

A HYPER-V FIRST AID KIT: Troubleshooting 5 Common Issues



ALTARO

CONTENTS

INTRODUCTION	3
STORAGE RELATED PROBLEMS.....	4
Slow Storage Performance	4
iSCSI Multi-Path Not Working Correctly	16
Painfully Slow File Copies.....	24
Virtual Machines Are Listed as Being in a Critical State and Cannot Be Powered On.....	27
PERMISSIONS PROBLEMS	30
An Error Occurred While Attempting to Connect to Server	30
Inadequate RunAs Permissions	38
LIVE MIGRATION FAILURE.....	39
Missing Permissions	39
An Incorrect Authentication Protocol	41
Mismatched Configurations	43
BACKUP RELATED PROBLEMS	48
Backup Related Checkpoints that Cannot Be Deleted.....	55
HIGH AVAILABILITY ISSUES.....	58
Virtual Machines Do Not Fail Over to Another Cluster Node	58
Inadequate Resources.....	59
CONCLUSION	63
ABOUT ALTARO	64
ABOUT BRIEN M. POSEY.....	66
FOLLOW ALTARO	67

INTRODUCTION

Although Microsoft Hyper-V is a mature, stable, and reliable server virtualization platform, problems can, and sometimes do occur. That being the case, this eBook has been written in an effort to help Hyper-V administrators to diagnose various problems with the hypervisor and Hyper-V virtual machines.

Because it is nearly impossible to discuss every problem that could potentially occur in a Hyper-V environment, this book focuses on the more common problems that Hyper-V admins are likely to encounter. For each problem that is discussed, you will find a short description of the problem and one or more step by step solutions to the problem.

The solutions presented within this book are grouped by hardware components (storage related problems, network related problems, etc.). It is worth noting however, that problems can sometimes have multiple causes, so if you don't initially find any mention of the problem that you are experiencing, then you might try looking in a different section.

STORAGE RELATED PROBLEMS

Many of the most common problems that Hyper-V administrators tend to experience are storage related. A variety of problems ranging from poor virtual machine performance to issues with high availability can potentially be related to performance.

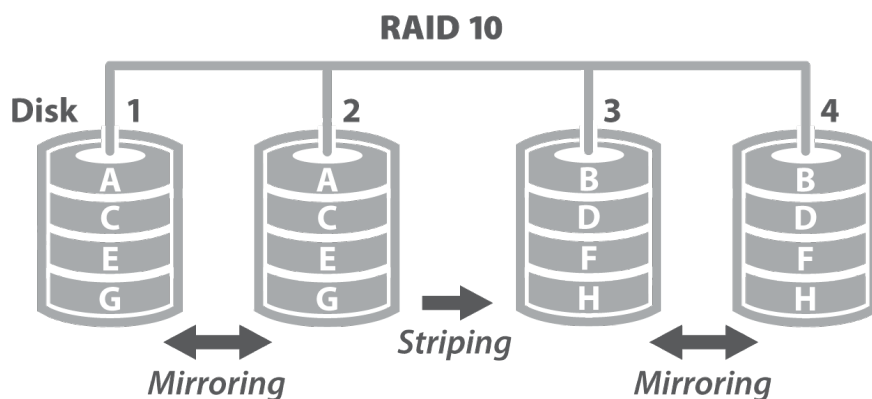
SLOW STORAGE PERFORMANCE

Poor disk performance tends to be one of the more difficult problems to troubleshoot in a Hyper-V environment. This is because there are so many different things that can cause slow storage performance.

Storage Architecture

One common cause is resource contention. In any virtualized environment, there is a finite amount of storage I/O available, and this I/O must be shared among the virtual machines. If the I/O demand exceeds (or approaches) the I/O capacity, then performance will suffer. In these types of situations, it is usually advisable to move some virtual machines to an alternate Hyper-V host (assuming that local storage is being used). However, there are some other things that you can check to ensure optimal storage performance.

The first thing that you should check is virtual machine component placement. Virtual machine components should reside on dedicated storage, where they will not have to compete with the operating system for storage I/O. Microsoft recommends that this volume be structured as RAID 1+0 (sometimes referred to as RAID 10). RAID 1+0 delivers the performance of striping, with the redundancy of mirroring. Although some organizations use RAID 5 or RAID 6 volumes, RAID 5 and 6 are poor choices for write intensive virtual machines, because of the overhead involved in writing parity data.



