Exam
Manual

LearnSmart

Microsoft Server 2008 R2 Server Virtualization

(70-659) Microsoft Certified IT Professional (MCITP)

This LearnSmart exam manual breaks down complex topics and emboldens IT professionals with all the knowledge and confidence necessary to pass the Server 2008 R2 Server Virtualization exam (70-659). By studying this guide, candidates will become familiar with an array of concepts found on the exam, including:

- Hyper-V Configuration
- Hyper-V Remote Configuration
- Virtual Hard Drives
- Virtual Machines
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

Server 2008 R2 Server Virtualization (70-659) LearnSmart Exam Manual

Product ID: 012457
Production Date: July 12, 2011

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

This manual is designed to cover every aspect of Microsoft's Hyper-V product as it pertains to Server 2008 R2. With the release of R2, Microsoft heavily invested in a number of substantive changes to the Hyper-V product, in order to meet growing demand for virtualization products and services. As such, Microsoft released a completely separate exam covering Hyper-V from the R2 perspective. We have structured this exam as a top-down approach to the entire Hyper-V R2 system, from basic installation routines to more advanced procedures such as physical machine migration. You'll see information and routines for creating complex virtual networks and assuring high availability in Hyper-V R2 mitigated virtual machines.

What you will not see is a manual rigidly structured to the objectives document released by Microsoft. Rather, we have intended that this manual serve you well beyond the exam as a quick reference manual to all the important skills and procedures necessary to a working Virtualization Administrator. Every exam objective for the 70-659 is covered in this manual, but is organized in a more meaningful way, covering the topics as you might encounter them in the real world.

What to Know

Microsoft recommends that candidates for the 70-659 exam have at least a year and a half's experience working with their virtualization products, and a successful candidate will especially have experience with Server 2008 and Server 2008 R2 environments. This includes Hyper-V, of course, but also Virtual Machine Manager and System Center Virtual Machine Manager, PowerShell 2.0, System Center Operations Manager and System Center Data Protection Manager.

On top of all that, the exam will require candidates have operational knowledge of the following tasks:

- Installing and Configuring Host and Parent Settings
- Configuring Child Settings
- Managing and Monitoring Virtual Environments
- Ensuring High Availability and Recoverability
- Performing Migration
- Configuring Remote Desktop (RD) Role Services Infrastructure

Tips

The 70-659 exam will test your knowledge from both a factual and process-oriented standpoint. Therefore, it is important not only to remember facts (such as the different kinds of VHD files, or what the CPU requirements for Hyper-V are), but also how to perform tasks in both the Hyper-V manager and SCVMM. Although SCVMM is a separate exam, 70-659 expects you to be able to perform and verify the results of common tasks related to VM management. An example of this would be adding an item to a library share on an SCVMM host.

Therefore, not only should you study the content in this Exam Manual, but you should practice these concepts on a personal lab. A lab computer should meet the requirements of running Hyper-V, and have at least 2 gigabytes of RAM for concurrently-running virtual machines. SCVMM can run on the lab server or it can be virtualized. Since Hyper-V cannot run inside a virtual machine, at least one physical server is required.

For your lab, you do not need to activate Server 2008 or any of the guest operation systems. Server 2008 will be fully functional without activation long enough to at least study for the 70-659 exam.

If you want to run the standalone Hyper-V product from Microsoft, that should be fine for the exam, but you will need another PC to manage the Hyper-V server.

The standalone edition of Hyper-V can be downloaded free from Microsoft. SCVMM is available as a free trial download that will work without purchase for 365 days. Microsoft has also released a trial of SCVMM in VHD format for importing to Hyper-V.

Experimenting with failover clustering in a lab can be more complicated. Not only will you need a second Hyper-V server with the same architecture, you will also need a shared storage SAN such as Fibre Channel and or iSCSI, and multiple network cards. We recommend studying clustering from a textbook perspective and understanding the concepts, rather than actually building a failover cluster for your lab.

70-659 also introduces students to running Remote Desktop Services. This is a major difference between 70-652 and 70-659. 70-659 also puts more emphasis on the understanding of Migration – moving a virtual machine's point-in-time state from one host to another.

Chapter 1: Introducing Windows Server 2008 Hyper-V

Understanding Virtualization

Hardware virtualization enables multiple OS instances to run simultaneously on a single physical host computer. Each guest OS instance runs in a Virtual Machine (VM) that mirrors a complete computer in software, including the processor, memory, graphics card, network interface, and storage devices (such as disk and CD-ROM drives). The hardware is shared with other OS instances.

Virtualization consolidates many servers onto a single system to provide lower total cost of ownership (TCO), and increased optimization. Virtualization also increases environment flexibility and integrates 32-bit and 64-bit workloads in the same environment. Virtualization is beneficial when current chip technology exceeds utilization. The server operating system is separate from the hardware, allowing many servers to run on one machine as a virtual machine.

Introducing Hyper-V

Hyper-V is installed as a role in Server 2008 to take advantage of 64-bit, hardware-assisted virtualization technology. It uses a **hypervisor** to manage virtual machines. Each virtual machine is given a portion of memory and processing power (up to 4 virtual processors) and 64 GB of RAM.

Hyper-V uses partitions that include a parent (or root) partition that runs either a full installation of Windows Server 2008 or a Server Core installation, which is a minimal environment for running specific server roles. The virtualization stack, a collection of software components that work together to support the virtual machines, runs in this parent partition and has direct access to the hardware devices.
From the root partition, child partitions can be created. Child partitions can run different operating systems, including hypervisor-aware operating systems and older operating systems are not enlightened. Their requests are redirected through the parent partition via a virtual machine bus (VMBus), a subsystem for exchanging requests and data.

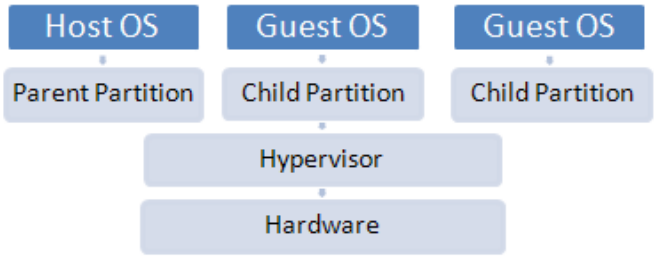


Figure 1: Basic Hypervisor Structure

Hyper-V Benefits

Hyper-V provides a scalable, reliable, and highly available virtualized server computing environment. Hyper-V enables one or more guest operating systems to run concurrently on a single physical computer. Virtual machine uses include:

- An agile environment that allows rapid deployment
- Ability to develop and test easily
- Server consolidation
- Consolidation of development and testing environments
- Simplified disaster recovery
- Quick migration, live migration and VM Failover capabilities to increase business continuity (minimize both scheduled and unscheduled downtime)
- Creates a dynamic datacenter with features such as:
    - Automated virtual machine reconfiguration
    - Flexible resource control
    - Quick migration
    - Dynamic IT environment that responds to problems and anticipates increased demands.
    - VM's run in isolated environment
    - Branch consolidation
    - Hosts desktop infrastructure
    - Host machine with memory of up to 1 terabyte and up to 64 GB per VM

Hyper-V has built-in licensing for Server 2008 child instances.

- Standard licenses up to 1 VM instance.
- Enterprise licenses up to 4 VM instances.
- Datacenter includes unlimited VM licenses.

In other words, by purchasing an edition of Server 2008, you are also purchasing the rights to Server 2008 virtual machines. However, the free bare-metal hypervisor product, Hyper-V Server, does not include any licensing benefits.

Installing Hyper-V

On full versions of Windows Server, Hyper-V can be added as Role from the Server Manager console.

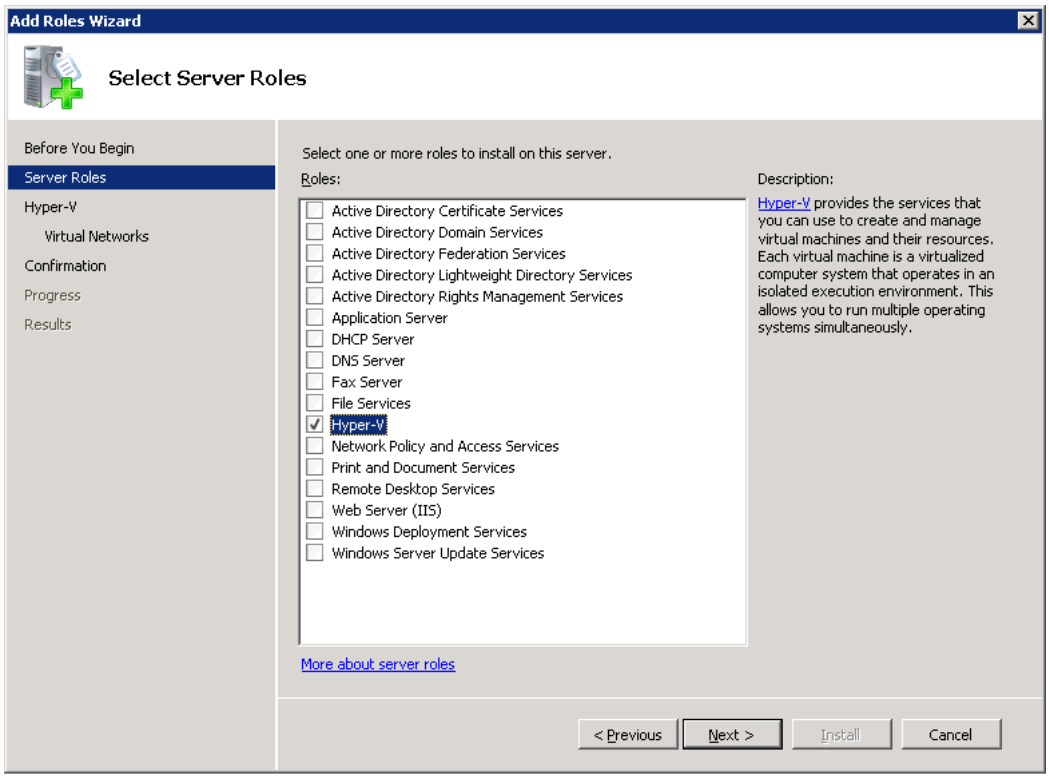


Figure 2: Installing the Hyper-V Role

The only configuration option you must select when installing the Hyper-V role is the network cards you want to use with Hyper-V. Note that in this wizard, Microsoft recommends leaving one network card for host management traffic, to keep host traffic out-of-band from guest traffic. This recommendation is discussed later in the text.

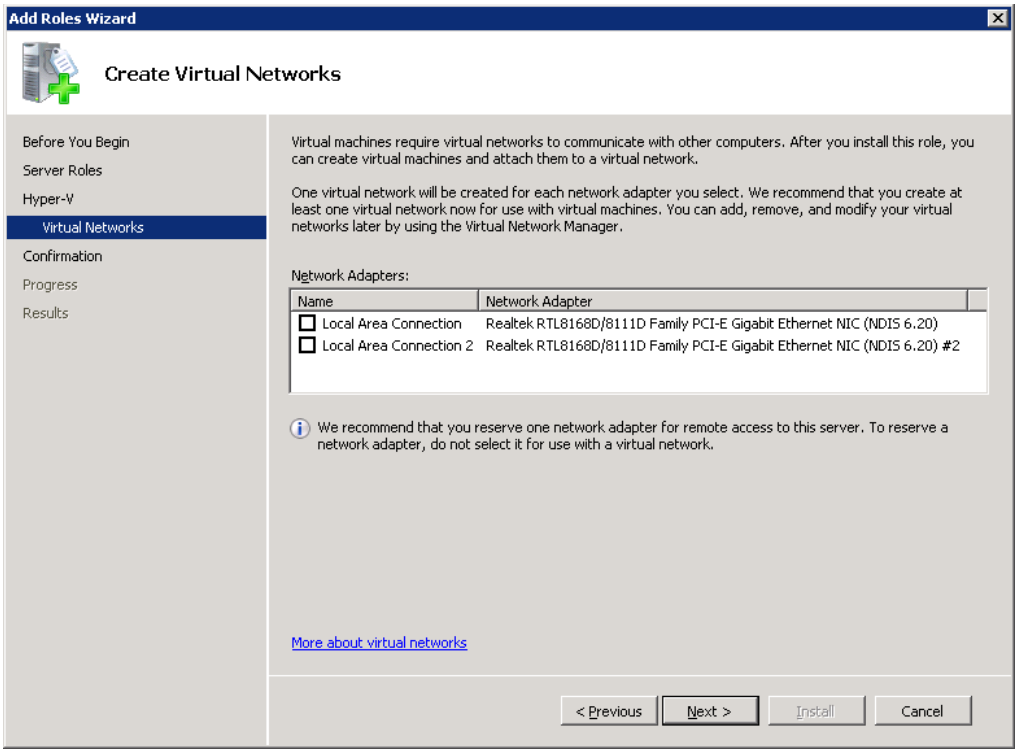


Figure 3: Select which network cards to make available to Hyper-V

Installing the Hyper-V role requires a reboot. After reboot, the Hyper-V Role in the Server Manager should then show 3 services that are running:

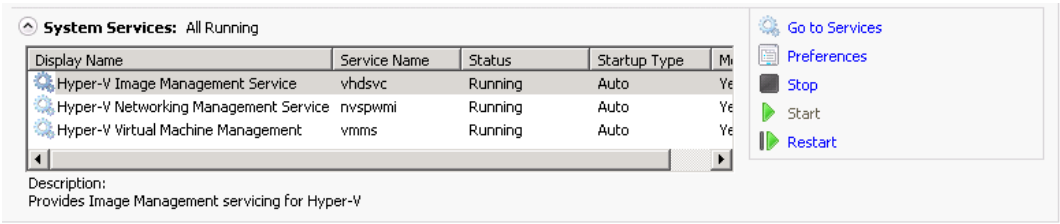


Figure 4: Verifying Hyper-V Services after a successful install

These services are important for your exam and in the real world. The three services are:

- The Hyper-V Image Management Service
- The Hyper-V Networking Management Service
- The Hyper-V Virtual Machine Management Service

Hyper-V is actually a kernel-level part of Server 2008 and is not controlled by any particular service, but these three services help provide management to various aspects of Hyper-V guests.

Installing Hyper-V on Server Core

Server Core provides a stripped-down version of Server 2008 with three main benefits as a Hyper-V host:

- Fewer services running, providing a smaller attack surface than full Server 2008
- Fewer components to update through Windows Update
- More RAM available for the guest operating systems

To install the Hyper-V role on server core, only one command is needed:

```
start /w ocsetup Microsoft-Hyper-V
```

This command is case sensitive and must be executed as a local administrator. There are some "auxiliary" commands used to make Server Core operational. The tasks you will need to perform for an operational Hyper-V Server Core host include:

- Installing Drivers if necessary.

  ```
  pnputil -i -a "c:\drivers\drivername.inf"
  ```

- Setting the system IP address and DNS servers with netsh.exe. In this example, the addresses are for illustration only.

  ```
  netsh interface ipv4 set address name="Local Area Connection"
  source=static address=192.168.0.2 mask=255.255.255.0
  gateway=192.168.0.1

  netsh interface ipv4 add dnsserver name="Local Area Connection"
  address=8.8.8.8 index=1
  netsh interface ipv4 add dnsserver name="Local Area Connection"
  address=4.2.2.2 index=2
  ```

- Setting the firewall options with netsh.exe.

  ```
  netsh advfirewall firewall set rule group="remote administration"
  new enable=yes
  ```

- Setting the system name and domain with netdom.exe.

  ```
  netdom renamecomputer /NewName:hyperv1
  netdom join /domain:corp.net /userd:admin /password:*
  ```

- Activating windows with the slmgr.vbs script.

  ```
  slmgr -ato
  ```

- Enabling remote desktop with scregedit.wsf.

  ```
  cscript %windir%\system32\scregedit.wsf /ar 0
  ```

- Configuring windows updates with scregedit.wsf.

  ```
  cscript %windir%\system32\scregedit.wsf /au 4
  ```

- Enabling remote management with WinRM. To accept the default settings, use this command:

  ```
  winrm quickconfig
  ```

Installation of Server Core will have other settings that you should customize to your needs. The 70-659 exam requires that you be able to at least recognize the business logic behind the decision to use Server Core (particularly in a Hyper-V environment) and know the baseline commands to get Server Core operational.

Hyper-V Components

Hyper-V is the amalgamation of several interacting components that provide support for virtualized servers.

At the heart of Hyper-V is the hypervisor itself. The hypervisor services VM requests and provides the virtual hardware to guest operating systems.

Navigating the Hyper-V Console

After Hyper-V has been installed, the next step is to install guest images that will run on the virtual server. Before doing so, below is a quick review on navigating the Hyper-V Administrative console and the virtual server guest session settings that are available for configuration.

Launching the Hyper-V Administrative Console

Open the Hyper-V Administrative console to access the configuration options. Use the Server Manager tool and administer the host server through Server Manager, or launch the freestanding Microsoft Management Console (MMC) to perform administrative tasks for the host system.

Using the Server Manager Tool to Manage Hyper-V Systems

Use the Server Manager to administer Hyper-V systems from a centralized console. The Server Manager tool provides a common administrative interface for all of the server roles installed on a particular system.

Starting the Server Manager:

1. Click **Start** and then click **Run**.
2. In the **Run** dialog box, type in ServerManager.msc, and click OK to start the Server Manager application if it is not already running on the system.
3. Click on the + to expand the Roles section of the tree.
4. Expand the Hyper-V branch of the tree.
5. Expand the Virtualization Services branch of the tree.

Use the Hyper-V MMC Tool to Manage Hyper-V Systems

Use the Hyper-V tool to administer Hyper-V systems from a dedicated console.

Starting the Hyper-V MMC Tool

1. Click **Start → All Programs → Administrative Tools.**
2. Choose **Hyper-V Management** for the tool to launch.
3. Click on **Virtualization Services** to see the connected virtual servers.
4. Click on the name of one of the virtual servers listed to see the virtual machines and actions available for the confirmation of the server system. By default, the Hyper-V MMC will have the local virtual server system listed.

Connecting to a Different Virtual Server System
Log on and connect to another serve to administer and manage its virtual server system.

Log on to Virtual Server System:

1. In the left pane of the **Hyper-V Management Console**, click on the **Virtualization Services** option.
2. Select **Action** → **Connect to Server**.
3. Select **Another Computer**.
   a. Enter the name of the server.
   b. Click **OK.**
   c. Or click on **Browse** to search **Active Directory** for the name of the server that is to be remotely monitored and administered.
4. When the server appears in the Hyper-V Management Console, click to select the server and the actions available for administering and managing that server.

Navigating and Configuring Host Server Settings
Server Manager and MMC tool configuration options and settings are the same.

When the Virtualization Settings action item is selected, access to configure default paths and remote control keyboard settings becomes available. Settings include:

- **Default Paths –** allows ability to set the location drive path where virtual hard disks and snapshots are stored. The default path could be on the server system on a local disk or stored on an external SAN.
- **Remote Control** – remote control settings include how to switch to Local, Remote, or Full Screen mode. There is also a remote control setting that allows selecting which keystroke is used to release the mouse and keyboard control back to the host when administering a guest session.
- **Keyboard Release Key** – by default, the key that releases the guest session so the administrator can gain keyboard control back to the host console is **Ctrl+Alt+Left Arrow**. The Remote Control/ Release Key option allows for the selection of other key options.

Launching the Hyper-V Manager

Launch Hyper-V Manager with the Administrative Tools Manager, Server Manager or Search.

- **Administrative Tools Menu** – launch Hyper-V Manager by clicking on the **Start** → **Administrative Tools** → **Hyper-V Manager** menu option.
- **Server Manager** – launch the **Server Manager** either from the **Start** → **Administrative Tools** → **Server Manager** menu option, or by clicking on the **Server Manager** icon in the task bar along the bottom of the desktop.
- **Search** – click on the **Start** button, enter **Hyper-V** into the **Search** box and press enter.

A Quick Tour of the Hyper-V Manager

Once the Hyper-V Manager has loaded, it will appear as illustrated in the following figure:

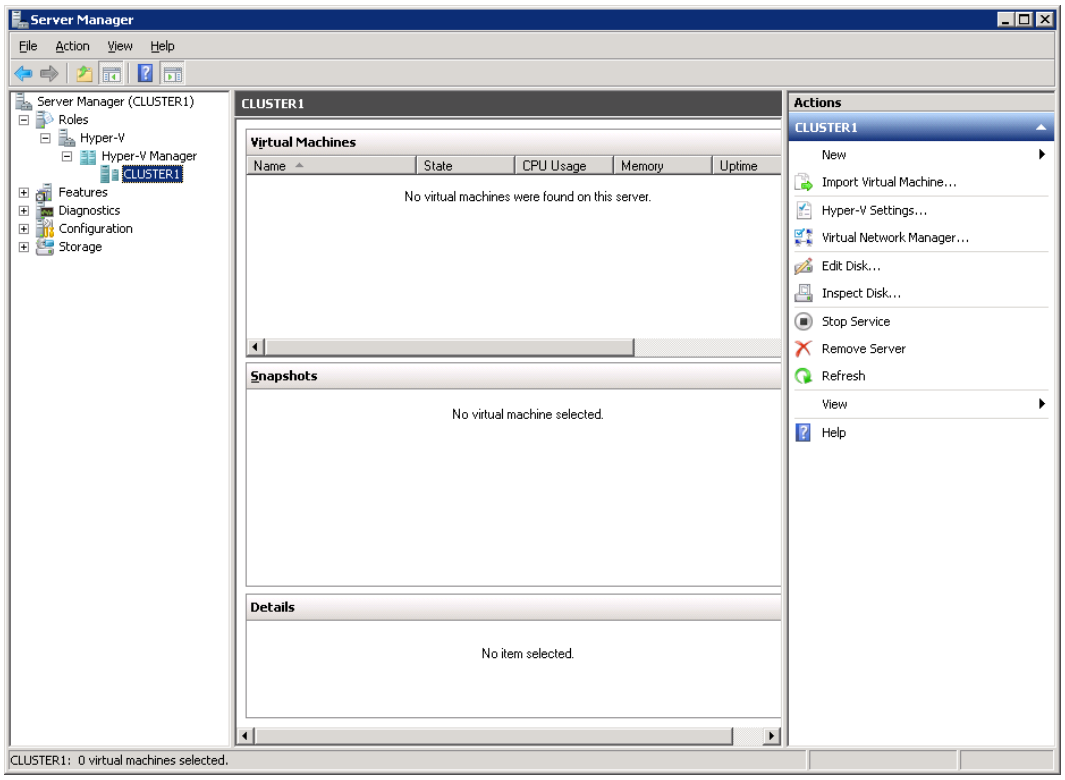


Figure 5: The Server Manager Hyper-V Console

The left hand side contains a list of Hyper-V servers that are available for administration. By default the local server will be listed.

Add remote Hyper-V servers to the list by right clicking on the **Hyper-V Manager** item in this panel and selecting **Connect to Server...**

When selected, this menu option will display the **Select Computer** dialog. Select the local system (if it is not already listed) or to browse the network to find other remote Hyper-V servers from this dialog.

When remote server connections are established, they will appear in the list along with the local system. To remove a server select the server and click on the **Remove Server** link in the **Actions** panel.

The central panel contains three sub-panels. The top panel provides a list of virtual machines that are configured on the server currently selected in the right hand panel. The list contains the VM name, CPU usage, uptime, and operations information. Right click the virtual machine to view the commands that can be accessed. Select the **Connect...** action option or double-click on the entry in the list to display the console. Once selected, the **Connection** tool will appear displaying the virtual machine console.

The central panel contains a list of snapshots that have been taken for the selected virtual machine. Select a snapshot from the list to display a list of actions in the right hand panel or right click on a specific snapshot in the list. The bottom panel displays additional information about the currently selected item.

Managing a Running VM

Hyper-V can boot the installer for any supported operation system from the ISO file. It can also perform a network boot (using the Legacy Network Adapter, discussed later). After booting, you can go through the install process just like you would if installing the OS on a physical machine. Figure 6 shows the familiar screen presented when Server 2003 is booted from its media.

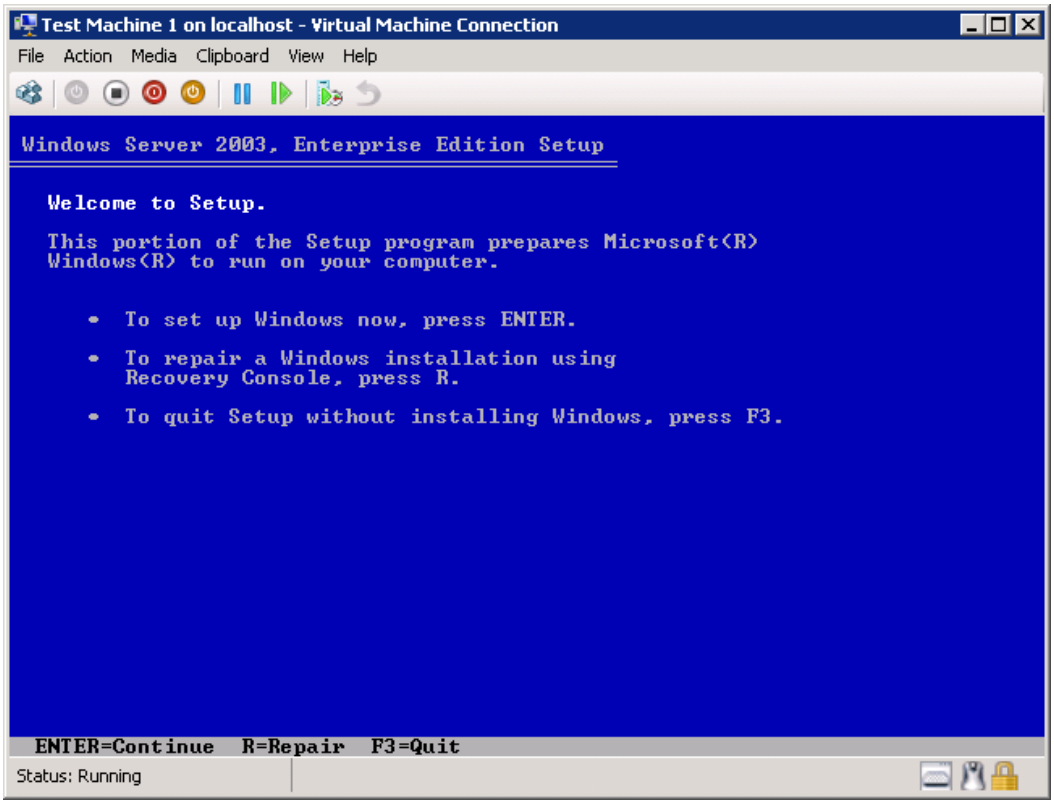


Figure 6: Installing an OS in Hyper-V is just like installing the OS on a physical system

Figure 7 shows what a VM looks like after it has booted up. The Windows 7 client inside this VM sees its host as any other hardware and has no reason to know it is running on a VM. We are connected to this host via VMConnect (discussed later), but we could enable RDP on the host and use Remote Desktop to connect.

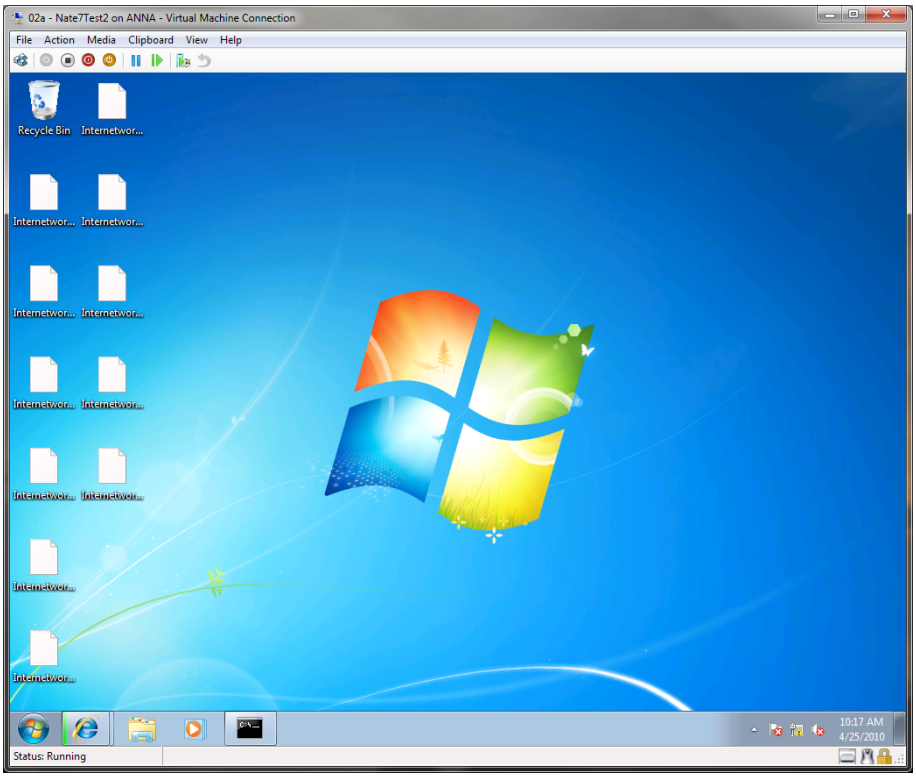


Figure 7: VMConnect displaying a running Windows 7 guest.

The toolbar of VMConnect gives us the option to Stop, Pause, Turn off, and Reboot a VM. Taking a closer look at the **Action** menu, we can see this is where we would insert the Integration Services disc if our guest OS required that (Figure 8). We can also take snapshots or revert to a snapshot (if the VM is turned off).

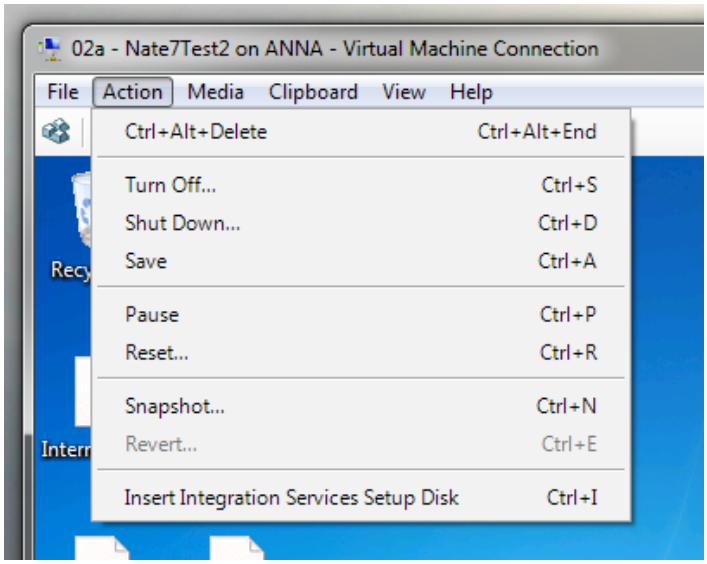


Figure 8: VMConnect Actions to perform on a running VM

Hyper-V allows guests to access two types of optical disks. First, Hyper-V adds the convenience of being able to use ISO images inside guests without having to burn them. Operating Systems can be installed directly from an ISO on a local disk, SAN, or network share. Secondly, Hyper-V guests can access the host's physical CD/DVD drive as if it were attached directly to the guest. This is called "capturing" the drive. The same can be done with Floppy Disks using VFD files and the host's floppy drive.

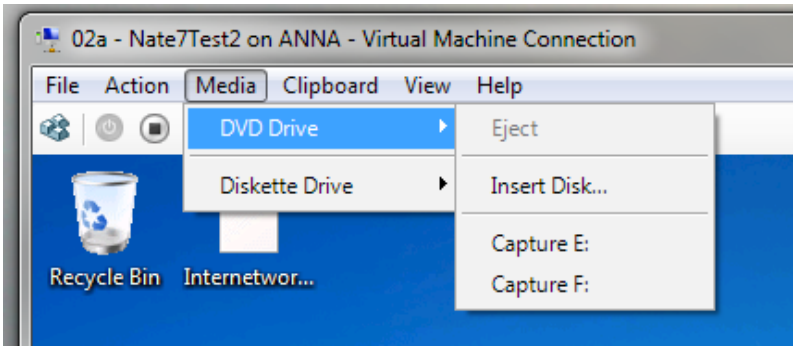


Figure 9: Insert Disk… will allow us to insert an ISO file on the guest, or Capture… a physical DVD drive

Customizing Hyper-V Manager

The sizes of the various panels may be changed by moving the mouse pointer to the border of a panel. The specific panels that are displayed may also be configured by selecting **View** from the **Actions** panel and clicking on **Customize**.

Hyper-V Configuration Settings

The Hyper-V Manager provides the ability to make changes. Click the **Hyper-V Settings** in the right hand **Actions** panel to access settings.

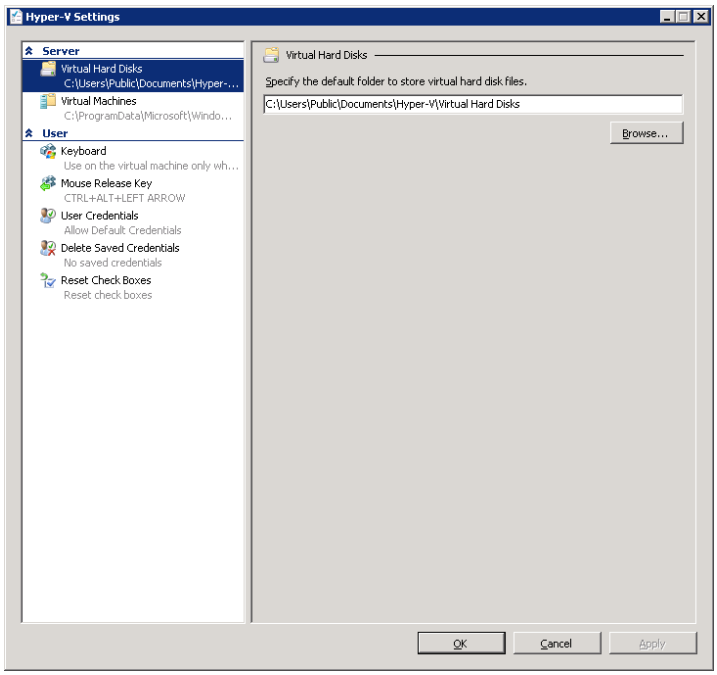


Figure 10: Hyper-V Settings

Understanding Hyper-V Server (Free Standalone Product)
Hyper-V Server is a free bare-metal Hypervisor based on Server 2008 that allows you to run the same VMs that you would run on either Full Server 2008 or Server Core. It does not require an existing or licensed copy of Windows to be installed on the hardware, but VMs inside Hyper-V Server should be licensed appropriately. The Hyper-V Server standalone product is a useful tool for testing environments and MCTS/MCITP study labs. VMs created on Hyper-V Server can be moved to full versions of Windows Server 2008 hosts. Hyper-V Server can access all the same hardware that Server 2008 can access, and includes an iSCSI initiator. Although the features it comes with are limited, it does have a configuration utility called hvconfig.cmd that runs on startup (Figure 11).

Limitations of Hyper-V Server:

- Hyper-V Server does not automatically license any guest instances of Server 2008.
- The parent partition of Hyper-V Server will not run any applications or roles besides Hyper-V.
- The parent partition of Hyper-V Server cannot be a domain controller.
- You cannot manage Hyper-V from the server itself. It must be done remotely.
- Powershell and BitLocker are not included.

Steps for installing Hyper-V Server:

1. Download the ISO file containing Microsoft Hyper-V Server from Microsoft.
2. Burn the 929 MB ISO file to a DVD or create a bootable USB disk or use a network-based install method.
3. Boot your Hyper-V capable server from the installation media.
   Wait until Windows is finished loading files.
4. Select your language.
5. Select your regional and keyboard settings. When done press **Next**.
6. Press **Install Now**.
7. Read the End User License Agreement (EULA) and select the **I accept the license terms** option before pressing **Next**.
8. Select the **Custom (advanced)** option for installation (**Upgrade** is unavailable)
9. Partition the disk(s) and press **Next** to commence installation.
10. Wait for the Installation wizard to copy files, expand files, install features and install updates.
11. Logon to the freshly created Hyper-V server installation by pressing the **Other User** button and specifying **Administrator** as the username and a blank password. Type a new password afterwards and confirm it.
12. After logon the Hyper-V Configuration Tool hvconfig.cmd automatically launches. Use it to:
    - Change workgroup settings or domain membership settings (requires restart)
    - Change the computer name (requires restart)
    - Change network settings
    - Add local Administrator accounts
    - Change Windows Update settings
    - Download and install Windows updates

- Change Remote Desktop settings
- Change Regional and Language settings (through inet.cpl)
- Change Date and Time settings (through timedate.cpl)
- Log off, restart and shutdown the box
- Exit to the command prompt

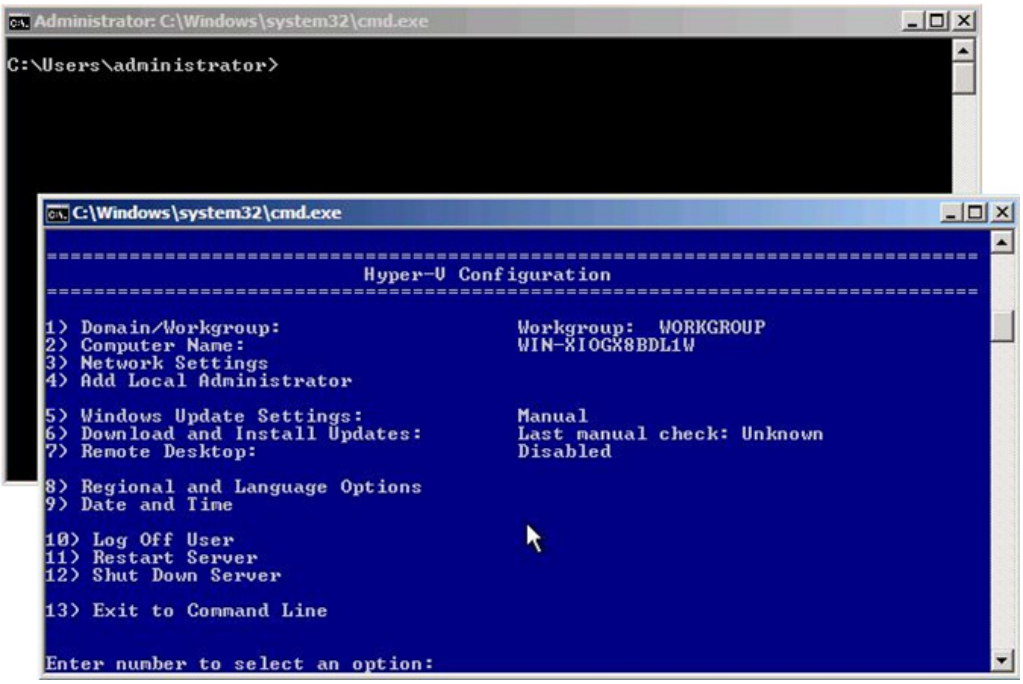


Figure 11: Hyper-V Server startup and hvconfig.cmd menu

What's New in R2

Microsoft's R2 release of Server 2008 adds many benefits to the operating system, but where R2 delivers the most functionality is in Hyper-V. R2 was designed to give Hyper-V performance improvements and adds some of the functionality that is found in VMWare. With the performance improvements and added functionality, Hyper-V is a strong competitor to other enterprise server virtualization platforms such as VMWare and Citrix.

Because of the improvements to Hyper-V, the 70-659 exam will most likely ask you about the differences between the original release of Server 2008 ("R1") and Server 2008 R2. Because this text is designed for R2 only, we will point out areas where R1 differs.

Apart from Hyper-V improvements, R2 adds improvements to Remote Desktop Services (RDS), previously known as Terminal Services. As part of Microsoft's initiative to virtualize both server workloads and desktop environments, RDS has become part of Microsoft's virtualization strategy: Microsoft refers to RDS as "Presentation Virtualization". The name comes from the fact that the user doesn't actually run the software on their machine, it runs on a server. The presentation of the application is all that the user needs, so the rest of the software is hidden. The user sees and hears the application and interacts with it, but the software is running on a remote server. The input and output between the user and the application is transmitted over the network via RDS. Since they can access their applications from anywhere, the software is not tied to the user's machine, and is thus "virtualized" from their perspective. From an administrators' perspective, RDS runs on a "farm" of servers, meaning that the application is not tied to any specific hardware.

Microsoft includes RDS as a major exam objective in the 70-659 exam:

Configuring Remote Desktop (RD) Role Services Infrastructure

- **Configure RD session host** – this objective may include but is not limited to: configuring session host settings, network-level authentication settings, license settings; restricting users to single remote session; allowing time zone redirection; configuring resource redirection, configuring encryption, configuring multi-monitor support.
- **Configure RD licensing** – this objective may include but is not limited to: activating and deactivating Remote Desktop License Service, installing and revoking client access licenses (CALs), reporting on CAL usage.
- **Configure RD Connection Broker** – this objective may include but is not limited to: installing the RD Connection Broker, configuring DNS for Connection Broker, configuring Connection Broker farms, integrating with RD Virtualization Host role service.
- **Configure RD Gateway** – this objective may include but is not limited to: configuring RD Gateway, integrating RD Gateway with network access protection (NAP), configuring authentication authorization.
- **Configure RD Web Access** – this objective may include but is not limited to: configuring RD Web Access, configuring authentication options (forms, single sign-on), configuring per-user RemoteApp program filtering, configuring public and private computer options.

The inclusion of RDS is the largest difference between 70-652, which is designed to test Hyper-V aptitude in R1, and 70-659. Therefore, we have included a chapter on RDS.

Hyper-V Performance Improvements

As stated, Hyper-V R2 has been given a number of improvements that make it a more competitive solution and provide a higher Virtual-to-Physical consolidation ratio. This means that administrators can take advantage of new server technology and further optimize their infrastructure by virtualizing more workloads to fewer servers.

Hyper-V R2's Hypervisor has been rebuilt to add the following architectural changes over Server 2008's initial release version:

Item	Server 2008 R1	Server 2008 R2
Physical/Logical CPUs	4/16	8/64
RAM Support	32 Gigabytes	1 Terabyte
RAM Support for VMs	32 GB total	64 GB per VM
Maximum Number of VMs running	128	384

Figure 12: R2 Capacity Enhancements

The requirements for using Hyper-V are the same for R1 and R2. You must have a 64-bit CPU with virtualization extensions (Intel's virtualization extensions are called Intel-VT; AMD's is called AMD-V). And you need No-Execute technology, which is also known as Hardware D.E.P. (Data Execution Prevention). Itanium CPUs are not supported.

CPU & Memory Enhancements

Hyper-V R2 features a memory optimization technology called Second-Level Address Translation (SLAT). SLAT is a feature provided by the CPU and system RAM that improves the overall performance of the child and host partitions. SLAT allows the CPU to look up guest memory mappings more efficiently and frees up the CPU for servicing other processes. SLAT must be supported by the CPU. In the Intel world, SLAT is called "Nested Page Tables" and in the AMD world it is called "Enhanced Page Tables" or "Rapid Virtualization Indexing". The reason for these names will become clear in this section.

In a Hyper-V enabled server, the guest operating system image is stored within a designated section in RAM. Hyper-V enabled servers maintain 3 spaces of RAM. These are the System Physical Address (SPA), the Guest Physical Address (GPA), and the Guest Virtual Address (GVA). The SPA is the memory that the server can physically address and does not include (from a Hyper-V perspective) the virtual memory in a pagefile. The SPA is what we traditionally think of when we think of RAM in a server. The GPA is the "physical" memory that the guest image runs in. It is the RAM that the guest image sees, and is what you are allocating when you assign RAM to a guest. The GVA is a service that Hyper-V provides to guests to give them a pagefile. The GVA is a special allocation of RAM that is stored on the guest's VHD file.

In order to make the GVA addressable by the guest, the server makes two lookups each time something changes in a guest's memory. It does this to determine if the specific data should be placed in the GPA (the virtual RAM) or the GVA (the pagefile hidden in the VHD). While this enables virtual memory in the guest OS (a hallmark of the Windows kernel since Windows 95), it means more pressure is put on the server's CPU as it now has to determine where memory on the guest is located. SLAT gets its name from this process because it requires 2 table lookups for all partitions.

Whenever the guest operating system makes a system call or needs to interact with the physical system, a HyperCall or interrupt is sent to the physical processor by means of the logical Hyper-V bus. In order to service the request, Hyper-V maintains a table of physical-to-guest addresses in RAM for each running guest. This table is called the Translation Lookaside Buffer (TLB). This table gives Hyper-V the ability to know where a running VM is stored in RAM. This entire process is transparent to the guest. The physical processor must access the TLB in order to service the guest's HyperCall or interrupt and ultimately process the guest's service call. Storage of the TLB is one reason why Microsoft recommends 32 megabytes of RAM for each running VM in addition to the memory necessary for the guest.

SLAT assists in the process of mapping virtual-to-physical RAM by giving the CPU a second address table to reference for guest memory. SLAT acts as a middle-man to provide faster address translations between the physical and virtual hardware. SLAT gives the processor a dedicated portion of the CPU to the lookups performed between the SPA and GPA. This allows for less overhead in the CPU thread execution pipeline and frees up the CPU for business activities rather than handling the overhead associated with maintaining address tables for each guest.

Microsoft unofficially has witnessed an overall speedup of approximately 20 percent with SLAT. It can be particularly useful for RAM-intensive applications such as Remote Desktop Services. For the 70-659 exam you can think of SLAT as a cache of memory addresses specifically designed to assist Hyper-V and provided by hardware.

R2 also utilizes Core Parking. This technology starts and stops cores on the fly, keeping the fewest number of cores running as possible. When workload increases, the kernel enables additional cores. This is a power-saving technique for modern multi-core processors and is automatically enabled. It effects R2 systems with and without Hyper-V and is also present in Windows 7.

