encryption](http://go.microsoft.com/fwlink/?LinkId=123534).
Also see Windows BitLocker Drive Encryption Frequently Asked Questions (http://go.microsoft.com/fwlink/?LinkId=134228) and the BitLocker Repair Tool (http://go.microsoft.com/fwlink/?LinkId=134229).

Important

Use BitLocker Drive Encryption in the Hyper-V management operating system and to protect volumes that contain configuration files, virtual hard disks, and snapshots. Do not run BitLocker Drive Encryption within a virtual machine. BitLocker Drive Encryption is not supported within a virtual machine.

- **Disable virtualization BIOS settings when they are not required.** When you are no longer using a server for virtualization, for example in a test or development scenario, you should turn off the hardware-assisted virtualization BIOS settings that were required for Hyper-V. For instructions on disabling these settings, consult your hardware manufacturer.

**Additional resources**

- Virtualization Security Best Practices Podcast (http://go.microsoft.com/fwlink/?LinkId=134225)
- Windows Server Virtualization and the Windows Hypervisor (http://go.microsoft.com/fwlink/?LinkId=134226)

**Using Authorization Manager for Hyper-V Security**

You use Authorization Manager to provide role-based access control for Hyper-V. For instructions on implementing role-based access control, see Configure Hyper-V for Role-based Access Control. For more information about getting started with Authorization Manager, see Appendix B: Authorization Manager Terminology and Checklist: Before you start using Authorization Manager (http://go.microsoft.com/fwlink/?LinkId=134197).

Authorization Manager is comprised of the following:

- **Authorization Manager snap-in (AzMan.msc).** You can use the Microsoft Management Console (MMC) snap-in to select operations, group them into tasks, and then authorize roles to perform specific tasks. You also use it to manage tasks, operations, user roles, and permissions. To use the snap-in, you must first create an authorization store or open an existing store. For more information, see http://go.microsoft.com/fwlink/?LinkId=134086.

- **Authorization Manager API.** The API provides a simplified development model in which to manage flexible groups and business rules and store authorization policies. For more information, see Role-based Access Control (http://go.microsoft.com/fwlink/?LinkId=134079).

Authorization Manager requires a data store for the policy that correlates roles, users, and access rights. This is called an authorization store. In Hyper-V, this data store can be maintained in an
Active Directory database or in an XML file on the local server running the Hyper-V role. You can edit the store through the Authorization Manager snap-in or through the Authorization Manager API, which are available to scripting languages such as VBScript.

If an Active Directory database is used for the authorization store, Active Directory Domain Services (AD DS) must be at the Windows Server 2003 functional level.

The XML store does not support delegation of applications, stores, or scopes because access to the XML file is controlled by the discretionary access control list (DACL) on the file, which grants or restricts access to the entire contents of the file. (For more information about Authorization Manager delegation, see http://go.microsoft.com/fwlink/?LinkId=134075). Because of this, if an XML file is used for the authorization store, it is important that it is backed up regularly. The NTFS file system does not support applications issuing a sequence of separate write operations as a single logical write to a file when multiple applications write to the same file. This means an Authorization Manager policy file (XML file) could be edited simultaneously by two administrative applications and could become corrupted. The Hyper-V VSS writer will back up the authorization store with the server running the Hyper-V role.

## Configure Hyper-V for Role-based Access Control

This topic describes how to configure role-based access control for virtual machines in Hyper-V. You use the Authorization Manager Microsoft Management Console (MMC) snap-in (AzMan.msc) to provide role-based access control for Hyper-V. For more information, see the following topics in this guide:

- Using Authorization Manager for Hyper-V Security
- Appendix B: Authorization Manager Terminology
- Planning for Hyper-V Security

To implement role-based access control, you must first define scopes and then organize operations into groups to accomplish tasks. You assign tasks to roles, and then assign users or groups to the role. Any user assigned to a role can then perform all of the operations in all of the tasks that are assigned to the role.

There are four general steps to setting up role-based access control for Hyper-V:

1. Define scope according to your organizational needs. For example, you can define scopes by geography, organizational structure, function (developer/test or production), or Active Directory Domain Services. For a sample script to create the scopes, see http://go.microsoft.com/fwlink/?LinkId=134074.

2. Define tasks. In Authorization Manager, you cannot change or create new operations. However, you can create as many tasks as you want and then combine these into role definitions. For example tasks that you can use in your role definitions, see Appendix A: Example Authorization Manager Tasks and Operations.
3. Create roles. For example, if you want to create an “IT Monitor” role that you can use to view properties of a virtual machine but not interact with the virtual machine, create a new task in Authorization Manager called “Monitor Virtual Machine”, with the following operations:
   - Read Service Configuration
   - View External Ethernet Ports
   - View Internal Ethernet Ports
   - View LAN Endpoints
   - View Switch Ports
   - View Switches
   - View Virtual Switch Management Service
   - View LAN Settings

4. Assign users or groups to roles.
   For example, assume you have two sets of virtual machines where one set belongs to the Human Resources department and the other set belongs to the Finance department. You want the virtual machine administrators for Human Resources to have full control over the virtual machines for that department, but to have no control over the virtual machines in Finance. You want the same arrangement for the virtual machine administrators for Finance—no access to the virtual machines in Human Resources. To accomplish this, you would define one role called “Departmental Virtual Machine Administrator”, define the appropriate tasks, and then assign each administrator to the “Departmental Virtual Machine Administrator” role assignment in the specific scope. You would scope the virtual machine administrators for Human Resources to the virtual machines in Human Resources and the virtual machine administrators for Finance to the virtual machines in Finance. Then, you would assign the virtual machines to their respective scopes.

**Configuring role-based access control**

Use the following procedures to set up role-based access control for virtual machines in Hyper-V.

⚠️ Important

To complete these procedures, you must open Authorization Manager using an account that is a member of the Administrators group.

▶ To create a scope

1. Open Authorization Manager by running `azman.msc` from a command prompt.
   
   The default authorization policy is XML-based and stored at `\ProgramData\Microsoft\Windows\Hyper-V\InitialStore.xml`.
   
   📝 Note

   Note that `\ProgramData\` is in a hidden directory, you cannot browse to it. Type the location in **Store Name** in the **Open Authorization Store** dialog box.

2. In the console tree, right-click **Hyper-V services** and then click **New Scope**.
3. In the New Scope dialog box, in Name, type a name for the scope and then click OK.
4. (Optional) In Description, type a description for the scope and then click OK.
   The description has a maximum size limit of 1024 bytes. Enter a description that will help you apply the scope to achieve your goal. For example, you can use a description to distinguish the Human Resources scope from the Finance scope.

►To create a task
1. Open Authorization Manager by running azman.msc from a command prompt.
2. In the console tree, right-click the scope, and then click Definitions.
3. In the console tree, right-click Task Definitions and then click New Task Definition.
4. In the New Task Definition dialog box, in Name, type a name for the task.
5. Click Add to bring up the Add Definition dialog box and click the Operations tab.
6. In Operations, select each operation in the task, and then click OK.

►To create a role
1. Open Authorization Manager by running azman.msc from a command prompt.
2. Expand the scope, click Definitions, right-click Role Definition, and then click New Role Definition.
   The description has a maximum size limit of 1024 bytes.
3. In the New Role Definition dialog box, in Name, type a name for the role.
4. In Description, type a description for the role and then click OK twice.
5. (Optional) Click Add to specify the operations, tasks, roles, and authorization rules that you want to include, and then click OK twice.

►To assign a role
1. Open Authorization Manager by running azman.msc from a command prompt.
2. Expand the scope, right-click Role Assignments, and click New Role Assignment.
3. In the Add Role dialog box, check the role definitions to add and then click OK.
4. Right-click the role, click Assign Users and Groups, and then click From Windows and Active Directory or From Authorization Manager.
5. In the Select Users, Computers, or Groups dialog box, enter object names to select, and then click OK.

Additional resources
- Scopes in Authorization Manager (http://go.microsoft.com/fwlink/?LinkId=134198)
- Work With Scopes (http://go.microsoft.com/fwlink/?LinkId=134199)
- Authorization Manager How To… (http://go.microsoft.com/fwlink/?LinkId=134086)
Planning for Backup

When you plan a backup and recovery strategy for a virtualized server environment, there are several factors to consider. You must consider the different types of backups you can make, the state of the virtual machine, and the type of storage being used by the virtual machines. This topic discusses the advantages, disadvantages, and considerations for these factors.