Requires a minimum of four drives

While you are assessing your storage architecture, it is also a good idea to evaluate your storage connectivity. In some cases, the Fibre Channel or iSCSI connection between a storage array and the Hyper-V hosts may not perform as well as the actual storage array, and the connection can become a bottleneck.

Virtual Hard Disk Type

Microsoft also recommends using VHDX based virtual hard disks, and virtual hard disks in VHD format should be converted to VHDX (<https://blogs.technet.microsoft.com/askfeplat/2013/03/10/windows-server-2012-hyper-v-best-practices-in-easy-checklist-form/>). Microsoft also recommends the use of fixed length virtual hard disks (which are sometimes referred to as fixed size virtual hard disks), as opposed to dynamically expanding virtual hard disks (<https://technet.microsoft.com/en-us/library/mt589658.aspx>).

Dynamically expanding virtual hard disks make use of thin provisioning. This means that the virtual hard disk initially consumes only a small amount of physical storage space, regardless of the virtual hard disk's capacity. When dynamically expanding virtual hard disks are used, Hyper-V only claims physical disk space as data is added to the virtual hard disk. When data is written to a dynamically expanding virtual hard disk, the virtual hard disk file grows to accommodate the new data. Conversely, fixed length virtual hard disks claim the full amount of required physical disk space upon being created.

If you were to create a 100 GB virtual hard disk, then the amount of physical disk space that would initially be consumed would be determined by the type of virtual hard disk that was created. A fixed length virtual hard disk would claim the full 100 GB of space right away. A dynamically expanding virtual hard disk might eventually consume 100 GB of space if the disk is filled to capacity, but would initially consume only 4 MB of space.

The primary advantage to creating dynamically expanding virtual hard disks is that it allows administrators to create virtual hard disks with little regard for physical storage availability. Doing so works well for situations in which it is difficult to estimate how much storage space a workload will ultimately need, or in situations in which physical storage upgrades are planned, but have not yet been performed. An administrator might for example, create a virtual hard disk that is larger than the available physical disk space, knowing that physical disk space can always be added later on in order to accommodate growth.

In spite of their advantages, dynamically expanding virtual hard disks do have their disadvantages. First, the physical storage can be over committed, and it is possible for virtual hard disk growth to exceed the physical hardware's capacity.

Another disadvantage is that dynamically expanding virtual hard disks do not perform quite as well as fixed length virtual hard disks. This is because of the overhead involved in expanding the virtual hard disk file each time that new data is written to the virtual hard disk. In some situations, performance may also suffer as a result of virtual hard disk file fragmentation.

When you create a virtual machine through Hyper-V Manager, the virtual machine uses dynamically expanding virtual hard disks by default.

You can verify a virtual machine's virtual hard disk type by completing these steps:

1. Open the Hyper-V Manager.
2. Right click on the virtual machine that you want to inspect, and select the Settings command from the shortcut menu.
3. Select the virtual hard disk within the list of hardware, as shown in Figure 1.
4. Click the Inspect button.
5. Check the Type listing within the Virtual Hard Disk Properties dialog box, as shown in Figure 2.