Network Enhancements

Hyper-V R2's networking stack has been improved to get the VMs "closer" to the networking hardware by providing them with more features. The three features added are:

- TCP Chimney
- Jumbo Frame Support
- VM Queueing

TCP Chimney is also known as TCP Offload. TCP Chimney is a feature provided by the NIC to process the overhead associated with reliable IP communication in localized NIC hardware rather than depending on the CPU. Servers that have NICs with offload capability can now extend this capability to guest OSs. This is an especially important feature when using iSCSI, since iSCSI uses TCP to transmit storage blocks.

Jumbo Frames are provided to guest OSes in R2 with the standard Hyper-V network device installed in them. Jumbo Frames adjust the layer 2 frame size to provide higher throughput and lesser CPU usage on Ethernet networks.

By default the size of an Ethernet frame contains a payload of about 1500 bytes. It also includes source and destination address information that must be processed by switches and NICs in the transit path. The frame check sequence is a value computed and transmitted on every Ethernet frame to mathematically ensure that the frame was not altered in transit. These features add extra overhead to the switching process and slow down the network.

A **Jumbo Frame** is a normal Ethernet frame with its payload capabilities improved. A Jumbo Frame can be up to 9000 bytes in size and thus delivers more "bang for the buck". The frame contains all of the fields and data from a standard Ethernet frame but delivers a larger payload. This reduces CPU usage since the system computes fewer checksums. Because switches in the transit path don't have to compute checksums and analyze as many source and destination addresses, it provides better network throughput. For both of these reasons, Jumbo Frames make the virtualization of bandwidth intensive workloads more effective. Jumbo Frames are particularly valuable in iSCSI SANs and virtualized file servers.

VM Queuing is a new R2 feature that establishes a queue on each physical NIC for each VM that uses that NIC. The purpose is to allow packets to be routed to and from the virtual machine without processing by the Hyper-V kernel. From a user and administrator perspective there is no change in behavior aside from a performance increase. From the server's point of view, it now has to queue packets for interpretation by the VMs rather than processing each packet as it arrives on the physical CPUs.

The use of TCP Chimney requires that the NIC be capable of offloading TCP. Many enterprise-class NICs are optimized in this way to improve throughput in an iSCSI SAN, however, the storage network should remain separate from your regular network traffic. TCP Chimney and VM Queueing are not usable at the same time. Both of these are disabled by default due to potential compatibility issues. Enabling them requires you to use the **netsh** command and/or edit the registry, which is a topic covered in material focused on networking in Server 2008.

To use Jumbo Frames your server's NIC must support them as well as the network hardware and the destination host. None of these optimizations are available on legacy Hyper-V network cards.

Storage Enhancements

Compared to R1, R2 provides two storage improvements:

1. Hot-Swappable VHD
2. Cluster Shared Volumes

Within a guest OS, Hyper-V R2 can "hot swap" VHD files in a running guest OS without shutting down the guest OS. This increases uptime, scalability, and server flexibility. If a server is running out of space, a VHD can be added on the fly without a reboot. If data on a VHD is needed on another VM, a VHD file could be unmounted and moved to the other VM. More about this feature is discussed in the chapter about VHD files and storage.

The other storage improvement to Hyper-V is the addition of Cluster Shared Volumes (CSV). This is an improvement to the Hyper-V kernel itself and not guest VMs. A CSV is a special type of shared LUN that is accessible by two or more cluster members at the same time. CSVs are meant to be used with R2's new Live Migration feature. They are used to store the VHD and XML config files that make up a VM. Live Migration moves the running image of the VM in memory from one clustered server to another, and when the image is done being copied it transfers ownership of the VHD and XML files in the CSV to the other node. This feature provides almost no downtime, and even TCP sessions will stay active with the applications on the VM. Live Migration is discussed in more detail in a later chapter.

At this time, the CSV is only for use in the Hyper-V role. Using a CSV to store any data unrelated to the Hyper-V role is unsupported and not recommended. Also, your shared storage solution must meet some minimum requirements that are available from the "Validate a Cluster" tool in the Cluster Manager console. Like other forms of shared storage, the SAN for CSV LUNs should be certified for R2. Regardless of your use of FibreChannel or iSCSI, the SAN should meet SCSI-3 command standards. The Validate a Cluster tool will notify you if your SAN does not meet the specifications, but you shouldn't be relying on the Validate a Cluster tool to inform you that your SAN won't work with Hyper-V. Your configuration should be researched and approved long before the implementation process is initiated.

Chapter 2: Configuring Hyper-V

Configuration Options

Configuration settings include server and user settings which are used to specify where files are stored and control interactions such as keyboard combinations and logon credentials.

- Server settings specify the default location of virtual hard disks and virtual machines.
- User settings enable customized virtual machine connection interactions and display messages and wizard pages if hidden previously. Virtual Machine Connection settings include the mouse release key and Windows key combinations.

Configure Hyper-V Settings

1. Click **Start**.
2. Point to **Administrative Tools**.
3. Click **Hyper-V Manager**.
4. In the **Actions** pane, click **Hyper-V Settings**.
5. In the **Navigation Pane** click the setting to be configured.
6. Click **OK** to save the changes and close **Hyper-V Settings.**
7. Or click **Apply** to save the changes and configure other settings.

Additional Considerations

By default, membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure. However, an administrator can use Authorization Manager to modify the authorization policy so that a user or group of users can complete this procedure.

New Configuration Wizard

The virtual network manager new configuration wizard action item allows for the creation of new virtual machines, hard disks, and floppy disks.

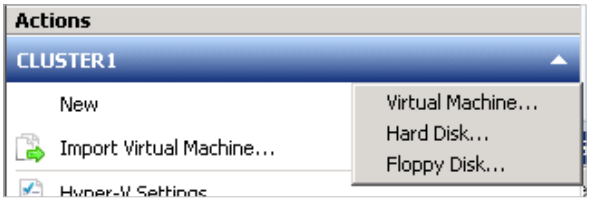


Figure 13: Starting the New Configuration Wizard

Configuration option specifics include:

- **New Virtual Machine –** creates a new virtual guest session.
- **New Hard Disk** – creates a new hard disk image. Usually, an entire new machine would be created in the first option that includes the RAM, network adapter, video, CD/DVD, and other settings. Create a new hard disk image for that configuration, and use the wizard to walk-through configuration of a hard disk image.
- **New Floppy Disk –** take an existing floppy disk and create a virtual floppy disk image from the physical disk. For example, you can use this to create an image of a bootable floppy disk that will later be used to configured or managed as a guest image.

Setting Permissions in Hyper-V

Authorization Manager is a snap-in available in Server 2008 that can set detailed permissions for Hyper-V security. Use the same measures to safeguard a virtualization server as for any server running Windows Server 2008. Use extra measures to help secure the virtual machines, configuration files, and data.

Authorization Manager contains:

- **Authorization Manager snap-in (AzMan.msc) –** uses the Microsoft Management Console (MMC) snap-in to select operations, group them into tasks, authorize roles to perform specific tasks, and to manage tasks, operations, user roles, and permissions. To use the snap-in, create an authorization store or open an existing store.
- **Authorization Manager API –** the API provides a development model to manage groups, business rules, and store authorization policies.

Start Authorization Manager

1. To open Authorization Manager, click on **Start** –**Run**. In **Run** prompt, enter **azman.msc.**
2. To open a command prompt, click **Start**, point to **All programs**, point to **Accessories**, and then click **Command prompt, enter azman.msc.**

Authorization Manager opens without a default authorization store. Authorization Manager requires a data store (authorization store) for the policy that correlates roles, users, and access rights, maintained in an Active Directory database or in a local server XML file running the Hyper-V role. 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.

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. Backup the XML file regularly. Secure the virtual machines running on the virtualization server according to individual procedures for securing that kind of server or workload.

Hyper-V Security Best Practices

The parent operating system uses a Server Core installation of Windows Server 2008 which is less likely to be compromised and reduces maintenance of patches, updates, and restarts. There is no way to upgrade from a Server Core installation to a full installation of Windows Server 2008. **Run all applications on virtual machines to reduce updates.**

- **Use the virtual machine security level to determine the security level of your management operating system –** deploy virtual machines onto virtualization servers that have similar security requirements to make management and movement of virtual machines easier.
- **Do not give virtual machine administrators permissions on the management operating system –** give virtual machine administrators the minimum permissions required. Use Role-based access control.
- **Ensure that virtual machines are fully updated before they are deployed in a production environment –** use the same methods and procedures to update virtual machines as used to update physical servers. Ensure that virtual machines are updated and/or patched before they are deployed.
- **Ensure integration services are installed on virtual machines –** timestamps and audit log entries are important for computer forensics and to ensure compliance. Integration services ensure that time is synchronized between virtual machines and the management operating system.

- **Use a dedicated network adapter for the virtualization server management operating system –** 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 un-trusted network traffic. Do not allow virtual machines to use this network adapter. Use one or more different dedicated network adapters for virtual machine networking.
- **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.

Non-Administrator Permission to Create VMs

In domain environments, the Domain Admins group will have full permissions to create and manage VMs on host servers. It's often necessary to grant additional permissions, such as the ability to start and stop VMs, to other users who should not also have full administrative permissions. Authorization Manager Snap-in, also known as AzMan.msc is the primary method for defining and managing permissions for Hyper-V.

The default location for the permissions settings XML file is in the following path:

%ProgramData%\Microsoft\Windows\Hyper-V\InitialStore.xml.

Using Authorization Manager
To access the AzMan Snap-In on full installations of Windows Server 2008, click **Start > Run** and then type **Azman.msc**. By default, AzMan is not connected to any specific security data store. To access the default Hyper-V settings, right-click on the **Authorization Manager** object and select **Open Authorization Store**. Select the **XML File** option and then browse to %ProgramData%\Microsoft\Windows\Hyper-V\InitialStore.xml.

Managing Hyper-V Permissions
To give non-administrator users full permissions:

1. On the **Hyper-V Authorization** – [Console Root\Authorization Manager\InitialStore.xml\Hyper-V service] window.
2. **Right-click** the **Administrator** object.
3. Select **Assign Users And Groups**.
4. Windows security principals or AzMan roles can be added.

Creating role definitions
Allow specific users to perform specific operations by creating new role definition objects. Regulate configuration roles by using AzMan.

Hyper-V Integration Services

Hyper-V Integration Services are available in a child partition only after they are installed in supported guest operating systems. Integration Services communicate with components in the parent partition virtualization stack that are implemented as virtual devices (VDEVs). Communications between the parent and child partition components takes place over the Hyper-V VMBus. The VMBus supports high-speed, point-to-point channels for secure inter-partition communication and enhances performance. A separate, dedicated VDEV manages each of the parent partition Integration Services function. A separate, dedicated service manages each of the Integration Services function in the child partition.

Integration Services target specific areas that enhance the functionality or management of supported guest operating systems. It is important to note that only a subset of Integration Components may be supported for some legacy or non-Windows guest operating systems. Since VSS is only supported in Windows operating systems beginning with Windows Server 2003, the VSS Integration Component is not be available for Windows 2000 Server, Windows XP, or supported Linux distributions.

Time Synchronization

Integration Services time synchronization includes:

- Keeping time synchronized in the guest operating system to account for time-drift in the virtual machine.
- Restoring a virtual machine from a snapshot or saved state where a significant period has passed since the guest operating system last synched time.

Parent partition-based time synchronization helps resolve the following issues:

- Lack of network connectivity which makes traditional network-based protocols unusable.
- Need for quicker time synchronization than network-based protocols can provide to allow fast virtual machine startup after a saved state or in restoring a snapshot.
- Need for successful time synchronization in the event that significant time has passed since the virtual machine was last online. (i.e., a saved state or snapshot).

Heartbeat

The Integration Services heartbeat detects whether a guest operating system running in a child partition becomes unresponsive. The parent partition sends regular heartbeat requests to a child partition and logs an event if a response is not received within a defined time boundary. If a heartbeat response is not received within the expected delay, the parent partition will continue to send heartbeat requests and generate events for missing responses.

Shutdown

Integration Services provides a virtual machine shutdown function. The shutdown request is initiated from the parent partition to the child partition using a Windows Management Instrumentation (WMI) call.

Key/Value Pair Exchange

Integration Services key/value pair exchange provides a means to set, delete, and enumerate specific information about the virtual machine and guest operating system configuration running in a child partition. The parent partition can request to set specific data values in the guest operating system, or retrieve the data to expose it to third-party management or other tools.

Key/value pair data is stored in the following guest operating system registry locations:

- HKLM\Software\Microsoft\Virtual Machine\Auto
- HKLM\Software\Microsoft\Virtual Machine\External
- HKLM\Software\Microsoft\Virtual Machine\Guest\Parameters

By default, the child partition exposes the data stored in **HKLM\Software\Microsoft\Virtual Machine\Auto** to the parent partition upon request.

The parent partition provides the values in **HKLM\Software\Microsoft\Virtual Machine\Guest\Parameters** to the child partition. Parent Partition values include; hostname, physicalhostname, physicalhostnamefullyqualified, and virtualmachinename.

Guest Operating Systems

For guest operating systems that support VSS, Integration Services allows the parent partition to request the synchronization and inaction of a virtual machine running in a child partition. If all guest operating systems support VSS, a backup of the entire Hyper-V server including all offline and online virtual machines can be accomplished using a VSS snapshot.

Integration Services Installation Procedure

The installation of Integration Services should be performed after the guest operating system loads for the first time. Launch the Virtual Machine Connection application from within the Hyper-V Manager console to connect to the guest operating system, and log in with an account that has administrative privileges. Select the Insert Integration Services Setup Disk option from the Action menu. This will attach an ISO image named vmguest.iso to the virtual machine DVD drive. The installation of Integration Services should begin automatically. Restart the virtual machine when the installation completes. Verify the Integration Services installed in the guest operating system by browsing services.

Hyper-V Integration Services Support

Hyper-V Integrated Services supported operating systems are illustrated in the following table. Only certain guest operating systems are supported. Some are only compatible.

Operating System	Time Synchronization	Heartbeat	Shutdown	Key/Value Pair Exchange	VSS
Windows Server 2008 x64	Y	Y	Y	Y	Y
Windows Server 2008 x86	Y	Y	Y	Y	Y
Windows Server 2003 x64 with SP2	Y	Y	Y	Y	Y
Windows Server 2003 x86 with SP2	Y	Y	Y	Y	Y
Windows 2000 Server with SP4	Y	Y	Y	Y	N
Windows 2000 Advanced Server with SP4	Y	Y	Y	Y	N
Windows Vista x64 with SP1	Y	Y	Y	Y	Y
Windows Vista x86 with SP1	Y	Y	Y	Y	Y
Windows XP x86 with SP2/SP3	Y	Y	Y	Y	N
Windows XP x64 with SP2	Y	Y	Y	Y	N
Suse Linux Enterprise Server 10 x64	N	N	N	N	N
Suse Linux Enterprise Server 10 x86	N	N	N	N	N

Figure 14: Hyper-V Integrated Services Supported Operating Systems

Hyper-V supports the following guest operating systems running in child partitions: Hyper-V Aware Windows Operating Systems, Hyper-V Aware non-Windows Operating Systems and Non Hyper-V Aware Operating Systems.

- **Hyper-V Aware Windows Operating Systems** (*enlightened* operating systems) – able to detect that they are running on the Hyper-V hypervisor and modify behavior to maximize performance (such as using hypercalls to directly call the hypervisor). These operating systems are able to host the Integration Services to perform such tasks as running Virtual Service Clients (VSCs) which communicate over the VMBus with the Virtual Service Providers (VSPs) running on the root partition for device access.
- **Hyper-V Aware Non-Windows Operating Systems** – also able to run Integration Services and, through the use of VSCs supplied by third parties, access devices via the root partition VSPs. The enlightened operating systems are also able to modify behavior to optimize performance and communicate directly with the hypervisor using hypercalls.
- **Non Hyper-V Aware Operating Systems** – unaware that they are running on a hypervisor and are unable to run the Integration Services. To support these operating systems, the Hyper-V hypervisor uses emulation to provide access to device and CPU resources. This approach allows unmodified, unenlightened operating systems to function within Hyper-V virtual machines.

Virtual Network Manager

Hyper-V Virtual Network Types

Hyper-V provides the virtual machine the ability to create multiple virtual networks. Virtual network types supported by Hyper-V are:

- **External Virtual Network** – access to external network via a physical network adapter installed in the host system; can communicate with parent partition and other virtual machines running on the same network.
- **Internal Virtual Network** – access to parent partition and other virtual machines attached to the same virtual network; do not require a physical network adapter, no access to external network.
- **Private Virtual Network** – access only to other virtual machines attached to the same virtual network; do not require a physical network adapter, no access to parent partition, no access to external network.

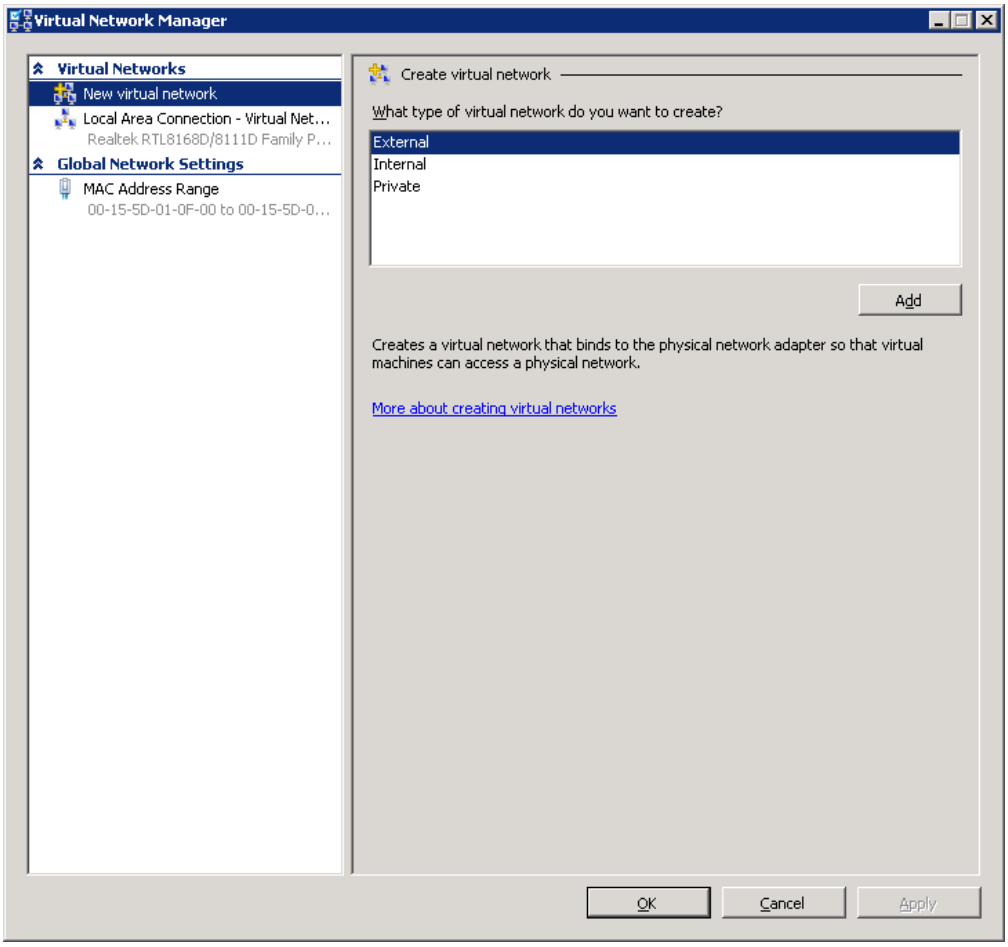


Figure 15: Adding a New Virtual Network Adapter

Existing Virtual Network Switches
Current VM configured network switches will be listed individually in the left pane of the **Virtual Network Manager** dialog box. Select an existing virtual network switch to change the name of the virtual switch, change the internal or external connection that the switch has access to, or remove the network switch altogether.

Hyper-V Server Remote Administration:

- One-to-one correspondence between external virtual networks and physical networks adapters.
- Not possible to bind more than one external virtual network to a physical network adapter.
- If multiple external virtual networks are required, a physical network adapter must be installed in the host system for each one.
- In Hyper-V server remote administration, a separate physical network adapter is necessary.

Creating a New Hyper-V Virtual Network

Access the **Virtual Network Manager**. Launch the **Hyper-V Manager** (**Start** → **Administrative Tools** → **Hyper-V Manager**). Unless the Hyper-V Manager is already connected to the required Hyper-V Server, connect to the appropriate server in the left hand panel by right clicking on Hyper-V Manager in the left hand panel. Select Connect to Server. When the server is connected, click on the Virtual Network Manager link in the Actions panel. Once loaded, the manager dialog will appear as follows:

The left hand pane in the Virtual Network Manager contains a list of existing virtual networks configured on the selected Hyper-V server. At the top of the list is the option to **Add Virtual Network** which, when selected, provides the option to add an **External**, **Internal** or **Private** virtual network. Once the virtual network type has been selected, the main panel will change to display the virtual network settings screen.

In the case of private and internal virtual networks, the name of the virtual network needs to be specified. For external private networks, select a physical network adapter from the drop down list.

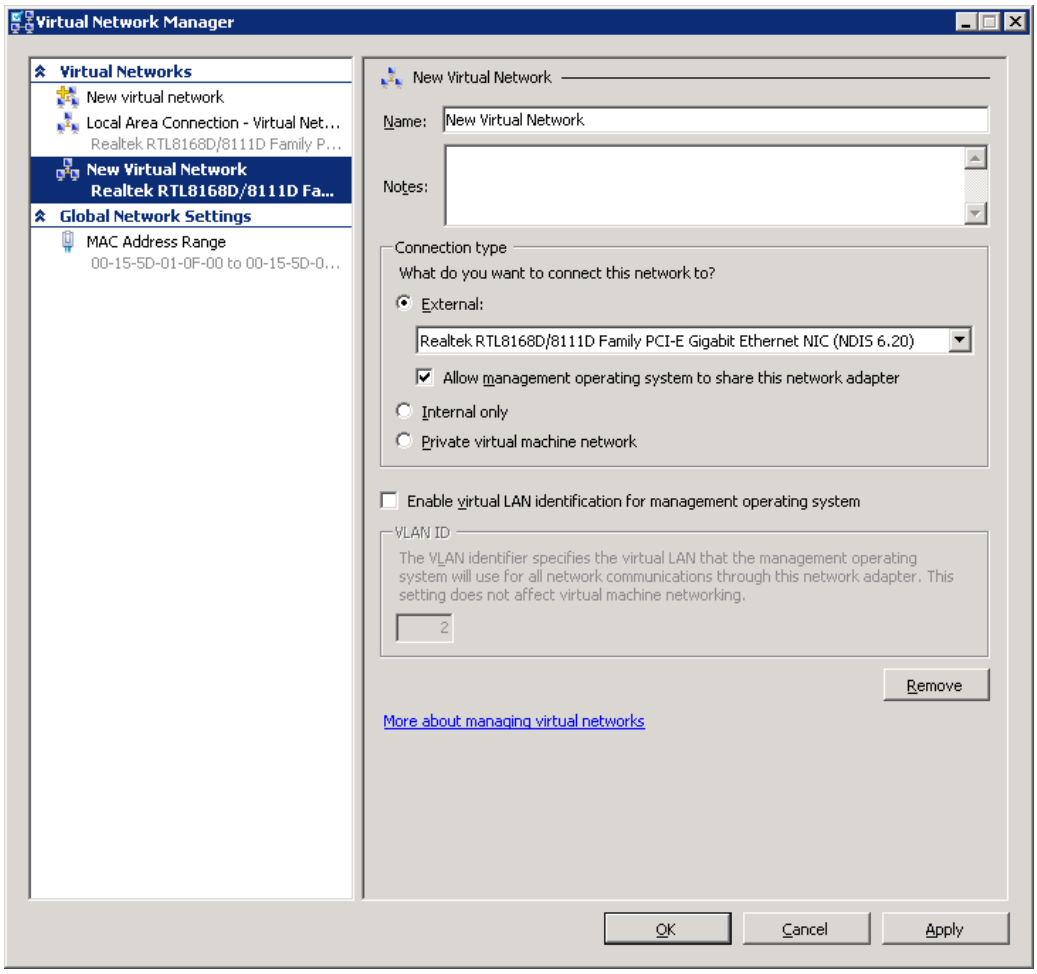


Figure 16: Adding a New Virtual Network

The **Enable virtual LAN identification for parent partition** option is only available for external and internal virtual networks, and requires a physical network adapter with VLAN support.

Assigning Virtual Machines to Virtual Networks

The virtual machine needs a virtual network adapter to connect to a virtual network. A single virtual machine can contain multiple virtual network adapters, though each virtual network adapter can be connected to only one virtual network. It is possible for multiple virtual adapters to connect to the same virtual machine.

Security Considerations

Firewall and antivirus software running on the host operating system do not protect guest operating systems. Install firewall and antivirus software directly on the guest operating systems to obtain this protection.

Connecting to an Existing Hyper-V Virtual Network
Ensure that a virtual network adapter is available. Right-click the virtual machine to view currently configured virtual hardware devices. Select **Settings...** The right hand panel of the settings dialog contains a list of hardware, including any virtual network adapters and information about the virtual networks to which they are attached.

To add a new adapter, select **Add Hardware** from the top of the device list, select **Network Adapter** from the list in the main panel and click **Add** to proceed to the settings screen for the new adapter. On this screen, select the virtual network to which the device is to be attached and click **Apply** to commit the configuration changes.

VLAN Tagging

Virtual LAN (VLAN) tagging allows for isolating network resources using a virtual switch.

VLAN tagging is a way to segment traffic on your network. VLAN tagging was originally implemented on physical switches and routers before it first appeared in virtual switches. The most common way to implement VLAN tags in an infrastructure is to apply a VLAN tag to a switch port. In this model the switch adds the tag to all frames that flow through that port.

It is important that the networking infrastructure knows how to handle the VLAN tags that have been setup because they affect the routing of the packets and are part of the TCP/IP packet itself. This means that routers and switches must know how to evaluate a VLAN tag in order to determine where to route a particular packet.

Network Adapter Performance

As mentioned in the "What's new in R2" section, 2008 R2 offers some opportunity for performance improvements, assuming your server hardware supports them. These improvements are:

- **VM Chimney** – also known as TCP/IP offload.
- **Jumbo Packets** – provides more payload per Ethernet frame.
- **VM Queueing** – improves throughput by bypassing the Windows kernel.

VM Chimney and Jumbo Packets are configured from the Properties of the **Microsoft Virtual Machine Bus Network Adapter** in the **Device Manager**. This is shown in Figure 17.

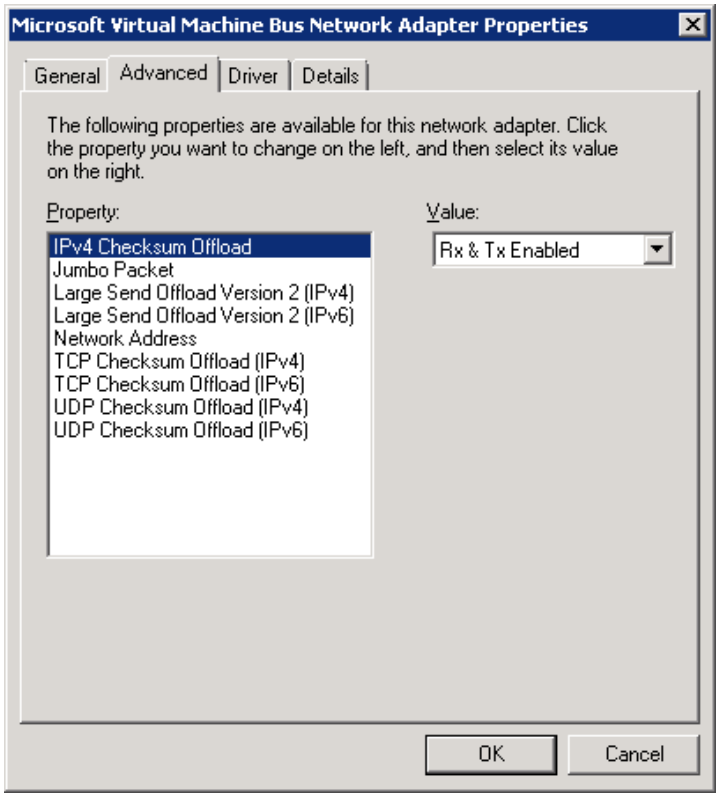


Figure 17: Enabling R2 NIC Enhancements on the Host

High Availability Configuration

Availability means that users are able to access a system to do their work. Whereas high availability ensures operational continuity which is accomplished through the use of the Windows Server 2008 Failover Cluster feature.

Virtual machines can be managed by the Failover Cluster which can be used inside virtual machines to monitor and move VM workloads.

Hosts and Guests

Guest is the Hyper-V OS and environment that is running in a child partition. Host is the physical machine being managed by the OS on the Hyper-V parent partition.

The Windows Server 2008 Failover Cluster configuration has the following advantages:

- VMs can be moved to other cluster nodes if the physical machine that Hyper V and the VM are running on needs updating, changes, or rebooting.
- If the physical machine that Hyper-V and the VMs are running on fails in some respect the other members of the Failover Cluster will bring the VMs online automatically.
- If the VM fails, it can be restarted on the same Hyper-V server or moved to another Hyper-V server.

Differences between Planned and Unplanned Downtime

- Planned downtime is normally a scheduled function such as in hardware servicing or software patching.
- Unplanned downtime is an unexpected situation, such as a server is offline and all the VMs running on that server need an automatic restart without interruption.

Quick Migration

Quick Migration both moves running virtual machines from one physical computer to another. There is downtime with quick migration because the VM is saved, moved, and restored.

To use quick migration a cluster needs to be created with either Windows Server 2008 Enterprise or Windows Server 2008 Datacenter. Standard edition does not support clustering. The following diagram shows an example of a cluster setup. The public network is used to connect these cluster nodes and the virtual machine, to other network resources. The private network is used for cluster-related network traffic such as a heartbeat and lets the cluster nodes verify the state of other cluster nodes.

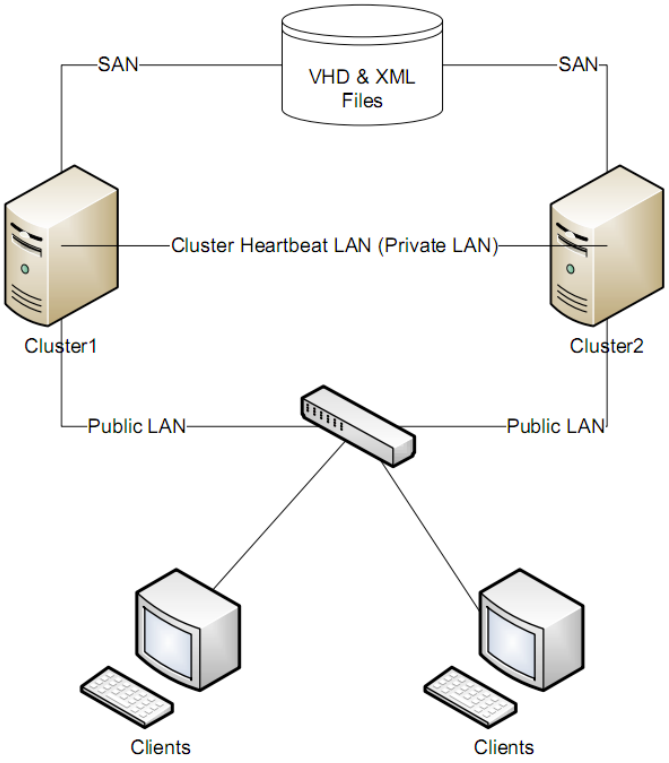


Figure 18: Clustering Scenario Schematic

System Requirements

System requirements for clustering include software, hardware, network and storage requirements and guidelines for a quick migration scenario.

Host Nodes Software Requirements

- Windows Server 2008 Enterprise or Windows Server 2008 Datacenter (with Hyper-V) must be installed on the nodes (Standard does not have Failover clustering capabilities).
- Licensed copies of the operating system and other software to run on the guest virtual machine.
- A name-resolution service; such as Domain Name System (DNS), DNS dynamic update protocol, Windows Internet Name Service (WINS), or Hosts file.
- All cluster nodes must be in the same Active Directory domain.

Hardware Requirements and Guidelines

- 64-bit server environment.
- Support for hardware-assisted virtualization technology.
- Cluster nods must have identical hardware and the same processor architecture. Moving between AMD and Intel will not work. Moving between an Intel Core 2 Duo and an Intel Core i7 will not work.
- Compatible hardware components because the failover cluster is installed on a storage area network (SAN), with multiple devices and clusters sharing the SAN with a cluster.
- Hardware minimum requirements: 1.0 GHz CPU speed, Intel VT or AMD-V, and Minimum RAM of 512 MB (additional needed for each guest operating system), DEP (Data Execution Prevention: AMD-ND or Intel-XD).

Network Requirements and Guidelines

- Each cluster node requires at least two network adapters and must be connected by two or more independent networks, and at least two LANs or VLANs are required to prevent a single point of failure.
- Nodes in cluster must be able to access an Active Directory domain controller. The domain controller should be in the same location and on the same LAN as the nodes in the cluster.
- Network configuration includes several NIC's for management and virtual networking.

Storage Requirements and Guidelines

- This external storage unit to be used as storage must be connected to all nodes in the cluster. Use some type of hardware redundant array of independent disks (RAID).
- If using iSCSI, each node must have a network adapter dedicated to the cluster storage.

Set Up a Cluster

For quick migration set up a cluster with your servers. Determine which servers will be in the cluster, and then use the wizard. Decide on the amount of memory available to a virtual machine, which can be altered depending on VM needs.

Install Windows Server 2008

First, install Windows Server 2008 Enterprise or Windows Server 2008 Datacenter in the same domain on the host servers that will become the cluster nodes. Log on locally with a domain account that is a member of the local administrators group on all nodes. Then install the failover cluster feature. Hyper-V is installed by default.

Once Windows Server 2008 Hyper-V is installed, manage with the Microsoft Management Console (MMC) in the same way that other server roles are managed.

Configure the Cluster

1. Set up network
2. Set up and configure cluster disks
3. Create the server cluster

Create a Virtual Machine

1. Use the Hyper-V New Virtual Machine Wizard to create a virtual machine.
2. Define name and location, memory size, and the network information.

Create the Host Cluster

The host cluster can be created once the virtual machine resides on the shared storage. Decide which resources need to be highly available and which machines need to be clustered. Set up the host cluster using a wizard within the Cluster Management snap-in. Select the service or application to be configured for high availability from a list of options.

Select Virtual Machine

A wizard scans for configuration files (VMCs) and a list of all available virtual machines, their status, and their host servers' displays. Virtual machines are added automatically. Select multiple virtual machines to make highly available. Now, the virtual machines are clustered, along with appropriate shared storage.

Fail Over a Workload with Quick Migration

When the virtual machine is online use quick migration to move it between host servers. Start in the **Failover Cluster Management** console. The console shows the virtual machines running on the individual nodes. Highlight a virtual machine to view a summary of its properties.

Right click the virtual machine name to display the **Actions** menu. The **Actions** dropdown displays with the option to move the virtual machine to another node and to select the destination node. Once the command has been run, the virtual machine enters a pending state before it is moved. After a few seconds, the virtual machine appears on the destination node and the status will return to Online. The quick migration process is complete.

Chapter 3: Hyper-V Remote Configuration

Understanding Remote Administration

Hyper-V is managed using Windows Management Instrumentation (WMI). WMI allows Hyper-V manager to be installed on a client machine that is running Server 2008, Windows 7, or Vista SP1.

Configuring Remote Administration

Install the Hyper-V management tools on a full installation of Windows Server 2008 and on Windows Vista Service Pack 1 (SP1). The minimum requirement to complete this procedure is Membership in the local **Administrators** group.

Installing the Management Tools

Obtain and apply the appropriate operate system update to install the management tools.
Update locations:

- **Windows Update** – if computer is not set up to install updates automatically, install manually.
- **Microsoft Download Center** – download the file to the computer and then double-click the .msu file.

If installing the tools on Windows Vista SP1, no additional installation steps are required, so proceed to the configuration instructions.

If installing the tools on Windows Server 2008, complete the remaining steps.

1. Open Server Manager.
2. In Server Manager, under **Features Summary**, click **Add Features**.
3. On the **Select Features** page, expand **Remote Server Administration Tools**, and then expand **Remote Administration Tools**.
4. Click **Hyper-V Tools**, and then proceed through the rest of the wizard.

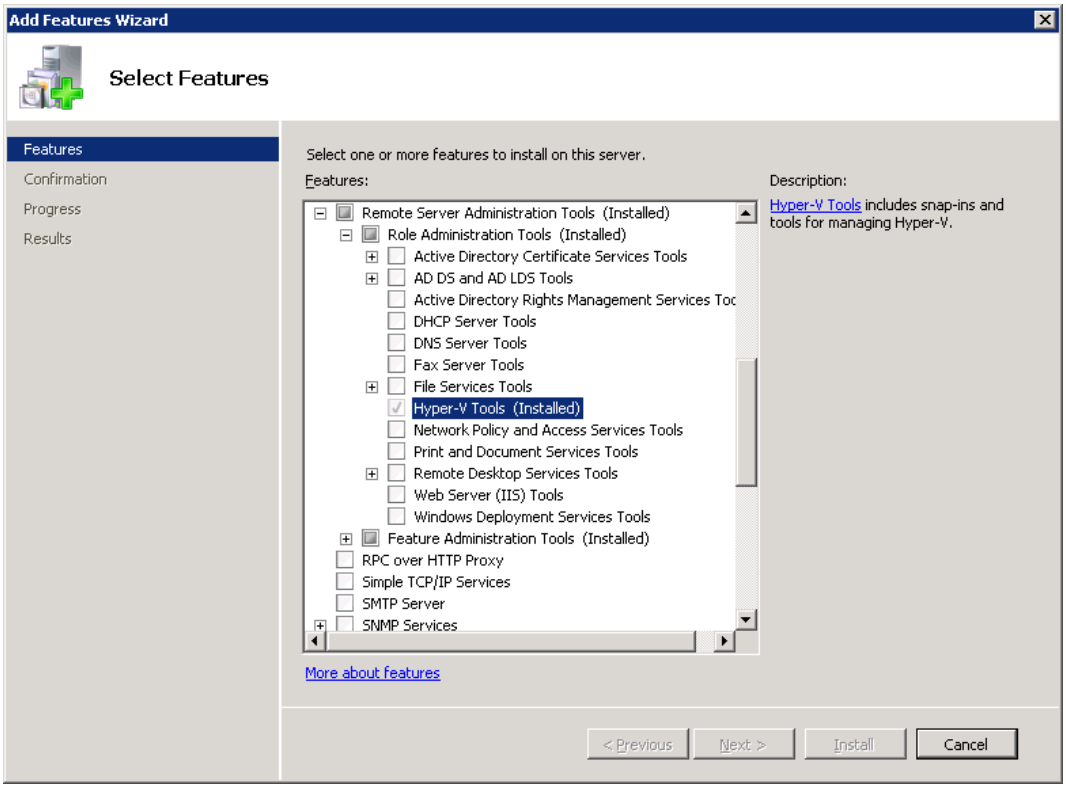


Figure 19: Installing Hyper-V Remote Administration Tools on Server 2008.

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 the Hyper-V management tools will be run.

No additional configuration is required if 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, modify the authorization policy, but skip the steps for modifying the Distributed COM Users group and the Windows Management Instrumentation (WMI) namespaces.

Remote Management Connections

Full installation of Windows Server 2008

The following procedures assume the Hyper-V role is installed on the server. Enable the WMI firewall rules.

1. From an elevated command prompt, type:
   ```
   netsh advfirewall firewall set rule group="Windows Management
   Instrumentation (WMI)" new enable=yes.
   ```

2. If the command succeeds, the display should read: **Updated 4 rules(s). Ok.** To verify, view the results in **Windows Firewall with Advanced Security**.
   a. Click **Start** → **Control Panel**. Use **Classic View**.
   b. Click **Administrative Tools** → **Windows Firewall with Advanced Security**.
   c. Select inbound rules or outbound rules and then sort by the **Group** column. There should be three inbound rules and one outbound rule enabled.

3. Add Remote User to the Distributed COM Users group.
   a. Click **Start** → Point to **Administrative tools**. Click **Computer Management**
   b. If User Account Control is enabled, click **Continue**. Component Services opens.
   c. Expand **Local Users and Groups**, and then click **Groups**.
   d. Right-click **Distributed COM Users** and click **Add to Group**.
   e. In the **Distributed COM Users Properties** dialog box, click **Add**.
   f. In the **Select Users, Computers, or Groups** dialog box, type the name of the user and click **OK**.
   g. Click **OK** again to close the **Distributed COM Users Properties** dialog box.
   h. Close **Component Services**.

4. The remaining steps grant the required remote user WMI permissions for two namespaces: the CIMV2 namespace and the virtualization namespace.
   a. Click **Start**, click **Administrative Tools**, and then click **Computer Management**.
   b. In the **Navigation** pane, click **Services and Applications**, right-click **WMI Control**, and then click **Properties**.
   c. Click the **Security tab** → **Root** → **CIMV2**. Below the namespace list, click **Security**.
   d. Check to see if the appropriate user is listed in the **Security for ROOT\CIMV2** dialog box. If not, click **Add**. In the **Select Users, Computers, or Groups** dialog box, type the name of the user and click **OK**.
   e. On the **Security** tab, select the name of the user.
   f. Under **Permissions for <user or group name>**, click **Advanced**.
   g. On the **Permissions** tab, verify that the user is selected and then click **Edit**.
   h. In the **Permission Entry for CIMV2** dialog box, modify the following:
      i. For **Apply to**, select **This namespace and subnamespaces**.
      ii. In the **Permissions** list, in the **Allow** column, select the **Remote Enable** check box.
      iii. Below the **Permissions** list, select the **Apply these permissions to objects and/or containers within this container only** check box.
      iv. Click **OK** in each dialog box until you return to the **WMI Control Properties** dialog box.

5. Repeat the process for the virtualization namespace.
   a. Scroll down to see the virtualization namespace. Click **virtualization**.
   b. Below the namespace list, click **Security**.
   c. 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**.
   d. On the **Security** tab, select the name of the user.
   e. Under **Permissions for <user or group name>**, click **Advanced**.
   f. On **Permissions** tab, verify that the user is selected, click **Edit**. In the **Permission Entry for virtualization** dialog box, modify the following settings:
      i. For **Apply to**, select **This namespace and subnamespaces**.
      ii. In the **Permissions** list, in the **Allow** column, select the **Remote Enable** check box.
      iii. Below the **Permissions** list, select the **Apply these permissions to objects and/or containers within this container only** check box.
      iv. Click **OK** in each dialog box and then close Computer Management.

6. Restart the server to apply the changes to the authorization policy.

Server Core installation of Windows Server 2008

1. Enable server Windows Management Instrumentation firewall rules. From an elevated command prompt, type:
   ```
   netsh advfirewall firewall set rule group="Windows Management
   Instrumentation (WMI)" new enable=yes
   ```
2. If the command is successful, it displays the message: **Updated 4 rules(s). Ok.**
3. Next, 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 who will have remote access.
4. Next, connect remotely to the server running the Server Core installation to modify the authorization policy and the two WMI namespaces, using MMC snap-ins that are not available on the Server Core installation.
5. Log on to the computer on which the Hyper-V management tools are run, using a domain account that is a member of the Administrators group on the computer running a Server Core installation.
6. Authorization policy configuration instructions assume that the default authorization policy has not been modified, including the default location, and that the account remote requires full Hyper-V role administrative access.
7. 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. Authorization policy configuration assumes that the default authorization policy has not been modified, including the default location, and that the account for remote access requires full Hyper-V administrative role access.
   a. Click **Start** → **Start Search** and type **azman.msc**.
   b. If prompted to confirm the action, click **Continue**.

c. Authorization Manager Microsoft Management Console (MMC) snap-in displays.

d. In the Navigation pane, right-click **Authorization Manager**.

e. Click **Open Authorization Store**.

f. Make sure that **XML file** is selected.

g. Browse to the %system drive%\Program Data\Microsoft\Windows\Hyper-V folder. Select InitialStore.xml > click **Open** and click **OK.**

8. By default, the Program Data folder is a hidden folder. If the folder is not visible, type: **<system_drive>\ProgramData\Microsoft\Windows\Hyper-V\initalstore.xml.**
9. In the Navigation pane, click **Hyper-V services → Role Assignments.**
10. Right-click **Administrator**, then point to **Assign Users and Groups;** point to **From Windows and Active Directory.**
11. In the **Select Users, Computers, or Groups** dialog box, type the domain name and user name of the user account, and then click **OK**.
12. Close **Authorization Manager**.
13. The remaining steps grant the required WMI permissions to the remote user for two namespaces: the CIMV2 namespace and the virtualization namespace. These are identical to those described in the normal Server 2008 installation.

Configuring Windows Vista SP1

Configure Windows Vista SP1 when domain-level trust is not established. Log on to the computer running Windows Vista SP1. Enable Windows Management Instrumentation firewall rules. From an elevated command prompt, type:

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

If the command is successful it will display the message: **Updated 8 rules(s). Ok.**

To verify that the command succeeded, view the results in **Windows Firewall with Advanced Security**. Click **Start**, click **Control Panel**, switch to **Classic View** if not currently 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.

1. Enable a Microsoft Management Console firewall exception. From an elevated command prompt, type: **netsh firewall add allowedprogram program=%windir%\system32\mmc.exe name="Microsoft Management Console"**
2. Start Hyper-V Manager to verify connection has been made with the remote server. Click **Start**, click the **Start Search** box, type **Hyper-V Manager** and press **Enter**. If 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 configured virtual machines configured on the server.