Note

This topic discusses considerations for backup strategies that are implemented using backup applications that support the Hyper-V Volume Shadow Copy Service (VSS) writer. VSS snapshots are not the same as virtual machine snapshots. This topic does not cover the use of virtual machine snapshots because we do not recommend them as a permanent data or system recovery solution. Virtual machine snapshots are intended mainly for use in development and test environments because they provide a convenient way to store different points of system state, data, and configuration. However, there are some inherent risks of unintended data loss if they are not managed appropriately. For more information about virtual machine snapshots, see [http://go.microsoft.com/fwlink/?LinkId=133342](http://go.microsoft.com/fwlink/?LinkId=133342).

Understanding backup options and considerations

The backup integration service (identifiable as Hyper-V Volume Shadow Copy Requestor service in the guest operating system) and the Hyper-V Volume Shadow Copy Service (VSS) writer provide the mechanism for backing up virtual machines as well as system-wide settings that apply to Hyper-V. To implement the backup and recovery scenarios discussed in this section, you must use a backup application that is compatible with the Hyper-V VSS writer. If you want to use Windows Server Backup, you must add a registry key to register the Hyper-V VSS writer. For more information, see [http://go.microsoft.com/fwlink/?LinkID=133354](http://go.microsoft.com/fwlink/?LinkID=133354).

There are two basic methods you can use to perform a backup. You can:

- Perform a backup from the server running Hyper-V. We recommend that you use this method to perform a full server backup because it captures more data than the other method. If the backup application is compatible with Hyper-V and the Hyper-V VSS writer, you can perform a full server backup that helps protect all of the data required to fully restore the server, except the virtual networks. The data included in such a backup includes the configuration of virtual machines, snapshots associated with the virtual machines, and virtual hard disks used by the virtual machines. As a result, using this method can make it easier to recover the server if you need to, because you do not have to recreate virtual machines or reinstall Hyper-V. However, virtual networks are not included in a full server backup. You will need to reconfigure the virtual networking by recreating the virtual networks and then reattaching the virtual network adapters in each virtual machine to the appropriate virtual
network. As part of your backup planning, make sure you document the configuration and all relevant settings of your virtual network if you want to be able to recreate it.

- **Perform a backup from within the guest operating system of a virtual machine.** Use this method when you need to back up data from storage that is not supported by the Hyper-V VSS writer. When you use this method, you run a backup application from the guest operating system of the virtual machine. If you need to use this method, you should use it in addition to a full server backup and not as an alternative to a full server backup. Perform a backup from within the guest operating system before you perform a full backup of the server running Hyper-V. For more information about storage considerations, see the following section.

### Storage considerations

As you plan your backup strategy, consider the compatibility between the storage and backup solutions:

- **Virtual hard disks.** These offer the best compatibility and can be stored on many types of physical media. For more information about the types of storage you can use with Hyper-V, see [Hardware Considerations](#).

- **Physical disks that are directly attached to a virtual machine.** These disks cannot be backed up by the Hyper-V VSS writer. As a result, this type of disk will not be included in any backup performed by a backup program that uses the Hyper-V VSS writer. In this situation, you would need to use some other process to back up the physical disk, such as running a backup application within the guest operating system.

- **iSCSI-based storage.** This storage is supported for backup by the Hyper-V VSS writer when the storage is connected through the management operating system and the storage is used for virtual hard disks.

- **Storage accessed from a virtual machine by using an Internet SCSI (iSCSI) initiator within the guest operating system.** This storage will not be included in a backup of the physical computer. In this scenario, you must use another process to back up the data from the iSCSI-based storage before you perform a full server backup. For example, you could run a backup of the data on the iSCSI storage from a backup application running in the guest operating system.

For more information about deploying storage for Hyper-V, see [Implementing Disks and Storage](#).

### Understanding online and offline backups

Whether a backup is performed online or offline depends on whether the backup can be performed without downtime.

You can perform an online backup with no downtime on a running virtual machine when all of the following conditions are met:

- Integration services are installed and the backup integration service has not been disabled.
All disks being used by the virtual machine are configured within the guest operating system as NTFS-formatted basic disks. Virtual machines that use storage on which the physical partitions have been formatted as dynamic disks or the FAT32 file system prevent an online backup from being performed. This is not the same as dynamically expanding virtual hard disks, which are fully supported by backup and restore operations.

Volume Shadow Copy Service must be enabled on all volumes used by the virtual machine with a specific configuration. Each volume must also serve as the storage location for shadow copies of the volume. For example, the shadow copy storage for volume C: must be located on C:

If an online backup cannot be performed, then an offline backup is taken. This type of backup results in some degree of downtime. A variety of factors can affect the time required to take an offline backup. If the virtual machine is running or paused, it is put into a saved state as part of the offline backup process. After the backup is completed, the virtual machine is returned to its existing state.

Understanding the restore process

The restore process is straightforward as long as the recommendations outlined in the previous sections were followed when the backups were created. This includes taking the recommended steps to ensure that data which is not included in a full server backup can be recovered or recreated.

To restore when all components of your backup set are supported by the Hyper-V VSS writer, have all the media and equipment available and then perform a restore of the entire system or the virtual machine, depending on your circumstances. The Hyper-V VSS writer treats Hyper-V as an application that can be backed up. This means that you can recover individual virtual machines. However, you cannot use this method to recover only a portion of a virtual machine.

To restore when your backup set includes media that is not supported by the Hyper-V VSS writer, you must perform an additional step. First, perform a restore of the entire system or the virtual machine, depending on your circumstances. Then, restore the unsupported media from within the guest operating system.

Note

If you attempt to restore a virtual machine while it is running, it is turned off and deleted before the backed-up version of the virtual machine is restored.

Note

If you restore a virtual machine from an online backup, when you start the virtual machine you may receive a message that the operating system was not shut down properly. You can ignore this message.
Considerations about clustered virtual machines

If you plan to cluster virtual machines, there are additional factors that you need to consider when planning to backup and restore those virtual machines. Before you attempt to back up or restore clustered virtual machines, consider the following:

- Apply a hotfix to prevent possible failure of a full server backup on a node when a virtual machine uses a volume mounted with a GUID. When the hotfix applied, a directory path that cannot be resolved will prevent only the virtual machine that uses the directory path from being backed up. However, when the hotfix is not applied, a volume mounted with a GUID may cause the entire backup operation to fail. For more information, see http://go.microsoft.com/fwlink/?LinkId=133348.

- You may need to take the virtual machine offline before you run a backup or restore a virtual machine. For instructions on taking a clustered virtual machine offline, see http://go.microsoft.com/fwlink/?LinkId=129063.

Several factors can affect backup and recovery operations when a virtual machine is clustered. The following tables identify the factors you need to consider and the action you need to take to perform the backup or recovery operation. The information in both tables assumes that you will run the backup or recovery operation on node 1.

**Considerations for backing up clustered virtual machines**

<table>
<thead>
<tr>
<th>Location of cluster group</th>
<th>Cluster resource state</th>
<th>Configuration resource state</th>
<th>Storage resource state</th>
<th>Backup type</th>
<th>Action required to prepare for a backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td>Online</td>
<td>Online</td>
<td>Online</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>Node 1</td>
<td>Online</td>
<td>Online</td>
<td>Online</td>
<td>Offline (due to storage configuration of the virtual machine)</td>
<td>Use the Cluster service to take the virtual machine cluster resource offline</td>
</tr>
<tr>
<td>Node 1</td>
<td>Offline</td>
<td>Offline</td>
<td>Online</td>
<td>Offline</td>
<td>None</td>
</tr>
<tr>
<td>Node 1</td>
<td>Offline</td>
<td>Online</td>
<td>Offline</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Node 2</td>
<td>Any state</td>
<td>Any state</td>
<td>Any state</td>
<td>Virtual machine not reported for backup on node 1</td>
<td>Move the virtual machine to node 1</td>
</tr>
</tbody>
</table>
Considerations for restoring clustered virtual machines

<table>
<thead>
<tr>
<th>Location</th>
<th>Cluster resource state</th>
<th>Configuration resource state</th>
<th>Storage resource state</th>
<th>Action required to prepare for a restore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td>Online</td>
<td>Online</td>
<td>Online</td>
<td>Take the cluster resource and configuration resource offline.</td>
</tr>
<tr>
<td>Node 1</td>
<td>Offline</td>
<td>Online</td>
<td>Online</td>
<td>Take the configuration resource offline.</td>
</tr>
<tr>
<td>Node 1</td>
<td>Offline</td>
<td>Offline</td>
<td>Offline</td>
<td>None</td>
</tr>
<tr>
<td>Node 2</td>
<td>Any state</td>
<td>Any state</td>
<td>Any state</td>
<td>The cluster resource and the configuration resource need to be taken offline on Node 2 to avoid a conflict.</td>
</tr>
</tbody>
</table>

Installing Hyper-V

The release version of the Hyper-V technology in Windows Server 2008 is distributed in update packages that are available from the Microsoft Web site. To install the release version of any of the Hyper-V components, you must obtain and install the appropriate update package. This topic describes the packages and provides links to the installation procedures for each package.