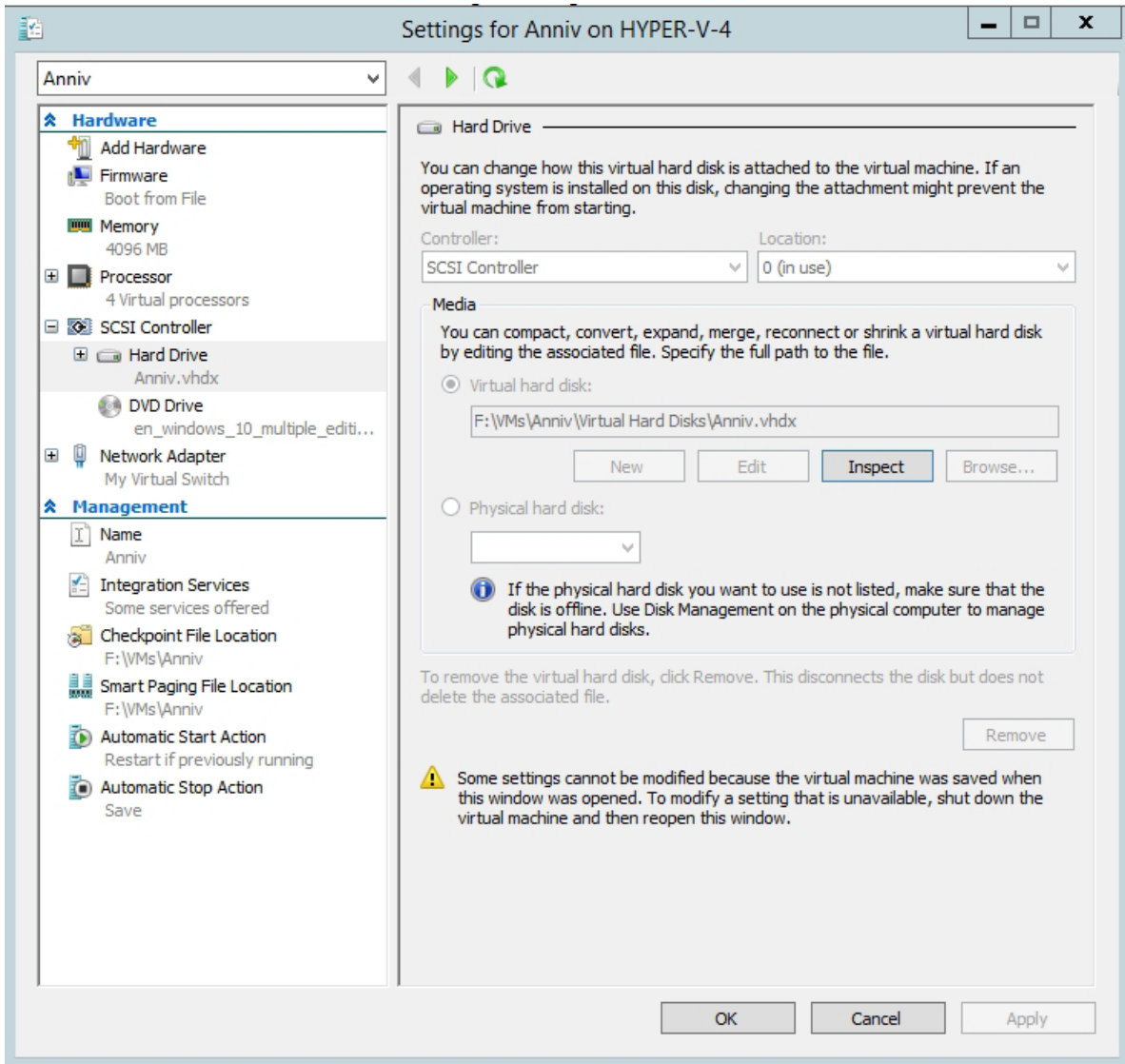


Figure 1. Select the virtual hard disk that you want to inspect.