Install Hyper-V Manager on Windows 7

Download the Hyper-V Remote Management Configuration Utility and its documentation. Now, download and install the Remote Server Administration Tools for Windows 7 (RSAT). After installing RSAT, open **Control Panel**, go to **Programs and Features**, and choose **Turn Windows features on or off**. Expand the **Remote Server Administration Tools Heading** and the **Role Administration Tools** subheading, and then select **Hyper-V Tools** as show below.

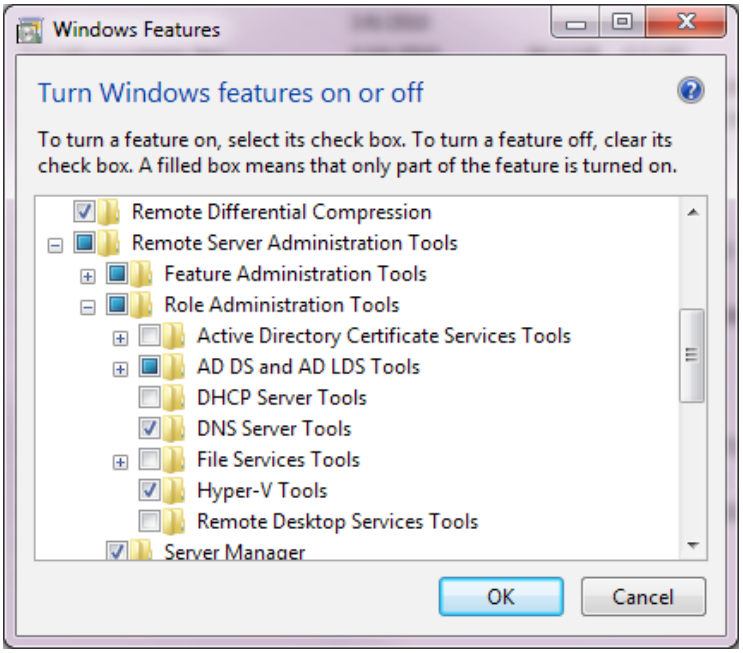


Figure 20: Hyper-V Remote Administration feature in Windows 7

Remote Connectivity

Use the Virtual Machine Connection application to connect to a Hyper-V virtual machine, via the **Connect** option under the virtual machine **Action** pane. By default, only administrators have unrestricted access to the Hyper-V Manager console, including all VMs defined on permitted servers.

Use Remote Desktop Connection (mstsc.msc) to reach VMs from a distance. Windows Server 2008 licenses two built-in Remote Desktop connections out-of-the-box.

For Windows Server 2008 and Server Core, this feature must be enabled. Verify that the version of Remote Desktop Connection on the connecting host supports Network Level Authentication and Remote Desktop Protocol 6.1, required to successfully connect to Windows Server 2008 default installations and remote Server Core. RDC 6.0.6001 ships with these enhancements as part of Windows Server 2008.

To enable remote desktop on the full version of Server 2008, go to **Control Panel**, then **System**, then click the **Advanced System Settings** link. The remote desktop settings are found under the **Remote** tab.

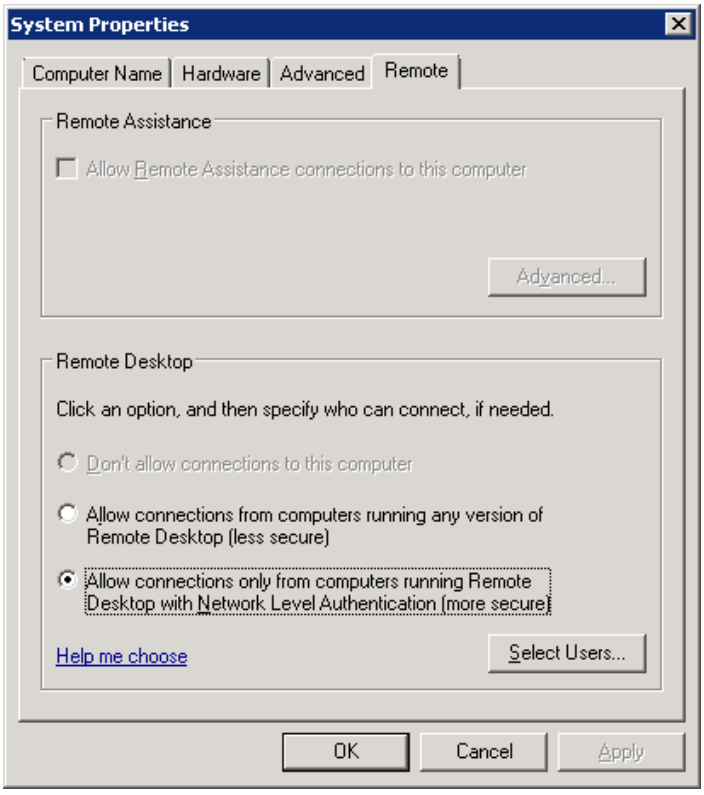


Figure 21: Allowing Remote Desktop in Server 2008.

To enable remote desktop on Server Core, run the following command from the Windows shell:

```
cscript %windir%\system32\SCRegEdit.wsf /ar 0
```

Using RDP helps to maintain security on the box by minimizing the need for an administrator to grant unneeded Hyper-V Manager access privileges. In addition, there is also a significant decrease in memory resources per VM connection and with multiple VMs per host machine, this could significantly increase performance. Text can also be copied from the guest VM to the host machine. This cannot be accomplished with the Virtual Machine Connection application.

Remote Administration

Remote administration can be used to manage server settings, create and configure VM's, configure virtual networking, and control VM state.

Manage Server Settings

Use Failover Cluster Manager snap-in to access virtual machine settings to make configuration changes. The cluster updates configuration changes automatically. However, if changes are made to the virtual machine settings from the Hyper-V Manager snap-in, update the cluster manually after the changes have been made. If the configuration is not refreshed after networking or storage changes are made, a subsequent failover may succeed, but if it doesn't the virtual machine may be configured incorrectly.

Modify VM Settings
In the Failover Cluster Manager snap-in expand **Services and Applications**, and then click the virtual machine to modify its settings. In the center pane right-click the virtual machine resource and then click **Settings**. If **Settings** does not display, collapse the virtual machine resource and then right-click it. The **Settings** interface appears. This is the same interface that is seen in Hyper-V Manager. Configure the settings for the virtual machine.

If the Hyper-V Manager is used instead of the Failover Cluster Manager to configure settings for a virtual machine, be sure to refresh the virtual machine configuration in Failover Cluster Manager. To do this, expand **Services and Applications**, and then click the virtual machine that needs to have its configuration refreshed. In the **Actions** pane, scroll down, click **More Actions**, and then click **Refresh virtual machine configuration**.

Run-Time Requirements

Virtualization services require x64-based system that supports hardware-assisted virtualization running Hyper-V. Programs that interact with the WMI interfaces however, can run remotely on any system that supports WMI.

About the Virtualization WMI Provider

Microsoft Windows Server 2008 Hyper-V allows system administrators to consolidate separate hardware servers on to a single server running Microsoft Windows Server 2008 as the host OS.

Each hosted virtual machine runs in its own separate and isolated virtual environment. Just some of the advantages, include:

- Easier administrator management
- Testing and support advantages
- Support and test legacy hardware
- Snapshot support
- User is able to monitor and control VM environment
- Easy customization
- WMI scripting can be done directly

The Resource Virtualization Profile defines two different virtual resource classes:

- **Shared Resource** - represents the resources of the host that are, or are capable of being shared among multiple virtual systems.
- **Synthetic Resource** - represents the virtual resources that have no corresponding host resource. **Msvm_EmulatedEthernetPort** is an example of a synthetic resource.

Virtualization WMI includes the following classes: BIOS, Input, Integration Components, Memory, Networking, Processor, Profile Registration, Resource Management, Serial Devices, Storage, Video, Virtual System, Virtual System Management.

USNs

Active Directory Domain Services (AD DS) uses update sequence numbers (USNs) to keep track of data replication between domain controllers. Each time that a change is made to data in the directory, the change is added to the USN. Source and destination domain controllers use the Up-to-dateness vector and High water mark (direct up-to-dateness vector) replication process values to filter destination domain controller required updates. USN rollback occurs when the USN normal updates are circumvented and a domain controller tries to use a USN that is lower than its latest update.

Although it may not appear on your exam, do not pause any DC that is running as a Hyper-V guest. Doing so can cause USN synchronization with other DCs to fail.

Read-only Domain Controllers

Read-only domain controllers (RODCs) are domain controllers in an Active Directory database that host read-only copies of the partitions. RODCs avoid most USN rollback issues because they do not replicate any changes to the other domain controllers. However, if an RODC replicates from a writeable domain controller that has been affected by USN rollback, the RODC is affected as well. Restore an RODC using an Active Directory compatible backup application rather than using a snapshot.

Security and image files - Secure VHD host operating system files and the guest operating system with the same physical restrictions and software restrictions used to secure a physical domain controller.

Avoid Creating Single Points of Failure

Implement system redundancy to avoid introducing potential single points of failure. Consider the following recommendations while keeping in mind potential for increases in administration costs:

- Run at least two virtualized domain controllers per domain on different virtualization hosts to reduce the risk of losing all domain controllers if a single virtualization host fails.
- Diversify the hardware to limit damage that might be caused by a malfunction that is specific to a vendor configuration, a driver, or a single piece or type of hardware.
- Domain controllers should be running on hardware that is located in different regions of the world, if possible to help reduce the impact of a disaster or failure that affects a domain controller site.
- Maintain physical domain controllers in each domain to decrease the risk of a virtualization platform malfunction which would affect all host systems that use that platform.

Security Considerations

Manage the host computer that is running virtual domain controllers as carefully as a writeable domain controller, even if that computer is only a domain-joined or workgroup computer. This is an important security consideration in minimizing attacks that can compromise all virtual machines, domains, and forests that the computer is hosting.

Local administrator should have credentials equivalent to the default domain administrator. To avoid security and performance issues use a host running a Server Core installation of Windows Server 2008, with no applications other than Hyper-V. In a branch office or other locations that cannot be satisfactorily secured, a read-only domain controller (RODC) is recommended. If a separate management network exists, the host should be connected only to the management network.

Security boundaries

Using virtual machines makes it possible to have many different domain controller configurations. Consider carefully the way that virtual machines affect boundaries and trusts in the Active Directory topology.

Remote Desktop Protocol (RDP)

The most common remote connection is an RDP. Instead of using Virtual Machine Remote Control (VMRC) to control virtual machines on a Hyper-V host by remote control, SCVMM uses the Remote Desktop Protocol (RDP). All supported versions of Windows Server 2008 and Windows Vista SP1, SCVMM connect to the host via RDP with the default port of 2179. For any other operating system, SCVMM connects via RDP to the guest operating system with the default port of 3389.

Change Remote Connections to Virtual Machines

Applies To: System Center Virtual Machine Manager 2008 (including R2):

When a Windows Server-based host is added to System Center Virtual Machine Manager (SCVMM) using **Add Hosts Wizard**, remote connections to virtual machines on that host are enabled by default, and the default remote control connection port is obtained from the General Settings in Administration view. After a Windows Server-based host has been added, you can change the remote connection settings in the Host properties. In the Administration view, set the default port in **General Settings**.

By default, encryption for VMRC connections is not enabled when a Virtual Server host is added. To enable encryption for VMRC connections, modify the remote connection host properties in the SCVMM Administrator Console.

Modify Hyper-V host remote connection settings

1. In **Hosts** view, locate the host group that contains the host to be modified.
2. In the **Results** pane, double-click the host.
3. Click the **Remote** tab.
4. To enable or disable remote connections, select or clear the **Allow remote connections to virtual machines on this host** check box.
5. If remote connections are enabled, in the **Remote connections port** box, set the port that SCVMM will use to communicate with virtual machines on the Hyper-V host. The default port is 2179; enter any value from 1 to 65535. No firewall exception for the port is needed.

Modify Virtual Server host remote connection settings

1. In **Hosts** view, locate to the host group that contains the host to be modified.
2. In the **Results** pane, double-click the host.
3. Click the **Remote** tab.
4. To enable or disable remote connections, select or clear the **Allow remote connections to virtual machines on this host** check box. If remote connections are disabled, all other configuration options become unavailable.
5. If remote connections are enabled, in the **Remote connections port** box, set the port that SCVMM will use to communicate with virtual machines on the Virtual Server host. The default port is 5900; enter any value from 1 to 65535. No firewall exception for the port is needed. If multiple users will be allowed to access virtual machines on this host, select the **Allow multiple VMRC connections** check box.

6. If a time-out will be enforced for VMRC connections, select the **Enable remote connection timeout** check box and then specify the time-out interval. The default time-out interval is 15 minutes; Enter any value from 1–600.
7. If there will be VMRC remote connection encryption for this host, select the **Secure remote connection with this host** check box. This option enables Secure Sockets Layer (SSL) encryption by using an unsigned certificate from Virtual Server. It is recommended that SSL security for VMRC remote connections be implemented, particularly if Basic authentication is used to transmit plain text passwords.
8. If using a signed certificate from a certification authority to implement SSL encryption, do one of the following:
    a. Click **Upload or replace certificate** and then click **Browse** to upload or to replace a certificate.
    b. Click **Generate Certificate Request** to open the **Secure VMRC Certificate Request** dialog box. Then, perform the following steps to generate a certificate request file that can be sent to a certification authority to obtain a certificate to upload:
        i. In the appropriate boxes, type information about your organization.
        ii. Do not type more than two characters in the **Country/Region** box, or more than 64 characters in any other box. If exceeding these limits is expected, the certificate request file is created but is not valid for creating a certificate from a certification authority.
        iii. In the **Key length** list, choose the level of encryption the certificate will use. The default key length is 512 bits; select 1024, 2048, or 4096 bits from the list.
        iv. A certificate request with a key length greater than 4096 bits can be generated by using the New-VMRCCertificateRequest cmdlet in Windows PowerShell - Virtual Machine Manager command shell. Generating a certificate request with a key length over 4096 bits may take quite awhile. Track the progress of the process in Jobs view.
        v. In the **Save request file to** box, type the file path and file name for the certificate file, or click **Browse** to navigate to a folder, type the file name, and then click **Save**.
        vi. Click **Generate** to generate the certificate request file.

Hyper-V Integration Components

Install the Hyper-V integration components through the SCVMM Administrator Console. Right-click powered-off virtual machine and select **Install Virtual Guest Services**. Hyper-V integration components are also automatically installed with:

- P2V conversion
- V2V conversion

Authorization Manager allows administrators to integrate role-based access control to applications. The System Center Virtual Machine Manager (SCVMM) is an easy-to-use and cost-effective application for administrators who are responsible for managing virtual networks. SCVMM 2008 is a single application that allows you to configure and manage your entire virtual environment.

Virtual networking is the way a virtual environment is configured to work on the physical components to allow other machines to access virtual resources through the physical network. In this chapter you learned about different virtual network concepts, such as VLANs, virtual switches, VLAN tagging, and the communication settings. One of the advantages that an administrator has is the ability to configure Hyper-V remotely.

Objective Summary

Know how to use Authorization Manager. Authorization Manager allows integration of role-based access control to applications. This gives flexibility to assign application access to users based on their job functions.

Understand System Center Virtual Machine Manager. Understand that System Center Virtual Machine Manager is an easy and cost-effective application for administrators that are responsible for managing virtual networks. Since SCVMM works with the Windows Server 2008 technology, understand that SCVMM allows the configuration and manipulation of the physical and virtual machines, consolidate underutilized physical machines, and implement new virtual machines.

Know how to implement virtual networking. Be familiar with VLANs, virtual switches, VLAN tagging, and the three communication settings that you can configure. Be able to set up a network adapter in the Virtual Network Manager tool.

Understand how to configure Hyper-V remotely. Know how to remotely configure and maintain Hyper-V remotely. Understand how to configure the Windows Firewall and RDP settings to allow for the remote administration.

Chapter 4: Creating Virtual Hard Drives

Creating Hyper-V Virtual Hard Drives (VHD)

Virtual hard disks can be created as part of the virtual machine creation process or they can be created independently from the virtual machine. The VHD file stores the disk image that holds the data for a virtual machine's hard drive.

Differing VHD Options

There are three different Hyper-V virtual hard disk types:

- **Fixed-size disks** – use the amount of physical space that is specified when created. Fixed disks are ideal for performance but are less portable due to size.
- **Dynamically expanding disks** – expand in size only as data is written. Dynamically expanding disks are very portable but have some drawbacks such as fragmentation. Hyper-V provides the ability to convert a fixed-size disk to a dynamically expanding disk, and vice-versa. VHD file size can be increased, but the VHDs must be taken offline before this can be done.
- **Differencing Disks** – are dynamically expanding VHD files that are related to a parent virtual hard disk file as an overlay that can be used to create very simple or very complex parent-child hierarchies. Each parent and child VHD is stored as an individual file.

Automatic Differencing Disks

Automatic differencing disks are used to support Hyper-V virtual machine snapshots and are created when a virtual machine snapshot is taken.

Differencing Disk Structure

- Similar to a dynamic VHD
- Contains associated parent VHD modified disk blocks
- Parent VHD read only

- Differencing VHD must be modified
- Sometimes referred to as a child VHD
- Parent VHD can be one of the three VHD types (dynamic, static, differencing)
- Do not modify parent
- Keep parent VHD and differencing VHD in same directory on local volume for native boot situations
- Attaching VHD – not used for native boot so parent VHD can be in different directories, and on a different volume or on a remote share

Pass-Through Disks

Pass-through disks allow virtual machines to access storage mapped directly to the Hyper-V server without requiring the volume be configured. Pass-through disks cannot be dynamically expanded, snapshots cannot be taken and differencing disks cannot be used.

Disk Types

- IDE
  - You must use at least one IDE drive for booting
  - 2 IDE controllers with up to 2 devices each
- SCSI
  - Are synthetic devices vs. emulated
  - 4 controllers with up to 64 devices each
  - Operates over the VM Bus which is less overhead

Select Virtual Hard Disk (VHD) Location

Once the type of disk is selected, click **Next** to specify a name and location for the virtual disk. Any location accessible to the host system may be used, or the default location accepted. Click **Next** to proceed to the **Configure Disk**. Continue through the creation process. Click **Finish** when completed.

Modifying Existing Hyper-V Virtual Hard Drives

Modify using the **Edit Virtual Hard Disk Wizard**. This allows you to convert or expand a VHD.

Hyper-V includes Compact, Convert, Expand, Merge, and Reconnect virtual hard disk options.

- **Compact –** decreases size of VHD image file.
- **Convert –** to and from dynamic hard disks.
- **Expand –** increases size of dynamic expandable fixed virtual hard disks.
- **Merge –** merges content from differencing VHD into applicable parent VHD.
- **Reconnect –** differencing disks must be associated with parent VHD to be able to reconnect.

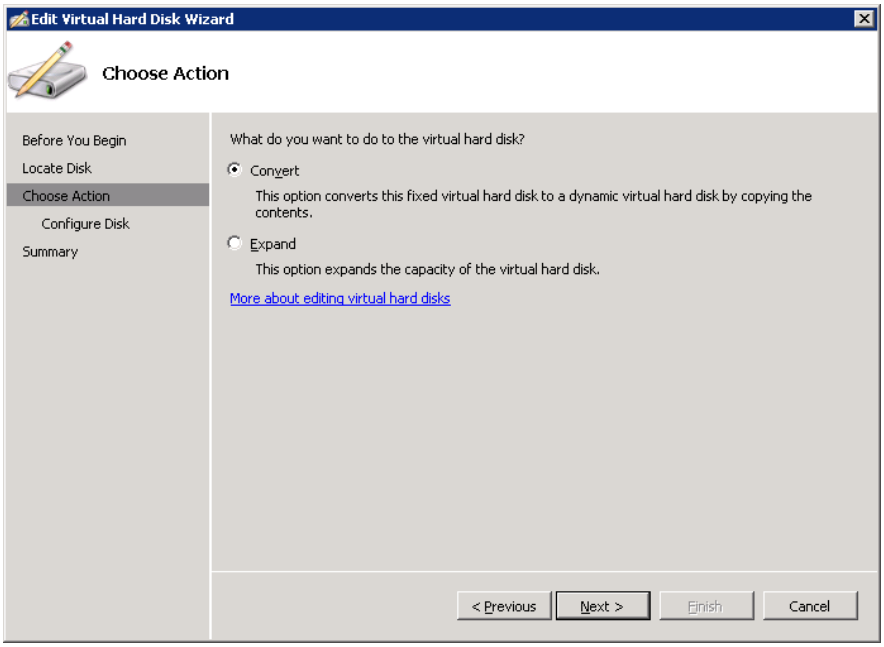


Figure 22: Example options for editing a fixed VHD.

Creating Virtual Machines (VM)

Hyper-V supports the following Guest operating systems:

- **Windows Server 2008 x64/x86**
- **Windows Server 2003 x86/x86**
- **Windows 2000 Advanced Server / Server SP4**
- **Windows HPC** Server **2008**
- **Windows Vista x86 (Business, ultimate & Enterprise) SP1 x86/x64**
- Windows XP Professional **SP2/3 x86/x64**
- **SUSE Linux** Enterprise Server **10 with SP1/2 x86/x64 Edition**

Only SUSE Linux Enterprise Linux is officially supported, but Open SUSE works fine as a Guest OS.

Add Guest Virtual Machine

The virtual machine wizard is used to configure; Networking**,** Installation options**,** Storage Location**,** and VM name.

Storage Location

In the **Before you begin** wizard introduction window, click **Next.** In the **Specify Name and Location** window, enter the name of the Guest Operating System. If the Virtual Machine is not going to be saved in the default location then check the box for **Store the Virtual Machine in a different location** and browse and locate the new location. When stored in new location, click **Next**.

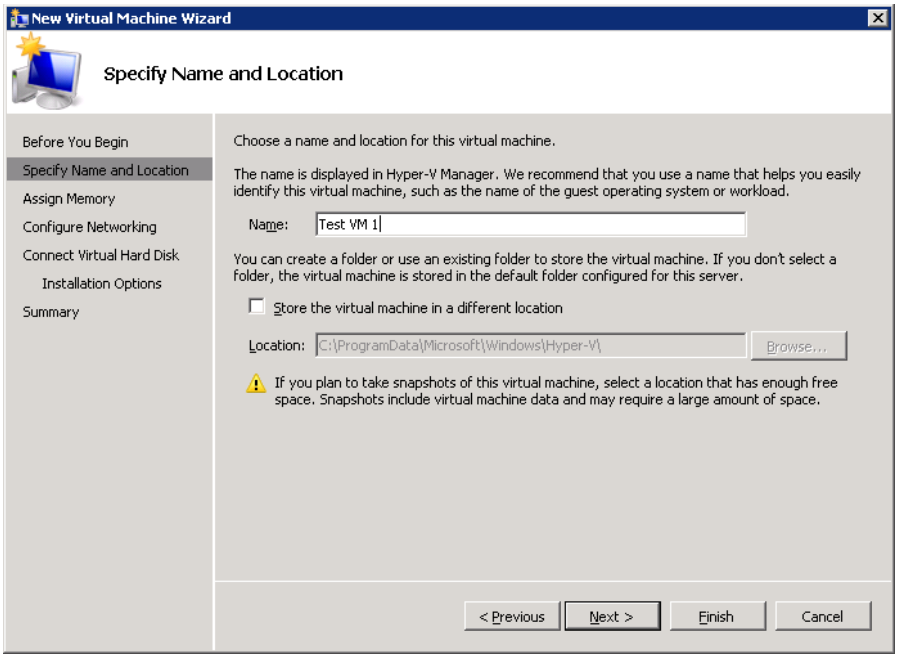


Figure 23: Starting the New VM Wizard

Installation Options

In the **Assign memory** window, set the memory for the Guest OS and click **Next**. The Default is **512MB.**

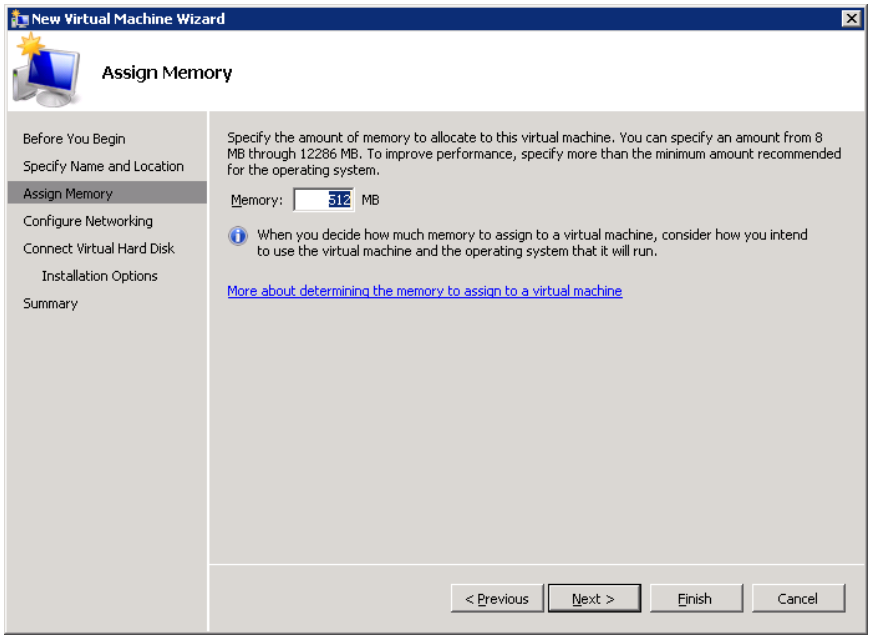


Figure 24: Allocating VM RAM. This can be changed later, but the VM must not be running.

In the **Configure networking** window, select the Virtual Network which should have been created at the time of enabling the Hyper-V roles or can be done later on. If choosing to connect to the virtual network later, select **Not connected** and click **Next**.

In the **Connect Virtual Hard Disk** window create a new Virtual Hard disk and set its size. The **Default is 127GB**. Save the disk in a different location than the defaults that are given as an option. Use a Virtual Disk that already exists or choose to attach a Virtual Hard Disk later. When the Virtual Hard Disk (VHD) is created, click **Next**.

In the **Installation Options** window, choose the media to perform the installation. Choose the installation option and click **Next**.

In the **Summary** window, check options and click **Finish**. Choose to Start the Virtual Machine immediately after it is created or use the default **to keep the VM off**.

1. In the **New Virtual Machine Wizard**, choose the method to be used to install the operating system.

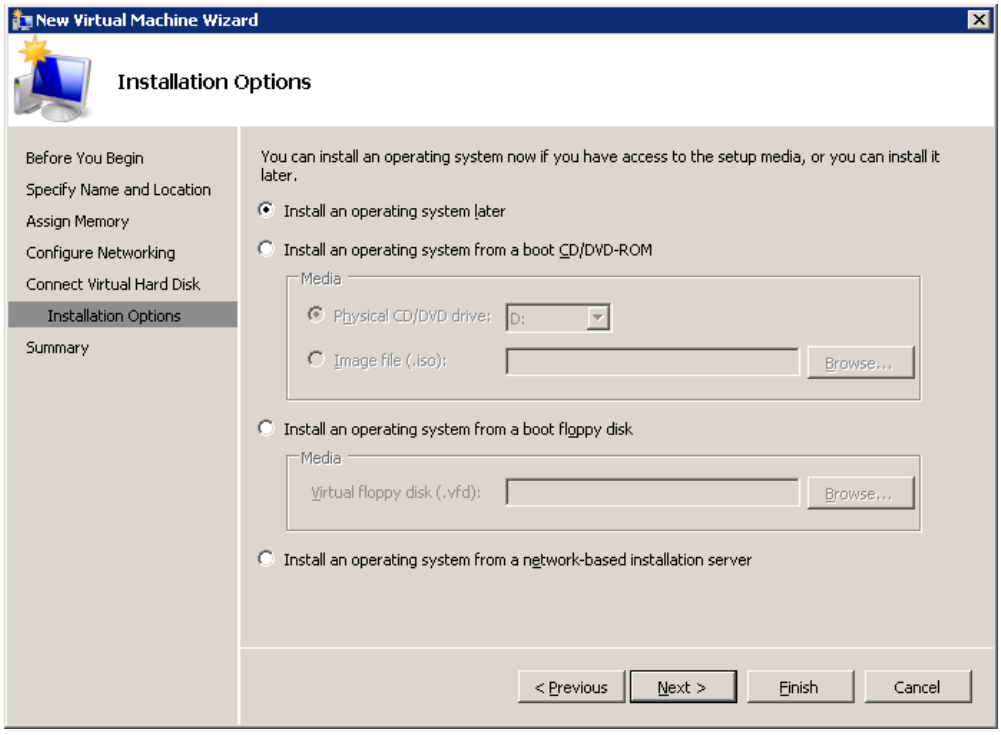


Figure 25: Specifying how the guest VM will be installed.

   a. Install an operating system from a boot CD/DVD-ROM. Use either physical media or an image file (.iso file).
   b. Install an operating system from a boot floppy disk.
   c. Install an operating system from a network-based installation server. To use this option, configure the virtual machine with a legacy network adapter connected to an external virtual network. The external virtual network must have access to the same network as the image server.

2. Click **Finish.**

Moving Hyper-V Virtual Hard Disks between IDE and SCSI Disk Controllers

A VHD assigned to a virtual machine will be attached either to an IDE or a SCSI disk controller, depending on the configuration. Sometimes the guest operating system may dictate that the virtual hard disk be connected to a different type of disk controller than the one to which it is currently connected. A virtual hard disk may also be moved between different disk controllers.

Snapshots

Snapshots are 'point-in-time' images of each virtual machine. This means that a virtual machine can be running and a snapshot can be taken at any point with the ability to revert back to that point, including exact memory, virtual hardware, processes, state, etc.

Snapshots do not change the virtual machine hardware, applications, or the currently running processes. Deleting a snapshot does not change the virtual machine however the option to go back to that point to rectify a mistake cannot be done.

The snapshot files consist of a copy of the VM configuration .xml file, save state files, and a differencing disk which is the new working disk with all child writes prior to taking the snapshot.

If snapshots are created one after another and a previous snapshot is never applied, the tree will only have one branch. If a previous snapshot is applied, another branch is created with the snapshot tree starting at the applied snapshot.

Snapshots create a point-in-time copy of a VM and are used for configuration, not as a backup.

Creating Snapshots

To create a snapshot, in the Hyper-V Manager console highlight the VM, then right-click and select the **Snapshot** menu option. The Hyper-V Manager Snapshots pane displays a tree structure to represents the VM snapshot hierarchy. The root node of the tree is the first snapshot that was created. Under the root node, there is a child named **Now** which represents the VM running version. By default, snapshots are labeled using the VM name connected with the creation timestamp. In order to rename the snapshot, highlight it, then right-click and select **Rename** from the menu.

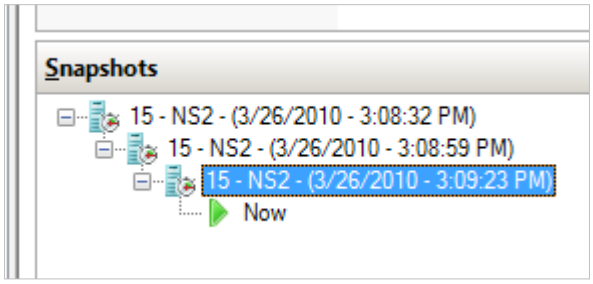


Figure 26: 3 Sequential Hyper-V Snapshots

Revert Option

Use the Revert option to return the VM to the state of the last snapshot that was taken.
The snapshot hierarchy view does not change after the Revert was performed because none of the snapshots are altered during this operation. However, using the Revert option again will continue to return the VM to the configuration and state of the last snapshot taken.

Apply Option

To return to a snapshot that is higher than one level up from the running VM (represented by the **Now** marker in the Snapshot pane), highlight the snapshot, right-click, and choose the **Apply** option from the menu. If the snapshot is not taken prior to the Apply operation the running virtual machine configuration and state is lost.

Delete Option

Hyper-V provides two different Delete options to permanently remove one or more snapshots from the snapshot hierarchy. Deleting a single snapshot will not affect other snapshots, but it will delete the configuration file and save state files associated with the snapshot. Deleting a snapshot subtree immediately deletes the configuration and save state files associated with all the snapshots in the subtree.

Microsoft Volume Shadow Copy Service (VSS)

Hyper-V snapshot technology includes the Microsoft Volume Shadow Copy Service (VSS) to make a duplicate copy of a file. In virtualization, the file is the entire virtual server guest image. The first time a snapshot is taken, the snapshot contains a compressed copy of the contents of RAM on the system along with a bitmap of the guest session virtual disk image. If the original guest image is 8GB in size, the snapshot will be much smaller in size; however, the server storage system still needs to have additional disk space to support the original disk image, plus the amount of disk space needed for the contents of the snapshot image.

Storage Considerations

Window Server 2008 storage options include:

SCSI and IDE – if there are more than four virtual disks to a guest SCSI must be used. If there are no guest operating integration components, use IDE to start the virtual disk. Both IDE and SCSI can be used with the same virtual machine. For SAN migrations, make sure that the LUN is visible on both hosts.

iSCSI – use iSCSI to expose disks directly to the guest operating system. The Hyper-V virtual BIOS does not support starting from the iSCSI disk directly. That means at least one IDE disk must be available. iSCSI disks can be accessed by the guest OS using the iSCSI initiator Control Panel Applet. Using iSCSI requires the Microsoft iSCSI Initiator service to be running.

Pass-through disks – by-pass the Host VHD file to access a disk directly. Use either a Hyper-V internal physical disk or a Storage Area Network (SAN) Logical Unit (LUN) mapped to the Hyper-V server. Unlike other storage types, pass-through disks are not limited to 2040 GB.

Storage Types

The following physical storage types are available with a server that runs Hyper-V:

- **Direct-attached storage (storage attached to the management operating system) -** 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) -** use Internet SCSI (iSCSI), Fibre Channel, and SAS technologies.

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

Storage Configuration Options

Use either virtual hard disks or physical disks that are attached to the VM on the management operating system. Virtual hard disks with a capacity of up to 2040 gigabytes include the following types:

- **Fixed size** - occupies physical disk space on the parent operating system equal to the maximum size of the disk.
    - Takes longer to create because its size is allocated when it is created.
    - Provides improved performance.
    - Recommended for VMs in production environment.
- **Dynamically expanding** - grows as data is written to the disk, providing the most efficient use of disk space.
- **Differencing** - stores the differences from the VHD on the management operating system.
    - Can be shared with virtual machines
    - Should remain read-only

Each virtual machine supports storage of up to 512 TB; whereas physical disks that are directly attached to a virtual machine have no size limit other than what is supported by the guest operating system.

VM Storage

- Store VM configuration files separately from VHDs to enhance performance.
- Disk images (VHD files) should be stored on a separate drive from your host operating system for best performance.
- Where VHD files are located is important when a failover cluster is being used because the configuration file must be accessible by all nodes.

Editing VHDs

The virtual hard disk wizard is used to:

- Create disks
- Compact disks
- Convert disks
- Expand disks
- Merge disks
- Reconnect disks

Configuring iSCSI

The 70-659 exam expects that you be able to understand and configure iSCSI at a baseline level. This includes:

- The iSCSI Initiator
- Using iscsicli.exe
- Configuring Multipath I/O with mpiocpl.exe
- Dynamic I/O Redirection

A Storage Area Network (SAN) consolidates storage from many servers into a single physical location and transports data over a network instead of an internal bus. One popular SAN implementation method is using iSCSI. iSCSI wraps SCSI commands and data inside an IP packet and sends them over a standard Ethernet network, creating a SAN out of existing hardware. It doesn't require Fibre Channel equipment such as Host Bus Adapters and Fiber switches. That being said, iSCSI should run on dedicated switches and network adapters. Most servers acting as iSCSI Initiators use one or more 1 gigabit NICs dedicated to storage traffic.

The iSCSI Target hosts the data and exposes them via Logical Unit Numbers (LUNs). The iSCSI Initiators can be virtual or physical systems and they **initiate** the connection to the target. In R1, there was a 1 to 1 mapping between LUNs and virtual machines. With the introduction of Cluster Shared Volumes in R2, a LUN can keep multiple virtual machines.

For the examples in this section, we have equipped our lab with a demo version of Starwind Software's iSCSI target for Windows. If you do not have access to an iSCSI SAN to practice with, this software can be a substitute when studying for the 70-659 exam. There are also a variety of Linux distributions designed as storage appliances that can act as an iSCSI target. Since iSCSI is an open standard, the underlying implementation shouldn't matter, as long as it is certified for Windows Server 2008.

An iSCSI connection is formed by using the iSCSI Initiator Administrative Tool. The first time you run the applet, you will be prompted to start the iSCSI service, as it doesn't run by default. Figure 27 shows the default iSCSI Initiator screen after we have connected to the SAN front-end. The Volumes and Devices tab specifies which logical disks we connect with, shown by the iSCSI target LUN ID. After adding the LUN with the iSCSI Initiator, the disk can be partitioned, formatted, and used for storage using the Disk Manager or **diskpart**.

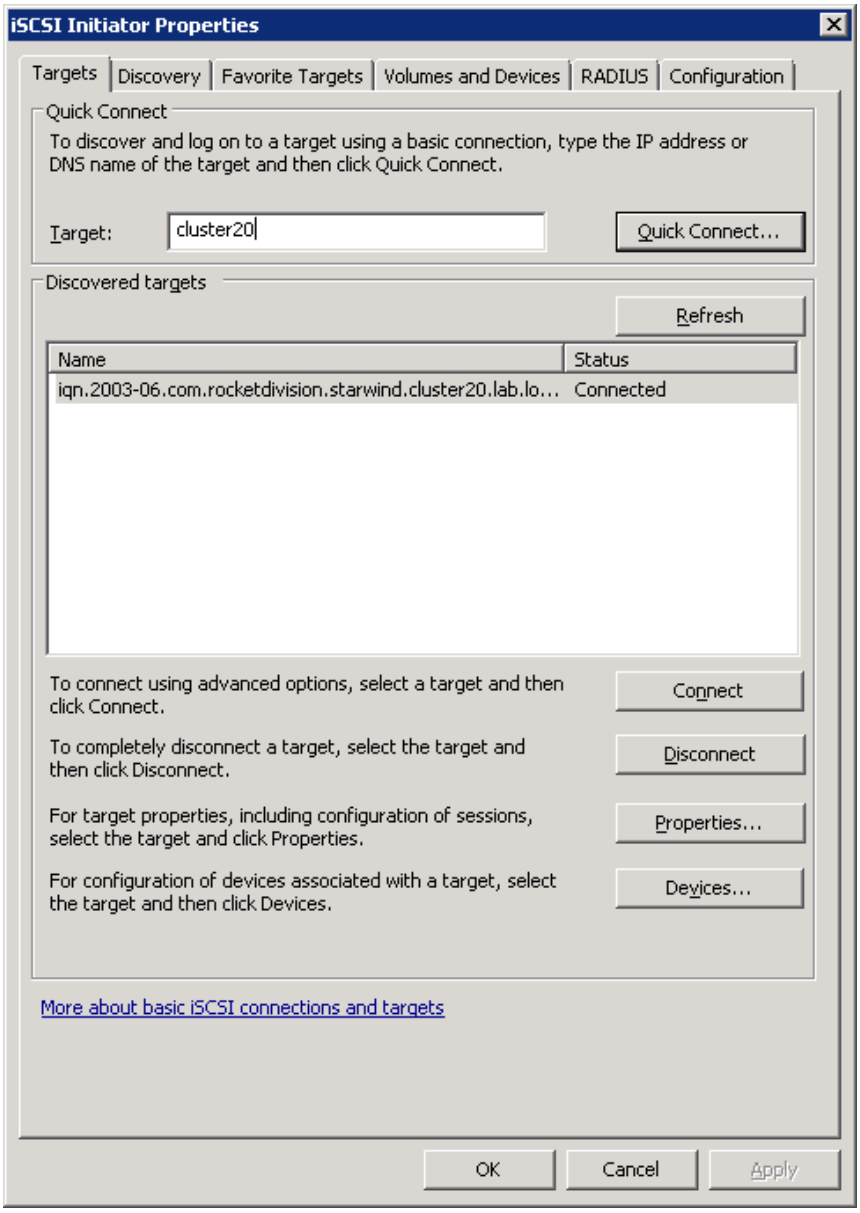


Figure 27: iSCSI Initiator (client) configuration with cluster20 as the SAN DNS name

iscsicli.exe

iscsicli.exe is Microsoft's command line tool for managing iSCSI connections. iscsicli is useful for both Server Core installations and scripted environments. iscsicli's commands follow the same logical flow as the graphical version of Microsoft's iSCSI initiator. The iSCSI service's startup type can be modified and it can be started from the command line if it has not already been started through the GUI:

```
C:\>sc config msiscsi start= auto
    (note that the space between = and auto is required)

C:\>sc start msiscsi
```

After the service is running, the first thing we must do is connect to the portal hosting the target:

```
iscsicli addtarget cluster20 10.10.1.113
```

Use of the addtarget verb can be confirmed using the listtargets command. This command will also enumerate all of the iSCSI devices the Target has exposed to us:

```
C:\>iscsicli ListTargets
Microsoft iSCSI Initiator Version 6.1 Build 7600

Targets List:
 iqn.2003-06.com.rocketdivision.starwind.cluster20.lab.local.
imagefile0
The operation completed successfully.
```

The long string, "iqn.2003-06.com.rocketdivision.starwind.cluster20.lab.local.imagefile0", is known as the IQN (iSCSI Qualified Name) that identifies each device target LUN.

Finally, we can connect to a specific target exposed by the iSCSI Target using this command:

```
C:\iscsicli QLoginTarget iqn.2003-06.com.rocketdivision.starwind.
cluster20.lab.local.imagefile0
```

iscsicli will produce some numbers identifying the connection and end with "The operation completed successfully". After we have a connection to this target, we can partition and format the disk and use it like we would any other disk.

If we want to make this disk connection persistent (reconnecting upon reboot like a normal fixed disk), we would use the following:

```
C:\>iscsicli.exe PersistentLoginTarget iqn.2003-06.com.
rocketdivision.starwind.cluster20.lab.local.imagefile0 T * * * * *
* * * * * * * * * * * 0
```

In iscsicli, the * indicates to use the default value. In our example, there are 15 values that are set to the default.

We can verify the Persistent Targets by using the ListPersistentTargets verb:

```
C:\>iscsicli ListPersistentTargets
Microsoft iSCSI Initiator Version 6.1 Build 7600

Total of 1 persistent targets
    Target Name           : iqn.2003-06.com.rocketdivision.
starwind.cluster20.la
b.local.imagefile0
    Address and Socket    : 10.10.1.113 3260
    Session Type          : Data
    Initiator Name        : ROOT\ISCSIPRT\0000_0
    Port Number           : <Any Port>
    Security Flags        : 0x0
    Version               : 0
    Information Specified : 0x20
    Login Flags           : 0x8
    Username              :

The operation completed successfully.
```

Configuring Multipath I/O with mpiocpl.exe

As more data is aggregated on to a SAN, the cost of losing connectivity to the SAN increases. Multipath I/O (MPIO) is a feature and to provide redundancy and performance improvements between hosts and disk subsystems. An administrator implements MPIO by creating separate physical paths between the host and the storage by using different host bus adapters, switches, and controllers. Traffic can be load balanced across up to 32 paths, or the paths can be configured in a redundant configuration which fails over to a secondary path if the primary path fails. With MPIO enabled, a host sees a path to a SAN as one logical connection, rather than separate connections to separate units inside the SAN. The connections can be load-balanced in an Active/Active configuration in 2008.

MPIO has been present in certain drivers since Windows 2000, but has only come of age in Windows Server 2008. Multipath IO is not installed by default on Server 2008. It is provided in 2008 as a Feature and is installed n the Server Manager. Successful installation will provide an **MPIO** control panel applet.

MPIO is a framework from Microsoft that uses Device Specific Modules (DSMs) provided by third-party vendors to enable multipath IO. In the MPIO realm, DSMs provide the algorithms by which load balancing occurs, such as Round-Robin, Fair-Queueing, or a proprietary algorithm). DSMs also provide failover detection mechanisms.

The basic configuration of MPIO is to specify which adapters will belong to the MPIO set. The DSMs should be provided from the storage vendor in the form of an INF file, similar to other Windows drivers. Successful installation of MPIO will result in the ability to use the "Discover Multi-Paths" tab in the MPIO Control Panel Applet.

Paths to a device can be managed in the device manager for that specific MPIO-ed device (Figure 28). The policies allowed by the MPIO are specific to the DSM, which is provided by the hardware vendor.

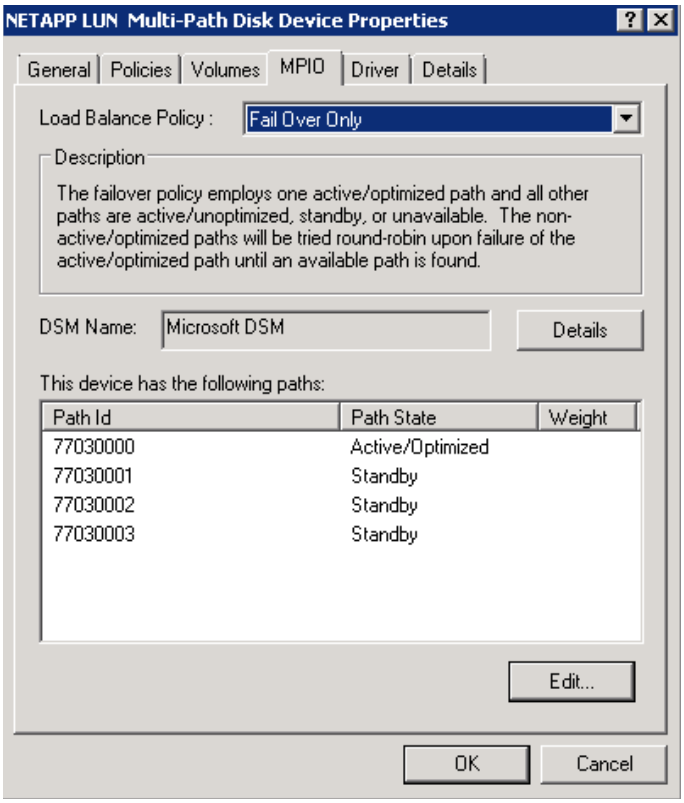


Figure 28: MPIO enabled on a logical disk

In summary, as more workloads are consolidated in to fewer disks and fewer servers, the reliability of connections between devices becomes more important. Specifying multiple paths to a disk improves uptime and performance. MPIO is Microsoft's technology used to aggregate connections, and is made possible by DSMs. DSMs are vendor-provided drivers which specify algorithms for multipath connections, error detection and failover, and performance optimization.