About the Hyper-V update packages

Several update packages are available. Each update package is described below, including information about how to obtain the package.

Hyper-V role package

The release version of Hyper-V is distributed in the package 'Hyper-V Update for Windows Server 2008 x64 Edition (KB950050)'. The package consists of the Hyper-V role, including the x64 version of the remote management tools, and integration services for the supported versions of the Windows operating system.
This update is offered through Windows Update as a recommended update. However, you also can obtain the update through the Microsoft Download Center. To download this update, see http://go.microsoft.com/fwlink/?LinkId=123539.

⚠️ Important
The Hyper-V role update package is a permanent package. Once you install the update package, you cannot remove it.

For instructions about installing the role, see Install the Hyper-V Role on a Server Core Installation of Windows Server 2008 or Install the Hyper-V Role on a Full Installation of Windows Server 2008.

If you used a prerelease version of Hyper-V to create virtual machines and installed integration services on the virtual machines, you must upgrade the integration services to the release version. Integration services are specific to the build of Hyper-V. To install the integration services, from the Action menu of Virtual Machine Connection, click Insert Integration Services Setup Disk. On Windows operating systems, if the New Hardware Wizard appears, you must close the wizard to start the installation. If Autorun does not start the installation automatically, you can start it manually. Click anywhere in the guest operating system window and navigate to the CD drive. Use the method that is appropriate for the guest operating system to start the installation package from the CD drive.

If you are interested in migrating from Virtual Server to Hyper-V, a migration guide is available. For more information, see the Virtual Machine Migration Guide.

### Hyper-V Remote management tools packages

The Hyper-V management tools are available separately to allow remote management of a server running Hyper-V. Packages are available to install the tools on Windows Vista with Service Pack 1 (SP1) and on 32-bit editions of Windows Server 2008. The following download packages are available:

- For 64-bit editions of Windows Vista with SP1, see [http://go.microsoft.com/fwlink/?LinkId=123540](http://go.microsoft.com/fwlink/?LinkId=123540).
- For 32-bit editions of Windows Vista with SP1, see [http://go.microsoft.com/fwlink/?LinkId=123541](http://go.microsoft.com/fwlink/?LinkId=123541).
- For 32-bit editions of Windows Server 2008, see [http://go.microsoft.com/fwlink/?LinkId=123542](http://go.microsoft.com/fwlink/?LinkId=123542).

⚠️ Important
The remote management tools update package for the 32-bit editions of Windows Server 2008 is a permanent package. Once you install the update package, you cannot remove it.

For instructions about installing the tools, see Install and Configure Hyper-V Tools for Remote Administration.
Hyper-V Language Pack for Windows Server 2008

The Hyper-V Language Pack for Windows Server 2008 installs the language pack for the release version of Hyper-V and supports the following additional languages:

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Hungarian
- Korean
- Polish
- Portuguese (Brazil)
- Portuguese (Portugal)
- Russian
- Swedish
- Turkish

For more information about the language pack and links to download the packs, see article 951636 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkID=123536).

Additional considerations

- To find out whether an update has been applied to your computer, you can check the update history:
  - On a full installation of Windows Server 2008, click Start, click Windows Update, click View update history, and then click Installed Updates.
  - On a Server Core installation, at the command prompt, type:
    `wmic qfe list`
    Look for update number `kbid=950050`, which indicates that the update for Hyper-V has been installed.

Install the Hyper-V Role on a Server Core Installation of Windows Server 2008

The Server Core installation option of the Windows Server 2008 operating system installs a minimal server installation of Windows Server 2008 to run supported server roles, including the Hyper-V role. You can use the Server Core installation option to help secure the server running Hyper-V and all the virtual machines running on it. The benefits of using the Server Core installation option include a reduced attack surface and reduced maintenance. For information about the minimum hardware requirements for a server running a Server Core installation, see Installing Windows Server 2008 (http://go.microsoft.com/fwlink/?LinkID=123538).
When you select the Server Core installation option, Setup installs only the files that are required for the supported server roles. For example, the Explorer shell is not installed as part of a Server Core installation. After you have enabled the Hyper-V role, you can manage the Hyper-V role and virtual machines remotely using the Hyper-V management tools. The management tools are available for Windows Server 2008 and Windows Vista Service Pack 1 (SP1). For more information, see article 950050 (http://go.microsoft.com/fwlink/?LinkId=122188) and article 952627 (http://go.microsoft.com/fwlink/?LinkId=123537) in the Microsoft Knowledge Base. For more information about configuring tools for the remote management of Hyper-V, see Install and Configure Hyper-V Tools for Remote Administration.

You can use unattended installation to configure a server running a Server Core installation and Hyper-V. For more information about unattended installation settings, see the Windows Automated Installation Kit (http://go.microsoft.com/fwlink/?LinkId=81030). You can find more information and a sample Unattend.xml file in the Server Core Installation Option of Windows Server 2008 Step-By-Step Guide (http://go.microsoft.com/fwlink/?LinkID=100959). This guide is also available as a download (http://go.microsoft.com/fwlink/?LinkID=68556).

**Important**

- Once you install these server updates, you will not be able to remove them. There is no way to upgrade from a full installation of Windows Server 2008 or a previous version of Windows Server to a Server Core installation. Only a clean installation is supported. There is no way to upgrade from a Server Core installation to a full installation of Windows Server 2008. If you need the Windows user interface or a server role that is not supported in a Server Core installation, you should install a full installation of Windows Server 2008. For instructions about installing the Hyper-V role on a full installation of Windows Server 2008, see Install the Hyper-V Role on a Full Installation of Windows Server 2008.

- If you close all local command prompts while installing the Hyper-V role, you will have no way to manage the Server Core installation. If this happens, press CTRL+ALT+DELETE, click Start Task Manager, click File, click Run, and type cmd.exe. Alternatively, you can log off and log on again.

**To install Hyper-V on a Server Core installation**

1. You must perform a Server Core installation before you install the Hyper-V role. For instructions, see the Server Core Installation Option of Windows Server 2008 Step-By-Step Guide (http://go.microsoft.com/fwlink/?LinkID=100959).

2. After you have installed Windows Server 2008, you must apply the Hyper-V update packages for Windows Server 2008 (KB950050). For links and more information about installing the update for the release version of the Hyper-V technology for Windows Server 2008, see Installing Hyper-V. You should also apply any other required updates before you install the Hyper-V role.

To view the list of software updates and check if any are missing, at the command prompt, type:
wmic qfe list
If you do not see “kbid=950050”, download the Hyper-V updates and then type the following command at a command prompt:

`wusa.exe Windows6.0-KB950050-x64.msu /quiet`

There are three update packages. After you install the updates, you must restart the server. The Update for Windows Server 2008 x64 Edition (KB 950050) and Language Pack for Hyper-V (KB951636) must be installed on the parent partition of the Server Core installation.

The Update for Windows Server 2008 (KB952627) is for remote management of the Server Core installation if you are managing the server from a computer running Windows Vista Service Pack 1 (SP1), and must be installed on the computer running Windows Vista SP1.

**Important**

Before you enable the Hyper-V role, ensure that you have enabled the required hardware-assisted virtualization and hardware-enforced Data Execution Prevention (DEP) BIOS settings. Checks for these settings are performed before you enable the Hyper-V role on a full installation, but not on a Server Core installation.

After you make the BIOS configuration changes to enable the required hardware features, you may need to turn off the power to the computer and then turn it back on (restarting the computer may not apply the changes to the settings). If you enable the Hyper-V role without modifying the BIOS settings, the Windows hypervisor may not work as expected. If this happens, check the event log for details, modify the BIOS settings according to the server hardware manufacturer instructions, turn off and turn on the computer running a Server Core installation, and then install Hyper-V again.

To check if your server hardware is compatible, see the Windows Server catalog ([http://go.microsoft.com/fwlink/?LinkId=123535](http://go.microsoft.com/fwlink/?LinkId=123535)). Click the list of **Certified Servers**, and then click **By additional qualifications – Hyper-V**. For instructions about how to enable the BIOS settings, check with your hardware manufacturer.