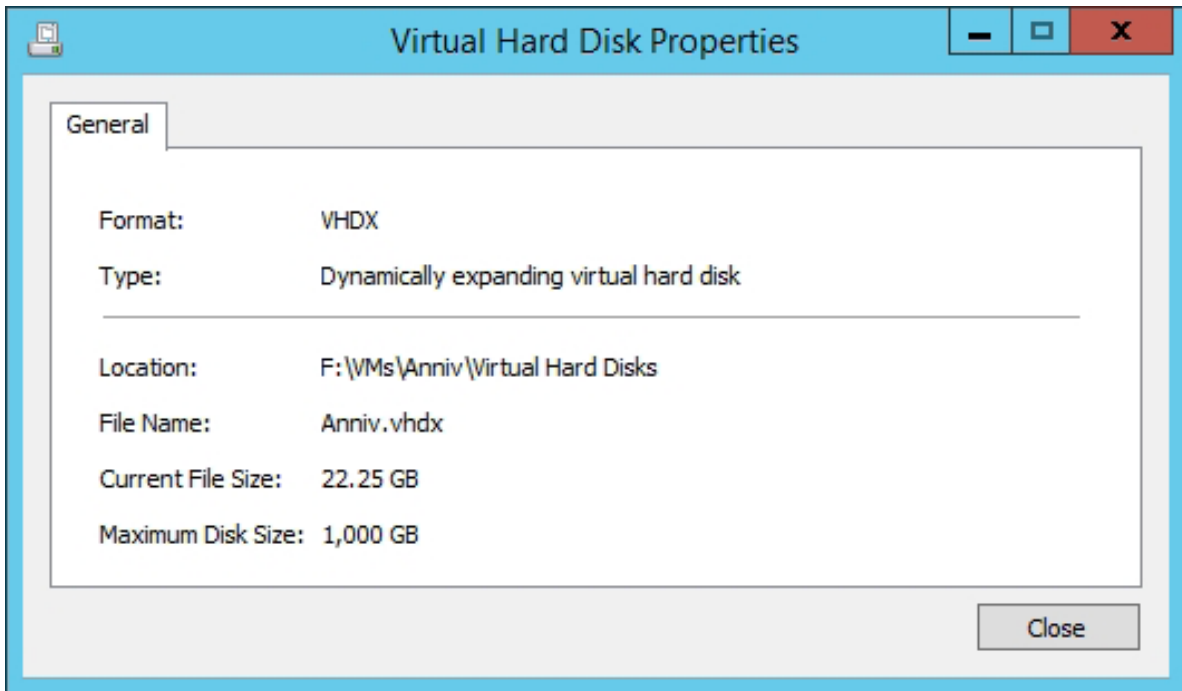


Figure 2. The Virtual Hard Disk Properties dialog box lists the virtual hard disk type.

If you prefer to use PowerShell, then you can do so by using the Get-VHD cmdlet. The only parameter that you will have to specify is the Path. However, it can be helpful to append the Select-Object cmdlet as a way of filtering the output so that the cmdlet shows you only the information that you are interested in. For example, the following command displays the virtual hard disk's path, format, and type:

```
Get-VHD -Path <virtual hard disk path and filename> |
Select-Object Path, VhdFormat, VhdType
```

You can see what this command looks like in action in Figure 3.

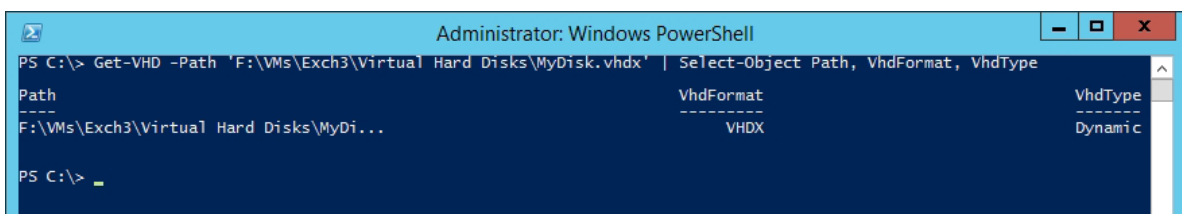


Figure 3. You can use the Get-VHD cmdlet to retrieve information about a virtual hard disk.

Converting a Virtual Hard Disk

Even if you discover that a virtual hard disk is configured to use thin provisioning, it does not necessarily mean that you have a problem. Thin provisioning does have its place. However, if you do decide that it is in your best interest to convert a dynamically expanding virtual hard disk into a fixed length virtual hard disk, then you can do so by completing these steps:

1. Within the Hyper-V Manager, right click on the virtual machine whose virtual hard disk you wish to convert, and select the Settings command from the shortcut menu. This will cause Windows to display the Settings dialog box for the virtual machine.
2. Click on the virtual hard disk that you wish to convert, and click on the Edit button, shown in Figure 4. This will cause Windows to launch the Edit Virtual Hard Disk Wizard.