Dynamic I/O Redirection

Dynamic I/O Redirection is a feature inherent to Failover Clusters using Cluster Shared Volumes that allows IO to be redirected through another host, should a connection to a SAN fail. Consider this in figure 29. For 70-659, you should know what dynamic I/O redirection is.

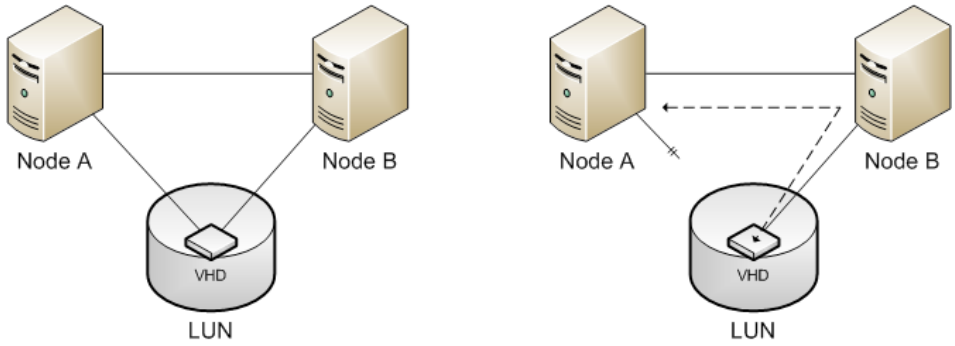


Figure 29: In the event of a failure between Node A and the SAN, Node A will recognize it can still reach the target data by traveling through Node B. It will use this path for I/O to the SAN.

Dynamic I/O Redirection requires the use of Failover Clustering, and is automatically enabled when Failover Clustering is enabled on R2 Hyper-V enabled servers. Dynamic I/O Redirection is not available in R1, because R1 doesn't support CSVs.

Objective Summary

To configure Hyper-V properly, it is important to understand virtual hard disks (VHDs) and the various configuration options. There are three VHD types: fixed size, dynamic, and differencing. Fixed-size VHDs have a set amount of hard disk space, and that amount does not change. Dynamic VHDs only use the amount of space that is currently being used for the VHD. Differencing disks are configured in a parent-child relationship with another disk that stays intact.

Shadow copies are included with Hyper-V virtual machines, and they are called virtual machine snapshots. Virtual machine snapshots will take a copy of your virtual machine and place that copy in a specified location.

Pass-through disk access allows Hyper-V to work without VHDs. Virtual machines can access a file system directly through the use of this feature.

Understand virtual hard disks (VHDs). A VHD is a virtual hard drive that the guest operating system is installed onto. During the installation of the guest operating system, determine the size and location of the virtual hard disk that the virtual machine will use.

Be able to list the three VHD types. There are three VHD types. Fixed-size VHDs have a set amount of hard disk space, and that amount does not change. Dynamic VHDs only use the amount of space that is currently being used for the VHD. The fixed-size VHD option offers better performance than the dynamic VHDs by eliminating the fragmentation associated with a growing file. Differencing disks are configured in a parent-child relationship with another disk that stays intact. This allows changes to the operating system or data without affecting the parent disk.

Be familiar with virtual machine snapshots. Understand that Microsoft Hyper-V has also included the shadow copies advantages to your virtual machines and they are called Virtual Machine Snapshots. Virtual machine snapshots will take a copy of the virtual machine and place that copy in a specified location. Understand the recovery and rollback advantages of using virtual machine snapshots.

Understand pass-through disk access. Pass-through disk access allows Hyper-V to work without the use of virtual hard disks (VHD). Virtual machines can access a file system directly, thus eliminating the need for VHDs. Be sure to know that VHDs are inaccessible to non-virtualized systems due to the VHD formatting. Pass-through disk access helps solve this problem by allowing the virtual machine to directly access the writable file system. Using pass-through disk access allows you to surpass the 2040GB limitation of VHDs.

Chapter 5: Configuring Virtual Machines

Guest OS Components

Before creating the virtual machine, consider the following when using the **New Virtual Machine Wizard**.

- Installation media (physical media, a remote image server, or an .ISO file)
- Memory allocation
- Where the virtual machine will be stored
- Network card usage
- Name for the virtual machine

Managing Virtual Machines

System Center Virtual Machine Manager (SCVMM) 2008 provides management interface across multiple virtualization software environments, including Hyper-V and VMware ESX hosts if the VirtualCenter application is installed. SCVMM abstracts the differences between hypervisor APIs and allows running an action without disturbing the virtual machine software.

With SCVMM 2008, virtual machines can be created and managed on Hyper-V hosts. If a host is added that is running Windows Server 2008 and it does not have Hyper-V enabled, SCVMM 2008 will automatically enable the Hyper-V role on the host.

Working with Snapshots

Virtual machine snapshots capture the state, data, and hardware configuration of a running virtual machine. Virtual machine snapshots are intended mainly for use in development and test environments. The ability to revert a virtual machine can be useful in recreating an event or state for troubleshooting purposes. In production environments snapshots can provide a way to revert an operation such as a software update.

Snapshot data files, stored as .avhd files, and are normally stored in the same folder as the virtual machine by default.

Exceptions:

- If virtual machine was imported with snapshots then snapshots are stored in their own folder.
- If virtual machine does not contain any snapshots, a specific folder to store snapshots can be named upon configuring the VM snapshot setting.

Do not delete .avhd files directly from the storage location. Instead, use Hyper-V Manager to select the virtual machine, and then delete the snapshots from the snapshot tree.

In production environment keep in mind:

- VM snapshots reduce disk performance.
- When a snapshot is deleted, the .avhd files that store the snapshot data remain in the storage location until the virtual machine is shut down, turned off, or put into a saved state. Put the production virtual machine into one of those states at some point to complete removal.
- It is best not to use snapshots on virtual machines that provide time-sensitive services, or when performance or storage space is critical.

Configure a Highly Available Virtual Machine

Highly available virtual machines (**HAVMs)** can be migrated to a different virtual machine host in a failover cluster to provide continuing service when their current host needs maintenance. If their current host fails, the HAVMs automatically migrate to a different host in the cluster through a process known as **failover**.

System Center Virtual Machine Manager (SCVMM) 2008 supports HAVMs deployed on Windows Server 2008 failover clusters. System Center Virtual Machine Manager 2008 R2 supports HAVMs deployed on Windows Server 2008 failover clusters or Windows Server 2008 R2 failover clusters.

- If a virtual machine is configured as a highly available virtual machine, SCVMM places the virtual machine on the most suitable host in a host cluster. To configure a virtual machine as highly available, in the advanced settings on the **Configure Hardware** page of the New Virtual Machine Wizard, display **Availability** settings, and select **Make this virtual machine highly available**.
- If a virtual machine is not configured for high availability it can become highly available during placement because all hosts including clustered hosts will be available. When a clustered host is chosen, click **Yes** to make the virtual machine highly available. Then, the VM will be deployed on a clustered host and becomes highly available.
- Virtual Machine Manager places highly available virtual machines only on clustered hosts. Virtual Machine Manager places virtual machines that are not highly available only on non-clustered hosts. SCVMM does not allow the creation of non-HAVMs on clustered hosts. If such virtual machines are created outside SCVMM, they are imported and treated as non-HAVMs, just like virtual machines on non-clustered hosts.

Monitoring Performance

Ensure that Hyper-V Integration Services are installed on both the host and the guest operating systems. Hyper-V integration services provide virtual server client (VSC) code for Hyper-V enlightened I/O, which increases the performance of operating system functions such as memory management and network performance. Run solutions such as; roles, features, or custom services on a Hyper-V virtual machine rather than on the host operating system.

Using Perfmon.msc

Because Hyper-V is a kernel-level addition to Server 2008, monitoring Hyper-V performance is a little different than monitoring a legacy server. Since the default Hyper-V management console only displays CPU usage and RAM allocation, we need to dig deeper to assess Hyper-V performance and troubleshoot performance problems. When you install the Hyper-V role, Windows will add several series of counters for use with Perfmon.msc. If you monitor Hyper-V using the standard counters, you may not be getting an accurate picture of your server's performance.

To get an accurate picture of performance of a host partition, you can no longer use the plain old "Processor Time" counter, because the Processor Time will include jobs running on virtual machines, which will skew your assessment of host partition performance. Host partition performance is most accurately viewed by using the counters underneath the "Hyper-V Hypervisor Root Partition Virtual Processor". Since the host partition handles IO for the guests, a high CPU usage on the host partition may indicate an IO issue in one of the guests.

Useful counters include:

- **Health Counters** – the counters under "Hyper-V Virtual Machine Health Summary" can provide you with a glance of which VMs need attention. If you are not using SCVMM or some other monitoring software, you could configure Events when occur when these numbers drop below a certain value, indicating VM trouble.
- **CPU Utilization** – monitoring the "Processor" counters from the parent partition will give you an accurate view of the physical processor usage on a Hyper-V host. The values will be the aggregate of the parent partition + the child partitions. The "Hv LP" values are Logical Processes, which is the device Hyper-V uses for interrupts to the physical system. If you are not running with Integration Services installed, you may see the CPU Utilization stay consistently at a value higher than it should be.
- **Interrupts/Second** – although CPU usage may be low, a Hyper-V server may have to process a large number of interrupts for both hosts and guests. How many interrupts a CPU can handle is large dependent on the architecture, but this counter may be a starting point when troubleshooting a slow Hyper-V server when other counters are within acceptable ranges.
- **Network Utilization** – network utilization is available in the Hyper-V Virtual Network Adapter Bytes Received/Sec and Bytes Sent/Sec. This will include all enlightened guests and guests with synthetic network adapters installed through integration services. Hyper-V Legacy Network Adapter Bytes Received/Sec and Sent/Sec. will show the throughput for all synthetic network adapters. "Virtual Switch" monitors can be helpful to know how much traffic is being sent between VMs on Internal networks.
- **Disk Utilization** – disk utilization can either be monitored by looking at the virtual IDE or SCSI adapter installed on an individual VM, or it can be monitored by VHD file (using the "Hyper-V Virtual Storage Device" counters. "Physical Disk" will give you the overall system disk performance. Typically we are looking at "Disk Bytes/Sec", but we can also see bottlenecks if a lot of IO operations are waiting in the queue. This can be determined by looking at the "Current Disk Queue Length", which should be about 2 operations per drive.

- **Memory Utilization** – Hyper-V cannot oversubscribe RAM to guests. Each guest must stay resident in memory, as paging the running guest images to disk is not allowed. Therefore, the RAM counters in Perfmon are accurate and include all partitions. The TLB is the Translation Lookaside Buffer and is a processor technology that is required for mapping Hyper-V guest RAM to physical RAM. A high number of TLB If your "Hyper-V Hypervisor Partition/Virtual TLB Flush Entries/Sec" is high, consider upgrading processors to a newer processor supporting Second-Level Address Translation (SLAT) and moving to Server 2008 R2. SLAT was designed to help address memory translation problems in hardware and is one of the advantages of using Hyper-V on Server 2008 R2.

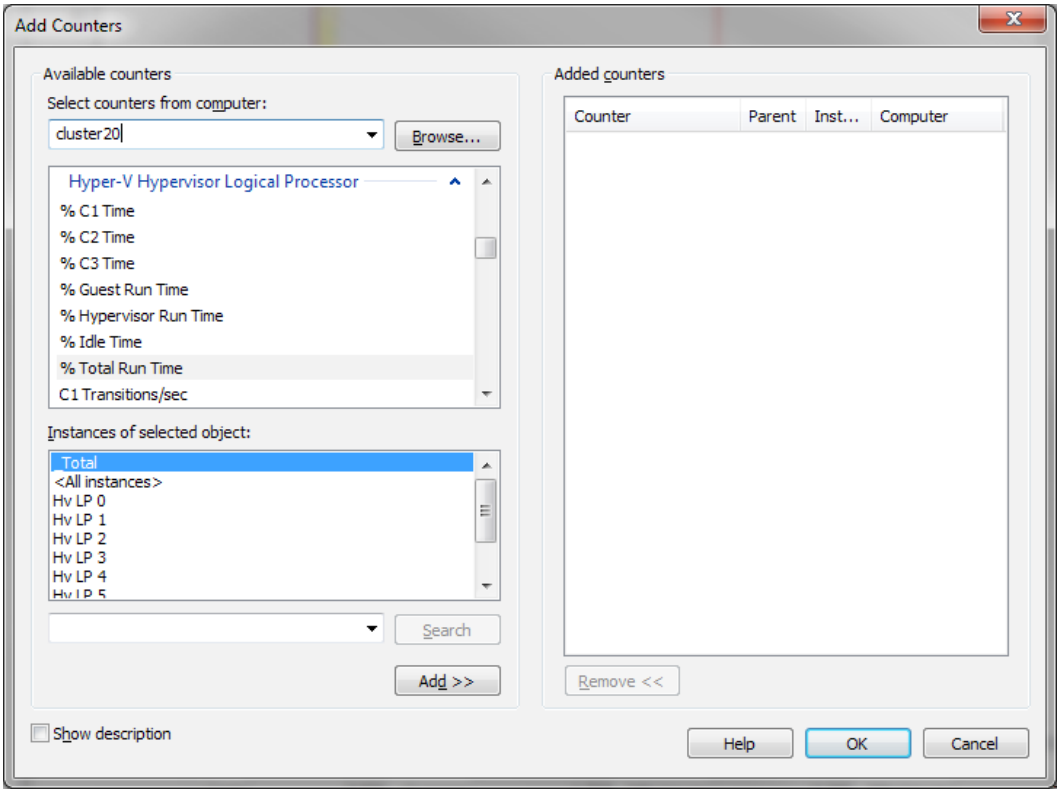


Figure 30: Hyper-V performance can be monitored if you know what to look for

Optimize Disk Performance

- For best performance of the SQL Server subsystem running in a Hyper-V virtual machine, configure the disks used by SQL Server as "pass-through" disks in the Hyper-V Manager. Pass-through disks are physical disks/LUNs attached to a virtual machine that do support some of the functionality of virtual disks, such as Virtual Machine Snapshots.
- **Ensure Hyper-V data file optimal disk I/O** by installing integration services on both the host and guest operating system. Then configure pass-through disks for data volumes with the SCSI controller.
- Do not attach a system disk to a SCSI controller. A virtual hard disk that contains an operating system must be attached to an IDE controller.

Optimize Memory Performance

- Ensure there is sufficient memory installed on the physical computer that hosts the Hyper-V virtual machines. Each virtual machine must reside in non-paged-pool memory, or memory that cannot be paged to the disk. This creates the need to have enough memory on the physical computer that hosts the virtual machines equal to the sum of the memory allocated for each virtual machine plus 300 MB for the Hypervisor, 32MB for the first GB of RAM for each VM, another 8MB for each additional GB of RAM for each VM, plus 512 MB for the host operating system running the root partition.
- If possible use a 64-bit operating system for each guest operating system to take advantage of the memory installed on the physical computer that hosts the Hyper-V virtual machines.

Optimize Network Performance

Configure guest operating systems to use a Network Adapter rather than a Legacy Network Adapter.

Optimize Processor Performance

- CPU intensive application configuration is a 1-to-1 mapping of virtual processors in the guest operating system to the host operating system available logical processors. Configuration such as 2:1 or 1:2 is less efficient.
- The hosted application's performance can be affected by the number of processor cores available to the guest operating system running in a Hyper-V virtual machine. Therefore, consider carefully which operating system will be installed in the Hyper-V virtual machine.

Virtual Machine Settings

Some of the VM settings:

- BIOS boot order
- Processor settings (virtual processors)
- Configure reserve/limit percentage
- Amount of memory allocated to the VM

Peripheral and Integration Settings include:

- Server settings that specify the virtual machine(s) and virtual hard disk(s) locations and settings
- User settings which allow customized interactions with VM connections (mouse release key and Windows keys), and display messages and wizard pages

Configure Hyper-V settings

1. Open **Hyper-V Manager**.
2. Click **Start.**
3. Point to **Administrative Tools.**
4. Click **Hyper-V Manager.**
5. In the **Actions** pane, click **Hyper-V Settings.**
6. In the Navigation pane, click the setting to be configured.
7. Click **OK** to save the changes and close **Hyper-V Settings** or click **Apply** to save the changes and configure other settings.

Note: Must be a member of the local Administrator group or use the Authorization Manager to modify the authorization policy to include user(s) or group(s) authorized to perform these tasks.

Adding IDE or SCSI devices

- **IDE devices –** Hyper-V uses devices with IDE controllers; up to two IDE controllers Hyper-V with two disks on each controller. The startup disk can be either a virtual hard disk or a physical disk (boot disk) must be attached to one of the IDE devices.
- **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. This means that SCSI controllers cannot be used as startup disks.

Adding Adapters

Multiple Adapters can be added to Hyper-V. The network hardware. If using a failover cluster, they must be marked as "Certified for Windows Server 2008." If using iSCSI, network adapters should be dedicated to either network communication or iSCSI, not both. Connect cluster nodes by multiple, distinct networks or with one network that is constructed with teamed network adapters, redundant switches, redundant routers, or similar hardware that removes single points of failure to avoid single points of failure.

1. Go to **Administrative Tools.**
2. Click **Hyper-V Manager.**
3. In the results pane, under **Virtual Machines**, select the virtual machine to be configured.
4. In the **Action** pane, under the virtual machine name, click **Settings**.
5. In the **Navigation** pane, click **Add Hardware.**
6. On the **Add Hardware** page, choose a network adapter or a legacy network adapter.
7. **Note:** can be added only when virtual machine is turned off.
8. Click **Add**. The Network Adapter or Legacy Network Adapter page appears.
9. Under **Network**, select the virtual network to connect to.
   If configuring a static MAC address or virtual LAN identifier, specify the address or identifier to be used.
10. Click **OK**.

Modify virtual machine settings

1. In the **Failover Cluster Manager** snap-in, if the cluster to be configured is not displayed, in the console tree, right-click **Failover Cluster Manager.**
2. Click **Manage a Cluster**, and then select the cluster to be configured.
3. If the console tree is collapsed, expand the tree under the cluster to be configured.
4. Expand **Services and Applications**.
5. Click **FailoverTest**.
6. In the center pane, right-click the virtual machine resource, and then click **Settings**. (If **Settings** does not display, collapse the virtual machine resource and then right-click it.)
7. Configure the settings for the virtual machine.

Start/Stop Actions - configured to control the virtual machine when the Host is stopped.

- **Automatic Start Action** – defines VM actions that should be taken when the host system boots; not starting the virtual machine, starting the virtual machine or only starting the virtual machine if it was running when the host last shut down or to delay the start up by a specified number of seconds. This delay prevents all virtual machines starting at the same time and allows critical virtual machines to start before less critical ones.
- **Automatic Stop Action** – defines VM actions that should be taken when the host system shuts down, including; powering off the virtual machine, saving the virtual machine state and performing guest operating system shutdown. Guest operating shutdown requires the Hyper-V Integration Services installation on the guest and the Operating Shutdown Control option supported and enabled.

Live Backups - Enable VSS integration

1. Use the backup software (VSS requestor) to start the backup (creation of a shadow copy).
2. Hyper-V services forwards a backup request to all VM's.
3. The software in the VM's SQL/Exchange (VSS writer) "pauses".
4. The SAN hardware (VSS provider) creates a snapshot of the data.
5. Hyper-V services are notified the shadow copy is done and OK.
6. The backup software (VSS requester) tells you that the shadow copy was successfully created.

Managing Snapshots

Snapshot Settings:

Create Snapshot

1. Highlight the VM.
2. Right-click and select the Snapshot menu option
   Snapshot pane displays with tree structure.
3. Root node is the first snapshot that was created.
4. Under root is child named Now (current running version).
5. Highlight snapshot.
6. Right-click, select Rename from menu.

Apply Snapshot

To return to a snapshot that is higher than one level up from the running VM (represented by the **Now** marker in the Snapshot pane), highlight the snapshot, right-click, and choose the **Apply** option from the menu. If the snapshot is not taken prior to the Apply operation the running virtual machine configuration and state is lost.

Delete Snapshot

Deleting a single snapshot does not affect other snapshots, but it does delete the configuration file and save state files associated with the snapshot.

Delete Sub-tree

Deleting a snapshot sub-tree immediately deletes the configuration and save state files associated with all the snapshots in the sub-tree. If the running virtual machine AVHD is not a child of any snapshot in the sub-tree, then all of the AVHDs in the sub-tree will also be deleted.

Revert
Using the Revert option allows you to return the VM to the state of the last snapshot that was taken. The last object in the hierarchy, marked by Now, indicates the running VM.

Configure Memory or Processors for a Virtual Machine

Virtual machines consume memory only when they are running or paused. If the physical computer has multiple processors and uses non-uniform memory architecture (NUMA), it is recommended that a VM is not assigned more processors or memory than are available on a single NUMA node.

Configure Virtual Machine Memory or Processor

1. Open **Hyper-V Manager.**
2. Click **Start.**
3. Point to **Administrative Tools.**
4. Click **Hyper-V Manager.**
5. In the **Results** pane, under **Virtual Machines**, select the virtual machine that you want to configure.
6. In the **Action** pane, under the virtual machine name, click **Settings**.
7. In the **Navigation** pane, click the appropriate hardware setting:
   - To configure the memory, click **Memory**. On the **Memory** page, specify the new amount of memory.
   - To configure the processor, click **Processor**. If multiple processors are supported by the guest operating system, specify the number of processors to assign to the virtual machine. Click **OK**.

Configure Resource Allocation for a Virtual Machine

Hyper-V contains the following resource controls:

- Virtual machine reserve specifies the percentage that is reserved for the virtual machine.
- Virtual machine limit specifies the maximum percentage that can be used by the virtual machine.
- Relative weight specifies how Hyper-V allocates resources to this virtual machine when more than one virtual machine is running and the virtual machines compete for resources.

Configure VM resource allocation

1. Open Hyper-V Manager. Click **Start.**
2. Point to **Administrative Tools.**
3. Click **Hyper-V Manager.**
4. In the **Results** pane, under **Virtual Machines**, select the virtual machine to be configured.
5. In the **Action** pane, under the virtual machine name, click **Settings**.
6. In the **Navigation** pane, click **Processor.**
7. Under **Resource** control, specify the amount for each control you want to use. Click **OK.**

Memory Usage

Allocate memory so there is at least a 2 GB difference between the sum total of the memory being used by all virtual machines and the total amount of memory that is installed in the server. Hyper-V should be the only server role that is installed. Additional roles should be installed in a guest operating system. Multiple network cards can be installed in the server, and a different NIC can then be assigned to each virtual server instance. If possible have a NIC for the host operating system, and a dedicated NIC for each guest operating system. When assigning NICs remember that some virtual machines will receive more traffic than others. Hyper-V is able to reallocate NIC usage at a later time if necessary. Switching NICs requires a virtual machine shut down.

Microsoft Offline Virtual Machine Servicing Tool

Although bringing up new virtual machines in Hyper-V using either SCVMM, PowerShell, or some manual method can make server deployment much more effective than installation from an imaging server, it can be problematic if a source VHD file hasn't been turned on for a while to get updates. Deployment of new servers can slow to a crawl and security holes can be introduced into your environment as out-of-date VMs are booted up for the first time. Although the source VMs could be booted occasionally for updates (or even automatically with a scheduled PowerShell task), Microsoft has released a tool called the Offline Virtual Machine Servicing Tool that will automatically deploy your offline VHD images to a host, start them and trigger a software update, and shuts down the VMs. They are then placed back in the library. It can also the antivirus instance that lives in the offline VM so it has up-to-date definitions when it is deployed into production. The Offline VM Servicing tool requires SCVMM, WSUS 3.0 SP1 or later, and System Center Configuration Manager 2007 or later.

Chapter 6: Conversion of Systems to Hyper-V

Hyper-V Conversion Overview

Hyper-V role conversion moves the operating system, files, and associated settings from a physical or virtual system to Hyper-V. To move a Hyper-V image from one system to another, use the **Export** function in the Hyper-V management tool. The Export function captures the majority of the Hyper-V settings that are required for migration, including configurations, networks, and hard disks. The DCOM and WMI namespace security settings must be migrated separately. Turn off or remove the source server from the network before running the import function on the destination server.

Conversion may impact any computer that relies on the applications or workloads running in the virtual machines to be converted because the virtual machines will be offline for the duration of the migration. If a virtual machine hosts a database, any applications that require access to that database will be impacted. Plan accordingly for this downtime. The user account that runs the **cmdlets** and tools must be a member of the local Administrators group on the source and the destination servers. Conversion time is affected by the size of the source data, host server load, and network bandwidth.

Moving between Hyper-V Hosts

Exporting a Hyper-V Virtual Machine

1. Launch the Hyper-V Manager console (**Start->Administration Tools->Hyper-V Manager**).
2. Ensure virtual machine to be exported is either powered off or in a saved state:
   - Select VM from the list.
   - Select the appropriate action from the **Actions** panel.

3. Once the virtual machine is powered off or saved, click on the **Export** action link to display the **Export Virtual Machine** dialog.
4. In the **Export Virtual Machine** dialogue, enter the target location or use the **Browse** button. Location must have sufficient free space to store the virtual machine configuration, virtual hard drives and snapshots.
5. If only the configuration files for the virtual machine are to be exported, select the **Export only virtual machine configuration** option. Within the designated location, a sub-folder with the VM name will be created to contain the exported data.
6. Click on the **Export** button.
7. Once the Hyper-V Manager indicates that the export process has completed, use Windows Explorer to navigate to the specified export location and review the files that have been created.

When a virtual machine has been exported, the following files and folders are created in the specified export location:

- **config.xml** - contains the Virtual Machine basic configuration information in XML format. Information includes original VHD locations assigned to the virtual machine and some state information. If the **Export only virtual machine configuration** option was selected during the export process this is the only file which will be present in the folder.
- **Virtual Machines** - the file contained within this folder is named using a combination of the virtual machine's globally unique identifier (GUID) and the .exp file extension. This file contains the detailed virtual machine configuration and is in binary format. When imported into the target Hyper-V server the information is converted to XML format.
- **Virtual Hard Drives** - this folder contains copies of any virtual hard drive file images associated with the exported virtual machine.
- **Snapshot** - contains all snapshot data associated with the exported virtual machine including configuration files, saved state file, differencing disk image files and the memory image file.

If the option to export only the virtual machine configuration was selected, only the **config.xml** file and the **.exp** file in the **Virtual Machines** folder will be exported.

Importing a Hyper-V Virtual Machine

1. Upon successful exporting, import the virtual machine into the target Hyper-V Server.
2. Transfer the files to the target system.
3. Launch the Hyper-V Manager (**Start->Administration Tools->Hyper-V Manager**) and click on the **Import Virtual Machine** link in the **Actions** panel.
4. Once the virtual machine has been imported, the folder cannot be used to import a second time. The new virtual machine will be using the folder for the imported virtual machine.
5. When the import is completed the dialog closes and the virtual machine is ready to run.

Integration Components

Install Integration Services

1. From the **Virtual Machines** section of the results pane, right-click the name of the virtual machine.
2. Click **Connect**. The Virtual Machine Connection tool will open.
3. From the **Action** menu in the Virtual Machine Connection window, click **Start**.
4. Proceed through the installation.

Import/Export
Consider the following before using import/export to migrate between servers:

- A virtual machine can only be exported if it is shut down or saved. A running or paused virtual machine cannot be exported.
- The set of files comprising an exported virtual machine may only be imported once into a Hyper-V server. If an exported virtual machine is to be imported into multiple Hyper-V servers, separate copies of the export folder will need to be used for each import.
- The Hyper-V Import feature is only able to import Hyper-V based virtual machines. The configuration format used by Virtual Server 2005 and Virtual PC is incompatible with that used by Hyper-V in this context.
- In addition to virtual machine configuration and virtual disk image files, the Import/Export process will also transfer any existing snapshots for the virtual machine.

Managing VMWare
System Center Virtual Machine Manager (SCVMM) controls virtualized environments with the use of a single console and automates tasks by using one Windows PowerShell interface across multiple hypervisors. SCVMM uses the API interface exposed by the VMware VirtualCenter server to manage VMware ESX Server hosts. For ESX Server-specific management, such as creating or removing resource pools and patching ESX Server computers, use VirtualCenter. Use SCVMM for tasks such as; managing, creating, placing, deploying, and removing virtual machines and adding or removing hosts.

VMware Support

SCVMM supports the VMware ESX hypervisor and VMware VirtualCenter, including the following:

- VMware ESX Server 3.0 or above, and VMware ESX Server 3.5i
- VMware VirtualCenter (VC) 2.5 (VMware Infrastructure 3 [VI3])
- VMware vSphere 4 (VI3 features only)

SCVMM does not support VMware Server.

VirtualCenter

SCVMM operates with VMware by connecting to the VirtualCenter server through Web service calls. A SCVMM agent is not required on the VirtualCenter server or on the ESX Server hosts. The SCVMM server periodically refreshes VMware environment information and maps it to SCVMM. VirtualCenter server is required for SCVMM to manage ESX Server hosts. SCVMM contacts the ESX Server hosts directly using Secure FTP (SFTP) or HTTPS to transfer data between ESX Server hosts and Windows Server computers. SCVMM uses VirtualCenter to access VMotion functionality.

Organize and store VMware virtual machines, VMDK files, and VMware templates in the SCVMM Library. SCVMM supports creating new virtual machines from templates and converting stored VMware virtual machines to Hyper-V. Use the **Import templates** action, available in **Administration** view of the SCVMM Administrator Console when the **Virtualization Managers** node is displayed.
Supported templates include:

- **Customized templates** - require an operating system profile to automate deployment.
- **Non-customized templates** - do not have an operating system profile attached, used for operating systems that cannot be customized.

VirtualCenter PowerShell Automation

VirtualCenter daily administration tasks can be done through SCVMM PowerShell or through the SCVMM Administrator Console.

Examples include:

- Start
- Stop
- Pause
- Checkpoint
- Migrate
- VMotion
- Add-remove properties
- Add-remove hardware settings
- View live console
- Expose through Self-Service

VMware Support for Highly Available Virtual Machines

- **HA (High Availability)** - used for fast recovery.
- **VMotion** - SCVMM supports VMware VMotion through VMware VirtualCenter.
- **Migrate storage** - SCVMM 2008 R2 uses Storage vMotion when it moves virtual machine configuration files and virtual disk files on a running virtual machine from one independent storage location to another on an ESX Server host.
- **PRO** - SCVMM uses PRO to enable dynamic load-balancing using VMotion.

VMware Hosts in Maintenance Mode

When an ESX Server host is placed in maintenance mode, SCVMM automatically makes that host unavailable for placement in SCVMM. To make available for placement in SCVMM, must remove the host from maintenance mode by using the VMware VirtualCenter console.

Adding a VMware Infrastructure to SCVMM

Add the VirtualCenter Server

To integrate a VMware infrastructure into your SCVMM-managed virtualized environment, begin by adding your VMware VirtualCenter server to SCVMM. When a VirtualCenter server is added, SCVMM discovers all VMware ESX Server hosts and clusters that the VirtualCenter server is managing and adds the objects to SCSCVMM.

To add the VirtualCenter server, use the **Add VMware VirtualCenter server** action, available in all views of the SCVMM Administrator Console. Appropriate VirtualCenter administrator credentials must be provided to perform this action.

Newly created ESX Server hosts initially have OK (Limited) status. To be able to perform all management tasks that SCSCVMM supports, enter credentials with appropriate authority in the host properties. If managing the VMware environment in secure mode; retrieve and accept a security certificate and, in some cases, a public key. The security information for an ESX Server host is specified on the **Security** tab of the host properties.

In secure mode, SCVMM authenticates each ESX Server host:

- Secure Sockets Layer (SSL) over HTTPS for embedded ESX Server
- VMware ESX Server 3i and later requires certificate authentication
- SFTP over Secure Shell (SSH) for non-embedded ESX Server
- VMware ESX Server 3.5
- VMware® ESX Server 3.0.2

For non-embedded versions of ESX Server the SSH public keys need to be added to the SCVMM database. Validate the public key when security for individual hosts in VMM is configured or use a script to update the SCVMM database with public keys for all of non-embedded ESX Server hosts. When VirtualCenter server is added to SCVMM, SCVMM turns on secure mode by default. If this level of authentication is not required, turn off secure mode.

SCVMM must have access to virtual machine files on the host to perform file transfer operations between hosts running non-embedded versions of ESX Server and Windows-Server-based computers, (i.e., creating a virtual machine with a virtual hard disk stored on a SCVMM library server or storing a VMware virtual machine in the SCVMM library).

Use **Import Templates** action to import your VMware templates to the SCVMM library so they can be used to create virtual machines in SCVMM.

Converting VMware to Hyper-V

Convert a VMware virtual machine to a Hyper-V virtual machine using one of these two methods:

- **Offline Conversion (V2V)** - use the Convert Virtual Machine Wizard to perform a virtual-to-virtual conversion (V2V), which takes a set of VMware files that compose a virtual server and converts them into a Hyper-V compatible guest.
- **Online Conversion (P2V)** - use the Convert Physical Server Wizard to perform a physical-to-virtual machine conversion on the running guest operating system on VMware, as if the VMware guest was a physical machine.

Conversion of VMware Images

V2V is the most reliable way to ensure data consistency because it creates an exact copy of the source VMware images while they are not in use.

To complete a V2V conversion in SCVMM, follow these steps:

1. Turn off the VMware virtual machine.
2. VMware virtual machines can be stored in the library by copying the VMDK and VMfiles into the library share. The library share will take a while to update (or you can refresh it manually by right-clicking it).
3. Start the Convert Virtual Machine Wizard from the SCVMM hosts pane.
4. You will be prompted to select the source VM from the library (See below).

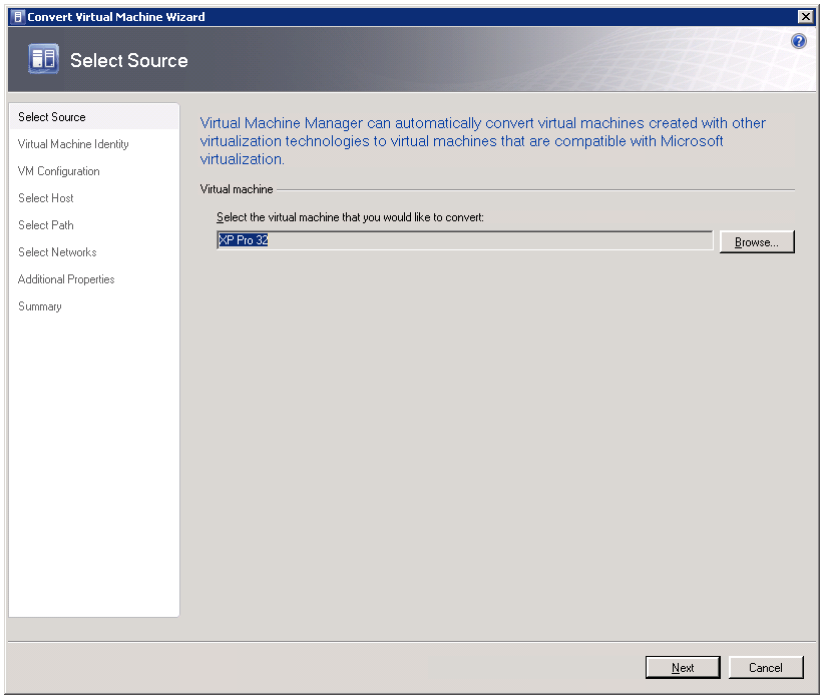


Figure 31: Selecting a non-Hyper-V VM to convert from the library.

5. Click Next to proceed through the wizard, you will have to specify all of the standard settings for creating a VM, including the number CPUs and RAM.
6. Choose a host to place the converted Hyper-V VM on. A summary of your hosts will be presented (see below).

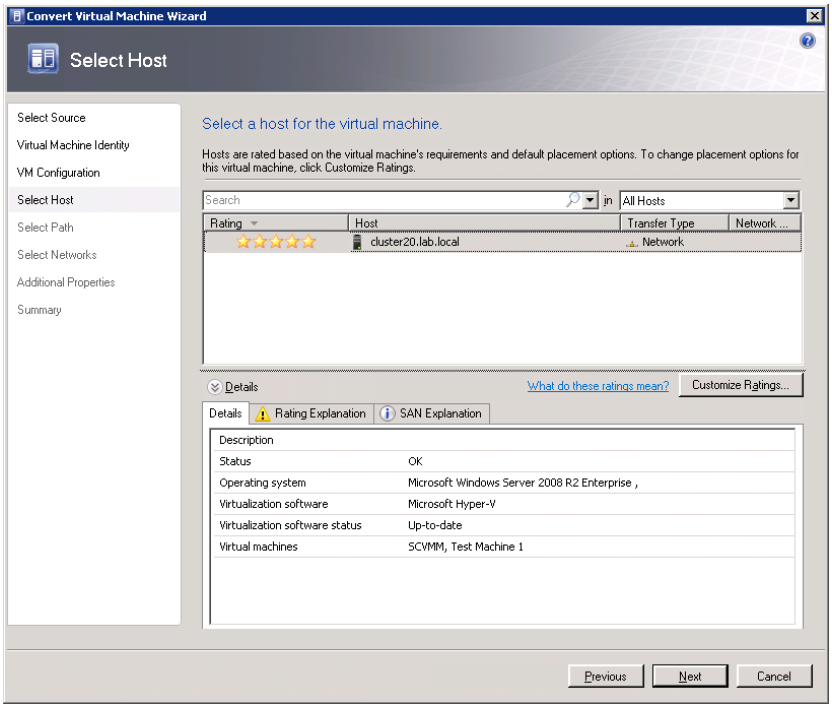


Figure 32: Setting a destination for a V2V Conversion.

7. Select the network settings and additional options, such as how the VM should shut down when the host shuts down and if the VM should be started automatically when the conversion process finishes.
8. SCVMM executes the conversion process and places a detailed description of its steps in the Jobs tab, as seen in Figure 33.
9. SCVMM will automatically boot and install Integration Services after the job finishes. It will also update the hardware in the HAL, which will require at least one additional reboot.

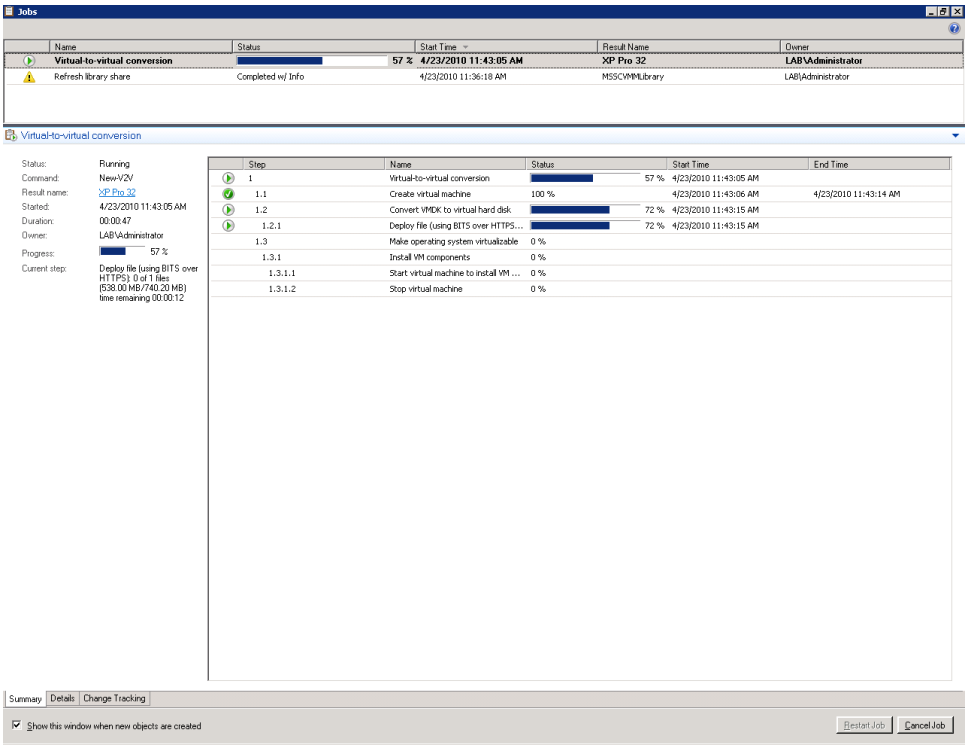


Figure 33: An SCVMM V2V conversion job in progress.

Before Hyper-V starts the V2V job, it will give you the PowerShell code that it uses, which will look something like this:

```
# ----------------------------------------------------------------------
# Convert Virtual Machine Wizard Script
# ----------------------------------------------------------------------
# Script generated on Friday, April 23, 2010 6:37:39 PM by Virtual
Machine Manager
#
# For additional help on cmdlet usage, type get-help <cmdlet name>
# ----------------------------------------------------------------------

$VMHost = Get-VMHost -VMMServer localhost | where {$_.Name -eq
"cluster20.lab.local"}
$VM = Get-VM -VMMServer localhost -Name "XP Pro 32" | where {$_.
LibraryServer.Name -eq "SCVMM.lab.local"} | where {$_.Location -eq "\\
SCVMM.lab.local\MSSCVMMLibrary\Virtual Machines\XP Pro 32"}
$VirtualNetwork = Get-VirtualNetwork -VMMServer localhost | where {$_.ID
-eq "83f206ea-5078-4631-a2b7-8c925d5fa86e"}
$VirtualNetworkAdapter = Get-VirtualNetworkAdapter -VMMServer localhost
-All | where {$_.ID -eq "1903d2f4-22ef-4dba-903e-dd44d83a2d40"}
New-V2V -VMMServer localhost -VMHost $VMHost -RunAsynchronously
-JobGroup 5a7f16ca-fdea-47cd-a56b-1420fde02fc9 -VM $VM -VirtualNetwork
$VirtualNetwork -VirtualNetworkAdapter $VirtualNetworkAdapter
-NetworkLocation "" -NetworkTag ""
```

```
$VM = Get-VM -VMMServer localhost -Name "XP Pro 32" | where {$_.
LibraryServer.Name -eq "SCVMM.lab.local"} | where {$_.Location -eq "\\
SCVMM.lab.local\MSSCVMMLibrary\Virtual Machines\XP Pro 32"}
$VMHost = Get-VMHost -VMMServer localhost | where {$_.Name -eq
"cluster20.lab.local"}
New-V2V -VM $VM -VMHost $VMHost -Path "C:\ProgramData\Microsoft\Windows\
Hyper-V" -Name "XP Pro 32" -Description "" -Owner "LAB\administrator"
-RunAsynchronously -JobGroup 5a7f16ca-fdea-47cd-a56b-1420fde02fc9
-Trigger -CPUCount 1 -MemoryMB 512 -RunAsSystem -StartAction
NeverAutoTurnOnVM -StopAction SaveVM
```

If your company is moving from VMWare or Virtual Server 2005 to Hyper-V, you may have many VMs to migrate. To automate this process, you can script a VM to VM Conversion in PowerShell with the code SCVMM generates.

OS Activation – Reuse Original Product Key

Windows Server 2003 has only one product key. If Windows Server 2008 was obtained from an OEM or as an FPP (fully packaged product), two keys (product key and virtual key) were included to activate the software. The product key is a 25-character key. Use this key when Windows Server 2008 is not running on any virtualization software or on a hypervisor layer. Use the virtual key to move instances of Windows Server 2008 from one virtual environment to another without the need to reactivate.

If the server came from an OEM with Windows Server 2008 preinstalled use a product key to reactivate if the server hardware configuration on which Windows Server 2008 is running has been greatly changed.

Virtual key

The virtual key (virtual product key) is a 25-character key. Use the virtual key for the following functions:

- Create and store Windows Server 2008 instances (depending on the edition)
- Run multiple instances of Windows Server 2008 in Hyper-V at the same time

Converting Physical Machines to Hyper-V

There are two ways (online and offline) to convert a physical machine to a Hyper-V virtual machine. This section will cover each.

Online Conversion

An online conversion is done while the source computer is operating. After scanning the source machine's hardware and software configuration (for permissions, Service Pack level, and VSS availability), SCVMM will install an Agent to the source machine. During the conversion, the agent sends disk images of the physical machine's fixed disks to new VHD files using BITS over HTTPS. After copying the files and creating the new XML configurations and VHD files, SCVMM removes the agent from the source computer and installs the integration tools on the new virtual machine (if necessary).

The following steps will use the P2V online conversion wizard to convert a physical machine to a virtual machine:

1. Clicking the "Convert Physical Server" action starts the wizard.
2. The wizard asks for the IP or hostname of the source system and credentials. You should be a local administrator on the source system. The wizard will also ask you to identify the destination virtual machine name and owner.
3. SCVMM scans the system using WMI to detect what hardware the physical system has, and determines how it should bring that hardware in to the virtual realm.