**Additional references**

- OCSetup Command-Line Options ([http://go.microsoft.com/fwlink/?LinkId=123532](http://go.microsoft.com/fwlink/?LinkId=123532))
- Command Reference ([http://go.microsoft.com/fwlink/?LinkId=91473](http://go.microsoft.com/fwlink/?LinkId=91473))
- Server Core installation blog on TechNet ([http://go.microsoft.com/fwlink/?LinkId=123531](http://go.microsoft.com/fwlink/?LinkId=123531))
Install the Hyper-V Role on a Full Installation of Windows Server 2008

Installing the Hyper-V role on a full installation of Windows Server 2008 installs all the components of the Hyper-V technology, including the remote management tools. The tools consist of Hyper-V Manager, which is a Microsoft Management Console (MMC) snap-in, and Virtual Machine Connection, which provides you with direct access to a virtual machine through a network connection.

The release version of this role is distributed in an update package. We recommend that you obtain and apply the update package before you install and begin using the Hyper-V role. For more information about the update packages for Hyper-V, see Installing Hyper-V.

Important

If you have installed an earlier version of Hyper-V, we strongly recommend that you review the information about migrating to the release version of Hyper-V before you apply the update package. Some components cannot be migrated, as explained in the support article that describes the role update package. For more information, see article 950050 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=122188).

Important

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

To install the Hyper-V role

1. If you recently installed Windows Server 2008, Initial Configuration Tasks may be displayed. You can install Hyper-V from Initial Configuration Tasks or from Server Manager:
   - In Initial Configuration Tasks, under Customize This Server, click Add roles.
   - In Server Manager, under Roles Summary, click Add Roles. (If Server Manager is not running, click Start, point to Administrative Tools, click Server Manager, and then, if prompted for permission to continue, click Continue.

2. On the Select Server Roles page, click Hyper-V.

3. On the Create Virtual Networks page, click one or more network adapters if you want to make their connection to a physical network available to virtual machines.

4. On the Confirm Installation Selections page, click Install.

5. The computer must be restarted to complete the installation. Click Close to finish the wizard, and then click Yes to restart the computer.

6. After you restart the computer, log on with the same account you used to install the role. After the Resume Configuration Wizard completes the installation, click Close to finish the wizard.
Additional considerations

- You can create a virtual network when you install the Hyper-V role. This action changes the configuration of the physical network adapter you selected when you installed the role. For more information about how a physical network adapter operates after you associate it to a virtual network, see Configuring Virtual Networks.
- You can install the management tools on some versions of Windows without installing the Hyper-V role. For more information about installing the tools without installing the Hyper-V role, see Install and Configure Hyper-V Tools for Remote Administration.
- When the Hyper-V role is installed, the use of Virtual Server or Virtual PC on the computer is not supported.

Install and Configure Hyper-V Tools for Remote Administration

You can install the Hyper-V management tools on a full installation of Windows Server 2008 and on Windows Vista Service Pack 1 (SP1). This topic describes how to install and configure the tools.

Note

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

Installing the management tools

Installing the tools consists of obtaining and applying the appropriate update to the operating system.

To install the management tools

1. Obtain the appropriate update package for the operating system on which you want to install the tools. For more information, see Installing Hyper-V.
2. Install the update package using the method appropriate for the way you obtained the package:
   - If you obtained the update from Windows Update and the computer is not set up to install updates automatically, install the update manually.
   - If you obtained the update from the Microsoft Download Center, download the file to the computer and then double-click the .msu file.
3. If you are installing the tools on Windows Vista SP1, no additional installation steps are required, so you can proceed to the configuration instructions. If you are installing the tools on Windows Server 2008, complete the remaining steps.
4. Open Server Manager. (If Server Manager is not running, click Start, point to Administrative Tools, click Server Manager, and then, if prompted for permission to continue, click Continue.)

5. In Server Manager, under Features Summary, click Add Features.


7. Click Hyper-V Tools, and then proceed through the rest of the wizard.

**Configuring the management tools**

The configuration process consists of modifying various components that control access and communications between the server running Hyper-V and the computer on which you will run the Hyper-V management tools.

![Note]

No additional configuration is required if you are using the management tools on a computer running Windows Server 2008 and the same user account is a member of the Administrators group on both computers.

**Configuring the server running Hyper-V**

The following procedures describe how to configure the server running Hyper-V. When domain-level trust is not established, perform all the steps. When domain-level trust exists but the remote user is not a member of the Administrators group on the server running Hyper-V, you must modify the authorization policy, but you can skip the steps for modifying the Distributed COM Users group and the Windows Management Instrumentation (WMI) namespaces.

![Note]

The following procedures assume that you have installed the Hyper-V role on the server. For instructions about installing the Hyper-V role, see [Install the Hyper-V Role on a Full Installation of Windows Server 2008](#) or [Install the Hyper-V Role on a Server Core Installation of Windows Server 2008](#).

To configure the Hyper-V role for remote management on a full installation of Windows Server 2008

1. Enable the firewall rules for Windows Management Instrumentation. From an elevated command prompt, type:

   ```
   netsh advfirewall firewall set rule group=“Windows Management Instrumentation (WMI)” new enable=yes
   ```

   The command has succeeded when it returns the following message: "Updated 4 rules(s). Ok."

   ![Note]
To verify that the command succeeded, you can view the results in Windows Firewall with Advanced Security. Click Start, click Control Panel, switch to Classic View if you are not using that view, click Administrative Tools, and then click Windows Firewall with Advanced Security. Select inbound rules or outbound rules and then sort by the Group column. There should be three inbound rules and one outbound rule enabled for Windows Management Instrumentation.

2. The next steps configure the authorization policy for the server running the Hyper-V role. If the user who requires remote access to the server running Hyper-V belongs to the Administrators group on both computers, then it is not necessary to configure the authorization policy.

   Note
   The instructions for configuring the authorization policy assume that the default authorization policy has not been modified, including the default location, and that the account you are configuring for remote access requires full administrative access to the Hyper-V role.

3. Click Start, click Start Search and type azman.msc. If you are prompted to confirm the action, click Continue. The Authorization Manager Microsoft Management Console (MMC) snap-in opens.

4. In the navigation pane, right-click Authorization Manager and click Open Authorization Store. Make sure that XML file is selected. Browse to the %system drive%\Program Data\Microsoft\Windows\Hyper-V folder, select InitialStore.xml, click Open and then click OK.

   Note
   The Program Data folder is a hidden folder by default. If the folder is not visible, type: <system_drive>\ProgramData\Microsoft\Windows\Hyper-V\Inititalstore.xml

5. In the navigation pane, click Hyper-V services, and then click Role Assignments. Right-click Administrator, point to Assign Users and Groups, and then point to From Windows and Active Directory. In the Select Users, Computers, or Groups dialog box, type the domain name and user name of the user account, and then click OK.


7. Next, you add the remote user to the Distributed COM Users group to provide access to the remote user. Click Start, point to Administrative tools, and click Computer Management. If User Account Control is enabled, click Continue. Component Services opens.

8. Expand Local Users and Groups, and then click Groups. Right-click Distributed COM Users and click Add to Group.

9. In the Distributed COM Users Properties dialog box, click Add.

10. In the Select Users, Computers, or Groups dialog box, type the name of the user and
11. Click **OK** again to close the **Distributed COM Users Properties** dialog box. Close Component Services.

12. The remaining steps grant the required WMI permissions to the remote user for two namespaces: the CIMV2 namespace and the virtualization namespace. Click **Start**, click **Administrative Tools**, and then click **Computer Management**.

13. In the navigation pane, click **Services and Applications**, right-click **WMI Control**, and then click **Properties**.

14. Click the **Security** tab, click **Root**, and then click **CIMV2**. Below the namespace list, click **Security**.

15. In the **Security for ROOT\CIMV2** dialog box, check to see if the appropriate user is listed. If not, click **Add**. In the **Select Users, Computers, or Groups** dialog box, type the name of the user and click **OK**.

16. On the **Security** tab, select the name of the user. Under **Permissions for <user or group name>**, click **Advanced**. On the **Permissions** tab, verify that the user you want is selected and then click **Edit**. In the **Permission Entry for CIMV2** dialog box, modify three settings as follows:

- For **Apply to**, select **This namespace and subnamespaces**.
- In the **Permissions** list, in the **Allow** column, select the **Remote Enable** check box.
- Below the **Permissions** list, select the **Apply these permissions to objects and/or containers within this container only** check box.

17. Click **OK** in each dialog box until you return to the **WMI Control Properties** dialog box.

18. Next, you repeat the process for the virtualization namespace. Scroll down if necessary until you can see the virtualization namespace. Click **virtualization**. Below the namespace list, click **Security**.