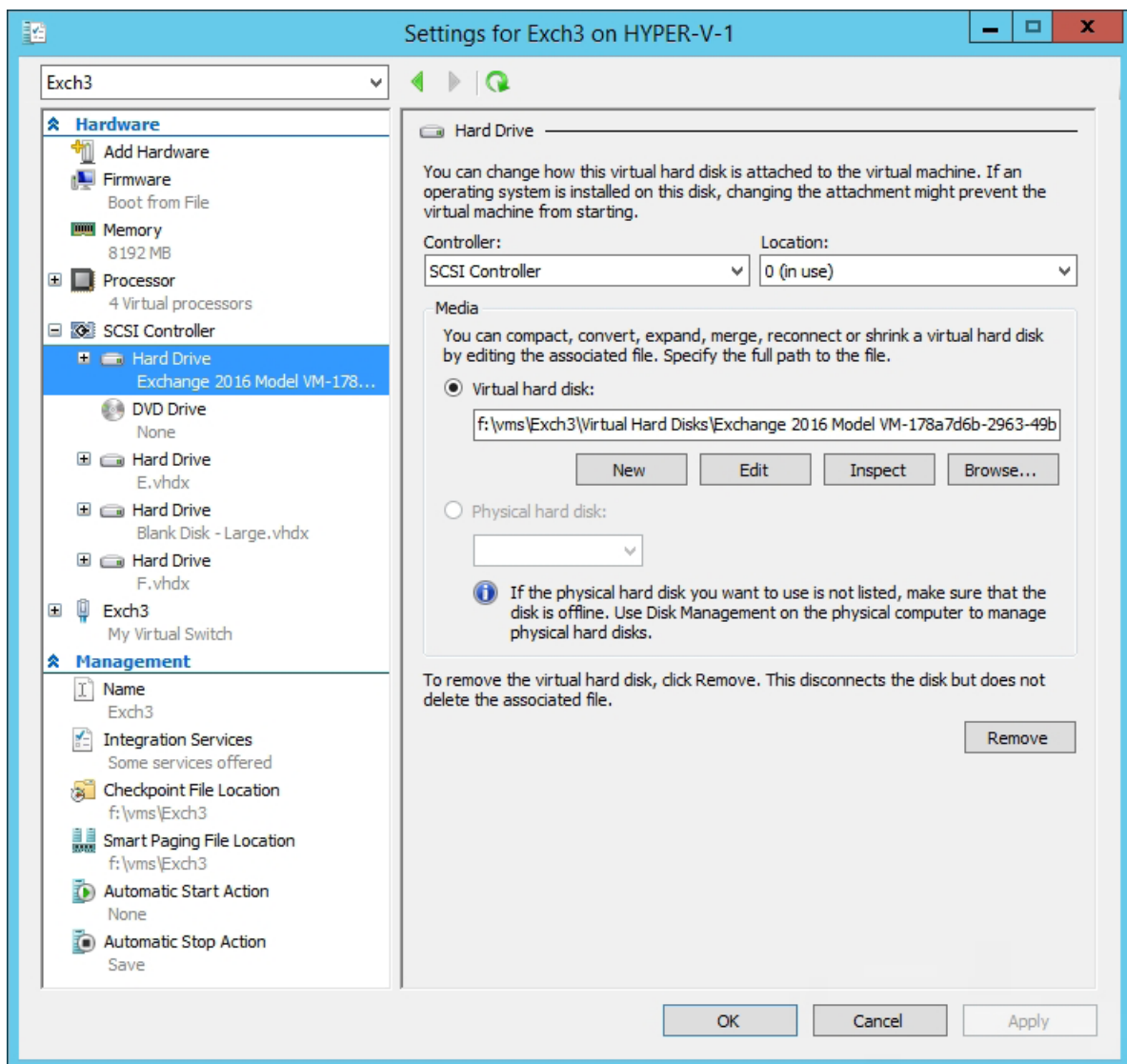


Figure 4. Click on the virtual hard disk, and then click the Edit button.

3. Click Next to bypass the wizard's Locate Virtual Hard Disk screen.
4. When you arrive at the wizard's Choose Action screen, choose the Convert option and click Next.
5. Choose VHDX as the disk format, unless you have a compelling reason to use the VHD format. Click Next to continue.
6. Choose the Fixed Size option, shown in Figure 5, from the wizard's Convert Virtual Hard Disk screen, and click Next.