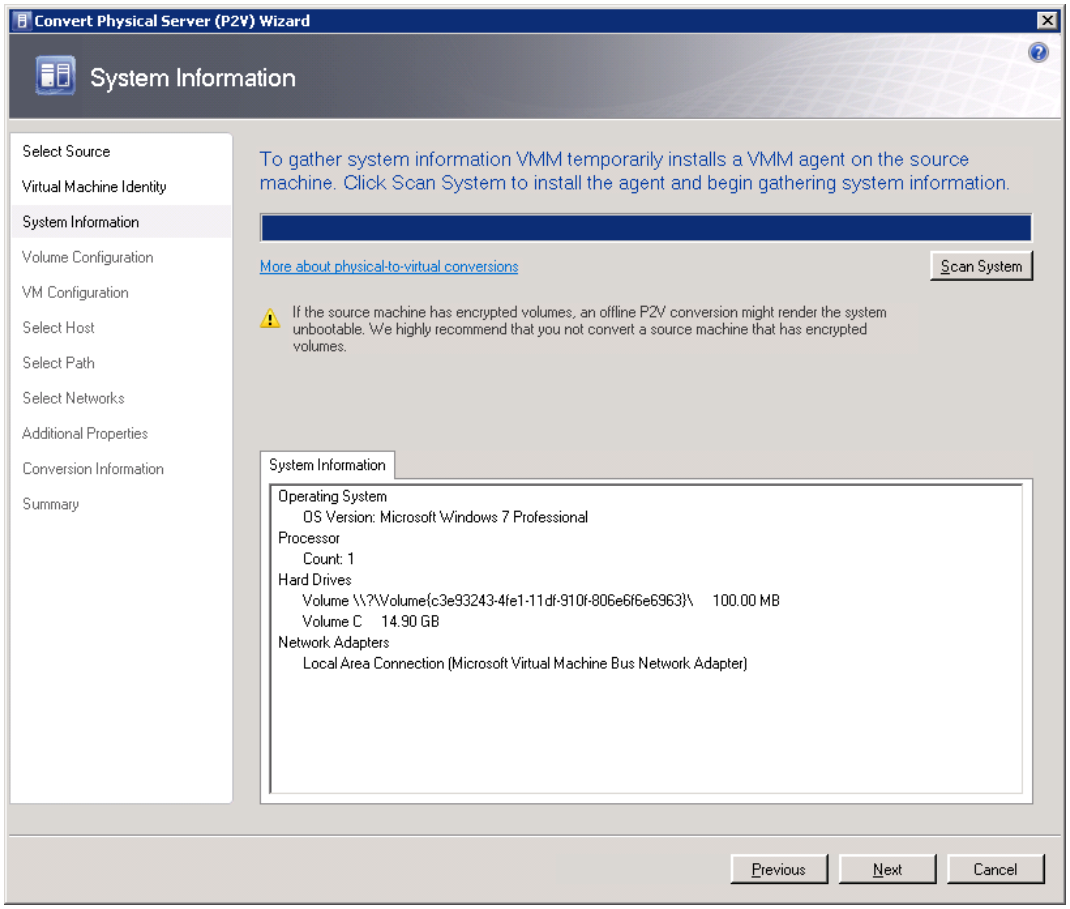


Figure 34: During an online conversion, SCVMM scans the systems hardware using WMI

4. Select the source volumes that you want to duplicate virtually and select if you want the destination VHD to be fixed or dynamic. At this step, you can also dynamically adjust the volume size.
5. Specify the number of processors and RAM allocation of the destination VM.
6. Select the host Hyper-V server & file destination where SCVMM should place the converted machine.
7. Configure the virtual network. Available options here depend on which host you have selected for placement.

8. Additional VM options, such as power-on and power-off behaviors can be defined in the wizard.
9. Finally, SCVMM will analyze the conversion wizard results and report if there are any errors that will prevent conversion.

SCVMM will perform the conversion and place the new VM on the selected host (Figure 35). Like all Hyper-V Jobs, the results are available on the Jobs tab. Hyper-V breaks the job into subtasks so you can watch the progress and determine which steps, if any, there are problems at. Hyper-V will also give you the PowerShell commands it generates to execute the job.

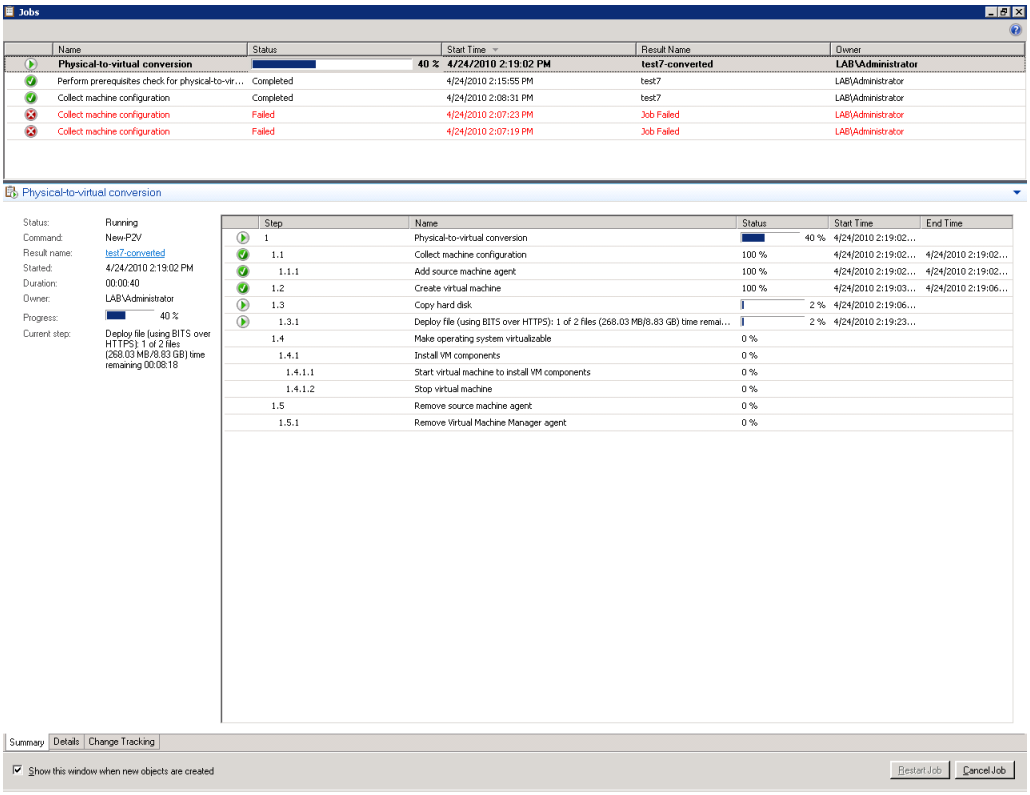


Figure 35: Online P2V in progress.

Offline Conversion

Offline P2V is also the only option for converting Windows 2000 Server, and non-NTFS volumes. The main reason for this is because these systems do not support Volume Snap Shots. Domain Controllers should also be converted offline to ensure Active Directory replications are not lost. Unlike online conversions, the user must provide any missing drivers if Windows PE does not support the source computer. The files to be converted must be added to the SCVMM Library.

Offline conversion includes:

1. Virtual Machine Manager installs the SCVMM agent on the source computer.
2. The SCVMM agent installs a Windows PE image on the source computer, modifies the boot record, and restarts in Windows PE instead of the base operating system.
3. SCVMM begins streaming physical disks. There are no snapshots in this process.
4. Continue the process much like the Fix-Up phase and Create Virtual Machine Phase in an online P2V.

Common Conversion Issues

1. Do not convert if the VM is not compatible with Hyper-V integration services. Ensure that the operating system is up to date with all required software updates and hotfixes. If running Windows Server 2003, upgrade to Windows Server 2003 Service Pack 2 (SP2). Uninstall Virtual Machine Additions version 13.813 (if converting from VMWare) and later after the virtual machine is converted to Hyper-V.
2. Prior to conversion, if the virtual machine was running on Virtual Server 2005 and using a shared SCSI bus as part of a test or development cluster, break the cluster, migrate one node, and move it to an alternate form of shared storage such as iSCSI.
3. Check hardware abstraction layer (HAL) compatibility. By default, Hyper-V installs an APIC MP HAL when integration services are installed on the virtual machine. If moving the virtual machine to Hyper-V while it has a different HAL, there will be a prompt to upgrade when installation of integration service begins. If needed, change the HAL before virtual hard disk migration.
4. Each host computer minimum hardware requirements include:
   - 2.0 GHz Minimum CPU speed.
   - Intel VT or AMD-V Processor Extensions.
   - DEP (Data Execution Protection, also known as the "No Execute" bit).
   - 512 MB - additional memory needed for each guest operating system, and required available hard-disk space of 2 GB on each node.

Chapter 7: System Center Virtual Machine Manager (SCVMM)

System Center Virtual Machine Manager Overview

Although we have already touched on SCVMM in our conversion chapter, we will take a deeper look at it. SCVMM is a software tool for provisioning, managing, and storing VMs for hardware virtualization. SCVMM provides management of physical and virtual machines, virtual infrastructure Performance and Resource Optimization (PRO), consolidation of underutilized physical servers, and rapid provisioning of new virtual machines. SCVMM also provides optimal data center resources and expertise and rapid provisioning and agility.

SCVMM Benefits include:

- Tightly integrates with Server 2008, offering high performance, enhanced security, high availability, scalability, and more. SCVMM uses a console that streamlines many virtualized infrastructure tasks.
- Can manage traditional physical servers and virtual resources in a single console.
- Manages VMware ESX virtualized infrastructure along with the Virtual Center in one tool.
- Compatibility with VMware VI3 through Virtual Center allows support of features such as VMotion and to provide SCVMM-specific features like Intelligent Placement to VMware servers.
- Performance and Resource Optimization (PRO) creates a dynamic IT environment, automatically reallocating virtual machine workloads based on resource utilization and available capacity. Supports queuing live migrations by defining multiple live migrations and running them one after another in sequence without waiting for the current live migration to complete.
- P2V and V2V Conversions.
- Intelligent placement is the ability to optimize management.
- Central Library for components.
- Works with Powershell to provide management and scripting environment. This version adds more PowerShell cmdlets and "view script" controls.
- Consolidation - SCVMM can assess and then consolidate suitable server workloads onto virtual machine host infrastructure to free up physical resources for repurposing or hardware retirement.

SCVMM Components

The **Single Computer** column shows which operating systems are supported for installing all SCVMM components on a single computer. This includes the SCVMM Server, SCVMM database, SCVMM library, SCVMM Administrator Console, and, optionally, the SCVMM Self-Service Portal. To manage a Hyper-V host that is running Windows Server 2008 R2, SCVMM 2008 R2 must be used.

Installing SCVMM

The SCVMM Installer comes with 6 main features to install:

- **The SCVMM Server** – this is the brains behind SCVMM. Every SCVMM network needs at least one of these.
- **The SCVMM Administration Console** – this is the SCVMM administration tool. It can be used to manage remote SCVMM Server installations from a local system.
- **The SCVMM Self-Service Web Portal** – this is the web portal that allows your administrators to manage their own virtual machines.
- **The Local Agent** – this agent is installed on Hyper-V servers that are going to be managed by SCVMM.
- **The Operations Manager Configuration Tool** – this item provides integration APIs with Systems Center Operations Manager (SCOM).
- **Pre-requisites** – this includes SQL Server 2005 Express and Windows Automated Installation Kit (AIK), which aides in deployment of VMs.

Of these features, the Self-Service Web Portal, Local Agent, and Operations Manager Configuration Tool are optional installs. The Local Agent will be pushed out to Hyper-V servers that you manage.
SCVMM has several hardware and software requirements that must be met:

- 64 bit Architecture - 2.0GHz or better
- 2GB RAM
- 200 GB Hard drive space

Software:

- Server 2008 with Hyper-V
- .NET 2.0 & 3.0
- SQL Server
- Powershell 1.0
- Windows Remote Management (WinRM)
- IIS 7 (For Self-Service Portal only) including:
    - IIS 6 WMI Compatibility Component
    - IIS 6 Metabase Compatibility function
    - ASP.NET

The Hyper-V role does not need to be installed on the SCVMM server, and SCVMM can be run from a VM and manage its own host. The SCVMM machine should, however, be a member of the domain.

When installing SCVMM, setup will prompt you for a SQL server (Figure 36), as this is how SCVMM stores data and creates reports. SCVMM will also prompt for a storage location for the library files (Figure 37).

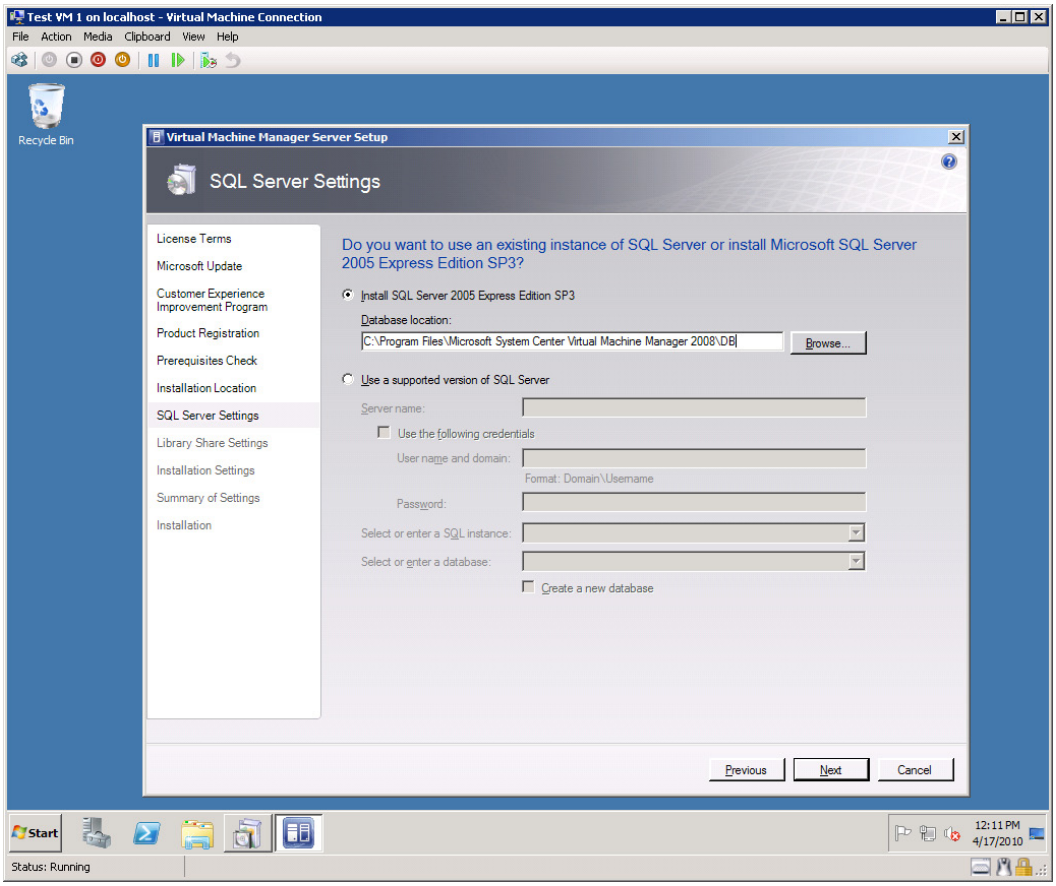


Figure 36: When installing SCVMM, you must either install SQL Express (included with the SCVMM download) or use a SQL Server.

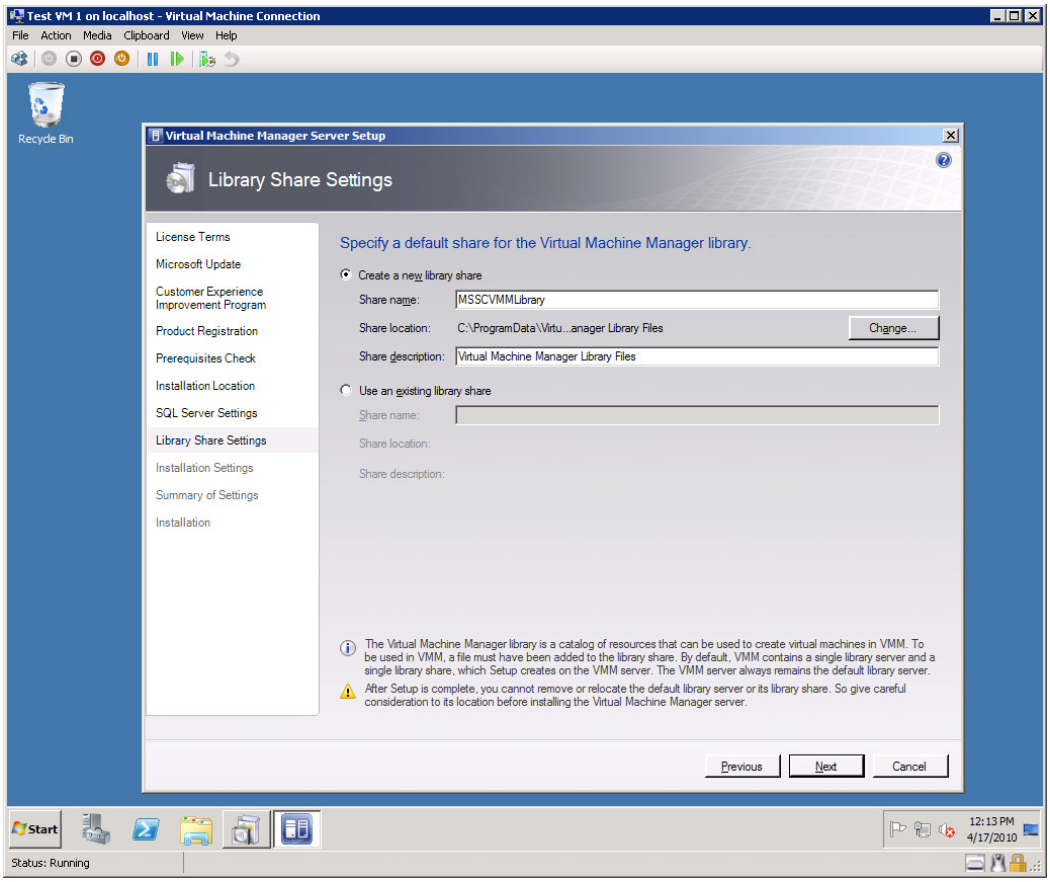


Figure 37: SCVMM requires you to specify where the library should be placed.

SCVMM Server

A virtual machine running on Virtual Server consists of a configuration file (.vmc) and one or more data files. These data files can include virtual hard disks (.vhd files), other media files, such as images (.iso files) and virtual floppy disks (.vfd files). Only the .vhd file can be used by Hyper-V. All of the other files used by Virtual PC or Virtual Server are incompatible with Hyper-V. Consider not converting virtual machines running operating systems that cannot take advantage of Hyper-V integration services.

VM Library Server

The SCVMM library stores and catalogs the many large files generated by virtualization products, including the following:

- VHD files for inactive VMs.
- CD or DVD images (e.g., ISO files) used as alternatives to physical media for software distribution.
- Hardware profiles, which are hardware specifications for a specific VM and contain information such as CPU type, amount of memory, and the priority given to the VM when it is running.
- OS profiles, which provide the most common OS settings, such as the computer name and domain or workgroup settings.

SCVMM Admin Console

The SCVMM Administrator Console is the front end through which all management tasks are performed. Virtual machine and host management of Virtual Server 2005 R2, including 2008 release, Hyper-V hosts and V13 infrastructure and features (i.e., DRS, HA, intelligent placement, templates, etc.) is achieved through the System Center Virtual Machine Manager (SCVMM). VMware's VirtualCenter can be added and ESX hosts can be managed from within SCVMM. Virtual Machine Manager 2008 provides most VirtualCenter Server functionality including VMotion.

Performance and Resource Optimization (PRO) can be integrated with other System Center products, such as:

- System Center Data Protection Manger (SCDPM) helps create a backup plan for your VM's as well as continuous data protection.
- System Center Operations Manager (SCOM) replaces MOM as a health monitoring program for your physical and VM's.
- System Center Configuration Manager replaces SMS as a scripting and configuration program.
- PowerShell.

SCVMM Administrator Console Overview

Once the SCVMM Administrator Console has connected to a SCVMM Server instance the main user interface displays. The console consists of a menu bar, toolbar and several different panes, dependent on the current view that is selected.

SCVMM Administrator Console Views

Console views are selected using the list in the bottom left hand corner of the window. The number of views available will depend on the current configuration of the SCVMM 2008 environment. The full list of views consists of the following:

Hosts

Displays information and options relating to managed host systems.

1. The first step in using SCVMM is to add a host which can be a Hyper-V, Virtual Server 2005 R2 or ESX host.
2. Create a host group called **HyperV** by right-clicking **All Hosts**.
3. Select **New host group**.
4. Click on the **Hosts** button in the left pane.
5. Click the **Add Hosts** link on the right. There will be an **Add VMware VirtualCenter Server** link.
6. A new wizard will start. Specify a hostname.
7. Add the host to the newly created **HyperV** hosts folder.
    - The **View Script button** with the PowerShell icon is where all underlying PowerShell code is executed. Every task performed in SCVMM can be scripted in PowerShell.
8. The host will be added to the SCVMM and all virtual machines currently running on it will be added to the SCVMM inventory. To view all virtual machines running on the host, click on the **Virtual Machines** link in the left pane.

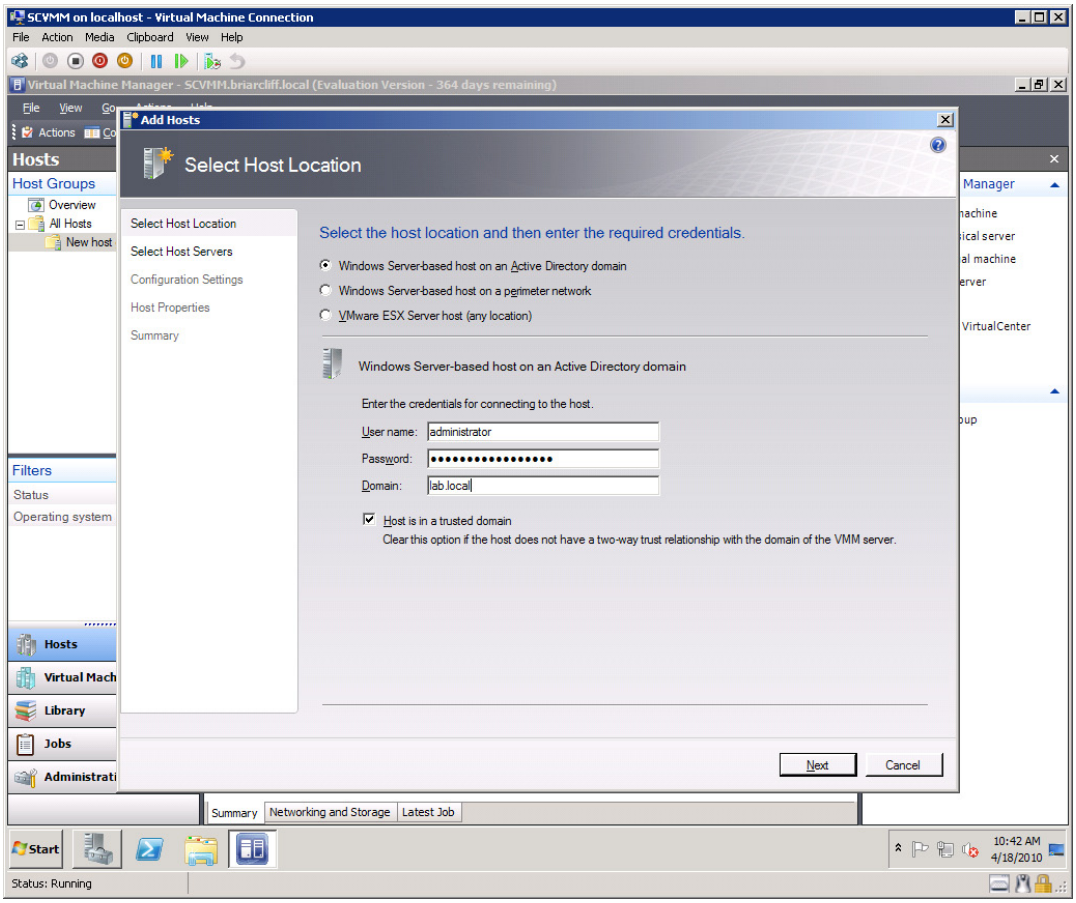


Figure 38: Selecting a host on an Active Directory network

The Hosts view can also be customized to see the guest status, CPU, RAM, Disk, and Network usage of each VM by selecting customizations from the **View** → **Select Columns**. Menu:

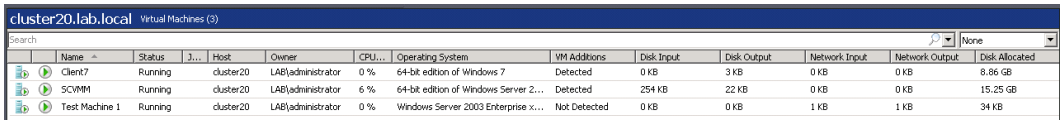


Figure 39: Customized Host tab columns displaying resource allocation and status

Other SCVMM Console Areas

The host will be added to the SCVMM and all virtual machines currently running on it will be added to the SCVMM inventory.

Virtual Machines - Displays information and options relating to the management all virtual machines installed on managed hosts (Figure 40).

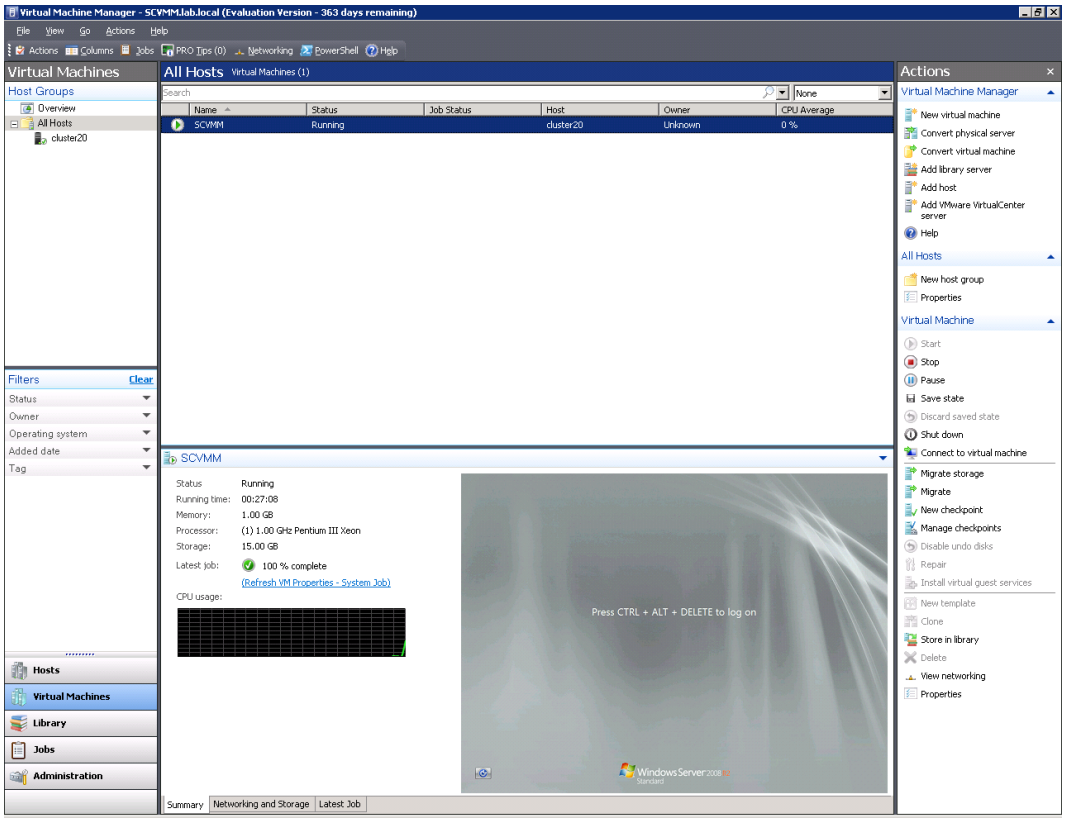


Figure 40: The Virtual Machines tab

Library

Displays information and provides options relating to the management of SCVMM Library Servers and library shares. By default, 2 blank VHD disks are provided in the library.

The library allows you to add items such as ISO files, starter VHD s, and guest OS profiles to assist in the deployment of new VMs. The New Guest OS Profile screen allows you to specify options such as computer name, administrator password, time zone, product key, and domain. This makes the guest OS profile similar to a stripped down version of Sysprep, and can even include Sysprep.inf or Unattend.xml files.

The new hardware profile allows you to specify a common configuration for machines you deploy based on that configuration. For example, you could configure your virtual development servers to only have 1 gigabyte of RAM, while new virtual production server could be allocated 4. You could be sure that all machines you deploy have like settings.

Jobs

Displays information and provides options to manage jobs. Virtual machine state can be managed by: stopping, starting, pausing or saving states. Jobs are steps that are initiated whenever a change is made within SCVMM. Jobs can be audited and are run independently. SCVMM administrator console provides filters to drill down into specific result categories.

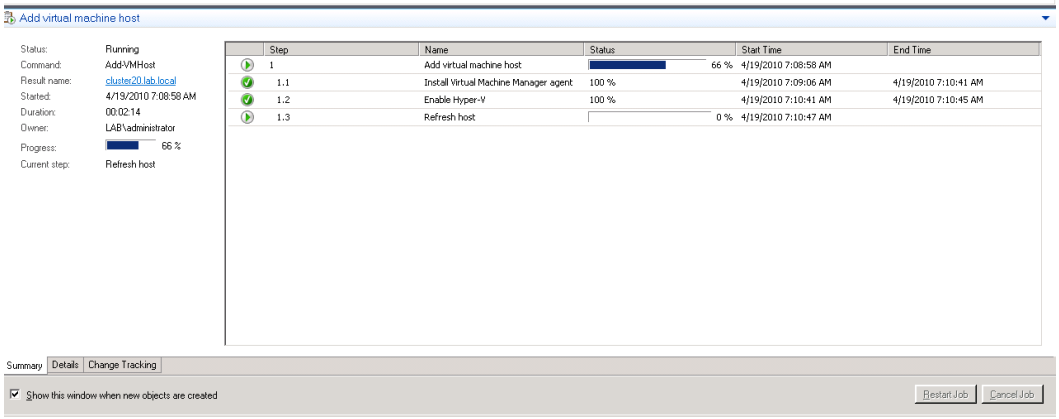


Figure 41: Running jobs in SCVMM display detailed statuses.

When you create a job in SCVMM, SCVMM generates the Powershell code that it will use behind the scenes to perform the task. Each wizard has a "View Script" button at the end of it, which will display the generated code in notepad. Because of powershell's verbose syntax, it is easy to read the scripts and modify them to automate Hyper-V operations. In the example code below, SCVMM creates a new virtual machine and places it on a host. It creates a virtual network adapter, DVD drive, and allocates a virtual CPU, before putting all these values into a hardware profile. Finally, it creates a VM called "Test VM 1" and places it on the "cluster20" host.

```
# ----------------------------------------------------------------
# New Virtual Machine Script
# ----------------------------------------------------------------
# Script generated on Monday, April 19, 2010 2:36:31 PM by Virtual
Machine Manager
#
# For additional help on cmdlet usage, type get-help <cmdlet name>
# ----------------------------------------------------------------
New-VirtualNetworkAdapter -VMMServer localhost -JobGroup 80df38d6-
7a75-4359-bb34-410bb125fa8b -PhysicalAddressType Dynamic
-VirtualNetwork "Local Area Connection - Virtual Network" -VLanEnabled
$false

New-VirtualDVDDrive -VMMServer localhost -JobGroup 80df38d6-7a75-4359-
bb34-410bb125fa8b -Bus 1 -LUN 0

$CPUType = Get-CPUType -VMMServer localhost | where {$_.Name -eq "1.20
GHz Athlon MP"}

New-HardwareProfile -VMMServer localhost -Owner "LAB\administrator"
-CPUType $CPUType -Name "Profile7950ac93-53f3-46e1-a78a-5d783349b3ff"
-Description "Profile used to create a VM/Template" -CPUCount 1
-MemoryMB 512 -RelativeWeight 100 -HighlyAvailable $false -NumLock
$false -BootOrder "CD", "IdeHardDrive", "PxeBoot", "Floppy"
-LimitCPUFunctionality $false -LimitCPUForMigration $false -JobGroup
80df38d6-7a75-4359-bb34-410bb125fa8b

$VirtualHardDisk = Get-VirtualHardDisk -VMMServer localhost | where
```

```
{$_.Location -eq "\\SCVMM.lab.local\MSSCVMMLibrary\VHDs\Blank Disk -
Small.vhd"} | where {$_.HostName -eq "SCVMM.lab.local"}

New-VirtualDiskDrive -VMMServer localhost -IDE -Bus 0 -LUN 0 -JobGroup
80df38d6-7a75-4359-bb34-410bb125fa8b -VirtualHardDisk $VirtualHardDisk
-Filename "Test Machine 1_Blank Disk - Small.vhd"

$VMHost = Get-VMHost -VMMServer localhost | where {$_.Name -eq
"cluster20.lab.local"}
$HardwareProfile = Get-HardwareProfile -VMMServer localhost | where {$_.
Name -eq "Profile7950ac93-53f3-46e1-a78a-5d783349b3ff"}
$OperatingSystem = Get-OperatingSystem -VMMServer localhost | where
{$_.Name -eq "Windows Server 2003 Enterprise x64 Edition"}

New-VM -VMMServer localhost -Name "Test Machine 1" -Description ""
-Owner "LAB\administrator" -VMHost $VMHost -Path "C:\ProgramData\
Microsoft\Windows\Hyper-V" -HardwareProfile $HardwareProfile
-JobGroup 80df38d6-7a75-4359-bb34-410bb125fa8b -RunAsynchronously
-OperatingSystem $OperatingSystem -RunAsSystem -StartAction
AlwaysAutoTurnOnVM -DelayStart 0 -StopAction SaveVM
```

After a job is run in SCVMM, a summary screen is displayed (Figure 42) that shows what changes SCVMM made to a host, library, or virtual machine.

Property	Previous Value	New Value
Host - cluster20.lab.local		
Cores per processor	0	8
CPU percentage reserve	(none)	20
Disk space reserve in MB	(none)	100
Enable VMRC	(none)	True
Flags	(none)	Available for Placement
Is non-trusted domain host	(none)	False
Is perimeter network host	(none)	False
L2 Cache size	0	2048
Logical processor count	0	8
Maximum disk I/O per second	(none)	10000
Maximum memory per virtual machine	0	12286
Memory space reserve in MB	(none)	512
Minimum memory per virtual machine	0	8
Name	(none)	cluster20.lab.local
Network percentage reserve	(none)	10
Operating system name	(none)	Microsoft Windows Server 2008 R2 Enterprise ,
Operating system version	0.0	6.1.7600
Optical drives	(none)	D:\;
Paths for virtual hard disks	(none)	C:\ProgramData\Microsoft\Windows\Hyper-V\
Physical processor count	0	1
Processor bus speed	0	133
Processor speed	0	2793
Secure Mode	(none)	True
SSH TCP Port number	(none)	0
SSL TCP Port number	(none)	0
Status	(none)	Responding
Suggested maximum memory per virtual machine	0	512
Total memory	0	12883316736
Use CA certificate	(none)	False
Virtual Server status	(none)	Running
Virtual Server version	(none)	6.1.7600.16385

Figure 42: A detailed status is given of all values changed by a job.

Administration - Provides a range of seven sub-options relating to the administration of the SCVMM 2008 environment:

- **Overview** - provides a graphical overview the status of virtual machines, jobs, libraries and hosts.
- **General** - access to SCVMM 2008 configuration such as database, library, remote control and placement (load balancing).
- **Managed Computers** - perform tasks relating to managed hosts such as updating and removing SCVMM Agents.
- **Networking** - manages the MAC address range used by SCVMM hosts.
- **User Roles** - view and manage user roles to control access and permissions within the SCVMM infrastructure. For example, this view allows profiles to be configured to control which users have access to the Self-Service portal, and what they can do when they log into it.
- **System Center** -provides access to System Center OpsMgr reports.
- **Virtualization Managers** - displays information on all virtual machine managers (including both SCVMM and VMware managers) currently being managed.

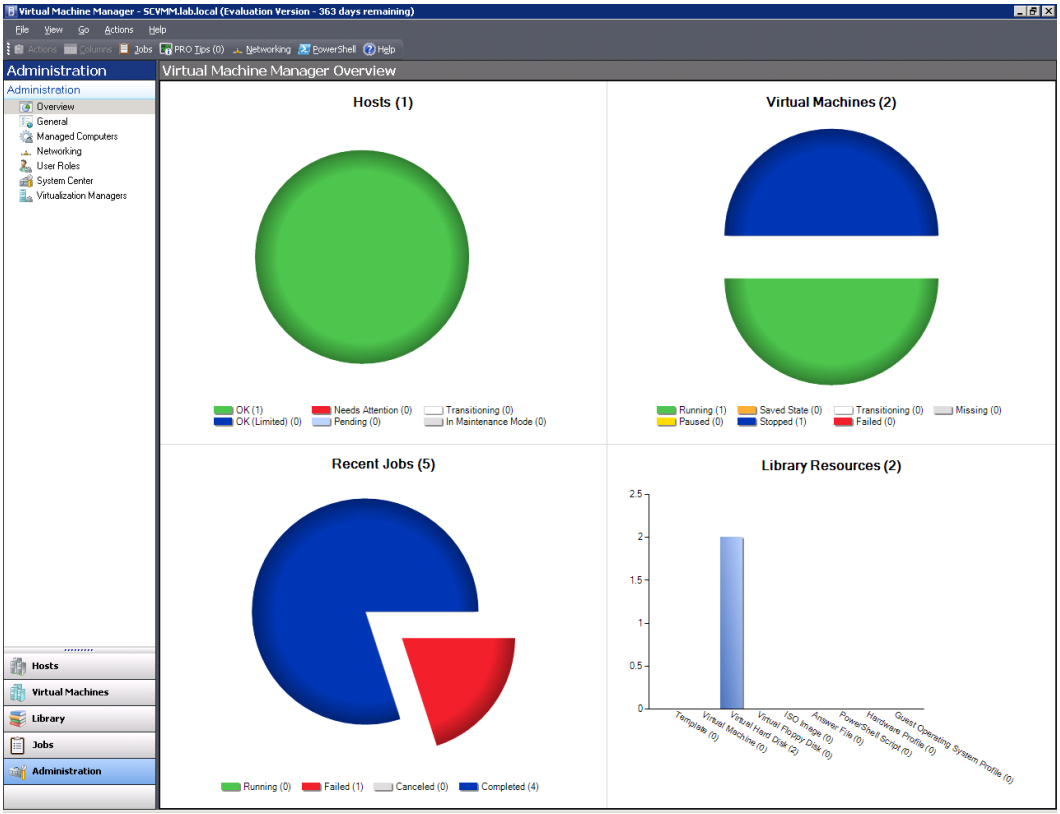


Figure 43: The administration view of the seven sub-categories of SCVMM.

- **Reporting** - Provides reporting options when the Operations Manager has been configured.
- **Diagram** - Provides monitoring of entire SCVMM environment (hosts, virtual machines, SCVMM Server, SCVMM Library Servers etc). This view is only available when the Operations Manager has been implemented.

SCVMM Self-Service Portal

The Virtual Machine Manager Self-Service Portal is a Web page through which self-service users can create and operate their own virtual machines within a controlled environment. In their sessions with the Self-Service Portal, self-service users see only the virtual machines that they own and the actions that their virtual machine permissions allow them to perform. With the SCVMM self-service portal feature, testers can set up and remove testing VMs as needed, without involving administrators.

The Self-Service Portal is installed by using a Setup wizard.

1. Open the **Start** menu.
2. Point to **All Programs.**
3. Point to **Microsoft System Center Virtual Machine Manager 2007.**
4. Click **Virtual Machine Manager Self-Service Portal.**
5. To open the SCVMM Self-Service Portal in a Web browser.
6. In a Web browser, specify the portal Web site in one of the following formats:
7. If the Self-Service Portal Web site is using a dedicated port, type http:// followed by the computer name of the Web server, a colon, and then the port number. For example, http://WebServer:80.
8. If not, type http:// followed by the host header name.
9. To open the Web site, press ENTER.

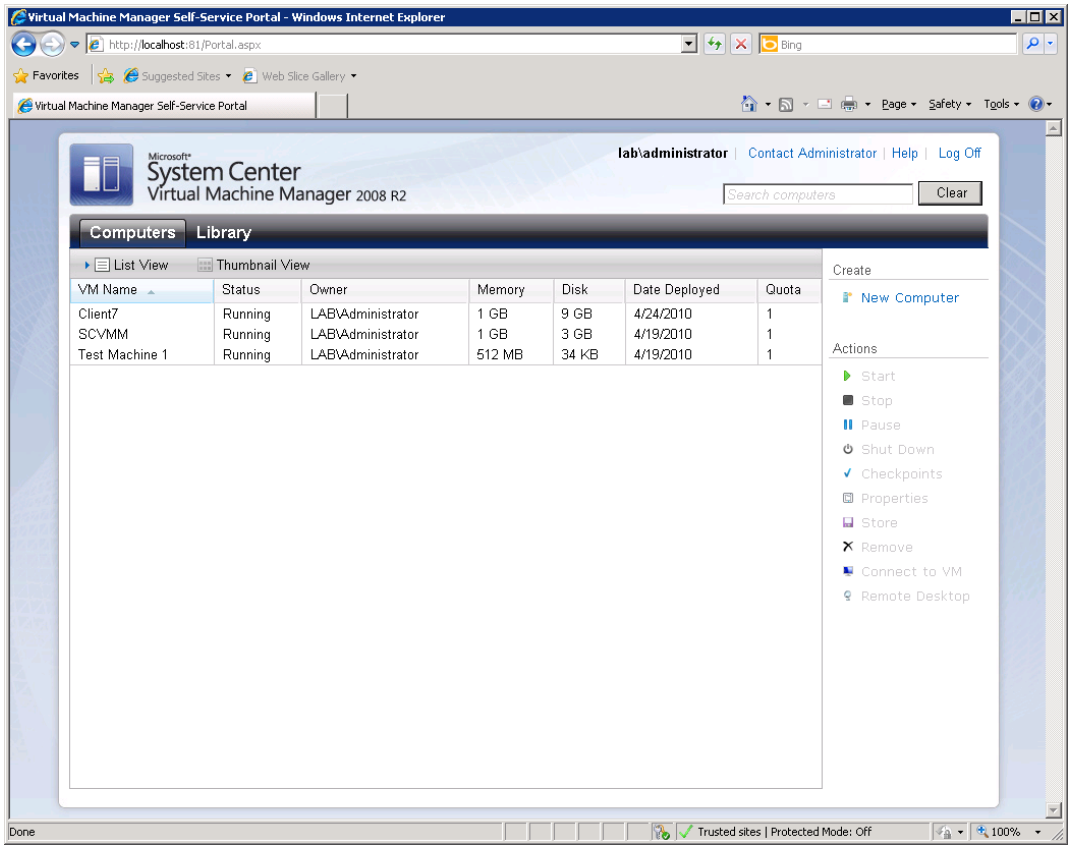


Figure 44: SCVMM Self-Service Portal's main screen. From here you can create, manage, and remove VMs and library items.

SQL Server Database

The SQL Server Database approach provides a virtualized and manageable solution with greater consolidation and less expense. This includes a standard library of server builds and an approach for replacing the current manual build process of development, test, and production environments. Not all SQL Server instances are good candidates for consolidation. The SQL Utility targets the majority of online transaction processing (OLTP) databases.

Consolidation and virtualization of resources is provided by the Storage Utility area network (SAN) storage. The SQL Utility and consolidation effort builds on the foundations that the Storage Utility and Compute Utility strategies provide. These strategies focus on consolidation and virtualization of resources. Microsoft IT Applications requirements and RightSizing data determine whether a virtual or physical server is needed, and to track all application and hardware resources.

SQL Server Consolidation Approaches include:

- **Host consolidation** – places additional SQL Server instances on each physical host.
- **Instance consolidation** - hosting more databases on each SQL Server instance, resulting in fewer overall SQL Server instances. Concerns and challenge include: more databases and applications, tempDB, memory, and service accounts; operating system that is shared in this model can influence patches, scheduled downtime, upgrade schedules, etc.
- **Database consolidation** - hosting more applications on each database. This consolidation can be achieved by using schemas, but doing so is not a cost-effective approach for consolidating existing databases and applications.

SQL Utility:

- Standard guest templates can be used for initial builds.
- Guests can be moved to newer hosts as needed for isolation, load balancing, or EOL server replacements.
- Guests can be reconfigured down or up to the next standard environment or guest.
- Small, medium, and large standard guests on a single host.
- Microsoft System Center Virtual Machine Manager 2007 can be used for capacity management.
- Consolidation platform is consistent with other consolidation efforts (i.e., Web servers).

Using SCVMM to Create VMs

Use the VM Wizard to create a new machine from:

- An existing VM
- Template in the library
- Disk stored in the library
- Clone VM's is an option

After Hyper-V has been installed, create a virtual machine and set up an operating system on the virtual machine.

1. Open Hyper-V Manager.
2. Click **Start.**
3. Point to **Administrative Tools.**
4. Click **Hyper-V Manager.**
5. From the **Action** pane, click **New.**
6. Click **Virtual Machine.**
7. From the **New Virtual Machine Wizard**, click **Next**.
8. On the **Specify Name and Location** page, specify the virtual machine name and it will be stored.
9. On the **Memory** page, specify enough memory to run the guest operating system to be used on the virtual machine.
10. On the **Networking** page, connect the network adapter to an existing virtual network if network connectivity is to be established at this point.
11. On the **Connect Virtual Hard Disk** page, specify a name, location, and size to create a virtual hard disk to install an operating system on it.
12. On the **Installation Options** page, choose the method for installing the operating system: Install an operating system from a boot CD/DVD-ROM, (physical media or an .iso image file).
    - Install an operating system from a boot floppy disk.
    - Install an operating system from a network-based installation server. To use this option, configure the virtual machine with a legacy network adapter connected to an external virtual network. The external virtual network must have access to the same network as the image server.
13. Click **Finish**.