19. In the **Security for ROOT\virtualization** dialog box, check to see if the appropriate user is listed. If not, click **Add**. In the **Select Users, Computers, or Groups** dialog box, type the name of the user and click **OK**.

20. On the **Security** tab, select the name of the user. Under **Permissions for <user or group name>**, click **Advanced**. On the **Permissions** tab, verify that the user you want is selected and then click **Edit**. In the **Permission Entry for virtualization** dialog box, modify three settings as follows:

- For **Apply to**, select **This namespace and subnamespaces**.
- In the **Permissions** list, in the **Allow** column, select the **Remote Enable** check box.
- Below the **Permissions** list, select the **Apply these permissions to objects and/or containers within this container only** check box.

21. Click **OK** in each dialog box and then close Computer Management.

22. Restart the server to apply the changes to the authorization policy.
To configure the Hyper-V role for remote management on a Server Core installation of Windows Server 2008

1. Enable the firewall rules on the server for Windows Management Instrumentation. From an elevated command prompt, type:

   `netsh advfirewall firewall set rule group=“Windows Management Instrumentation (WMI)” new enable=yes`

   The command has succeeded when it returns the following message: “Updated 4 rules(s). Ok.”

2. Next, you modify the Distributed COM permissions to provide access to the remote user. Type:

   `net localgroup “Distributed COM Users” /add <domain_name>\<user_name>`

   where `<domain_name>` is the domain that the user account belongs to and `<user_name>` is the user account you want to grant remote access to.

3. Next, you connect remotely to the server running the Server Core installation so you can modify the authorization policy and the two WMI namespaces, using MMC snap-ins that are not available on the Server Core installation.

   Log on to the computer on which you will run the Hyper-V management tools, using a domain account that is a member of the Administrators group on the computer running a Server Core installation. (If you need to add this user, see the instructions in Install the Hyper-V Role on a Server Core Installation of Windows Server 2008.)

   **Note**

   The instructions for configuring the authorization policy assume that the default authorization policy has not been modified, including the default location, and that the account you are configuring for remote access requires full administrative access to the Hyper-V role.

4. Click Start, click Start Search and type `azman.msc`. If you are prompted to confirm the action, click Continue. The Authorization Manager snap-ins opens.

5. In the navigation pane, right-click Authorization Manager and click Open Authorization Store. Make sure that XML file is selected and type:

   `\<remote_computer>\c$\ProgramData\Microsoft\Windows\Hyper-V\initialstore.xml`

   where `<remote_computer>` is the name of the computer running the Server Core installation.

   Click Open and then click OK.

6. In the navigation pane, click Hyper-V services, and then click Role Assignments. Right-click Administrator, point to Assign Users and Groups, and then point to From Windows and Active Directory. In the Select Users, Computers, or Groups dialog box, type the domain name and user name of the user account, and then click OK.

7. Close Authorization Manager.

8. The remaining steps grant the required WMI permissions to the remote user for two
namespaces: the CIMV2 namespace and the virtualization namespace. Click **Start**, click **Administrative Tools**, and then click **Computer Management**.

9. In the navigation pane, click **Services and Applications**, right-click **WMI Control**, and then click **Properties**.

10. Click the **Security** tab. Click **Root** and then click **CIMV2**. Below the namespace list, click **Security**.

11. In the **Security for Root\CIMV2** dialog box, check to see if the appropriate user is listed. If not, click **Add**. In the **Select Users, Computers, or Groups** dialog box, type the name of the user and click **OK**.

12. On the **Security** tab, select the name of the user. Under **Permissions for <user or group name>**, click **Advanced**. On the **Permissions** tab, verify that the user you want is selected and then click **Edit**. In the **Permission Entry for CIMV2** dialog box, modify three settings as follows:
   - For **Apply to**, select **This namespace and subnamespaces**.
   - In the **Permissions** list, in the **Allow** column, select the **Remote Enable** check box.
   - Below the **Permissions** list, select the **Apply these permissions to objects and/or containers within this container only** check box.

13. Click **OK** in each dialog box until you return to the **WMI Control Properties** dialog box.

14. Next, you repeat the process for the virtualization namespace. Scroll down if necessary until you can see the virtualization namespace. Click **virtualization**. Below the namespace list, click **Security**.

15. In the **Security for Root\virtualization** dialog box, check to see if the appropriate user is listed. If not, click **Add**. In the **Select Users, Computers, or Groups** dialog box, type the name of the user and click **OK**.

16. On the **Security** tab, select the name of the user. Under **Permissions for <user or group name>**, click **Advanced**. On the **Permissions** tab, verify that the user you want is selected and then click **Edit**. In the **Permission Entry for virtualization** dialog box, modify three settings as follows:
   - For **Apply to**, select **This namespace and subnamespaces**.
   - In the **Permissions** list, in the **Allow** column, select the **Remote Enable** check box.
   - Below the **Permissions** list, select the **Apply these permissions to objects and/or containers within this container only** check box.

17. Click **OK** in each dialog box and then close Computer Management.

18. Restart the computer running a Server Core installation to apply the changes to the authorization policy.

**Configuring Windows Vista SP1**

The following procedure describes how to configure Windows Vista SP1 when domain-level trust is not established.
To configure Windows Vista SP1

1. Log on to the computer running Windows Vista SP1.
2. Enable the firewall rules for Windows Management Instrumentation. From an elevated command prompt, type:
   ```
   netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
   ```
   The command has succeeded when it returns the following message: “Updated 8 rules(s). Ok.”

   **Note**
   To verify that the command succeeded, you can view the results in Windows Firewall with Advanced Security. Click **Start**, click **Control Panel**, switch to Classic View if you are not using that view, click **Administrative Tools**, and then click **Windows Firewall with Advanced Security**. Select inbound rules or outbound rules and then sort by the **Group** column. There should be six inbound rules and two outbound rules enabled for Windows Management Instrumentation.

3. Enable a firewall exception for the Microsoft Management Console. From an elevated command prompt, type:
   ```
   Netsh firewall add allowedprogram program=%windir%\system32\mmc.exe name="Microsoft Management Console"
   ```
4. Start Hyper-V Manager to verify that you can connect remotely to the server. Click **Start**, click the **Start Search** box, type **Hyper-V Manager** and press ENTER. If you are prompted to confirm the action, click **Continue**. In Hyper-V Manager, under **Actions**, click **Connect to Server**. Type the name of the computer or browse to it, and click **OK**. If Hyper-V Manager can connect to the remote computer, the computer name will appear in the navigation pane and the results pane will list all the virtual machines configured on the server.

---

**Configuring Virtual Networks**

This section describes the basics of virtual networking in Hyper-V and the different types of virtual networks you can configure. Networking in Hyper-V works differently than networking in Virtual Server 2005, and these differences are also discussed. Before configuring a virtual network, you should determine the design and type of virtual network you plan to use. You should be aware that Hyper-V does not support wireless networks.

For step-by-step instructions to configure a virtual network, see Step-by-Step Guide to Getting Started with Hyper-V ([http://go.microsoft.com/fwlink/?LinkID=119207](http://go.microsoft.com/fwlink/?LinkID=119207)).
Virtual network types

You can create virtual networks on the server running Hyper-V to define various networking topologies for virtual machines and the virtualization server. Using Virtual Network Manager (accessed from Hyper-V Manager), you have three different types of virtual networks to choose from.

- **External virtual networks.** Use this type when you want to allow virtual machines to communicate with externally located servers and the management operating system (sometimes referred to as the parent partition). This type also allows virtual machines on the same physical server to communicate with each other.

- **Internal virtual networks.** Use this type when you want to allow communication between virtual machines on the same physical server and virtual machines and the management operating system. An internal virtual network is a virtual network that is not bound to a physical network adapter. It is commonly used to build a test environment where you need to connect to the virtual machines from the management operating system.

- **Private virtual networks.** Use this type when you want to allow communication only between virtual machines on the same physical server. A private virtual network is a virtual network without a virtual network adapter in the management operating system. Private virtual networks are commonly used when you want to isolate virtual machines from network traffic in the management operating system and in the external networks.

Virtual networking basics

While Hyper-V allows you to configure complex virtual network environments, the basic concept of virtual networking is straightforward. For a simple virtual network configuration, we recommend that you have at least two network adapters on the server running Hyper-V: one network adapter dedicated to the physical machine for remote management, and one or more network adapters dedicated to the virtual machines. If you are running an Internet SCSI (iSCSI) initiator for virtual hard disk storage, we recommend that you use additional network adapters in the management operating system. The management operating system is a partition that calls the Windows hypervisor and requests that new partitions are created. There can be only one management operating system. For information on the backup and recovery strategy for a virtualized server environment, see Planning for Backup.