P2V Conversion
The P2V conversion process captures an image of the source disk and modifies the operating system and drivers to make them compatible with the Hyper-V or Virtual Server hardware.

Virtual-to-virtual (V2V) machine conversion is a read-only operation that does not delete or affect the original source virtual machine. V2V conversion can be accomplished directly from an ESX host, from the SCVMM library, or from a Windows or Network File System (NFS) share.

System Center Virtual Machine Manager (SCVMM) allows conversion of existing physical computers into Hyper-V virtual machines through a process known as physical-to-virtual (P2V) conversion. P2V uses an automated wizard ideal for large-scale conversions that can be completed through the Windows PowerShell command line. SCVMM P2V does not recognize clusters. If a guest cluster is set up, SCVMM will treat the cluster as individual virtual machines.

During the P2V process, SCVMM automatically installs:

- An agent is installed
- Hardware configuration is captured
- An image is made
- A fix-up is applied
- VM is created

SCVMM uses the BITS (Background Intelligent Transfer Service) protocol for receiving P2V images and other data.

Online Conversion

Online conversion does not require a restart of the source computer. The online conversion process consists of:

- Installing the agent on the source computer
- Retrieving hardware configuration
- Imaging
- Fixing up
- Creating the virtual machine

Intelligent Placement

Intelligent Placement is a capacity planning function. Performance data is collected from the VM and the host where the VM runs, including CPU, memory, disk, etc. This data is fed into the modeling module, and then given user-defined placement to generate a set of SCVMM host ratings, such as: host performance capability based on memory considerations, disk capacity, and existing load.

Microsoft Assessment and Planning Toolkit

Microsoft Assessment and Planning (MAP) toolkit is an inventory, assessment, and reporting tool assesses IT environments for various platform migrations and virtualization without the use of any software agents. It is not part of SCVMM, but a separate free download from Microsoft. You should at least be familiar with what MAP does for the exam.

The MAP toolkit provides:

- Quickly discovers clients, servers, and applications across the IT environment.
- Conducts conversion and virtualization assessments for IT projects.
- Auto-generates reports and proposals.
- Scales well to small businesses as well as large enterprises.

MAP monitors the environment to get a view of utilization over time. It gathers data on performance and usage and will ultimately use this data to report to you. The MAP Power Savings Calculator calculates potential power cost savings with Hyper-V prior to deployment. MAP will make a recommendation about which servers should be co-located on which hosts to optimize performance.

The following reports can be generated:

- **Server Consolidation Proposal** - readiness assessments and recommends a list of underutilized servers for consolidation
- **Server Consolidation Report –** detailed inventory of network servers and the potential efficiency gained by consolidating them into fewer physical servers
- **Power Savings Calculator and Proposal –** calculates the potential savings and benefits of virtualization

Chapter 8: Managing Libraries and Checkpoints

SCVMM Library

The Virtual Machine Manager server contains a SCVMM library, which is a catalog of resources that can be used to create and configure virtual machines in SCVMM. The library contains files stored on library shares, and it can contain file-based resources such as:

- VHD files for VMs.
- CD or DVD images (e.g., ISO files) used as alternatives to physical media for software distribution.
- Hardware profiles, which are hardware specifications for a specific VM and contain information such as CPU type, amount of memory, and the priority given to the VM when it is running.
- Templates.
- OS profiles, which provide the most common OS settings, such as the computer name and domain or workgroup settings.
- Stored VM's.
- Scripts.
- Guest operating system profiles, which can be used to create virtual machines.

When you add a library server, SCVMM automatically installs an agent on the library server.
The Virtual Machine Manager Library is a repository used to store a variety of virtual machine resources such as virtual hard disk and CD/DVD ISO images, virtual machine templates, stored virtual machines, virtual floppy disks, hardware and guest operating system profiles and SysPrep answer files. The primary purpose of the library is to promote re-use of information and objects in the creation and configuration of virtual machines deployed within the SCVMM infrastructure.

A SCVMM Library consists of resources stored in one or more network share folders on the SCVMM Library Server system combined with information cataloged in the SQL Server database associated with the SCVMM 2008 installation. By default, the SCVMM Library share folder is located in **%SystemRoot\ ProgramData\Virtual Machine Library Files** and shared under the name **MSSCVMMLibrary**.

A SCVMM 2008 configuration can have multiple SCVMM Library Servers configured. The Library Server is commonly installed on the same system as the SCVMM Server, although for larger mission critical configurations, it is recommended that the SCVMM Library Server be deployed on a failover cluster.

Understanding Templates

The SCVMM has the ability to create a template or guest/hardware profile. There are two ways to create a Virtual Machine template:

1. **Create a New Template**
   In the library, click the **New Template** link on the right side to launch the template wizard. Create a Virtual Machine that can be used as a template using the **new template wizard**. Select the source for the new template. In this example, select "**From an existing virtual machine currently located on a host"**. After configuring the hardware profile specify all OS relevant information such as product key, computer name, default password and domain joining rules. There is also where to insert a sysprep answer file, if desired.

   The new template will be ready for deployment and stored under **VMs and Templates**.

2. **From existing VHD**
   Navigate to VMs and templates in the library view, right-click the template and select **New Virtual Machine.** A wizard will guide the process.

Types of Library Resources

The SCVMM library is a catalog of resources you can use to create and configure virtual machines in SCVMM. The library contains:

- Files stored on library shares - This includes virtual hard disks, virtual floppy disks, ISO images, and scripts. To be used in SCVMM, file-based resources must be added to the library by storing the files on a library share of a library server. The SCVMM library initially contains a single, default library server and library share, and two blank .vhd files, which Setup creates on the SCVMM server. The SCVMM server always remains the default library server, and the default library server and library share cannot be deleted.

  More library servers and shares can be added based on business needs and objectives. Library files and resources can also be distributed to branch offices or other remote locations.

- Operating system and hardware configurations - This includes virtual machine templates, hardware profiles, and guest operating system profiles, which can be used to create virtual machines that have uniform configurations. These configuration resources are stored in the SCVMM database and are not represented by physical files.

- Virtual machine templates stored in the SCVMM database - Virtual machines that are not in use can be stored in the library. Stored virtual machines are displayed in Library view; however, the files for a stored virtual machine are not indexed and displayed in Library view, because those files cannot be used to create or configure new virtual machines.

Library resources are added, created, used, and managed in Library view.

Refreshing the Library

After adding files to a library share, the files do not appear in Library view until they are indexed by SCVMM during the next **library refresh**. Refresh the library share manually or wait until the next periodic library refresh.

Library Groups

As more library servers are added, **library groups** can be created. Coordinate library servers with the host groups that use their resources, especially when the library server is also connected to the SAN. This will tell which hosts and library servers are connected to the SAN to take advantage of faster file transfers on the SAN.

The library group **Properties** dialog box makes alignment easy by displaying the host groups in the **Library group** drop-down list.

Hardware Profile Components

1. Hardware resources can be manually allocated to use the hardware profile.
2. Click **Next** to be taken to the New Virtual Machine Wizard's Select Destination screen. Select whether to place the new virtual machine on a host or to store the virtual machine in a library. In most cases it is best to placed the cloned machine in the library.
3. What happens next really depends on the option that you select on this screen. If the server is placed in the library a prompt to enter the library server name and path displays. If hosting the virtual machine, specify the host and path and how the virtual machine will connect to the network.

SCVMM 2008 Pre-installation

Connect to SCVMM website

The **SCVMM Configuration Analyzer** scans computers to verify if they are suitable to function as a SCVMM Server, run the SCVMM Administrator console, function as a Self-Service Portal or be a Managed Host. Run the SCVMM Configuration Analyzer prior to actually beginning the setup process to examine the server that will be hosting the Virtual Machine Manager function. The SCVMM configuration Analyzer is not included with the product and must be downloaded from the Microsoft public download site.

First install the **Microsoft Baseline Configuration Analyzer** as a download on the Microsoft public download site. Run with an account that has administrative permissions to all machines that are being scanned. After the scan completes, a report is opened in Internet Explorer documenting the results of the scan.

Installing Virtual Machine Manager Server

1. Select SCVMM Server under SETUP on the main screen.
2. Accept the license.
3. Join the Customer Experience Improvement Program (CEIP).
4. Enter Product Registration information.
5. Execute the Prerequisites Check and make sure it completes successfully. If not, correct the problems and re-run the check.
6. Select an Installation location on the local machine.
7. Configure **SQL Server settings**.
8. Create a new library share on the SCVMM server or select a pre-configured share. As a 'best practice', you may want to consider using another volume on the SCVMM Server for better performance and storage capacity.

9. After setup is complete, the default library cannot be removed or relocated. An existing share on the SCVMM Server can be used in place of the default location; however it must reside on the SCVMM Server. Additional Library Shares and Servers can be added in the future.
10. Specify ports to support SCVMM communications and designate a domain account to use for the **SCVMM Service Account** (Default is to use local system). If the Self- Service portal is being hosted on the SCVMM server, Port 80 will already be taken by the Default Website. Either change the port in IIS Services Manager or set a different one for SCVMM communications.
11. Specify Local system or a domain account to use for the **SCVMM Service Account** (Default is to use local system).
12. Verify all the selections before selecting **Install**. If no issues, the install will complete. Check for Virtual Machine updates on the Microsoft website.

Note: When the SCVMM server is installed, all accounts in the local Administrators security group are automatically added to the SCVMM Administrator user role.

SCVMM Administration Console

It is recommended that the **Virtual Machine Manager Administrator Console** be installed on the same computer as the SCVMM server. Additional SCVMM Administrator Consoles can be installed on other computers to remotely access and manage the SCVMM server. When the SCVMM Administrator Console is installed, the Setup Wizard also installs Windows PowerShell - Virtual Machine Manager Command shell. To use the SCVMM reporting feature SCVMM Administrator Console must be installed on the same computer as the SCVMM server.

Installation Steps:

1. In the setup menu select Administrator Console.
2. Accept the License Terms.
3. Review customer Experience Improvement program (CEIP) information.
4. Execute the Prerequisites Check and make sure it completes successfully. If not, correct the problems and re-run the check.
5. Select an Installation location on the local machine.
6. Verify the Port Assignment. The default port is 8100.
7. Verify all the selections before selecting **Install.** If no issues the install completes. Check for Virtual Machine updates on the Microsoft website.
    - By default, a shortcut to the SCVMM Administrator Console will be placed on the desktop. Double-click on the shortcut and verify the Administrator console does open. The first time open the SCVMM Administrator Console is opened, the Connect to Server dialog box displays. In the Connect to Server dialog box, do one of the following:
        - If you installed the SCVMM Administrator Console on the same computer as the SCVMM server, click Connect to connect to the local SCVMM server (localhost) using the port that was assigned during the installation of the SCVMM server.
        - If using the SCVMM Administrator Console to connect to the SCVMM server on a different computer, in the Server name box, type the name of the computer where the SCVMM server is installed, followed by a colon and the port that assigned during SCVMM server installation.

Understanding Hardware Profiles

The Virtual Machine Manager library is a catalog that gives access to file-based resources (such as Sysprep scripts, ISO images, and virtual hard disks) that are stored on your library servers and to virtual machine templates, guest operating system profiles, and hardware profiles that reside in the SCVMM database. You can also store virtual machines in the library when they are not in use.

Templates and Profiles

By creating a virtual machine template, a reference image for a virtual machine can be used repeatedly. Templates are metadata only and exist in the SCVMM database, not in the file system.

In Library view, virtual machines and templates appear in the **VMs and Templates** node under any library server that stores physical files that the virtual machines or templates reference. A single template might appear on multiple library servers if, for example, it used an ISO image on one library server and a VHD on another.

All guest operation system profiles and hardware profiles appear in the **Profiles** node—the bottom node in the navigation pane.

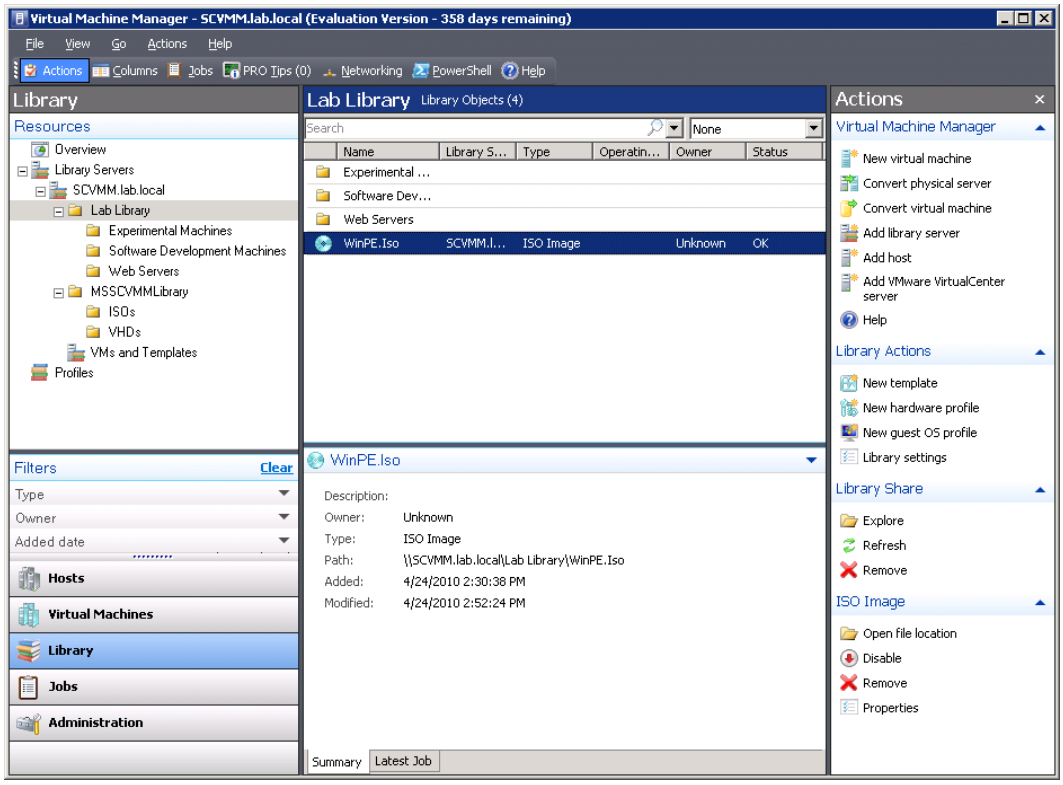


Figure 45: The SCVMM Library

Virtual Machine Configurable Virtual Hardware Settings

A hardware profile can be created based on defaults or based on an existing hardware profile. If no changes are made, the Virtual Machine Manager creates a default hardware profile.

Virtual Machine Hardware Profile Specifications include:

- Host CPU resources.
- Host Memory.
- Built-in virtual floppy drive.
- Built-in virtual IDE device - virtual hard disks cannot be attached to a stand-alone hardware profile.
- One or more optional virtual SCSI adapters that can be added. Virtual hard drives can be attached to the virtual SCSI adapter n a virtual machine or on a template but not on a stand-alone hardware profile.
- One or more optional virtual network adapters can be added.
- Priority settings.

Self-Service Portal is an optional component of SCVMM 2008 that allows users or server administrators to create and manage their own virtual machines using a web interface. The portal utilizes SCVMM 2008 self-service user roles which determine or limit the scope of the users' actions. The prerequisite software for installing the Self-Service Portal are:

- Windows Server 2008 x64 Standard, Enterprise, or Datacenter edition
- Windows Server 2003 (or R2) with SP2
- Internet Information Server (IIS)

Self-Service Portal hardware requirements are defined by the number of concurrent users that the portal will serve. Check for updates before attempting to install a Self-Service Portal.

To install the Self-Service Profile, complete the following steps:

1. Install the Self-Service Portal. It is one of the options on the SCVMM installer.
2. Determine which Hyper-V hosts should be used with to the Self-Service Portal to host virtual machines.
3. Create a host group and move all the Self-Service candidate Hyper-V hosts to that host group.
4. Create a Self-Service User Role.

The Self-Service portal can be installed on the SCVMM server or on a separate machine. In order to install the Self-Service portal a base operating system and IIS to host the web console are needed.

Installing Virtual Machine Manager Server Component

Once you have the SCVMM Administrative Console component installed, proceed to installing the Self-Service Portal.

1. Logon to the machine with domain administrator credentials.
2. Insert the SCVMM 2008 media and launch the setup.
3. From setup screen, click **SCVMM Self-Service Portal**. The SCVMM Setup will copy temporary files needed for installation and launch the installation wizard.
4. The installation files are copied to the server.

5. License Terms screen displays; select **I accept the terms of this agreement** and click Next.
6. On the Prerequisites Check screen, verify that all of the prerequisites have been met and click **Next.**
7. On the Installation Location screen, verify the path is correct and click **Next**.
8. On the Web Server Settings screen, verify the SCVMM Server fully qualified domain name, modify the default ports for the Administrative console if required, modify the port for the self service console, and then press **Next**.
9. On the Summary of Settings Screen, review settings and press **Install** to being installation of Self-Service Portal component.
10. At the end of the installation, success or failure of the Self-Service Portal installation message is received. Review status, click **Close**.

Determine the Hyper-V Hosts for Self-Service

Hyper-V hosts are typically dedicated for self-service use. Select as many Hyper-V hosts as necessary for the number of virtual machines that will be used as self-service that will run concurrently. Use Self-Service advanced features such as and VM templates to determine. For example, a VM template that is limited to 1GB RAM and a quota that allows only 2 VMs per self-service user will help predict the number of users in the self-service role.

Building Host Group for Self-Service

A Hyper-V host can only be a member of a single host group and a Self-Service Portal defines access by the assigned host group. If multiple self-service portals are to be grouped together in the host group hierarchy, create a host group called Self-Service, and then create the other host groups under Self-Service.

1. From the SCVMM console, click the **Hosts** option in the left hand pane.
2. In the navigation menu on the left hand pane, select **All Hosts**.
3. From the Actions menu, click **Add Host Group**.
4. Enter Self-Service for the new host group name and press **Enter**.
5. Drag and drop the Hyper-V hosts that are to be Self-Service hosts into the Self-Service host group.

Creating the Self-Service User Role

By default users cannot access the Self-Service Portal. Users, including Domain Admins, must be granted permission. To access the Self-Service Portal a self-service user role must be created and users added as members of that role.

1. Click the **Administration** button.
2. Click **New User Role** in the Actions menu to start the New Role Wizard.
3. In the General screen, type a **User role name** and **Description**, then select **Self Service User** in the profile list, press **Next**.
4. In the Add Members screen, click **Add** and then type the names of the users or groups you want to add to this role, press **Next**.
5. In the Scope screen, **select the host groups** on which users will deploy their virtual machines, press **Next**.

6. In the Virtual Machine Permissions screen, **select the actions** that you want to allow the members of this group to perform on virtual machines press **Next**.
7. In the Virtual Machine Creation Settings, **Select the options** the members of the self-service user will be allowed to perform. If desired, set a virtual machine quota to limit the number of virtual machines the users can deploy at one time, press **Next**.
8. In the Library Settings screen, select if self-service user group members will have access to a library share. If self-service users to store their virtual machines on a library share, the stored virtual machines do not count against any virtual machine quota that you set when allowing self-service users to create a virtual machine, press **Next**.
9. Review your choices and press **Create** to create the self-service user group.

Once self-service user permission and option roles are defined, the members of the role can access the Self-Service Portal. If the self-service member is assigned owner of any virtual machine(s) these machines will appear in the list as virtual machines they can manage. If they have the right to create new virtual machines, the **New Computer** option will allow them to select from the assigned predefined templates.

Managing Checkpoints

A checkpoint is a snapshot of a virtual machine at a specific point in time. Checkpoints are implemented using differencing disks and enable an administrator to roll the virtual machine back to its state at the moment the checkpoint was created. Checkpoints are portable; when a virtual machine is migrated from one virtual machine host to another, the checkpoints migrate along with the virtual machine. As many as 64 checkpoints can be created for a virtual machine however they are not a replacement for backups. Each checkpoint saves the state of each virtual hard disk that is attached to a virtual machine and all of the hard disk's contents, including application data files. Use the **Recover** action to restore a virtual machine to its state when a checkpoint was created. Merge the checkpoint to delete the associated files and recover disk space.

Creating a Checkpoint

Shut down the virtual machine or used a VM in a Stopped or Turned Off state. To avoid losing any data, ensure that the virtual machine is not in use and that no processes are running on the virtual machine.

1. In **Virtual Machines** view, expand **All Hosts** in the navigation pane, and navigate to the host on which the virtual machine is deployed.
2. In the results pane, select the virtual machine and then, in the Actions pane, click **New checkpoint**.
3. If the virtual machine is running, SCVMM warns that the checkpoint operation will turn off or shut down the virtual machine and ask if you want to continue.
4. To continue, click **Yes**.
5. Under **Checkpoint description**, enter a description to add to the timestamp that identifies the checkpoint.

Managing Networks in SCVMM

Although the networks in our examples example may seem trivial since only 1 NIC has been dedicated to Hyper-V, as more hosts, VMs, and adapters are added, the networks will become more complex and difficult to follow. Diagramming a large Hyper-V cluster can be difficult, showing how each virtual network card connects to each virtual switch and then to the physical hardware. This can be exceptionally challenging if you have NICs dedicated to a DMZ, LAN, a Backup Network, an iSCSI Network, and Cluster Heartbeat network. The process can be further complicated by redundancy.

SCVMM provides a tool that can help you visualize, secure, and utilize your host server's NICs. By selecting **Networking** from the **View** menu, SCVMM will generate a display of the Host's VMs and their Virtual Networks (Figure 46).

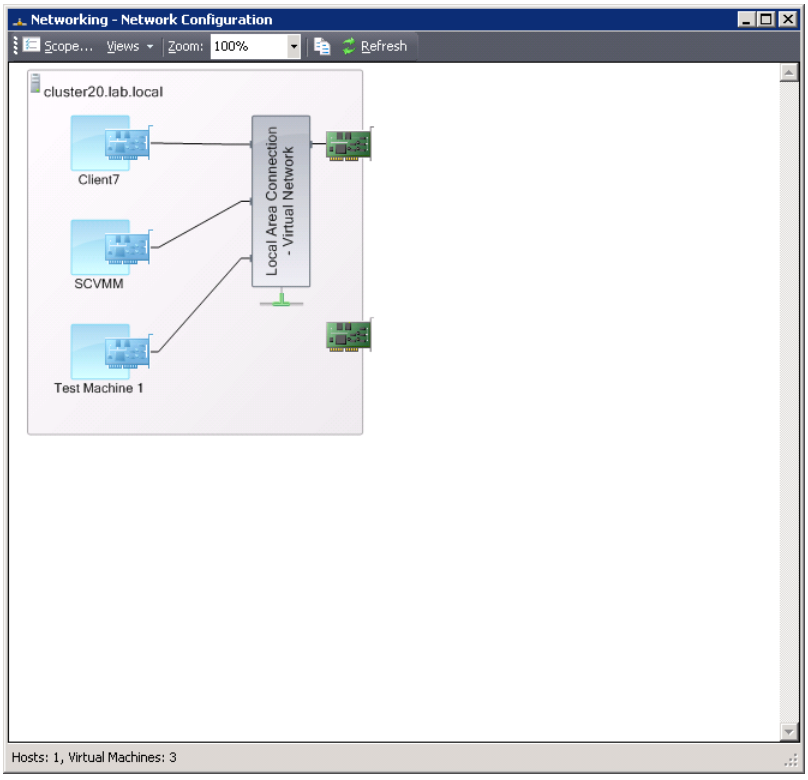


Figure 46: SCVMM Visualizing virtual and guest network connections.

Chapter 9: Powershell and Backups

SCVMM and PowerShell

The Virtual Machine Manager server product includes the Windows PowerShell - Virtual Machine Manager command shell. The command shell is used to manage virtual machine hosts, library servers and virtual machines, at the command line or by using task-based scripting.

Windows PowerShell built-in commands, called **cmdlets**, assist in managing computers from the command line. **Providers** allow easy access to data stores, such as the registry and certificate store, and PowerShell also includes a parser and a fully developed scripting language.

The SCVMM command shell includes the standard Windows PowerShell cmdlets, but also provides a specifically designed comprehensive set of cmdlets. Use standard Windows PowerShell cmdlets with SCVMM to create scripts. Windows PowerShell and the SCVMM command shell, supports programming functions such as variable assignment, looping, conditional statements, and flow control. The cmdlets perform all SCVMM actions which can be used individually or strung together for more complex tasks. This means that any task to be performed by using the SCVMM Administrator Console can also performed at the command line or by creating a Windows PowerShell script.

The SCVMM Administrator Console includes features to perform both methods:

- Like Exchange 2007 and higher, the Summary page of each wizard contains a **View Script** button that displays the Windows PowerShell cmdlets that the wizard will use to configure the changes based on individual specifications. The cmdlets can also be copied to be used in creating Windows PowerShell scripts.
- If Windows PowerShell scripts are stored in the SCVMM library, you can view, edit, or run the script in Library view.

Powershell Overview

Windows PowerShell provides centralized management of physical and virtual infrastructures when that infrastructure is managed by SCVMM. Built on the .NET Framework, Windows PowerShell helps to control and automate the administration of Windows operating systems and applications that run on Windows. Windows PowerShell 1.0 includes the following features:

- Standard cmdlets for performing common system administration tasks and using Windows Management Instrumentation. A cmdlet contains a verb-noun pair that is separated by a dash. The verb acts on a Windows PowerShell object (the noun). Most cmdlets are simple, but they are designed to work in combination with other cmdlets. For example, cmdlets that contain the **Get** verb retrieve data. Cmdlets that contain the **Set** verb specify or change data.
- Task-based scripting language and support for existing scripts and command-line tools.
- Common syntax and naming conventions provided data can be shared easily and the output from one cmdlet can be used as the input to another cmdlet without configuration changes.
- Operating system navigation is simplified with command-based navigation. For example, Active Directory objects can be enumerated and manipulated using Powershell.
- Backwards compatibility with **cmd.exe** and batch files. This means that Powershell can be used for manipulation of files and executing programs.
- Objects can be directly manipulated or sent to other tools or databases.
- Custom tools and utilities to administer software.

Begin Learning PowerShell

Windows PowerShell contains the following resources:

- **Getting Started** - brief introduction and tutorial. To open it, click **Start, All Programs, Windows PowerShell 1.0**, and then click **Getting Started**.
- **User Guide** - detailed introduction, including real-world scripts and scenarios.
- **Get-Help cmdlet** - Windows PowerShell cmdlet gives an overview of system cmdlets and providers. Start Windows PowerShell, and at the prompt, type: **Get-Help**.
- To learn about the Windows PowerShell scripting language and other concepts, read the "about" topics. To see a list of "about" topics, type: **Get-Help about**.

PowerShell Benefits

- Cmdlets allows performance of complex tasks with only a few words.
- Object-oriented commands allow rich objects from a text base.
- Integrates with Windows system by making calls into the Windows Registry, .NET Framework or WMI extensions.
- Certificate based scripting allows only secure scripts to run by default.

Cross-Product Scripting

SCVMM uses Windows Management Instrumentation (WMI) for cross-product scripting. A WMI interface provides programmatic access to a system so users can write command-line administration scripts and tools. The WMI interface also allows network administrators the ability to collect and set configuration details on a wide variety of hardware, operating system components and subsystems, and software. WMI does not consolidate the management data in a central location.

Enable Windows PowerShell Scripts to Run

When Windows PowerShell is started on a computer, the default security policy does not allow the running of scripts. The Windows PowerShell security policy for scripting is called an ***execution policy***. The execution policy gives the option to run scripts in your environment or to include a digital signature. Windows PowerShell does not allow a script to be run by double-clinging its icon due to the risks involved in using this method.

The following execution policies govern scripting in Windows PowerShell:

- **Restricted** - permits interactive commands only (no scripts). This is the default.
- **AllSigned** - permits scripts, but requires a digital signature from a trusted publisher for all scripts and configuration files, including scripts that you write on the local computer.
- **RemoteSigned** - permits scripts, but requires a digital signature from a trusted publisher for all scripts and configuration files that are downloaded from the Internet, including e-mail. A digital signature is not required for scripts that you create on the local computer.
- **Unrestricted** - permits scripts, including unsigned scripts.

Because the default Windows PowerShell execution policy is Restricted, Windows PowerShell scripts cannot be run until a change to a less restrictive execution policy is made. The following Windows PowerShell Help topics explain execution policies.

At the Command Prompt, enter:

- **Get-Help about_Signing** - displays information about Windows PowerShell execution policies and the levels of security that the execution policies provide.
- **Get-Help Get-ExecutionPolicy** - displays information that explains how to determine the current scripting security policy.
- **Get-Help Set-ExecutionPolicy** - displays information that explains how to change scripting security policy.

Creating Scripts

Windows PowerShell scripts are stored in the SCVMM library. They can be viewed, edited, and run in Library view.

To run a script from the SCVMM Administrator Console, enable scripting in Windows PowerShell on the local computer using one of the methods from the previous section on changing the signing policy.

To view or edit a Windows PowerShell script from the SCVMM library

1. In **Library** view, select the script to be viewed.
2. In the **Actions** pane, under **Script**, click **View PowerShell script** to open the script in Notepad.
   - If **Save As** is used to save a new script on the same share, the script will be added to the library during the next library refresh. Give the file a .ps1 file name extension to enable running it in the Windows PowerShell – Virtual Machine Manager command shell. Use the **Refresh share** action to perform a manual refresh on the library share.

To run a Windows PowerShell script from the SCVMM library:

1. In Library view, select the script to be run.
2. In the **Actions** pane, under **Script**, click **Run PowerShell script** to load the script in a Windows PowerShell runspace.
3. If an unsigned script, at the prompt, type R (Run Once).

Windows PowerShell Script Extensions

There are three script file extensions in Windows PowerShell, although most script files have the .ps1 extension.

1. **Windows PowerShell Scripts** have extension .ps1 – a standard Windows PowerShell script.
2. **Windows PowerShell Console Files** have extension .psc1 – defines the configuration of a specific Windows PowerShell console.
   - Microsoft System Center Virtual Machine Manager 2008\Bin\Cli.psc1 is the Windows PowerShell console file for Microsoft System Center Virtual Machine Manager.

- Microsoft.EnterpriseManagement.OperationsManager.ClientShell.Console.psc1 is the Windows PowerShell console file for Microsoft System Center Operations Manager.

  For more information about Windows PowerShell console files, type **Get-Help Export-Console** at the command prompt.

3. The **Windows PowerShell Format and Type** definitions have file extension .ps1xml - A type of script file Windows PowerShell home directory (***<C>***:\WINDOWS\SysWOW64\Windowspowershell\v1.0). For more information, type **Get-Help about_Types** at the command prompt.

Running Windows PowerShell Scripts

When running a Windows PowerShell script, indicate the full path with the name of the script even if working in the directory in which the script is located. The following methods can be used to run a Windows PowerShell script:

- Use the dot and the backslash (.\) to indicate the local directory, i.e.: **.\ <ScriptName>.ps1**
- Specify the full path of the script, i.e., **C:\Scripts\<ScriptName>.ps1**
- Specify the path of the script, omit the extension, i.e., **C:\Scripts\<ScriptName>**
- Use the **Invoke-Expression** cmdlet to run a script, i.e., **Invoke-Expression C:\Scripts\<ScriptName>.ps1**
- Use double quotation marks for any paths that include spaces, i.e., **Invoke-Expression "C:\My Scripts\<ScriptName>.ps1"**
- Use the ampersand to run a script. Example: **& C:\Scripts\<ScriptName>.ps1**

SCVMM PowerShell Examples

By default, Hyper-V does not include any cmdlets. The only cmdlets that run with Hyper-V are provided by SCVMM. SCVMM provides the following PowerShell namespaces:

- **MSVM_VirtualSystemManagementService** – create, import, export, snapshot, and delete virtual machines.
- **MSVM_VirtualSwitchManagementService** – allows you to control virtual networks.
- **MSVM_ImageManagementService** – allows you to create, mount, and manipulate VHD files.

In this section, we will show some examples of how PowerShell can be used to manage SCVMM and Hyper-V hosts.

Example 1. Use PowerShell to list the vitals of each virtual machine that SCVMM knows about. This is useful for inventorying Virtual Machines.

```
PS C:\Windows\system32> get-vm | select name, status, hostname, memory

Name                 Status HostName                    Memory
----                 ------ --------                    ------
SCVMM                Running cluster20.lab.local        1024
Test Machine 1       PowerOff cluster20.lab.local       512
```

Example 2. Use PowerShell to create a checkpoint of a VM and restore to that checkpoint at a later time. This example might be useful for software testing teams who need to roll a test image back to a previous version.

```
PS C:\Windows\system32> $checks = get-vmcheckpoint -vm "Test VM 1"
PS C:\Windows\system32> restore-checkpoint -vmcheckpoint $checks
```

A checkpoint is the same thing as snapshot. Snapshots are used in Hyper-V without SCVMM, while SCVMM refers to them as Checkpoints. Just like a snapshot, restoring a checkpoint will turn off the virtual machine if it isn't already.

Backup and Recovery

The Windows Server Backup consists of a Microsoft Management Console (MMC) snap-in and command-line tools that provides a complete solution for day-to-day backup and recovery needs. You can use four wizards to guide you through running backups and recoveries. Use Windows Server Backup to:

- Back up a full server (all volumes), selected volumes, or the system state. The backup can recover volumes, folders, files, certain applications, and the system state.
- A system recovery will restore the complete system onto the new hard disk in case of a disaster.
- Use Windows Server Backup to create and manage backups for the local computer or a remote computer.
- Use schedule backups to run automatically and perform one-time backups to augment the scheduled backups.

Windows Server Backup is available in all editions of Windows Server 2008 (both 32-bit and 64-bit versions). The Windows Server Backup snap-in is not available for the Windows Server 2008 Server Core installation option. With a Server Core installation, either use the command line or manage backups remotely from another computer. The Server Core installation option does not include Windows PowerShell, so the cmdlets for Windows Server Backup are also not available on this type of installation.

Windows Server Backup
Install the **Windows Server Backup, Command-line Tools**, and **Windows PowerShell** items that are available in the Add Features Wizard in Server Manager. This installs the following tools:

- Windows Server Backup Microsoft Management Console (MMC) snap-in
- **Wbadmin** command-line tool
- Windows Server Backup cmdlets (Windows PowerShell commands)

Installation of the Windows server Backup features in Service Manager must be performed by a member of the Backup Operators or Administrators group. Access the Windows Server Backup from Server Manager by click on the **Storage** node.

To install backup and recovery tools

1. Click **Start**, click **Server Manager.**
2. In the left pane click **Features**, and then in the right pane click **Add Features**.
3. This opens the Add Features Wizard.
   In the Add Features Wizard, on the **Select Features** page, expand **Windows Server Backup Features**, and then select the check boxes for **Windows Server Backup** and **Command-line Tools.**
4. A message displays that Windows PowerShell is also required to be installed with these features.
5. If only installing the snap-in and the **Wbadmin** command-line tool, expand **Windows Server Backup Features**, and then select the **Windows Server Backup** check box. In this case, Windows PowerShell is not required.
6. Click **Add Required Features**, and then click **Next**.
7. On the **Confirm Installation Selections** page, review the choices that you made, and then click **Install**. Any errors in installation will be noted on the **Installation Results** page.
8. Then, to access these backup and recovery tools, do the following:
   - Windows Server Backup snap-in:
   - Click **Start**, click **Administrative Tools**, and then click **Windows Server Backup**.
   - Access and vie w the syntax for **Wbadmin**:
     Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**. At the prompt, type: **wbadmin /?**
   - Instructions to access and view the Help for the Windows Server Backup cmdlets are located at GettingStarted.rtf at: C:\Windows\System32\WindowsPowerShell\v1.0\Documents\<***language***>.

Backup with Hyper-V

There are three ways to back up Hyper-V servers. First, you can run a backup from inside the guest OS, as if the guest server isn't virtualized at all. The only caveat to this approach is not to schedule all of your backups at the same time, since backups can be disk and network intensive.

The second way to backup Hyper-V is by backing up the parent partition, which provides a backup of all of the VHD and XML files that compose a child server. This is known as an **online** backup. When a Hyper-V backup program such as Windows Server Backup begins a job, it will do 2 things:

1. Ask the parent partition's disk subsystem to perform a Volume SnapShot.
2. Ask the child partitions, by means of the integration services, to perform a Volume SnapShot.

The third method to backing up Hyper-V is to shut down all of the VMs, run the backup, and then restart them. Sometimes this is necessary if the VMs are not capable of running integration services and the guest OS is not enlightened. This is known as an **offline** backup.

Understanding Online and Offline Backups

An online backup can be performed 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.
- Disks that are being used by the virtual machine are configured within the guest operating system as NTFS-formatted basic disks. Virtual machines that use dynamic disks or the FAT32 file system prevent an online backup from being performed.
- Volume Shadow Copy Service is enabled on all volumes used by the virtual machine with a specific configuration. Each volume must have its own storage location for its shadow copies and that mapping must be available to the Hyper-V VSS writer.
- If an online backup cannot be done, offline backup is necessary. This results in downtime.

Chapter 10: Live Migration and Cluster Shared Volumes

Live Migration is a new R2 feature that allows a point-in-time copy of a running VM to be moved from one host to another. If you are familiar with VMWare, this high-availability solution is similar to VMWare's vMotion product for moving live machines between hosts.

Designing your SAN solution is covered in the 70-693: Pro: Windows Server R2, Virtualization Administration. 70-659 assumes you know enough about SANs to migrate virtual machines between hosts. Live Migration (LM) requires several items to be present in your physical configuration:

1. Systems in a LM cluster must be running the same processor architecture. LM will not work between AMD and Intel. They must also be running the same processor generation. An Intel Core i7 CPU will have unpredictable results when attempting to use Cluster Shared Volumes with an Intel Core 2 Duo CPU.
2. Each system in a LM cluster must have access to some kind of shared storage that can make use of Cluster Shared Volumes (CSVs). This includes Fibre Channel and iSCSI. There are trade-offs to each architecture in terms of price, performance, and features, and not every SAN supports the SCSI-3 standard needed for LM.

When a request for a Live Migration takes place in a cluster, the cluster begins copying memory pages from the host that is currently running the VM to the new host. Since this may take some time, any pages in RAM that change during the copy are recorded and sent to the new host. Hyper-V will do this for up to 8 iterations of the system's current image in memory, each time computing a hash of the contents. The purpose of the hash is to compare if the VM running in RAM matches the VM's RAM image, which is being transferred to the new host. As soon as the two have identical copies of the VM's memory image, ownership of the VM is transferred to the new host and ownership of any resources (such as VHD files on the SAN) are switched over to the new host.

Live Migration, when performed correctly, means nearly zero downtime for the clients connected to whatever application is running on the guest. The active TCP sessions between the guests and clients are maintained. Although you may lose a few network packets at the moment ownership changes from hosts, these packets will most likely be retried (depending on your application) and at the very worst, you should notice less than 1 second worth of lost traffic.

Live Migration & Cluster Shared Volumes

Live Migration is a feature new to R2 that allows you to copy a running VM from one host to another. It is present in Enterprise, Datacenter, and the standalone Hyper-V Server products in both Server Core and Full modes. It is not present in Server 2008 Standard Edition because Standard Edition does not support failover clustering.

Cluster Shared Volumes (CSV) are new to R2 and are to be used exclusively for the Hyper-V role. They provide a many-to-many mapping of Hyper-V failover cluster nodes to VHD files and allow multiple host servers to access the same LUN at the same time. Using them is a requirement for live migration. Storing data other than Hyper-V related files (VHDs and XML configuration files) is not supported and Microsoft warns against this practice.

A CSV is a special type of SAN volume that allows the consolidation of many LUNs hosting VMs in to a single LUN. It takes the smallest level of ownership of an item from the disk object to the file. Therefore, many VHD files can reside on a single disk, and that disk can be shared among many owners (with similar architectures). Figure 47 shows the relationship between disks and VHD files in R1, while figure 48 shows the relationship in R2. R2 not only makes better use of storage space, it simplifies management and enables the owner of a VHD file to be dynamically switched at a moment's notice. This last feature means that CSV's are necessary for live migration between hosts.

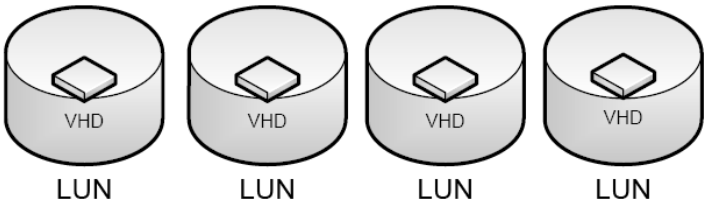


Figure 47: Pre-R2 VHD Storage

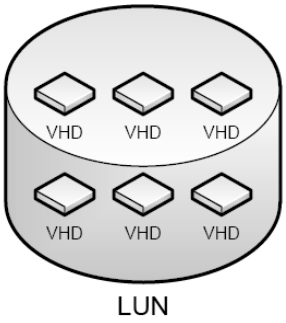


Figure 48: R2 VHD Storage with Cluster Shared Volumes

	Non-CSV	CSV
VHD Expansion	LUN can run out of storage if the VHD gets too large	VHDs can grow as needed
Free Space	Wasted	Can be used by other VHDs
Smallest level of node ownership	LUN	VHD
Management	Complex: Many LUNs used	Simple: Only one LUN for all VHDs
Migration	Quick	Quick or Live
Dynamic I/O Redirection	No	Yes –failure of a Failover Cluster node will dynamically reassign ownership

Figure 49: CSV vs. Non-CSV Comparison

Configuring Live Migration

The first step in configuring LM is to connect each physical host the shared storage and configure networking between them. On the hosts, install the Hyper-V role and the Failover Clustering feature. After doing this, the Failover Clustering feature can be administered from the Server Manager. The first page of the **Failover Cluster Manager** option has a wizard for configuring a cluster.

You can run the "Create a cluster" wizard from any system running the Failover Cluster role. Clustered systems should be in the same Active Directory domain (see figure 50). In this example, we join physical systems cluster10 and cluster20 to the cluster. You must be a local administrator to manipulate clusters.

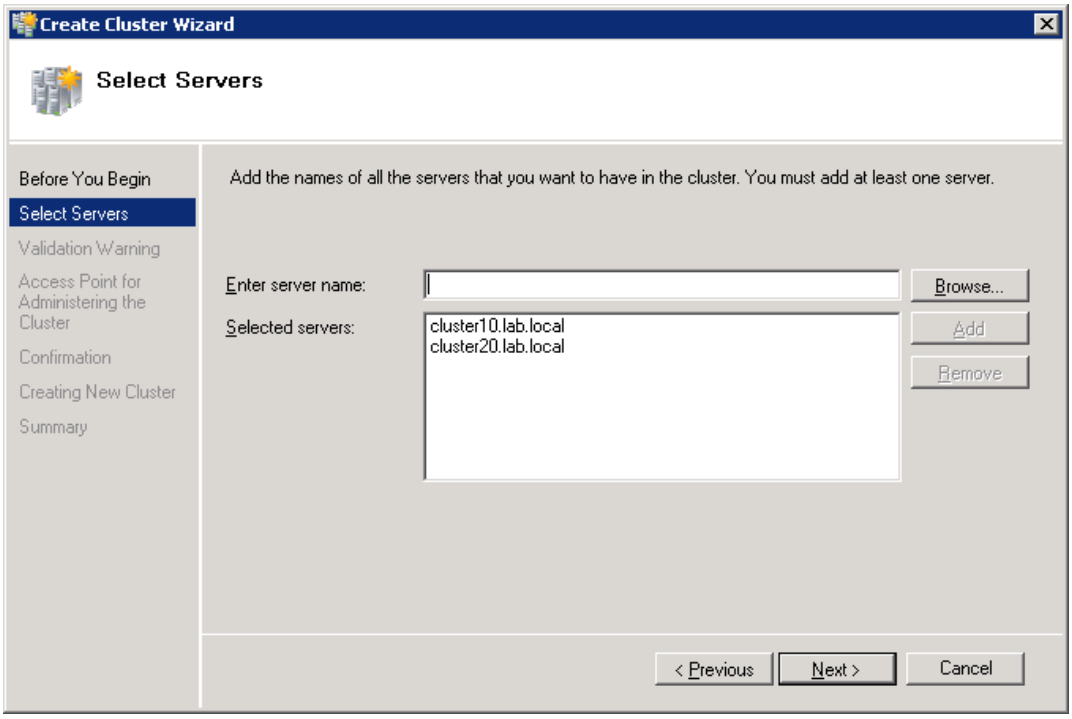


Figure 50: Adding cluster members

Microsoft recommends, but does not require, that a cluster be validated against a series of predetermined tests. When you click Next after configuring which hosts should be included in the cluster, you will be prompted for which tests to include in the analysis. Although you don't have to have your storage configured when you create the cluster, having storage available will allow the storage to be validated against Microsoft's cluster tests. The tests may take some time to run. Since every cluster is different, the output from these Validation tests is not given as an example in this chapter.

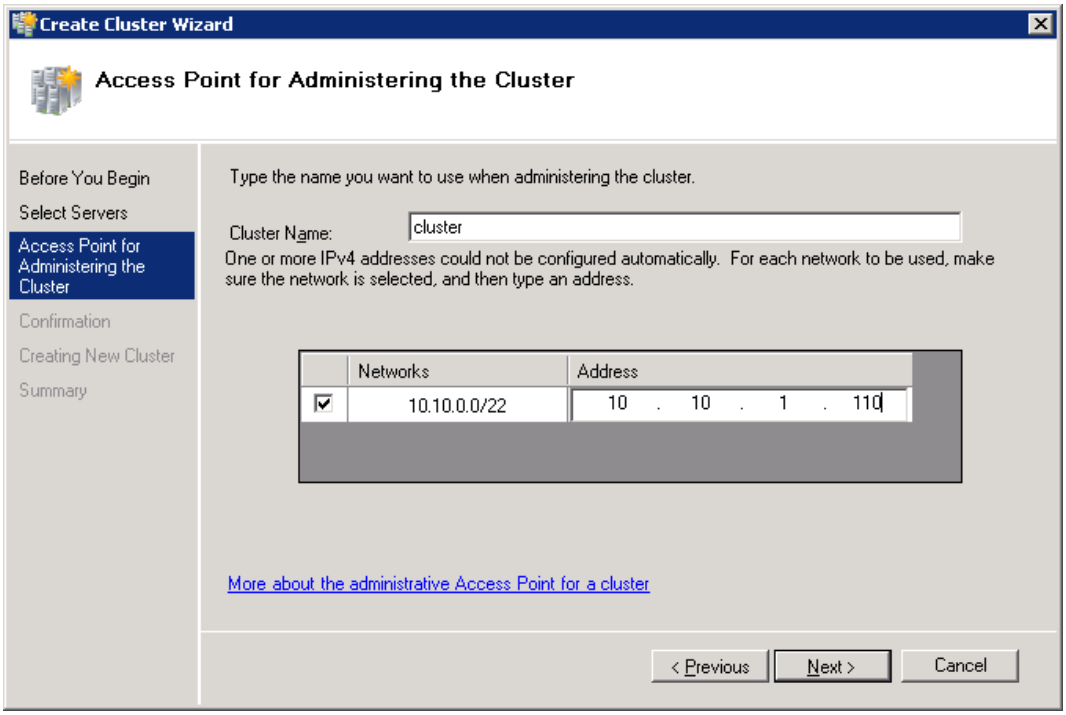


Figure 51: Defining the cluster's main IP address and its name

We have added 2 iSCSI targets using the iSCSI Initiator to each physical host in our cluster. They are a 12 gigabyte disk and a 1.5 gigabyte disk. The 1.5 gigabyte disk will be used for the cluster quorum disk, which is required for the nodes to determine if they can communicate with each other in the event of a network or host failure. The Quorum can be much smaller than the disk where the data is stored. Both the quorum disk and the data disk should be accessible by both hosts.

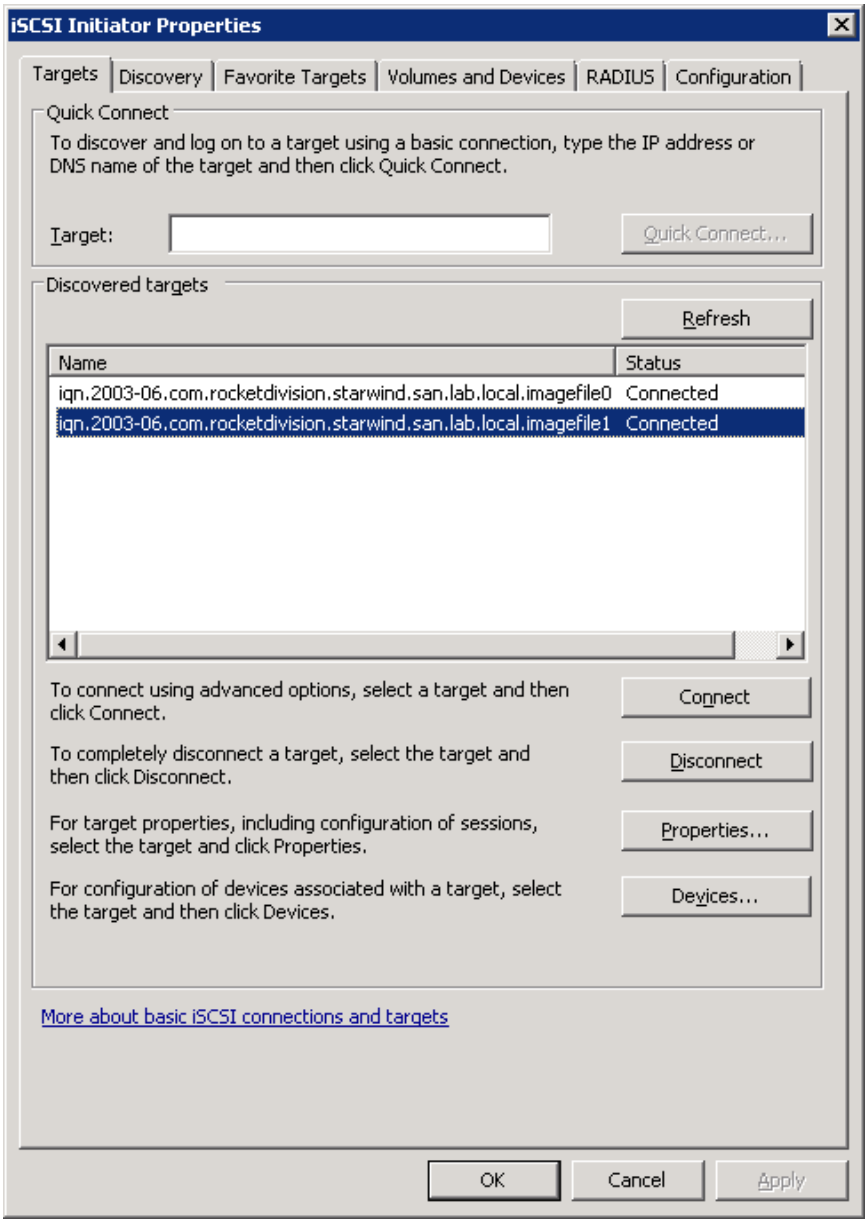


Figure 52: Connect both Data and Quorum drives on both hosts. Initialize and Format the disks, but take them offline in Disk Manager

Using Disk Manager, we can mount the 12 gigabyte data disk and the quorum disk and format each one in NTFS, then unmount them. This can be done from any node with a connection to the storage devices. We have used the same LUN target from both hosts.

Figure 52 shows the next step in the wizard, which asks us to define a point where we can administer the cluster. 10.10.1.110 is created as a virtual IP address and the hostname "cluster" is put in DNS on our AD-Integrated DNS Zones.

The next step is to add storage to the cluster. Do this by clicking the **Enable Cluster Shared Volumes** item. Aside from the warning in Figure 53, you should not receive any output from this command. At this time, Microsoft does not support and does not recommend that any data other than Hyper-V files be placed on a CSV.

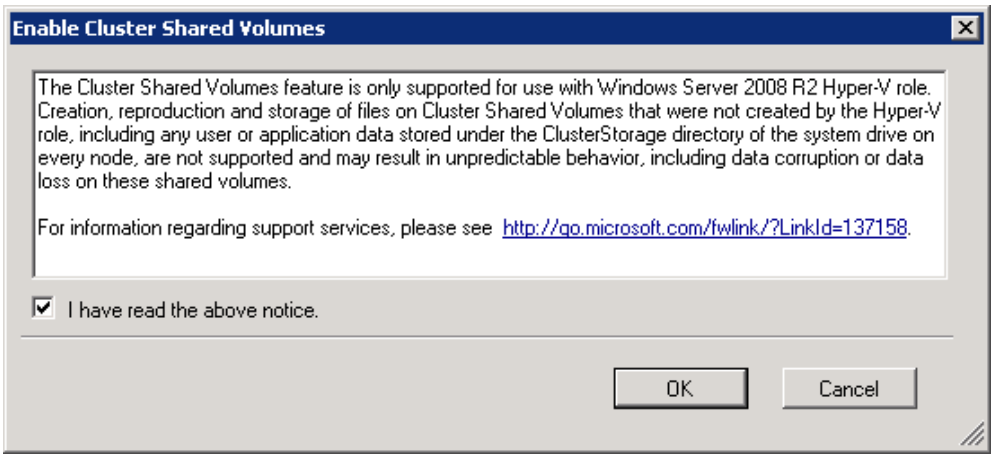


Figure 53: CSVs should only be used with Hyper-V

You should CSV-enable both the data disk and the quorum disk. If the disk is not listed as an option, it might still be online or in use from another host. When you CSV-enable a disk, its mount-point automatically becomes a folder under C:\ClusterStorage (See figure 54). It will be viewable at the same time by both hosts in the cluster in Windows explorer.

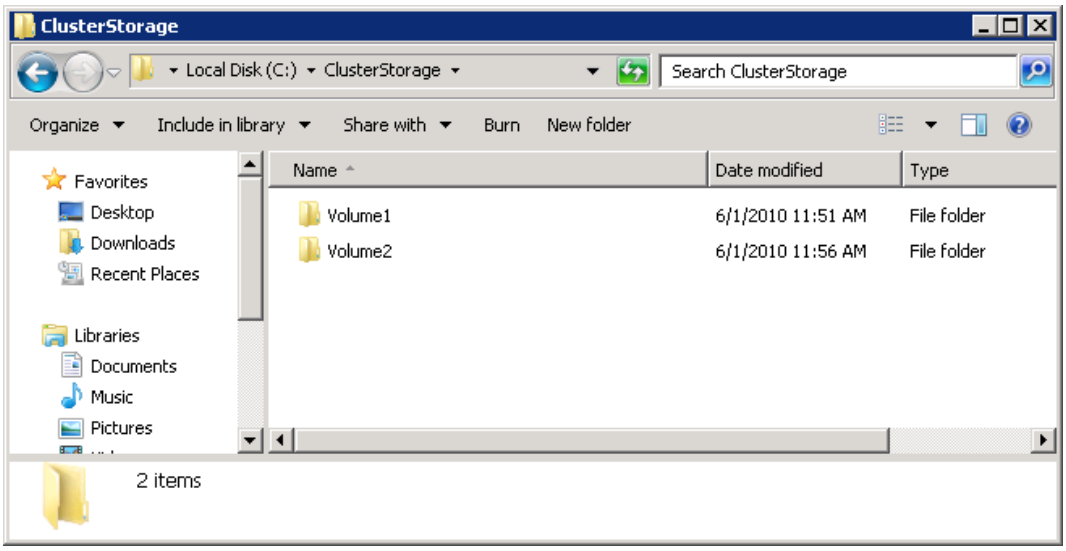


Figure 54: C:\ClusterStorage will contain a mount point for each CSV-enabled disk

After enabling CSVs and adding your partitioned and formatted disks (having them online is not required), right-click the **Services and Applications** object under the cluster and select "Configure a Service or Application". You can then select any existing Virtual Machine. The VM will be copied to the CSV and must be in an off state for this to happen.

After a VM has been "placed" on a cluster host, the VM can be moved between hosts. In this context, "Placed" is not the same as placement through SCVMM, but placement in that a member of the cluster is currently executing the virtual machine. Figure 55 shows a VM called "LM Test1" assigned to the host cluster20. VMs can be managed from any node in the cluster.

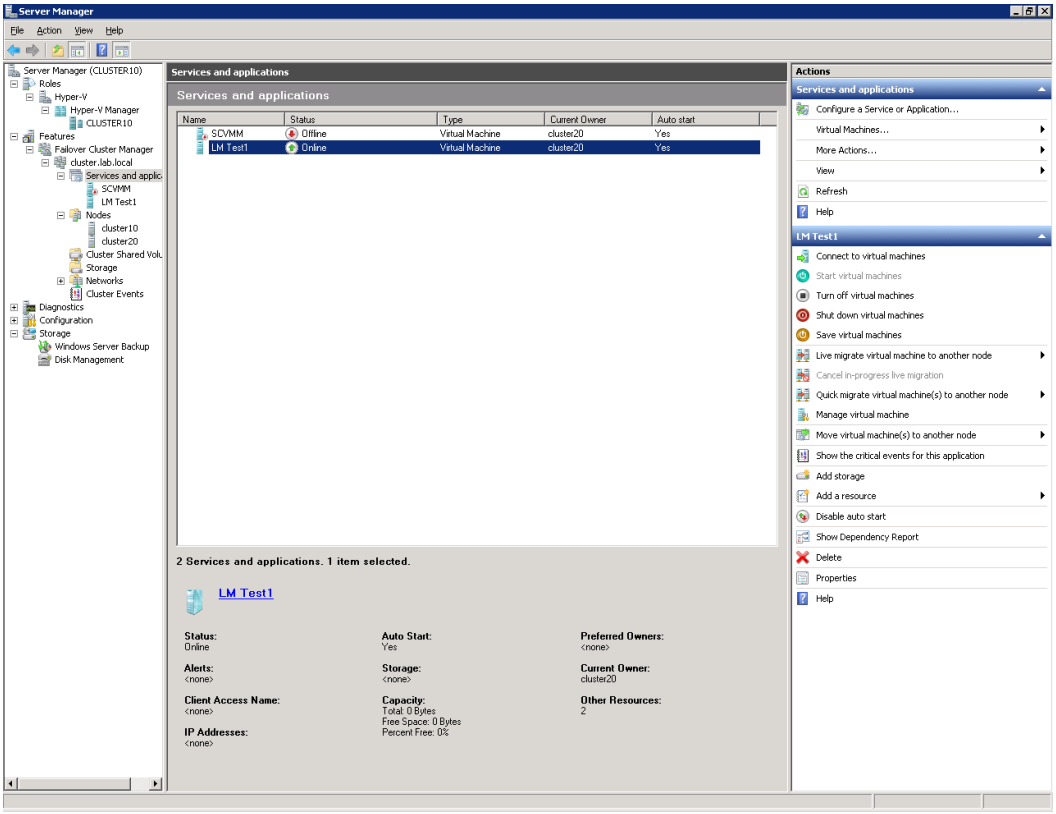


Figure 55: Successfully managing VMs in the Failover Cluster console. By clicking the action pane on the right side, the VM can be live migrated to another host in the cluster.

Figure 56 shows the Action Pane of the failover cluster. Because we have imported Hyper-V resources into Failover Clustering, we have most of the functionality of the Hyper-V administration console built-in to the Failover Cluster Snap-In.

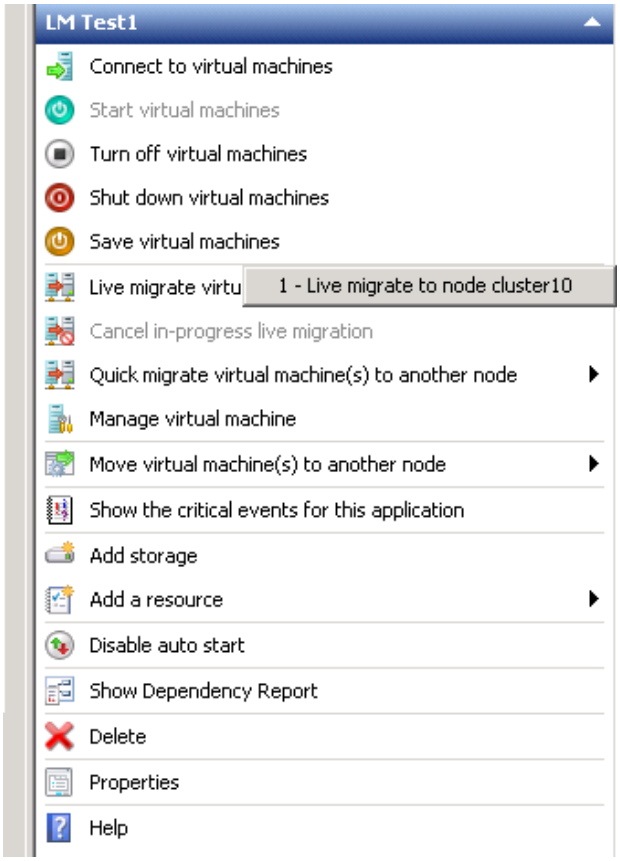


Figure 56: Since the host cluster20 is the current owner of the VM called LM Test1, we can migrate it to cluster10.

When a live migration is in progress, its status will be shown in the console (Figure 57). In-progress migrations can be cancelled if necessary.

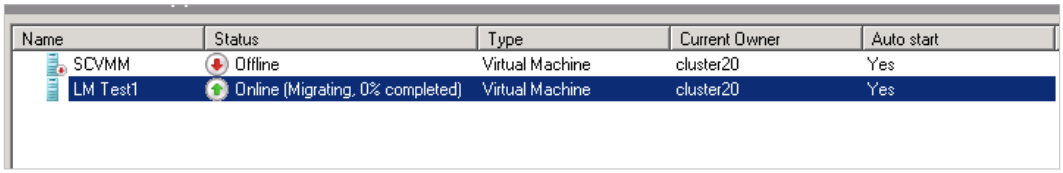


Figure 57: Live Migration of a VM in action. During this process, memory pages are copied one by one to the new owner host. When the copies are synchronized, ownership is transferred and the target host takes over control of the file on the CSV.

Chapter 11: Installing & Configuring Remote Desktop Components

Introduction

Remote Desktop Services (RDS) is Microsoft's "Presentation Virtualization" component. With RDS, applications can be abstracted from a PC and "virtualized" to be hosted on a network-based server. In previous versions of windows, this is known as Terminal Services (TS). The name change reflects the fact that the technology behind TS is now an integral part of Microsoft's virtualization strategy. In addition to this, 2008 R2 allows administrators to create a Virtual Desktop Infrastructure (VDI) – which are virtual machines run by Hyper-V, delivered by RDS, and integrated with objects in Active Directory. The 70-659 exam covers the basics of RDS and the various roles, while the 70-669: Windows Server 2008 R2 Desktop Virtualization exam covers VDIs in more depth. Both exams are required as part of the MCITP: Virtualization Administrator certification.

Remote Desktop Session Host

For 70-659, all relevant roles can be implemented in Hyper-V or another virtualization environment, so only 1 server is required for studying. However, the Remote Desktop Virtualization Host, used in VDI, requires Hyper-V installed and therefore can't run in a virtual machine. The more advanced configuration of these roles is also reserved for another exam.

Installing Remote Desktop Session Host (RDSH) is as simple as following the wizard after clicking **Add Roles** in the Server Manager. The option we want for RDS is labeled "Remote Desktop Services". There are some caveats you should consider when designing your infrastructure. First, a RDSH should never be placed on a domain controller. Since the RDSH is the component that runs the users' programs, you want them to be separate from your DCs. Another RDSH caveat is that during implementation, installing RDSH should be the first step on a server. Install RDSH before installing any of the applications that you want your end users to use. This helps ensure application compatibility. An RDSH installation has no pre-requisites to run other than being joined to the domain.

A major difference between Terminal-Services era remote desktops and the current RDS model is the addition of Network Level Authentication (NLA). NLA asks for a login before the standard login screen is sent to the client. This helps reduce Denial of Service attacks where an attacker could potentially open a huge number of RDS sessions and never actually log in, but overload the server. NLA is built in to Windows Vista and higher computers. Right-clicking on the top icon (in the menu bar) of the Remote Desktop Connection application (found in the start menu) and clicking **About** on your client will tell you if NLA is supported or not (Figure 58).

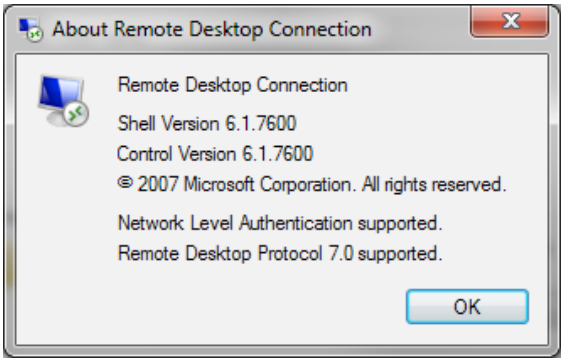


Figure 58: NLA is supported in Windows Vista and higher

On your Windows desktop, the main tool to connect to RDS is the "Remote Desktop Connection" application. It can be found in the start menu of XP and greater, and can be executed as "mstsc.exe" from **Start > Run**. The configuration of remote desktop sessions on the client side can be saved as .RDP files. By default, Windows saves your preferences in a hidden file called **Default.rdp** in My Documents.

By default, RDP, the protocol that RDS uses, runs on TCP port 3389. When you enable remote desktop or RDS on a workstation or server, the Windows Firewall will automatically be adjusted to allow incoming TCP connections on port 3389. If you are having trouble connecting to your RDS, there may be a problem with a firewall.

During the Role install wizard, RDS can be configured to reject connections from older versions of Windows (Figure 59). It is important that if you are running systems older than Vista, you should not require NLA.

The wizard will also ask you what type of CALs you will use. A CAL is a Client Access License and permits a user to use to RDS. CALs will be discussed in this chapter in the "RDS Licensing" section.

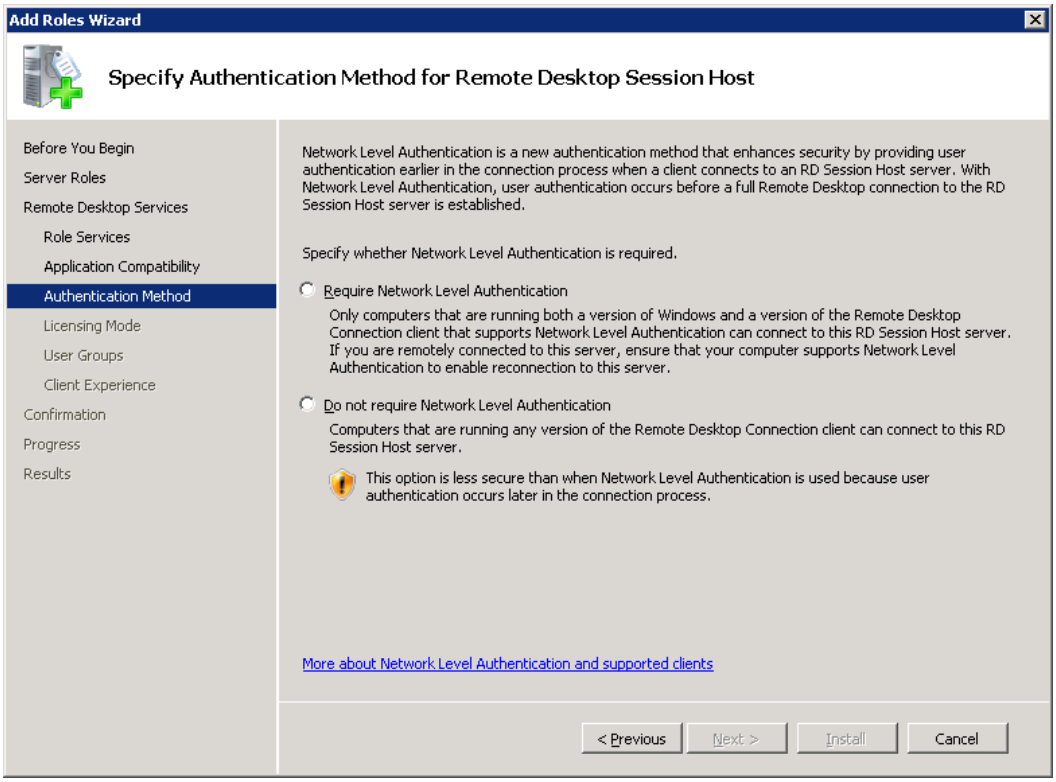


Figure 59: Requiring NLA can help secure your RDS environment, but should be planned carefully.

The Wizard will prompt you to configure the Client Experience. You can permit bidirectional audio between the client and the RDS server, but it will require more resources. You can also enable Windows Aero for a more familiar graphical experience, at the expense of bandwidth.

After installation and rebooting completes, you should have 3 new management tools under Roles in the Server Manager:

- RemoteApp Manager – Used to configure how applications are delivered via RemoteApp. RemoteApp is a way of sending applications to users where they only receive the application, not the entire remote desktop.
- RD Session Host Configuration – This is where the main Session Host subrole configuration is.
- Remote Desktop Services Manager – Used to terminate users sessions and remote control their session for assistance. This is used if clients need administrator assistance, forgets to log off, or has an application hang. Also allows you to keep an eye on who is logged in without sorting through the Event Log.
- The bulk of the configuration for the RDSH is done by right-clicking the **Connections** object with the **RD Session Host Configuration** item highlighted and selecting **Properties**.

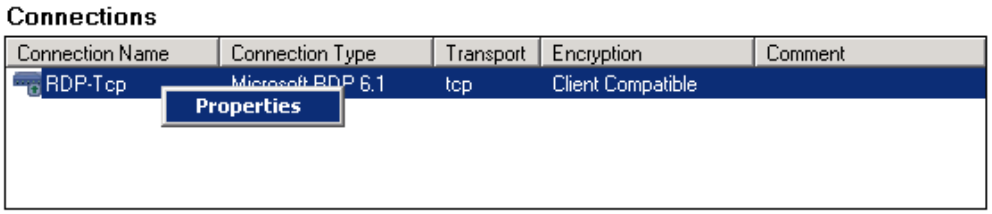


Figure 60: The configuration menu for RDSH is in an unintuitive location.

RDSH is configured by Connections. New connections can be created by following the wizard provided by **Create New Connections** under the **Actions** panel. The selections made for the "baseline" RDP connection are simple, but can be tweaked by accessing the **Properties** dialog box.

It is important to note that all data exchanged over RDP between a server and client is encrypted. The encryption can be selected from the Properties of the RDSH's connection. If set to Client Compatible (the default), the server will select the highest level of encryption that the client supports. If set to High, then clients that don't meet the server's standards will be dropped. High Encryption uses 128-bit encryption, while Low uses 56-bit encryption. This is SSL encryption. FIPS compliant encryption will use whatever settings you have specified as an encryption set in group policy. The use of encryption not only secures your connection, but in a remote-teleworker or branch office setting, it eliminates the need for a VPN.

When a user connects to RDS, RDS determines what should be shared between the server and the guest. Microsoft calls this "Resource Redirection". By default, the server will allow any devices the client requests to be redirected to the server. This allows a user to have access to their printer or audio devices inside an RDS session. Items can be disabled in the Client Settings tab of the server connection's properties. You may choose to do this for security. For example, it could be used to prevent a user from redirecting their own C: drive to a RD session, which could be a vector for malware propagation or transferring confidential company files to their disk. Understanding Resource Redirection is part of the 70-659 requirements, so it would be a good idea to test some of these in your own lab. The screen for configuring Resource Redirection is given in Figure 61.

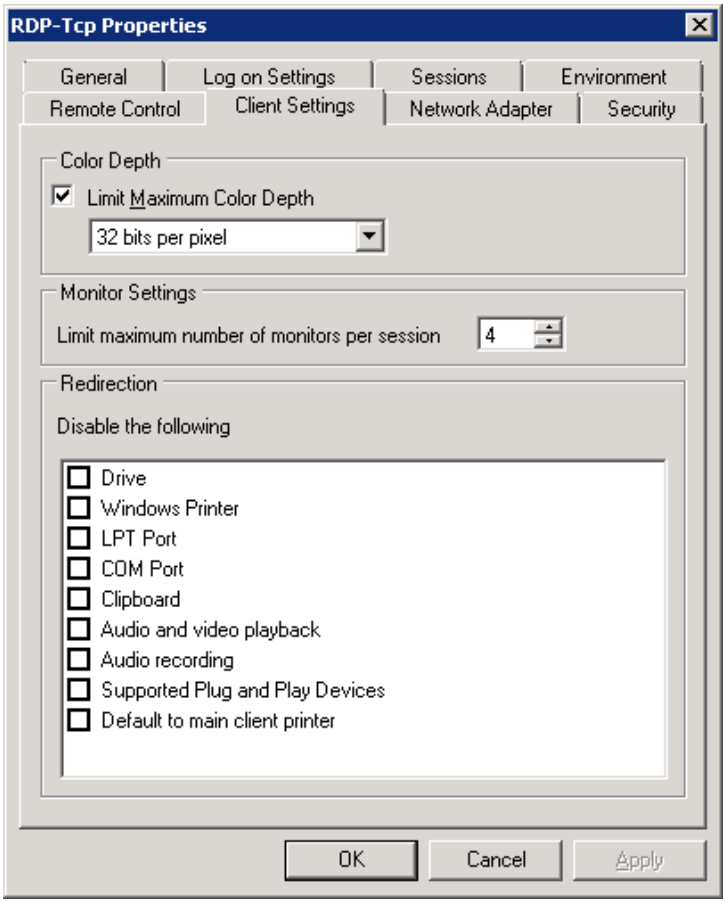


Figure 61: A User's local device can be used in the remote session through Resource Redirection

On the client side, Resource Redirection must be configured. An example of this is given in Figure 62. Also in the Properties for the RDSH connection in the figure above, you can specify the maximum number of monitors the client can use. This feature is new to R2 and requires Windows 7. The maximum number of monitors can be specified by the server or by group policy applied to the client.

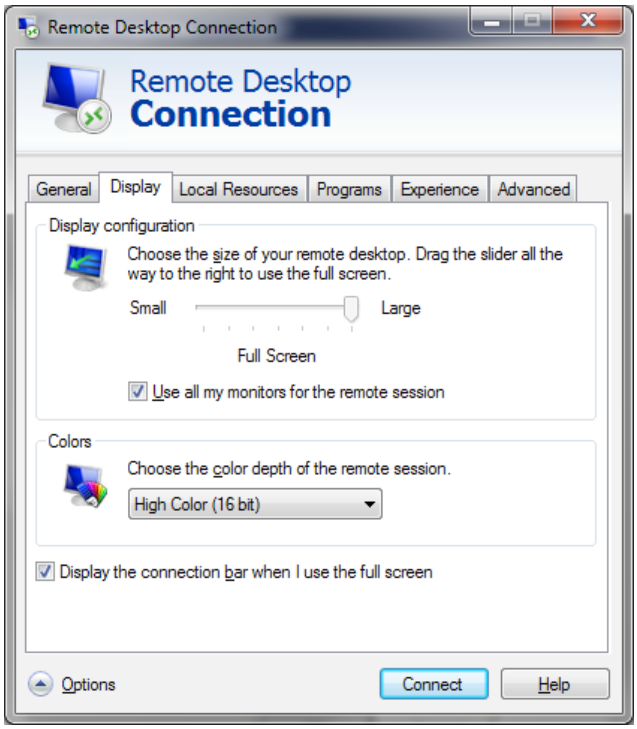


Figure 62: Enabling multiple monitors from the client perspective.

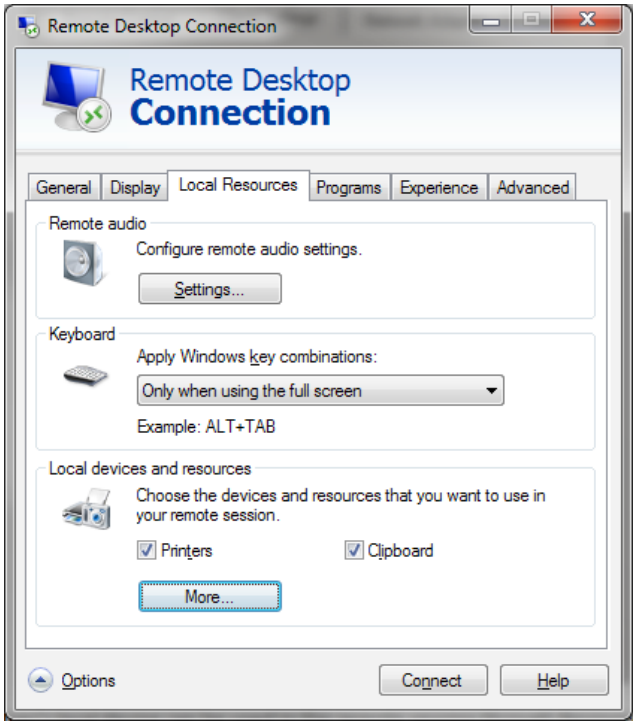
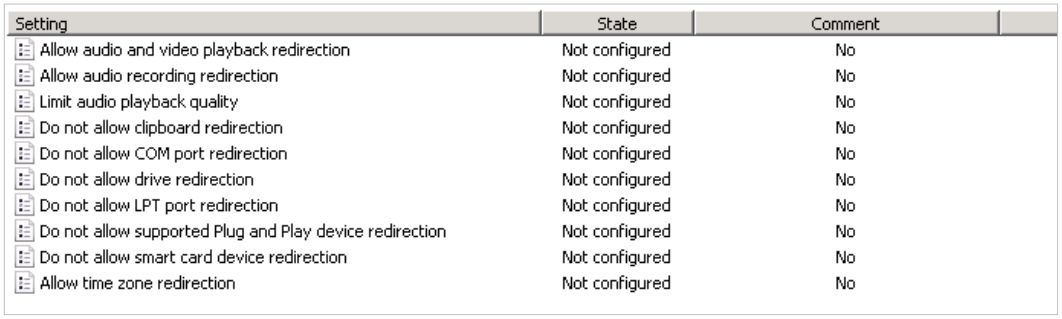


Figure 63: Selecting what local resources your session can utilize.

Closing the properties window brings us back to the main RD Session Host Configuration screen. Below the **Connections** box, the **Edit Settings** box gives values that are changeable. Unlike many of the settings from the **Properties** window, these are server-wide settings.

By clicking the top option under general, RDS allows you to limit each user to a single session. This is so a user doesn't inadvertently create conflicting sessions or use too many server resources. By default, user profiles will be cleaned up when a user disconnects from a terminal server.

There are also a number of settings that can be changed by Group Policy. On R2, the path to the Group Policy configurations related to RDS is at "Policies/Administrative Templates/Windows Components/Remote Desktop Services". RDS can be modified on a User or Computer basis, and can be modified for either the server or the client. Time zone redirection, a setting not found in the RDS Management Tools, can be enabled or disabled. Time zone redirection enables the client to send time zone data to the server. You may do this so the timestamps of file access times make sense to the user.



Setting	State	Comment
Allow audio and video playback redirection	Not configured	No
Allow audio recording redirection	Not configured	No
Limit audio playback quality	Not configured	No
Do not allow clipboard redirection	Not configured	No
Do not allow COM port redirection	Not configured	No
Do not allow drive redirection	Not configured	No
Do not allow LPT port redirection	Not configured	No
Do not allow supported Plug and Play device redirection	Not configured	No
Do not allow smart card device redirection	Not configured	No
Allow time zone redirection	Not configured	No

Figure 64: Server 2008 R2 provides a rich set of Group Policies, including some settings not found in the management tools.

Since the RDSH role is the heart of RDS, installing the RDSH role also installs the Licensing Diagnosis tool, accessible from the Server Manager. The Licensing Diagnosis helps you determine if the actual RDS configuration meets the one you've created by purchasing CALs, or Client Access Licenses. Since we haven't set up the RDS Licensing role yet, we are not compliant, as illustrated in Figure 65. The licensing server can be defined by pointing to it by name or IP in the **RD Session Host Configuration** window, which is accessed by double-clicking the Licensing options under **Edit Settings**. RDS Licensing can also be configured by group policy. With group policy you can tell a server farm to use a specific license server and specify the CAL type (user or device).

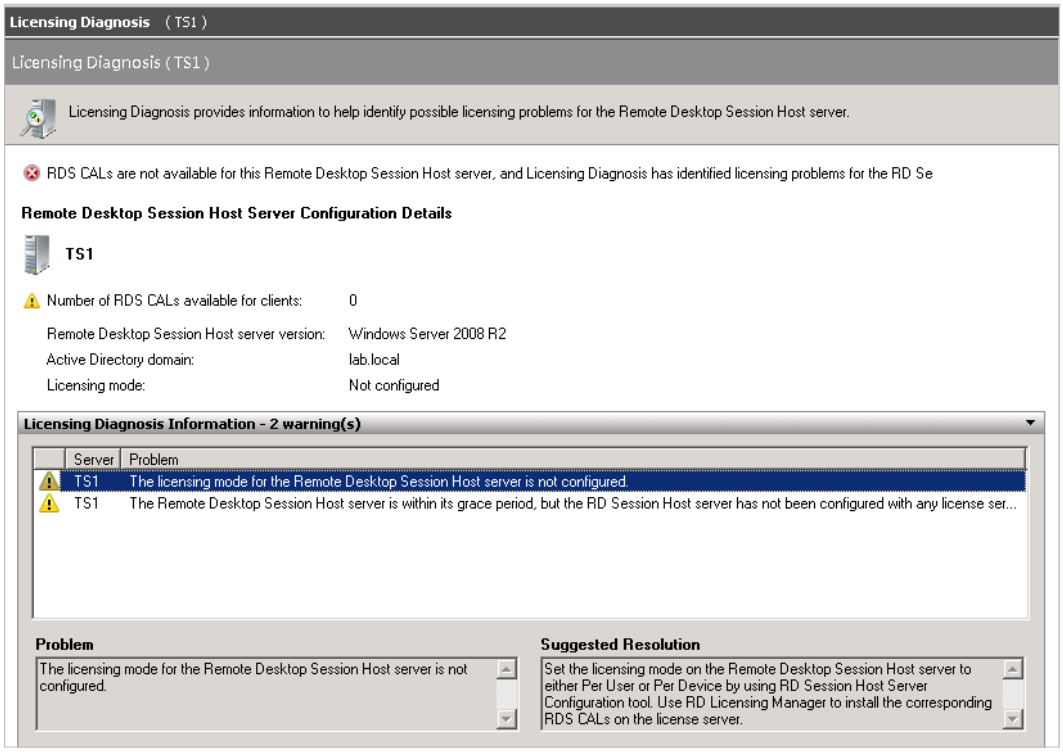


Figure 65: The Licensing Diagnosis server suggesting that we configure licenses for RDSH.

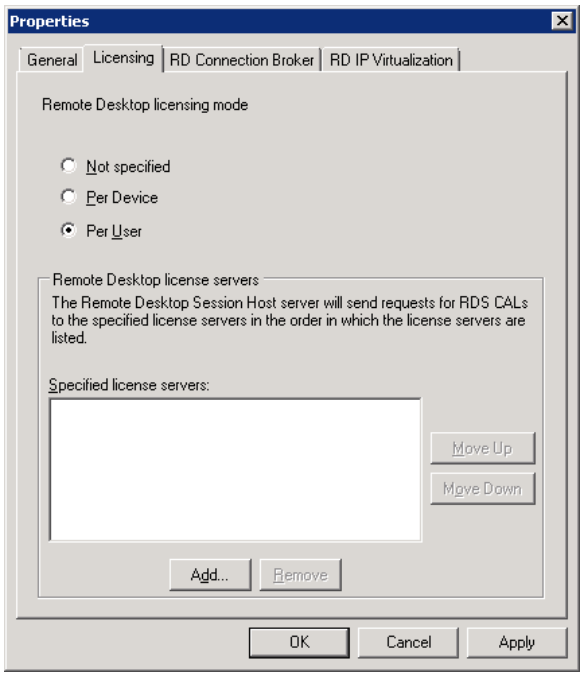


Figure 66: A license server is specified by double-clicking the server's Licensing Settings.

RD Licensing
Although RDS enables potentially thousands of users to receive interaction with applications over the network, it is not free. RDS Licensing is required for remote desktop connections to RDS servers. To connect to regular servers and clients (non RDS servers), licensing is not necessary.

By default, RDS will allow a 120-day grace period before the RDS Role becomes unusable on that system. The good news about this is that you can use an RDS lab at home to pass the 70-659 exam. The bad news is that in a production environment, you have to manage RDS licensing within 120 days of your deployment. As a best practice, you should have your licensing determined before deployment, but that is not always possible in the development lifecycle. For instance, you may need to deploy a prototype RDS to determine how well presentation virtualization fits your business requirements, how well hardware performs, or if applications will be compatible.

Rather than specifying a key on each server, licensing for RDS is handled by a server role that gives out Client Access Licenses (CALs) from a pool to the RDS servers that the users are connecting to. This makes deployment of a farm of remote desktop servers much easier, since the licensing server can be defined by group policy.

RD licensing requires installation of the RD License sub-role. This can be done from the Server Manager. The installation for RD Licensing will ask you to configure the scope – either none, workgroup, domain, or forest. In the context of RDS, a RDSH and RD License Server can automatically find each other if they are in the same scope. If you specify **none**, then you will have to manually define the name or IP of the licensing server in RDSH or in group policy. The installer also allows you to specify where the RD License database is kept. By default, it is stored in a subfolder under the windows directory. Installing the License Manager puts a new item in the Administrative Tools menu called "RD License Manager".

The majority of RD License Manager configuration is done by right-clicking the specific licensing server in the MMC snap-in. Before an RDSH host can utilize a CAL, the licensing server must be activated. The activation process issues a certificate to the server from Microsoft and automatically begins the Install Licenses wizard upon completion. After successfully completing the wizard, the RD Licensing Manager populates with more information and becomes more interesting. Figure 67 shows a successfully installed licensing manager screen.

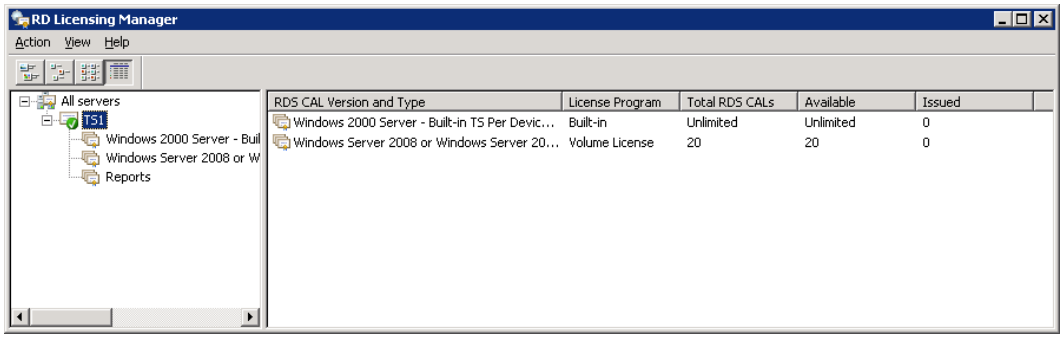


Figure 67: The view of TS1 after adding 20 device CALs

The context menu after clicking on the server gives us options who are self-explanatory, but listed in the 70-659 exam objectives (Figure 68). Mainly, these are "Reactivate Server" and "Deactivate Server", and "Install Licenses" and "Create Reports". The exam objectives also list configuring the revocation of CALs. This option is not available in the context menu, but appears only in the Action menu.

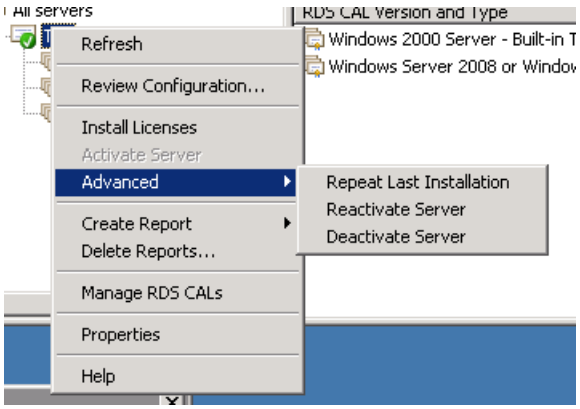


Figure 68: Management of RDS Licenses

RD Connection Broker

RD Connection Broker (RDCB) load balances clients across RDSH operating in an RDSH server farm. If virtual desktops (VDI) are being used, RDCB will delegate how they are deployed. RDCB's final task is to balance RemoteApp programs. RDCB's role in Microsoft's virtualization vision is to unify virtual desktops and virtual applications.

Installing the RDCB is done using the Server Manager. There are no initial configuration options in the Wizard. RDCB doesn't actually provide any way of accessing an application via RDP. For that, it must be tied to a RD Web Access server. Configuring RDCB is fairly straight forward. The main screen for the Remote Desktop Connection Manager MMC, will allow you add a RemoteApp or VDI Source.

As stated, the Connection Broker provides balanced workloads to farms of Session Hosts. To make a Session Host a member of a farm instead of a standalone server access the Properties of the RD Session Host Configuration in MMC (Figure 69).

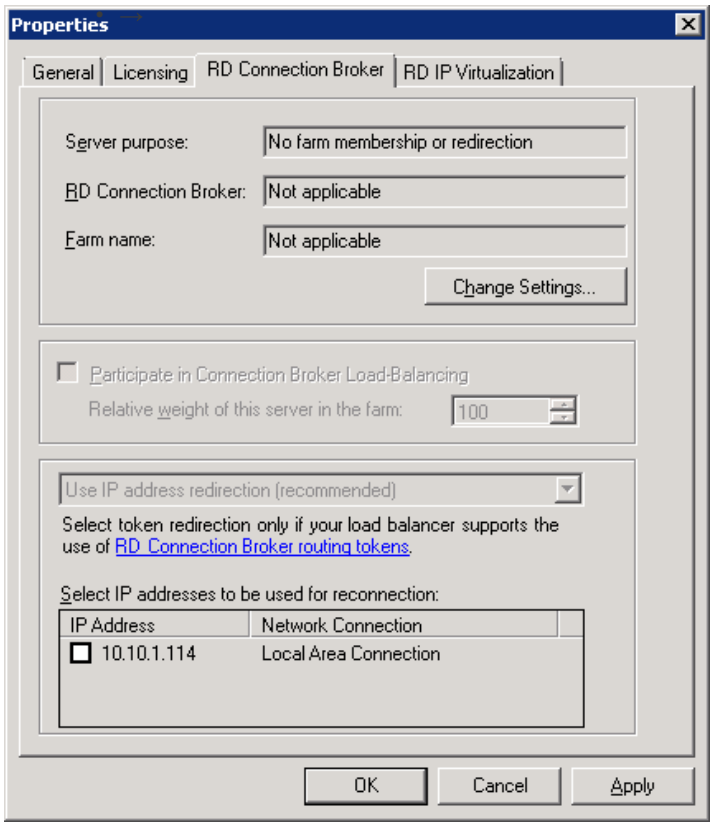


Figure 69: Use the RD Session Host properties to manage a server farm

Microsoft recommends that multiple RDCB servers be used with DNS Round Robin. DNS Round Robin replies to DNS queries for a name with a value from a pool of IP addresses instead of a single IP address.

Finally, one of the exam objectives is to configure RDCB to integrate with the Virtualization Host role, which is one step you would take when beginning to implement VDI. Connecting a RDCB to a Virtualization Host is a matter of defining which RDVH you want to connect to. In the Remote Desktop Connection Manager MMC snap-in, right-click the optioned **RD Virtualization Host Servers** and select **Add Virtualization Host Server**. You will be prompted for the hostname or IP of a server providing virtual desktop images. This server should be running Hyper-V, The RD Session Host, and the RD Virtualization Host. This is the physical server you are using as a backend to your virtual desktops. It must be a physical server, because the Hyper-V role cannot be installed or used inside a Hyper-V guest.