When you add the Hyper-V role during a full installation of Windows Server 2008, you have the option to configure one or more external virtual networks.

**Note**

This option is not available when performing a Server Core installation of Windows Server 2008. The virtual network adapters can be renamed to reflect if they are assigned to the physical machine or the virtual machines.

When you install Hyper-V and create an external virtual network, the management operating system uses a new virtual network adapter to connect to the physical network. The network connections consist of the original network adapter and the new virtual network adapter. The
original physical network adapter does not have anything bound to it. However, the virtual network adapter has all of the standard protocols and services bound to it. Hyper-V binds the Virtual Network Service Protocol to a physical network adapter when an external virtual network is created. You should be aware that external network connectivity will be temporarily disrupted when an external virtual network is created or deleted. Once it is created, a virtual network works just like a physical network except that the switch is software based and ports can be added or removed dynamically as they are needed. Once an external virtual network is configured, all networking traffic is routed through the virtual switch. For this reason, we recommend using at least one additional physical network adapter for managing network traffic. The virtual switch functions as a physical switch would and routes networking traffic through the virtual network to its destination. The following image is an example of an external virtual network.

**External virtual network**

![Diagram of external virtual network]

For internal virtual networks, only communication between virtual machines on the same physical server and between virtual machines and the management operating system is allowed. The following image is an example of an internal virtual network.
Use a private virtual network when you want to allow communication only between virtual machines on the same physical server. The following image is an example of a private virtual network.
Networking and virtual machines

In Hyper-V, when a virtual machine is created and attached to a virtual network, it connects using a virtual network adapter. There are two types of network adapters available for Hyper-V: a network adapter and a legacy network adapter. For the network adapter to work, integration services must be installed, which is part of the Hyper-V installation. If integration services cannot be installed because of the version of the operating system, the network adapter cannot be used. Instead, you need to add a legacy network adapter that emulates an Intel 21140-based PCI Fast Ethernet Adapter and works without installing a virtual machine driver. A legacy network adapter also supports network-based installations because it includes the ability to boot to the Pre-Boot Execution Environment (PXE). The legacy network adapter is also required if a virtual machine needs to boot from a network. You will need to disable the network adapter after the PXE boot.

The virtual machine is logically connected to a port on the virtual network. For a networking application on the virtual machine to connect to something externally, it is first routed through the virtual network adapter to the virtual port on the external virtual network to which the virtual machine is attached. The networking packet is then directed to the physical network adapter and out to an external physical network.

For the virtual machine to communicate with the management operating system, there are two options. One option is to route the network packet through the physical network adapter and out to the physical network, which then returns the packet back to the server running Hyper-V using the second physical network adapter. Another option is to route the network packet through the virtual network, which is more efficient. The option selected is determined by the virtual network. The virtual network includes a learning algorithm, which determines the most efficient port to direct traffic to and will send the network packet to that port. Until that determination is made by the virtual network, network packets are sent out to all virtual ports.

Configuring virtual local area networks (VLANs)

Hyper-V supports virtual local area networks (VLANs), and because a VLAN configuration is software-based, computers can easily be moved and still maintain their network configurations. For each virtual network adapter you connect to a virtual machine, you can configure a VLAN ID for the virtual machine. You will need the following to configure VLANs:

- A physical network adapter that supports VLANs.
- A physical network adapter that supports network packets with VLAN IDs that are already applied.

On the management operating system, you will need to configure the virtual network to allow network traffic on the physical port. This is for the VLAN IDs that you want to use internally with virtual machines. Next, you configure the virtual machine to specify the virtual LAN that the virtual machine will use for all network communications.

There are two modes in which you can configure a VLAN: access mode and trunk mode. In access mode, the external port of the virtual network is restricted to a single VLAN ID in the UI. You can have multiple VLANs using WMI. Use access mode when the physical network adapter is connected to a port on the physical network switch that also is in access mode. To give a
virtual machine external access on the virtual network that is in access mode, you must configure the virtual machine to use the same VLAN ID that is configured in the access mode of the virtual network. Trunk mode allows multiple VLAN IDs to share the connection between the physical network adapter and the physical network. To give virtual machines external access on the virtual network in multiple VLANs, you need to configure the port on the physical network to be in trunk mode. You will also need to know the specific VLANs that are used and all of the VLAN IDs used by the virtual machines that the virtual network supports.

To allow Hyper-V to use a VLAN
1. Open Hyper-V Manager.
2. From the Actions menu, click Virtual Network Manager.
3. Select the virtual network you want to edit, and, in the right pane, check to select Enable virtual LAN identification.
4. Enter a number for the VLAN ID. All traffic for the management operating system that goes through the network adapter will be tagged with the VLAN ID you set.

To allow a virtual machine to use a VLAN
1. Open Hyper-V Manager.
2. In the results pane, under Virtual Machines, select the virtual machine that you want to configure to use a VLAN.
3. In the Action pane, under the virtual machine name, click Settings.
4. Under Hardware, select the virtual network adapter connected to the external virtual network.
5. In the right pane, select Enable virtual LAN identification, and then enter the VLAN ID you plan to use.

If you need the virtual machine to communicate using additional VLANs, connect additional network adapters to the appropriate virtual network and assign the VLAN ID. Make sure to configure the IP addresses correctly and that the traffic you want to move across the VLAN is also using the correct IP address.

Implementing Disks and Storage

This section describes the various storage options that a server running Hyper-V supports. It also generally discusses how to plan for storage, how to create a virtual hard disk, and how to configure storage.

You can use the following types of physical storage with a server that runs Hyper-V:
- **Direct-attached storage (storage attached to the management operating system).** You can use Serial Advanced Technology Attachment (SATA), external Serial Advanced
Technology Attachment (eSATA), Parallel Advanced Technology Attachment (PATA), Serial Attached SCSI (SAS), SCSI, USB, and Firewire.

- **Storage area networks (SANs).** You can use Internet SCSI (iSCSI), Fibre Channel, and SAS technologies.

**Note**

Network-attached storage (NAS) is not supported for Hyper-V.

For more information about the requirements and other considerations about hardware, see [Hardware Considerations](#).

## Determining your storage options on the management operating system

On the management operating system, you can select to use either virtual hard disks or physical disks that are directly attached to a virtual machine. Virtual hard disks can have a capacity of up to 2040 gigabytes and include the following types:

- **Fixed.** A fixed virtual hard disk is a disk that occupies physical disk space on the management operating system equal to the maximum size of the disk, regardless of whether a virtual machine requires the disk space. A fixed virtual hard disk takes longer to create than other types of disks because the allocated size of the .vhd file is determined when it is created. This type of virtual hard disk provides improved performance compared to other types because fixed virtual hard disks are stored in a contiguous block on the management operating system.

- **Dynamically expanding.** A dynamically expanding virtual hard disk is a disk in which the size of the .vhd file grows as data is written to the disk. This type provides the most efficient use of disk space. You will need to monitor the available disk space to avoid running out of disk space on the management operating system.

- **Differencing.** A differencing virtual hard disk stores the differences from the virtual hard disk on the management operating system. This allows you to isolate changes to a virtual machine and keep a virtual hard disk in an unchanged state. The differencing disk on the management operating system can be shared with virtual machines and, as a best practice, must remain read-only. If it is not read-only, the virtual machine's virtual hard disk will be invalidated.

With virtual hard disks, each virtual machine supports up to 512 TB of storage. Physical disks that are directly attached to a virtual machine have no size limit other than what is supported by the guest operating system. Physical disks are discussed in more detail later in this document in [How to configure physical disks that are directly attached to a virtual machine](#).
Determining your storage options on virtual machines

You can select either integrated device electronics (IDE) or SCSI devices on virtual machines:

- **IDE devices.** Hyper-V uses emulated devices with IDE controllers. You can have up to two IDE controllers with two disks on each controller. The startup disk (sometimes referred to as the boot disk) must be attached to one of the IDE devices. The startup disk can be either a virtual hard disk or a physical disk. Although a virtual machine must use an IDE device as the startup disk to start the guest operating system, you have many options to choose from when selecting the physical device that will provide the storage for the IDE device. For example, you can use any of the types of physical storage identified in the introduction section.

- **SCSI devices.** Each virtual machine supports up to 256 SCSI disks (four SCSI controllers with each controller supporting up to 64 disks). SCSI controllers use a type of device developed specifically for use with virtual machines and use the virtual machine bus to communicate. The virtual machine bus must be available when the guest operating system is started. Therefore, virtual hard disks attached to SCSI controllers cannot be used as startup disks.

**Note**

Although the I/O performance of physical SCSI and IDE devices can differ significantly, this is not true for the virtualized SCSI and IDE devices in Hyper-V. Hyper-V IDE and SCSI devices both offer equally fast I/O performance when integration services are installed in the guest operating system.

The following table describes the various storage options available with IDE devices:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Local IDE virtual hard disk</th>
<th>Local directly attached IDE</th>
<th>Remote IDE virtual hard disk</th>
<th>Remote directly attached IDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage type</td>
<td>Direct-attached storage</td>
<td>Direct-attached storage</td>
<td>SAN, Fibre Channel/iSCSI</td>
<td>SAN, Fibre Channel/iSCSI</td>
</tr>
<tr>
<td>Type of disk that is exposed to the management operating system</td>
<td>Virtual hard disk on NTFS</td>
<td>Physical disk directly attached to a virtual machine</td>
<td>Virtual hard disk on NTFS</td>
<td>Physical disk directly attached to a virtual machine</td>
</tr>
<tr>
<td>Maximum supported disk size on virtual machine</td>
<td>2 terabytes</td>
<td>No size limit other than what is supported by the guest operating system</td>
<td>2 terabytes</td>
<td>No size limit other than what is supported by the guest operating system</td>
</tr>
</tbody>
</table>
The following table describes the various storage options available with SCSI devices:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Local SCSI virtual hard disk</th>
<th>Local directly attached SCSI</th>
<th>Remote SCSI virtual hard disk</th>
<th>Remote directly attached SCSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage type</td>
<td>Direct-attached storage</td>
<td>Direct-attached storage</td>
<td>SAN, Fibre Channel/iSCSI</td>
<td>SAN, Fibre Channel/iSCSI</td>
</tr>
<tr>
<td>Type of disk that is exposed to the management operating system</td>
<td>Virtual hard disk on NTFS</td>
<td>Physical disk directly attached to a virtual machine</td>
<td>Virtual hard disk on NTFS</td>
<td>Physical disk directly attached to a virtual machine</td>
</tr>
<tr>
<td>Maximum supported disk size on virtual machine</td>
<td>2 terabytes</td>
<td>No size limit other than what is supported by the guest operating system</td>
<td>2 terabytes</td>
<td>No size limit other than what is supported by the guest operating system</td>
</tr>
<tr>
<td>Virtual hard disk snapshots are supported</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### How to create virtual hard disks

You can use virtual hard disks as a storage option on the management operating system, and then make the storage available to virtual machines.

You can create and manage virtual hard disks using the Hyper-V Manager tool. To create a new virtual hard disk, you would use either the New Virtual Hard Disk Wizard or the New Virtual Machine Wizard. If you are creating dynamically expanding disks, the New Virtual Machine Wizard provides a way to create storage for the new virtual machine without running the New Virtual Hard Disk Wizard. This can be useful if you want to install a guest operating system in a virtual machine soon after you create it.

When creating a new virtual hard disk, a name and storage location is required. The disks are stored as .vhd files, which makes them portable but also poses a potential security risk. You should mitigate this risk by taking precautions such as storing the .vhd files in a secure location. Do not create the virtual hard disk in a folder that is marked for encryption. Hyper-V does not support the use of storage media if Encrypting File System has been used to encrypt the .vhd file. However, you can use files stored on a volume that uses Windows Bitlocker Drive Encryption.

#### To create a virtual hard disk

1. Open Hyper-V Manager. Click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the Action pane, click **New**, and then click **Hard Disk**.
3. Proceed through the pages of the wizard to customize the virtual hard disk. You can click **Next** to move through each page of the wizard, or you can click the name of a page in the left pane to move directly to that page.
4. After you have finished configuring the virtual hard disk, click **Finish**.

---

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Local SCSI virtual hard disk</th>
<th>Local directly attached SCSI</th>
<th>Remote SCSI virtual hard disk</th>
<th>Remote directly attached SCSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamically expanding virtual hard disk</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Differencing virtual hard disk</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Ability of virtual machines to dynamically (&quot;hot-add&quot;) access any disk</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
How to configure physical disks that are directly attached to a virtual machine

You can use physical disks that are directly attached to a virtual machine as a storage option on the management operating system. This allows virtual machines to access storage that is mapped directly to the server running Hyper-V without first configuring the volume. The storage can be either a physical disk which is internal to the server, or a SAN logical unit number (LUN) that is mapped to the server (a LUN is a logical reference to a portion of a storage subsystem). The virtual machine must have exclusive access to the storage, so the storage must be set in an Offline state in Disk Management. The storage is not limited in size, so it can be a multiterabyte LUN.

When using physical disks that are directly attached to a virtual machine, you should be aware of the following:

- This type of disk cannot be dynamically expanded.
- You cannot use differencing disks with them.
- You cannot take virtual hard disk snapshots.

To configure physical disks that are directly attached to a virtual machine

1. Map the storage device you plan to use to the server running Hyper-V. In Disk Management, the storage appears as a raw volume and is in an Offline state.
2. To initialize the raw volume, in Disk Management, right-click the disk you want to initialize, and then click Initialize Disk. Note that before you can initialize the disk, it must be in an Online state.
3. In the Initialize Disk dialog box, select the disk to initialize. You can select whether to use the master boot record (MBR) or GUID partition table (GPT) partition style.
4. After a disk is initialized, return it to an Offline state. If the disk is not in an Offline state, it will not be available when configuring storage for a virtual machine.
5. Follow the steps in “To create a virtual hard disk” and make sure to select Attach a virtual hard disk later in the New Virtual Machine Wizard.
6. Open Hyper-V Manager. Click Start, point to Administrative Tools, and then click Hyper-V Manager.
7. Under Virtual Machines, select the virtual machine that you want to configure.
8. In the Action pane, under the virtual machine name, click Settings.
9. In the navigation pane (left pane), click the controller that you want to attach the disk to. If you plan to use the disk as a startup disk, make sure you attach it to an IDE controller. Click Add.
10. On the Hard Drive page, select the location on the controller to attach the disk.
11. Under Media, specify the physical hard disk. If the disk does not appear in the drop-down list under Physical hard disks, make sure the disk is in an Offline state in Disk Management.
12. Once the physical disk is configured, you can start the virtual machine and store data on
the disk. If installing an operating system, the installation process automatically prepares
the disk for use. If you are using the physical disk to store data, it must first be prepared
by the virtual machine.

If you are installing an operating system on the physical disk and it is in an Online state
before the virtual machine is started, the virtual machine will fail to start. You must store
the virtual machine configuration file in an alternate location because the physical disk is
used by the operating system installation. For example, locate the configuration file on
another internal drive on the server running Hyper-V.

Appendix A: Example Authorization Manager
Tasks and Operations

You can use the example tasks and operations listed here to help create role definitions. Role
definitions, combined with scopes and role assignments, help you provide security for your
virtualization environment using role-based access control. For more information about role-
based access control in Hyper-V, see the following topics in this guide:

- Using Authorization Manager for Hyper-V Security
- Configure Hyper-V for Role-based Access Control

Note
You must be a member of the Administrators group on the local computer to modify the
default Authorization Manager policy (an XML file) to create role definitions and
assignments.

Example tasks and operations
You cannot create or change operations. You can create tasks and role definitions that include
different groups of operations to allow a user within that role to perform the task. Some tasks
require a complex group of operations. Suggested task names that describe what the tasks do
are listed in alphabetical order. The operations required are listed underneath each task name.

Add external network to server
- Bind to External Ethernet Port
- Create Internal Ethernet port
- Connect Virtual Machine
- Create Virtual Switch
- Create Virtual Switch Port
• View External Ethernet Ports
• View Internal Ethernet Ports
• View LAN Endpoints
• View Switch Ports
• View Switches
• View Virtual Switch Management Service
• View VLAN Settings

Add internal network to server
• Create Internal Ethernet Port
• Create Virtual Switch
• Connect Virtual Switch Port
• Create Virtual Switch Port
• View Internal Ethernet Ports
• View LAN Endpoints
• View Switch Ports
• View Switches
• View Virtual Switch Management Service
• View VLAN Settings

Add private network
• Connect Virtual Switch Port
• Create Virtual Switch
• View Switch Ports
• View Switches
• View Virtual Switch Management Service

Apply a snapshot
• Allow Output from Virtual Machine
• Pause and Restart Virtual Machine
• Read Service Configuration
• Reconfigure Virtual Machine
• Start Virtual Machine
• Stop Virtual Machine
• View Virtual Machine Configuration
Attach internal network adapter to virtual machine

- Read Service Configuration
- View Virtual Switch Management Service
- Connect Virtual Switch Port
- View Internal Ethernet Ports
- View LAN Endpoints
- View Switch Ports
- View Switches
- View Virtual Machine Configuration
- View VLAN Settings
- Allow Output from Virtual Machine
- Reconfigure Virtual Machine
- Create Virtual Switch Port
- Change VLAN Configuration on Port

Connect to a virtual machine

- Allow Output from Virtual Machine
- Allow Input to Virtual Machine
- Read Service Configuration

Create a virtual floppy disk or virtual hard disk

- Read Service Configuration

Create a virtual machine

- Allow Output from a Virtual Machine
- Change Virtual Machine Authorization Scope
- Create Virtual Machine
- Read Service Configuration
- Optional: Connect Virtual Switch Port

Note

If you do not need this virtual machine connected to a network, you can leave this out. If you want to connect your virtual machine to a network, add this operation.