To confirm that the RD Connection Broker has connected to the Virtual Desktop Hyper-V server, the RD Virtualization Host Server should be listed with the appropriate number of virtual machines.

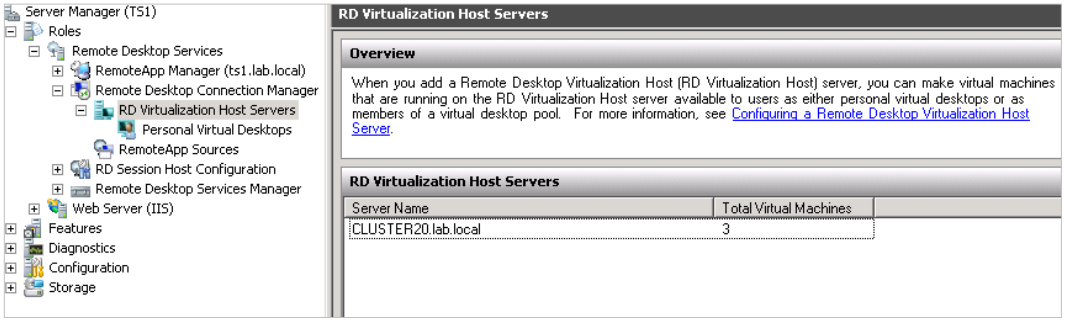


Figure 70: VDI Front-end configuration

We now have "dial tone" between the Connection Broker and the Virtualization Host. The business of deploying virtual desktops can begin. That configuration is part of another exam.

RD Gateway

Although RDS has many benefits, it can also become constricting when the users have the freedom to around. Since the users no longer have the application running on their desktop or laptop system, they need to have a network available to connect to RDS. Traditionally, this meant that the administrator would determine which ports the application ran on and "poke holes" in the firewall. It also meant that users may have to connect to the corporate network using a VPN, which can be complex to configure and maintain for a large number of mobile users. Mobile users can also introduce security vulnerabilities into a network. Microsoft has realized these roadblocks to virtualizing presentation and has built the RD Gateway role service as a solution.

RD Gateway provides a secure front-end to RD Session Hosts. The RD Gateway sits at the edge of the corporate network in the DMZ, and acts as a proxy between the RD Session servers inside the corporate network, and the client on the outside of the corporate network. RD Gateway tunnels RDP through HTTPS (TCP Port 443) and it also goes further by assessing the health of a client using Network Access Protection (NAP), which is another Role provided with Server 2008. NAP creates a posture of the client called a Windows Security Health Validator based on criteria like:

- Is there antivirus software installed? If so, is it up to date and functional?
- Has it been an antivirus scan in the last **x** days?
- Is Windows up to date with the latest updates?
- Are there any updates our corporate policy insists the client must have?
- Is a firewall enabled for all network connections?

The RD Gateway uses a Network Policy Server to a snapshot of the security settings detected on a client and either approve or deny the client's request to connect to applications or remote desktops. If a user does not meet the security requirements, the NPS can offer automatic remediation steps to reach compliance. Only systems running Windows 7, Vista, or XP SP3 can gain access through an RD Gateway when NAP is enforced.

RD Gateway is composed of two major components: the RD CAP and the RD RAP. The RD CAP is short for RD Connection Authorization Policy and it defines who can connect. The RD RAP stands for Resource Authorization Policy and defines what can be accessed.

As always, installing the RD Gateway role service is done in the server manager. The RD Gateway role service requires more configuration than other roles. First, you must select a security certificate that will be used for SSL. Like a web server, you can either use a self-signed certificate (for smaller installations) or a certificate issued by a Certification Authority. The goal of this process is for the client and server to agree that they are who they say they are.

The Installer then provides the opportunity to create RD CAP (Figure 71) and RD RAP (Figure 73) groups. They can also be added later.

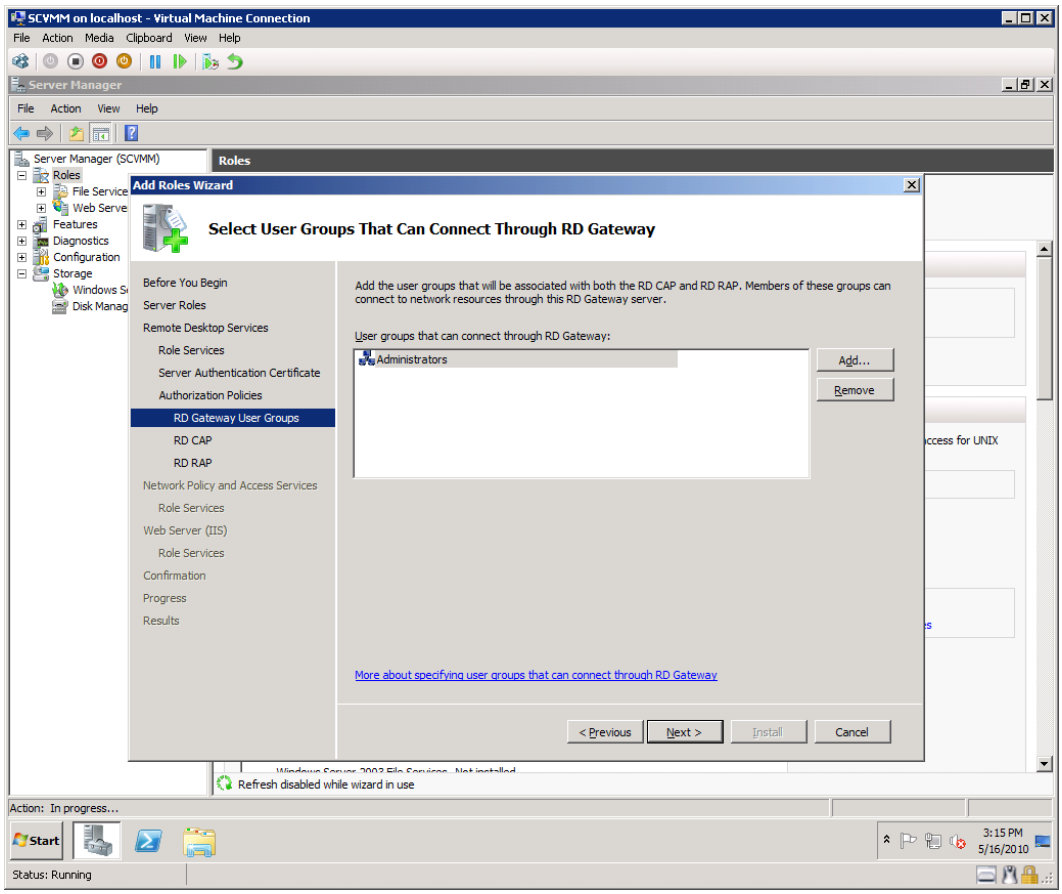


Figure 71: Selecting Users for an RD CAP

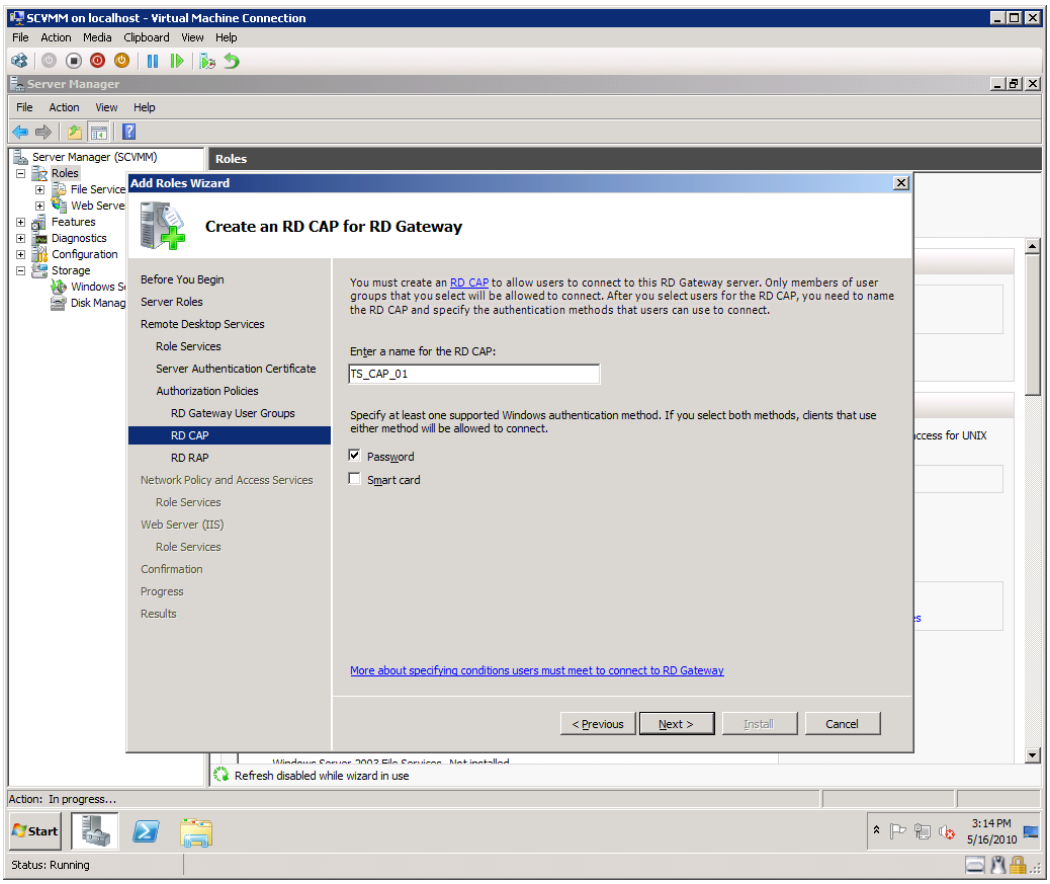


Figure 72: Finalizing the RD CAP

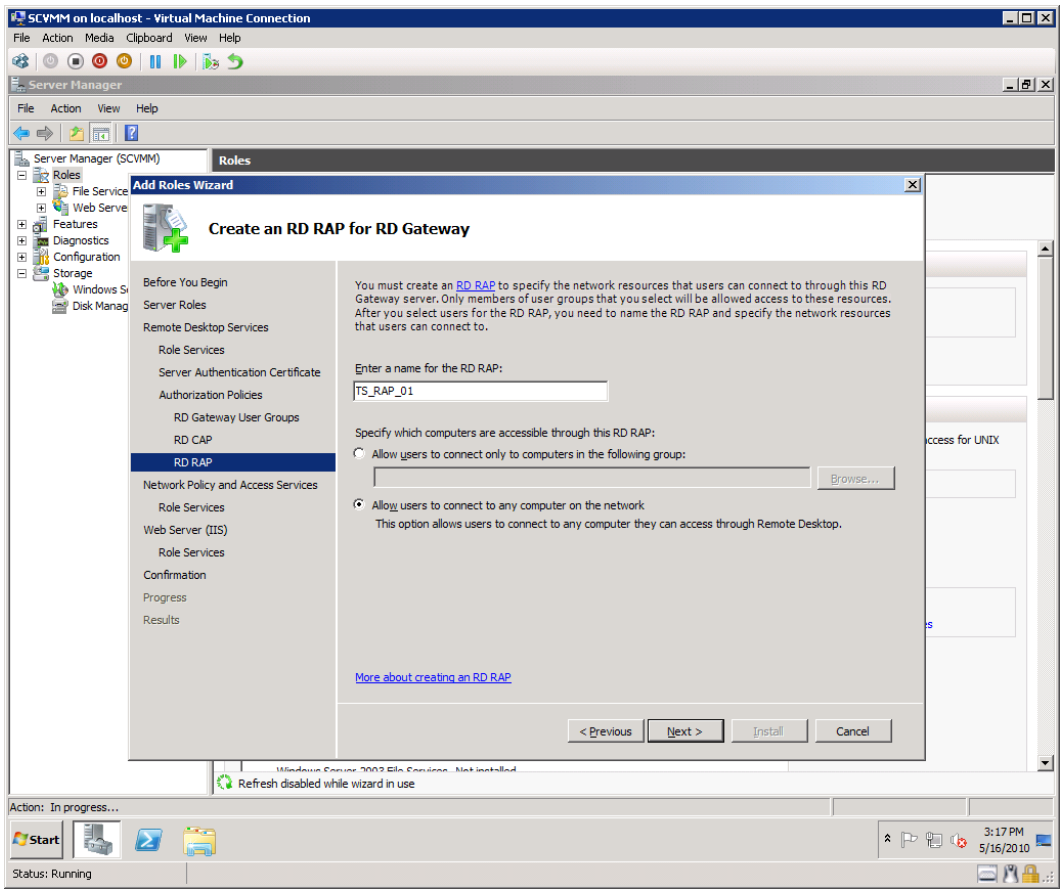


Figure 73: The RD RAP Configuration screen

Unless you are allowing All Users to connect to All Computers, configuring your RD RAP and RD CAP mappings will require planning and implementation of these items in Active Directory.

"Nexting" through the wizard completes the requirements for setting up an RD Gateway. By default, the RD Gateway acts as a standard Network Policy Server (NPS). The NPS is a replacement for Internet Authentication Service (IAS) in Windows 2003 and provides services such as RADIUS-based authentication and creation of dial-up connections. You can also choose to configure NAP at this time by installing the Health Registration Authority (HRA) and Health Credential Authorization Protocol. The NPS can be deployed locally or centrally and can either perform health validations, but it doesn't have to.

The RD Gateway Manager should register your server in it. Interacting with the Policies subfolder allows you to specify or revise CAPs and RAPs, while right-clicking the server itself and selecting **Properties** allows you to do things like integrate the server with a NAP (Figure 74).

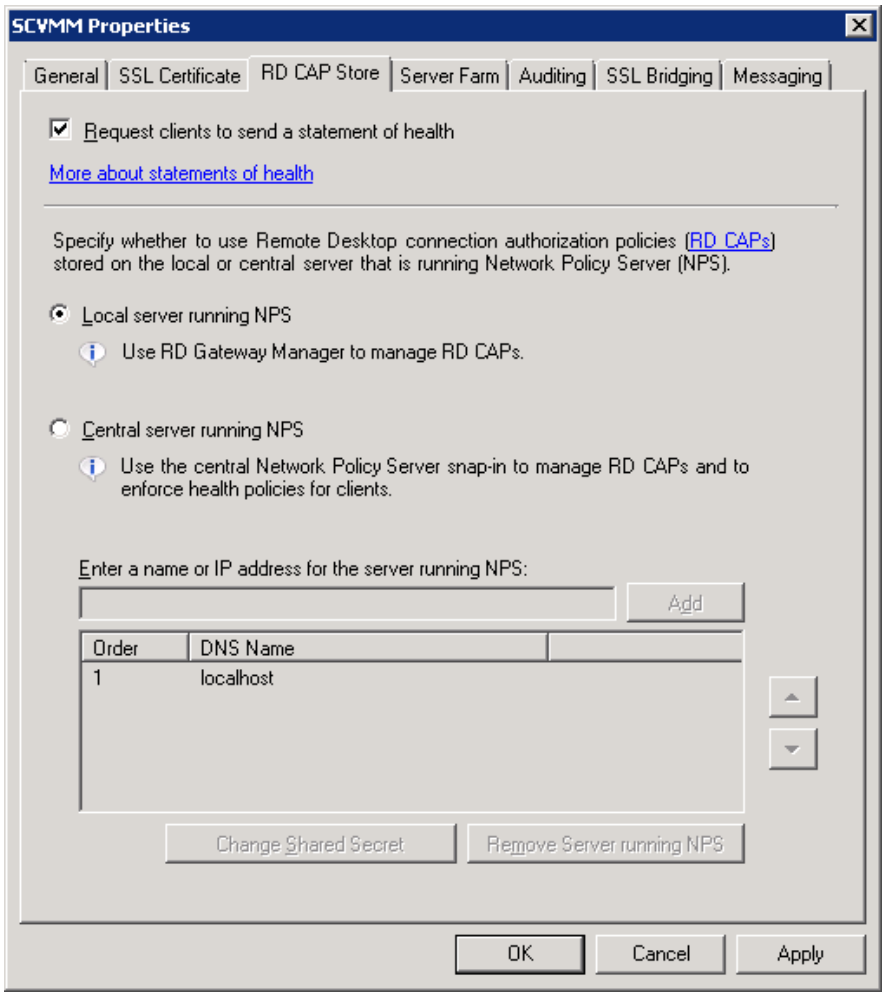


Figure 74: Integrating with a NPS for client posture assessment.

In summary, the purpose of the RD Gateway is to act as a choke-point for security. With only 1 port to open, the RD Gateway is often simpler and more secure to deploy than a typical firewall or VPN. RD CAPs determine who can connect through the gateway, and RD RAPs define what they can connect to. Users are authenticated via the standard Active Directory mechanisms via a Network Policy Server. In addition to validating users, the Network Policy Server can be configured to perform a health assessment on the client PC that is attempting to access inside RD Session Hosts.

RD Web Access

RD Web Access provides a front end to provide RemoteApp programs and VDI to users. It has fewer features than an RD Gateway-based solution, but requires fewer configurations. Installing the RD Web Access role service is done the same as any other of the RDS role services. RDWeb is built off IIS and when you install RDWeb, Server Manager will force you to install the IIS and the appropriate dependencies if you don't already have them installed.

After RDWeb is installed, you can browse to the default location, https://<servername>/RDWeb/. You will be prompted for your domain credentials and asked if the computer you're using is public or private.

After logging in, click the **Configuration** tab to tell RDWeb where it should be getting its sources from. These can either be RDSH servers or RDCB servers, with RDCB being the more flexible choice of the two. A screen shot of the configuration of RDWeb is given below. The RDWeb source configuration options can also be changed by right-clicking the Connection Manager MMC and selecting Properties.

The applications deployed via RD Web Access are the aggregate of applications from each server you list. This is subject, of course, to what the user has access to.

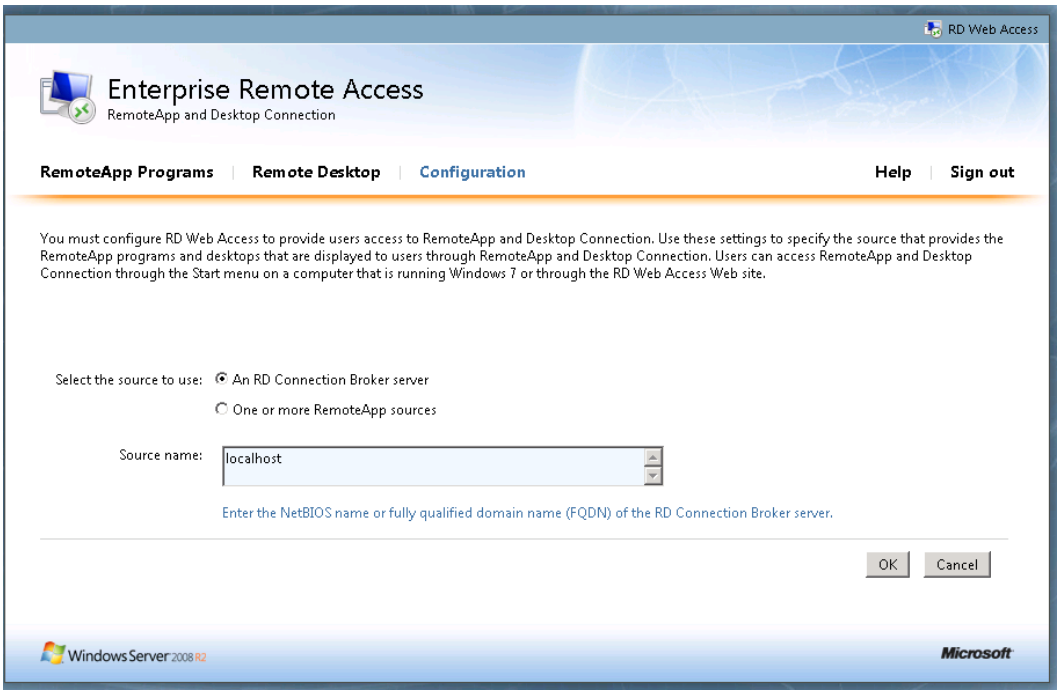


Figure 75: Configuring RDWeb to use a Connection Broker

By default, a RemoteApp program is accessible to all users through RDWeb. You can restrict what programs users can run in RDWeb by right-clicking the application in the RemoteApp Manager and selecting **Properties** (Figure 76).

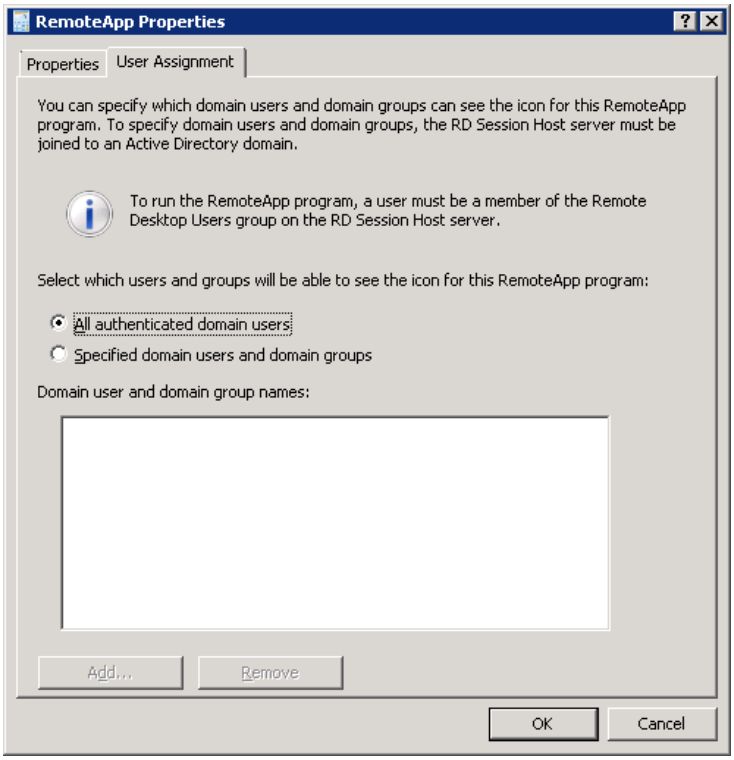


Figure 76: Creating user assignments for RemoteApp programs

In this interface, you can limit specific RemoteApp programs to specific users or groups like you would secure any other resource. The access list resides on the RDSH and is applied by RDWeb. If a RDCB is used, it will be applied by the RDCB instead RDWeb. You can also specify if the application should be available via RDWeb at all (Figure 77).

Figure 77: RemoteApp program filtering

Finally, RDWeb gives the user two options for logging in: either with a public computer or a private computer. The only difference is the amount of idle time RDWeb will wait before terminating the connection. For public users, the default is 20 minutes. For private users, the default is 4 hours. To edit these values, edit RDWeb's web.config file located at **c:\windows\web\rdweb\pages\web.config**. The following lines should be found in the config file, and they can be modified to whatever values you think are appropriate:

```
<!--  Public/Private Mode Timeout for FBA -->
<add key="PublicModeSessionTimeoutInMinutes" value="20" />
<add key="PrivateModeSessionTimeoutInMinutes" value="240" />
```

Practice Questions

Chapter 1

1. You plan to deploy several Windows Server VM guests on Hyper-V hosts. You must be able to support up to 4 virtual processors in each guest VM. What versions of Windows Server could you install as the guest OS? Choose all that apply.

   - ❍ A. Windows Server 2008 R2 Standard
   - ❍ B. Windows Server 2008 R2 Foundation
   - ❍ C. Windows Server 2003 Enterprise with Service Pack 2
   - ❍ D. Windows HPC Server 2008

2. You have a physical server that accesses three devices through COM ports. The server uses COM1, COM2 and COM3 to access these devices. All three devices must be connected to the same server as the application requires direct access to all three devices. You've tested the system and you can access each device individually from within a Hyper-V guest VM. You want to use a Windows Server 2008 R2 Standard Edition server as the Hyper-V host. Will you be able to run this application on a VM and access all three devices and why? Select the best answer.

   - ❍ A. No, because Hyper-V does not support applications that communicate with devices attached to COM ports.
   - ❍ B. No, because Hyper only supports two attached COM port devices.
   - ❍ C. No, because the Standard Edition does not support COM ports.
   - ❍ D. Yes, because Hyper-V VMs can support up to four COM ports.

3. You are configuring Windows Server 2008 R2 Server Core to run Hyper-V. Before you install Hyper-V, you want to join the server to a domain named AHJ.local. The domain administrator account has a password of Try8956. Which one of the following commands will join the server to the desired domain? Select the best answer.

   - ❍ A. Netdom join %computername% /domain:ahj.local /userD:Administrator /password:Try8956
   - ❍ B. Net domain /add /user:administrator /password:Try8956
   - ❍ C. Netdom /add /user:administrator /password:Try8956
   - ❍ D. Add-domain -cred:administrator -pass:password

4. You are configuring three virtual machines (VMs). All three VMs should communicate with nodes on external networks. You want to isolate the three virtual machines from communicating with each other via the virtual host. All three VMs will communicate using the same External virtual network. The nodes on the external network need to be able to communicate with the three VMs. Which one of the following configuration changes should be made? Select the best answer.

   - ❍ A. Configure VLAN IDs for each VM that are different so that they cannot communicate directly through the virtual host
   - ❍ B. Edit the External virtual network's properties to Disallow host-based communications
   - ❍ C. Setup on VM to use an internal virtual network, another VM to use a private virtual network, and the final VM to use the external virtual network
   - ❍ D. Edit each VM's network adapter so that the Force external communications checkbox is checked

5. You are running Hyper-V on a Windows Server 2008 R2 Enterprise Edition server. You will configure VMs on an iSCSI LUN. The LUN will be accessed using a network standard adapter. Client machines will access the virtual machines through the network. The Hyper-V host currently has one network adapter. Seven clients will use wireless connections to the LAN. What should you do to enable the desired configuration? Select the best answer.

   - ❍ A. Create two virtual networks on the network adapter; one for the client access and one for the iSCSI LUN access
   - ❍ B. Install another network adapter for the iSCSI communication
   - ❍ C. Configure a single virtual network to be shared for client access and iSCSI access
   - ❍ D. Install a wireless adapter for client access

Chapter 2

1. You have created a VM on Hyper-V. The VM boots, using pass-through, from an iSCSI LUN. What steps were required to make this happen? Each correct answer provides part of the solution. Choose all that apply

   - ❍ A. Attach the iSCSI LUN to the parent partition on the Hyper-V host.
   - ❍ B. Point the VM to the physical disk, which is the iSCSI LUN, attached to the parent partition.
   - ❍ C. Use the NET USE command to map the LUN to a drive letter.
   - ❍ D. Create a LUN in the shared iSCSI storage container.

2. You are working with VHDs on Windows Server 2008 Hyper-V. You want to compact the disk so that it is resized after removing free space in the disk image. The file format is FAT32. What must you do before you can select to compact the VHD? Select the best answer.

   - ❍ A. Nothing, select compact and let Hyper-V Manager do the work
   - ❍ B. Defragment the disk
   - ❍ C. Use PKZip to compress the VHD file
   - ❍ D. Perform a pre-compact operation with the utility that ships with Virtual Server 2005

3. You want to use a USB printer that is connected to the Hyper-V host within a guest VM. You have installed Integration Services in the guest VM. How can you access the printer from within the VM? Select the best answer.

   - ❍ A. Use the USB printer directly as it will show up as a USB device within the guest VM
   - ❍ B. Share the printer in the parent partition and access the shared printer across the virtual network from within the VM
   - ❍ C. Map an LPT port to the USB port in the VM
   - ❍ D. Map an IP address to the USB port in the VM

4. You want to create a VM template from an existing VM on a Hyper-V host. Currently, 11 users are connected to the VM using a SQL Server database. The option to create a template from the VM is not working. You can start and shutdown this VM from the SCVMM console. What should you do? Select the best answer.

   - ❍ A. Disconnect the users
   - ❍ B. Install the Integration Services in the VM
   - ❍ C. Stop the VM
   - ❍ D. Uninstall Integration Services

5. You are working with the SCVMM Library. You must generate VMs from the Library. Currently, you have the following items in the library for a specific VM template you wish to create:-A source VHD-A guest OS profile-An OS answer file-A hardware profileWhat else is needed to form a complete template? Select the best answer.

   - ❍ A. A template object
   - ❍ B. A WIM image
   - ❍ C. A network profile
   - ❍ D. A Ghost image

Chapter 3

1. You are configuring a server for use as a Hyper-V host. The server will use direct attached storage. You can connect up to four SATA drives in the server hardware configuration you've selected. The server supports RAID configurations. The VMs running on the host will not be mission critical but should perform as quickly as possible when up and running. A few hours of down time is acceptable, but ultimate performance when up is a must. Backups will be performed nightly and the loss of a day's changes is acceptable for all VMs. Which RAID level will you configure for the drives on which the VMs will be stored? Select the best answer.

   - ❍ A. RAID 0
   - ❍ B. RAID 1
   - ❍ C. RAID 5
   - ❍ D. RAID 2

2. You manage two Hyper-V hosts. Each host runs just one VM at this time. Each host is running on identical hardware with the root partitions configured exactly the same on each. The VM on each host is a Windows Server 2008 VM with no additional services running. One VM is not performing as well as the other. What should you check? Select the best answer.

   - ❍ A. Verify that the Integration Services are installed on the poorly performing VM.
   - ❍ B. Verify that the root partition is running the Reliability and Performance Monitor on the poorly performing VM.
   - ❍ C. Verify that the poorly performing VM can communicate with the network.
   - ❍ D. Verify that the Integration Services are installed on the well-performing VM.

3. You have a Hyper-V VM configured on a Windows Server 2008 R2 host. The VM is configured to use 2 processors, an emulated network adapter, 2 GB RAM and a 60 GB VHD for the operating system drive. The VM runs Windows Server 2008 and acts as a file server. The host has a single dual-core processor, 4 GB RAM and 2 TB of storage space. What single change can best improve the performance of this VM? Select the best answer.

   - ❍ A. Change the 2 processors to 4
   - ❍ B. Change the emulated network adapter to a synthetic adapter
   - ❍ C. Change the memory from 2 GB to 4 GB
   - ❍ D. Change the VHD size from 60 GB to 500 GB

4. You are planning a Hyper-V deployment using Windows Server 2008 R2 as the host operating system for all Hyper-V servers. The current Windows domain is a Windows Server 2003 domain running in the Windows 2000 mixed functional level supporting three Windows 2000 domain controllers and one Windows NT 4 domain controller. You want to use AzMan to store authentication and authorization information in Active Directory. What network environment change must be made while incurring the least cost? Select the best answer.

   - ❍ A. The domain must be upgraded to Windows Server 2003 functional level
   - ❍ B. The domain must be upgraded to all Windows Server 2008 or higher DCs
   - ❍ C. The domain must be upgraded to all Windows Server 2008 R2 DCs
   - ❍ D. The domain must be upgraded to Windows 2000 native functional level

Chapter 4

1. You manage snapshots for Hyper-V VMs running on Windows Server 2008 R2. You are searching for the storage location for the snapshots. You have not specified unique locations for snapshots and all default snapshots settings are in place. Windows Server 2008 R2 is installed to the C: drive and the VHD files for the VMs are located on the E: and F: drives. Where are they located? Select the best answer.

   - ❍ A. The snapshot files are located on the E: and F: drives
   - ❍ B. The snapshot files are located on the C: drive
   - ❍ C. The snapshot files are located on the E: drive only
   - ❍ D. The snapshot files are located on the F: drive only

2. When you revert back to a snapshot, what items are reverted in a Hyper-V R2 environment? Choose all that apply.

   - ❍ A. VM memory contents
   - ❍ B. VM running processes
   - ❍ C. Host running processes
   - ❍ D. Physical hardware

3. You are responsible for backups in a Hyper-V virtualization environment. You plan to use the Data Protection Manager. Which one of the following is not a requirement of the Data Protection Manager? Select the best answer.

   - ❍ A. The DPM server must be a member of a Windows Server 2003 or later domain
   - ❍ B. The DPM server must have SP2 installed if running on Windows Server 2003
   - ❍ C. The DPM server must be a member of a Windows Server 2008 or later domain
   - ❍ D. The DPM server must have 2 GB of RAM

4. You have performed a recover of a Hyper-V server by using the following process:1-Reinstall the Windows Server operating system2-Configure all OS settings as they were3-Add the Hyper-V role4-Configure role settings as they were5-Perform a file-based restore of VMsThe VMs are not displayed in the Hyper-V Manager. What action must you take that will require the least amount of time? Select the best answer.

- ❍ A. Redo the restoration from the backup as an Application restore
- ❍ B. You must apply SP2 before you can mount the VMs
- ❍ C. You cannot restore the VMs no; it is impossible
- ❍ D. Add the VMs back to the Hyper-V server using the VHD mount utility

Chapter 5

1. You have a Windows NT 4.0 server used as a file server and it offers no other function. All files shared from the server are available for public access to all users. You want to migrate the Windows NT 4.0 server to a VM. Which one of the following methods will work?
Select the best answer.

- ❍ A. Perform an online conversion with SCVMM
- ❍ B. Use the Convert Windows NT machine feature in the Hyper-V Manager on a Hyper-V host
- ❍ C. Perform an offline conversion with SCVMM
- ❍ D. Use a third-party tool to create an image of the server and then load that image in a VM and install the needed drivers

2. You are placing a VM that is IO intensive. You want Intelligent Placement to give more priority to hosts with faster disk performance. What action should you take? Select the best answer.

- ❍ A. On the Placement Options tab of the Customize Ratings dialog, select the enhance Disk I/O priority option
- ❍ B. On the Placement Options tab of the Customize Ratings dialog, drag the Disk I/O slider to the left
- ❍ C. On the Placement Options tab of the Customize Ratings dialog, deselect the reduce Disk I/O priority option
- ❍ D. On the Placement Options tab of the Customize Ratings dialog, drag the Disk I/O slider to the right

3. You want to install System Center Operations Manager to assist with information gathering in your VM migration projects. Which of the following are prerequisites to using the full feature set of System Center Operations Manager 2007? Choose all that apply.

   ❍ A. SQL Server 2000 or later

   ❍ B. Microsoft .NET Framework 2.0 or higher

   ❍ C. MSXML 6.0

   ❍ D. PowerShell

4. You have converted a XenServer VM for use in Hyper-V. The VM will not boot on the Hyper-V host. Which one of the following is a likely cause of the problem? Select the best answer.

   ❍ A. XenServer VMs cannot be converted to Hyper-V

   ❍ B. The XenServer paravirtualized drivers were removed before conversion

   ❍ C. The XenServer emulation option is not enabled

   ❍ D. The new Hyper-V VM has an IDE hard disk configured

5. You have exported a VM from a Hyper-V host to a location on the SAN. You want to import that VM into another host, but you want to run it from a different location than the export location. What action should you take? Select the best answer.

   ❍ A. Copy the contents of the export folded to the desired location before importing the VM

   ❍ B. Import the VM and indicate a new location during the import

   ❍ C. Use the Exported VM Relocation wizard

   ❍ D. Import the VM and select No when asked to run the VM from the current location

Chapter 6

1. You want to ensure that Network Level Authentication is required for all connections to a RDSH server. What option should you select in the Connection Properties dialog from within the Remote Desktop Session Host Configuration tool? Select the best answer.

   ❍ A. On the General tab, choose Allow connections only from computers running Remote Desktop with Network Level Authentication

   ❍ B. On the Security tab, choose Allow connections only from computers running Remote Desktop with Network Level Authentication

   ❍ C. On the Network Settings tab, choose Allow connections only from computers running Remote Desktop with Network Level Authentication

   ❍ D. On the Security tab, choose Allow connections from computers running Remote Desktop with Network Level Authentication only

2. What tool, available on a Windows Server 2008 R2 machine running Remote Desktop Connection Broker, is used to organize RemoteApp programs, personal virtual desktops and the virtual desktop pool? Select the best answer.

- ❍ A. Remote Desktop Resource Manager
- ❍ B. Remote Desktop Connection Manager
- ❍ C. Remote Desktop Client
- ❍ D. RemoteApp and Desktop Connection

Answers & Explanations

Chapter 1

1. Answers: A, D

Explanation A. Correct. Windows Server 2008 R2 Standard edition can support up to 4 virtual processors.

Explanation B. Incorrect. The foundation version of Windows Server 2008 R2 edition supports a maximum of 1 processor socket.

Explanation C. Incorrect. Windows Server 2003 guests support a maximum of only 2 processors.

Explanation D. Correct. The Windows HPC (high performance computing) Server 2008 can support a maximum of 4 virtual processors.

2. Answer: B

Explanation A. Incorrect. Hyper-V does support applications that communicate with devices attached to COM ports.

Explanation B. Correct. You can only attach two COM devices at a time and it cannot support three.

Explanation C. Incorrect. The Standard Edition does support COM ports, just as the Enterprise Edition.

Explanation D. Incorrect. The number of COM ports in this answer is too many.

3. Answer: A

Explanation A. Correct. The netdom command can be used to add the machine to the domain from the command prompt.

Explanation B. Incorrect. No such net domain option is available.

Explanation C. Incorrect. This is not the proper syntax for the netdom command.

Explanation D. Incorrect. No such command exists in Server core or the Full installation.

4. Answer: A

Explanation A. Correct. When you configure the VLAN IDs, it will force communications out through the network and back in through the network, but it will not allow internally directed communications through the virtual host.

Explanation B. Incorrect. No such option exists within the virtual networks.

Explanation C. Incorrect. If you take this action, nodes on the external network will be unable to communicate with two of the VMs.

Explanation D. Incorrect. No such option exists in the virtual network adapters.

5. Answer: B

Explanation A. Incorrect. When using a standard NIC for iSCSI LUN access, you must use a dedicated NIC.

Explanation B. Correct. You must dedicate a NIC to iSCSI communications when using a standard NIC for access to the LUNs.

Explanation C. Incorrect. When using a standard NIC for iSCSI LUN access, you must use a dedicated NIC.

Explanation D. Incorrect. The wireless clients will access the network through an access points, but the data will then travel the wired network to the VMs.

Chapter 2

1. Answers: A, B, D

Explanation A. Correct. You must attach the iSCSI LUN to the parent partition first. This causes the LUN to appear as a local drive to the VM.

Explanation B. Correct. Now, that the iSCSI LUN is mapped to the parent partition, it looks like a physical disk to the VM.

Explanation C. Incorrect. The drive letter association would be taken care of with the iSCSI initiator.

Explanation D. Correct. The LUN must exist before you can add it to the parent partition.

2. Answer: D

Explanation A. Incorrect. If the file system were NTFS, you could compact without preparation. Fat32 requires extra preparation.

Explanation B. Incorrect. Defragmenting is not sufficient. You must use a utility.

Explanation C. Incorrect. You should never compress a VHD file that you want to actively use.

Explanation D. Correct. Hyper-V does not include a tool that prepares VMs for compaction; however, you can get the tool from the Virtual Server 2005 distribution.

3. Answer: B
Explanation A. Incorrect. Integration Services do not support USB devices within the guest VMs.

Explanation B. Correct. USB devices are not directly supported; Integration Services does not support USB either.

Explanation C. Incorrect. USB devices are not supported - even in enlightened VMs.

Explanation D. Incorrect. You cannot map an IP address to a USB port.

4. Answer: C
Explanation A. Incorrect. You must completely stop the VM. Disconnecting the users is not enough.

Explanation B. Incorrect. Even with the Integration Services, you cannot create a template without first stopping the VM. This VM has Integration Services or you would not be able to send shutdown commands to the VM.

Explanation C. Correct. The VM must be in a stopped state in order to create a template from the VM.

Explanation D. Incorrect. You do not have to uninstall Integration Services to create a template.

5. Answer: A
Explanation A. Correct. The template object brings the VHD, OS profile, hardware profile and OS answer file together as an actual template.

Explanation B. Incorrect. Templates are not based on WIM images.

Explanation C. Incorrect. The issue in question doesn't have anything to do with network profiles.

Explanation D. Incorrect. Ghost images are not used in VM templates within SCVMM.

Chapter 3
1. Answer: A
Explanation A. Correct. RAID 0 is striping without parity. It provides the best performance, however, data must be restored from a backup should one of the drives fail.

Explanation B. Incorrect. RAID 1 will provide fault tolerance but seldom a performance gain. RAID 1 is mirroring.

Explanation C. Incorrect. While RAID 5 provides a nice balance between performance and reliability, the question demands only performance. RAID 5 is strip sets with parity.

Explanation D. Incorrect. RAID 2 is rarely supported by RAID controllers.

2. Answer: A

Explanation A. Correct. Integration Services will improve the performance of enlightened operating systems.

Explanation B. Incorrect. Running this tool will actually decrease performance slightly.

Explanation C. Incorrect. This ability should not impact the general performance of the VM.

Explanation D. Incorrect. If the machine is performing well, it probably has the Integration Services installed already.

3. Answer: B

Explanation A. Incorrect. You cannot select four processors when the host contains only 2 cores.

Explanation B. Correct. The synthetic adapter, which requires Integration Services, performs much better than the emulated adapter.

Explanation C. Incorrect. A file server rarely requires more than 1 GB, much less more than 2 GB.

Explanation D. Incorrect. While this action may provide most storage space, it will not increase performance.

4. Answer: A

Explanation A. Correct. The minimum functional level supporting AzMan is Windows Server 2003.

Explanation B. Incorrect. Windows Server 2003 DCs are fine, but you cannot have earlier DCs and use AzMan.

Explanation C. Incorrect. Windows Server 2003 DCs are fine, but you cannot have earlier DCs and use AzMan.

Explanation D. Incorrect. The Windows 2000 native functional level is not high enough.

Chapter 4

1. Answer: A

Explanation A. Correct. Snapshots are located in a subdirectory of the VM directory called snapshots. Each snapshot is stored in a uniquely named directory therein.

Explanation B. Incorrect. The snapshot files will not be stored on the C: drive as the default location is a subdirectory of the VM directory.

Explanation C. Incorrect. Snapshots are located with each VM so they would be on both the E: and the F: drive.

Explanation D. Incorrect. Snapshots are located with each VM so they would be on both the E: and the F: drive.

2. Answers: A, B

Explanation A. Correct. The snapshot does include the memory contents at the time of the snapshot.

Explanation B. Correct. Since memory contents are included, running processes are included as well.

Explanation C. Incorrect. The processes on the host are not considered in the snapshot.

Explanation D. Incorrect. Snapshots have no impact on physical hardware.

3. Answer: C

Explanation A. Incorrect. A 2003 or later domain is required.

Explanation B. Incorrect. SP2 must be installed on any Windows Server 2003 machine that is intended to run DPM.

Explanation C. Correct. The server may be a member of a Windows Server 2003 domain as well. The 2008 domain level is not required.

Explanation D. Incorrect. It is true that 2 GB is the minimum requirement, though 4 GB is recommended.

4. Answer: D

Explanation A. Incorrect. While this action would work, it would take more time.

Explanation B. Incorrect. SP2 is not required.

Explanation C. Incorrect. You can mount the VMs to the Hyper-V server.

Explanation D. Correct. The VHD mount utility can be used to add the VMs back. You can also create new VMs with the proper configuration and point them to the restored VHD files.

Chapter 5

1. Answer: D

Explanation A. Incorrect. SCVMM cannot convert a Windows NT 4 machine either online or offline.

Explanation B. Incorrect. No such feature exists.

Explanation C. Incorrect. SCVMM cannot convert a Windows NT 4 machine either online or offline.

Explanation D. Correct. Only third-party tools can convert a Windows NT 4 machine to a Hyper-V VM.

2. Answer: D

Explanation A. Incorrect. No such option exists.

Explanation B. Incorrect. Dragging the slider to the left decreases the importance of the resource.

Explanation C. Incorrect. No such option exists.

Explanation D. Correct. Dragging the slider to the right increases the importance of the resource.

3. Answers: B, C, D

Explanation A. Incorrect. OpsMgr requires SQL Server 2005 or later.

Explanation B. Correct. The .NET framework is a prerequisite on the server that runs OpsMgr.

Explanation C. Correct. The Microsoft Core XML (MSXML) 6.0 component must be on the Management Server and the machines running the agent. However, MSXML 6.0 will be installed automatically if the agent is deployed from the Operations Console.

Explanation D. Correct. If you wish to use the OpsMgr Command Shell, you must have PowerShell installed.

4. Answer: B

Explanation A. Incorrect. XenServer VMs can be converted to Hyper-V.

Explanation B. Correct. You must uninstall the XenServer drivers after booting the VM within Hyper-V.

Explanation C. Incorrect. No such option is available in the Hyper-V hosts.

Explanation D. Incorrect. IDE disks are allowed for booting in Hyper-V VMs and general storage.

5. Answer: A

Explanation A. Correct. The import process does not provide a move function during the import.

Explanation B. Incorrect. No such option is provided by the import process.

Explanation C. Incorrect. No such wizard exists.

Explanation D. Incorrect. No such option is provided.

Chapter 6

1. Answer: A

Explanation A. Correct. The option is located on the General tab of the Connection Properties dialog box.

Explanation B. Incorrect. This option is not located on the Security tab, which actually doesn't exist.

Explanation C. Incorrect. No such tab exists in the dialog.

Explanation D. Incorrect. No such tab or option exists.

2. Answer: B

Explanation A. Incorrect. No such application exists.

Explanation B. Correct. The RDCM tool is on any server running RDCB. The tool can be used to determine which resources will be available to users and groups.

Explanation C. Incorrect. The RDC is used to access Remote Desktop resources.

Explanation D. Incorrect. RemoteApp and Desktop Connection are used on Windows 7 clients, from within the Control Panel, to access the RemoteApps and desktops.