Delete a private network

- Delete Virtual Switch
- View Switch Ports
• View Switches
• View Virtual Switch Management Service

Delete a snapshot
• Read Service Configuration
• Delete Virtual Machine

Delete a virtual machine
• Allow Output from Virtual Machine
• Read Service Configuration
• Delete Virtual Machine

Export virtual machine
• Read Service Configuration
• Allow Output from Virtual Machine

Import virtual machine
• Allow Output from a Virtual Machine
• Create Virtual Machine
• Change Virtual Machine Authorization Scope
• Read Service Configuration
• View Virtual Machine Configuration

Modify virtual machine settings (reconfigure a virtual machine)
• Allow Output from a Virtual Machine
• Read Service Configuration
• Reconfigure Virtual Machine
• View Virtual Machine Configuration

Pass CTRL + ALT + DELETE (send control signals to a virtual machine)
• Allow Input to a Virtual Machine
• Allow Output from a Virtual Machine
• Read Service Configuration
Pause a virtual machine
- Allow Output from Virtual Machine
- Pause and Restart Virtual Machine
- Read Service Configuration

Remove external network from server
- Delete Virtual Switch
- Delete Virtual Switch Port
- Delete Internal Ethernet port
- Disconnect Virtual Switch Port
- Unbind External Ethernet Port
- View Virtual Switch Management Service
- View External Ethernet Ports
- View Internal Ethernet Ports
- View LAN Endpoints
- View Switch Ports
- View Switches
- View VLAN Settings

Remove internal network adapter from a virtual machine
- Allow Output from Virtual Machine
- Create Virtual Switch Ports
- Change VLAN Configuration on Port
- Disconnect Virtual Switch Port
- Reconfigure Service
- Reconfigure Virtual Machine
- Read Service Configuration
- View Internal Ethernet Ports
- View LAN Endpoints
- View Switch Ports
- View Switches
- View Virtual Machine Configuration
- View Virtual Switch Management Service
- View VLAN Settings
Remove internal network from server
- Delete Virtual Switch
- Delete Virtual Switch Ports
- Delete Internal Ethernet Ports
- Disconnect Virtual Switch Ports
- View Internal Ethernet Ports
- View LAN Endpoints
- View Switch Ports
- View Switches
- View VLAN Settings
- View Virtual Switch Management Service

Remove private network from server
- Delete Virtual Switch
- View Switch Ports
- View Switches
- View Virtual Switch Management Service

Rename a snapshot
- Allow Output from Virtual Machine
- Read Service Configuration
- Reconfigure Virtual Machine
- View Virtual Machine Configuration

Rename a virtual machine
- Allow Output from Virtual Machine
- Read Service Configuration
- Reconfigure Virtual Machine
- View Virtual Machine Configuration

Resume a virtual machine
- Allow Output from Virtual Machine
- Read Service Configuration
- Pause and Restart a Virtual Machine
Save a virtual machine and start a virtual machine
  • Allow Output from Virtual Machine
  • Read Service Configuration
  • Stop Virtual Machine
  • Start Virtual Machine

Start a virtual machine
  • Allow Output from Virtual Machine
  • Read Service Configuration
  • Start Virtual Machine

Turn off a virtual machine
  • Allow Output from Virtual Machine
  • Read Service Configuration
  • Stop Virtual Machine

View Hyper-V server settings
  • Allow Output from Virtual Machine
  • Read Service Configuration
  • Reconfigure Service
  • View Virtual Machine Configuration

View network management
  • View Switch Ports
  • View Switches
  • View Virtual Switch Management Service

View virtual machines
  • Allow Output from Virtual Machine
  • Read Service Configuration
  • View Virtual Machine Configuration
Appendix B: Authorization Manager Terminology

You use the Authorization Manager Microsoft Management Console (MMC) snap-in (AzMan.msc) to select operations, group them into tasks, and then authorize roles to perform specific tasks. You also use the snap-in to manage tasks, operations, and user roles and permissions. See Using Authorization Manager for Hyper-V Security and Configure Hyper-V for Role-based Access Control for more information about using role-based access control for virtual machines in Hyper-V.

Terminology

The following terminology is used in the context of Authorization Manager:

- **Operation.** A low-level permission in an application. Operations are the building blocks of your policy for role-based access control. For example, in Hyper-V “Allow Input to a Virtual Machine”, “Allow Output from a Virtual Machine,” and “Create a Virtual Machine” are operations.

- **Policy.** The data that Authorization Manager uses for role-based access control. This data, configured by a virtualization administrator, describes the relationships between roles, tasks, and operations. The policy is an XML file that you can edit using the Authorization Manager snap-in or with scripting tools. For more information about the elements of a policy, see Checklist: Before you start using Authorization Manager (http://go.microsoft.com/fwlink/?LinkID=134197).

- **Role.** A set of users and/or groups that define a category of user who can perform a set of tasks or operations. For example, the users assigned to the administrator role by default have the ability to perform any task or operation in Hyper-V. The administrator can create any number of other roles.

- **Authorization store.** The repository for the authorization policy. You must create a store to control resource access—you can do this either programmatically or using the snap-in. The default store location in Hyper-V is an XML file located at \ProgramData\Microsoft\Windows\Hyper-V\InitialStore.xml. Both Hyper-V and Authorization Manager support XML files and Active Directory Domain Services for storing a policy. However, Authorization Manager stores for other applications can be created in Active Directory Lightweight Directory Services and Microsoft SQL Server (new for Windows Vista and Windows Server 2008).

- **Scope.** A collection of resources with a common access control policy. In Authorization Manager, the scope can be a folder, an Active Directory container, a file-masked collection of files (for example, *.doc), a URL, or any object that can be accessed by the application and its underlying authorization store. The object can be assigned to only one scope. Any object that is not assigned to a scope takes the access control policy that is defined in the Authorization Manager application (or root) scope. The default scope is “Hyper-V Services”.


Hyper-V objects that you can use for scopes include virtual machines, virtual switches, and virtual switch ports.

For example, to grant administrator access to a set of virtual machines to a specific user or group, create a scope for those virtual machines. For more information, see Work with Scopes (http://go.microsoft.com/fwlink/?LinkID=134199).

- **Task.** A logical group of operations for accomplishing a task. Tasks can be categorized by objects and used to control access to the object.

  ![Note](https://example.com)

  No checks are made for dependent operations when you add tasks to a role definition. For example, the “Connect to a virtual machine” task requires the “Read Service Configuration,” “Allow Output from a Virtual Machine,” and “Allow Input to a Virtual Machine” operations.

- **Departmental administrator.** An administrator who only has permissions to perform the tasks that are outlined in the role description. At a higher organizational level, the virtualization administrator creates and maintains the role definitions and scopes. For example, the virtualization administrator can create a “Human Resources Administrator” departmental administrator role that is scoped only to virtual machines owned by the Human Resources department, and can create a different role (with the same operations and tasks) called “Finance Administrator” that is scoped only to the Finance department virtual machines.

- **Role definition.** The list of operations that a user can perform with the assigned role.

- **Role assignment.** A list of users who can perform the operations that are listed in the role definition.

  For example, the default administrator role definition includes all operations and the default role assignment is for all users in the BUILTIN\Administrators group. You can create a “User” role that can only use the “Start Virtual Machine”, “Stop Virtual Machine”, “Allow Input to Virtual Machine” and “Allow Output from Virtual Machine” operations. You can also create roles based on organizational structures. For example, you can create a role called “Virtual Network Administrator” and assign only the operations for virtual networking to that role. For more information, see Manage Groups, Roles, and Tasks (http://go.microsoft.com/fwlink/?LinkID=134517).

- **Virtualization administrator.** An administrator who has local administrator permission on the virtualization server management operating system and controls all other delegated administrator rights and permissions.