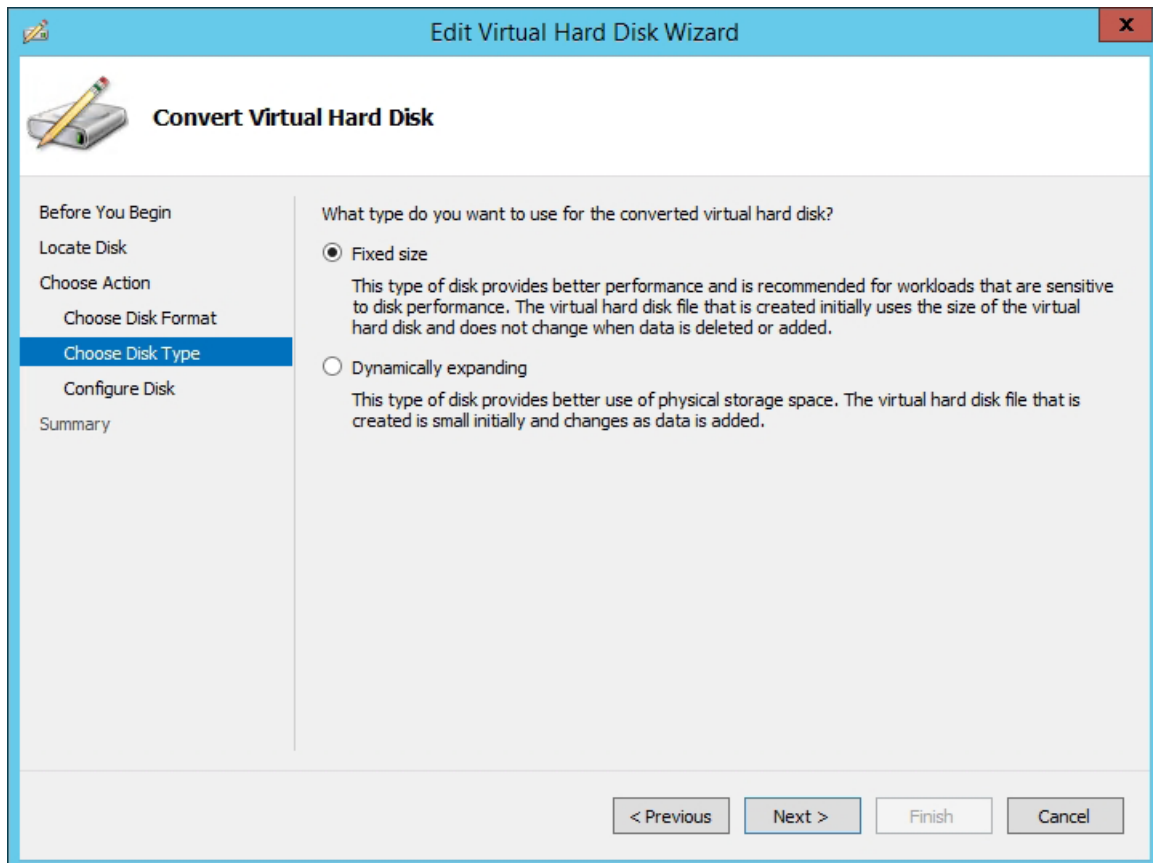


Figure 5. Choose the Fixed Size option, and click Next.

7. When prompted, enter a path and filename to use for the new virtual hard disk.

NOTE: Hyper-V does not actually convert the virtual hard disk to a new format, but rather creates a brand new virtual hard disk. As such, you will have to provide a virtual hard disk name that differs from the name that was originally used. Be sure to pay close attention to the path, because Hyper-V will attempt to place the virtual hard disk on the server's system drive by default. It is also worth noting that you will need to have a sufficient amount of free physical disk space to accommodate both copies of the virtual hard disk.

8. Click Next.
9. Click Finish.
10. After the virtual hard disk conversion completes, you will be returned to the Settings dialog box. The virtual machine will still be using the original virtual hard disk, so you will have to manually configure the virtual machine to use the new virtual hard disk.

NOTE: As a best practice, you should shut down the virtual machine before attempting this process.

11. You can switch to the new virtual hard disk by clicking the Browse button, selecting the virtual hard disk that you want to use, and clicking Open.
12. Click OK to complete the process.
13. Power the virtual machine on, and make sure that it is functioning normally. When you are done testing the virtual machine, don't forget to delete your old virtual hard disk.

If you prefer, you can use Windows PowerShell to convert a dynamically expanding virtual hard disk into a fixed length virtual hard disk. In order to do so, you will need to know the path and filename used by the original virtual hard disk. You will also have to provide a destination path and filename for the new virtual hard disk. The cmdlet that is used to convert the virtual hard disk is Convert-VHD. The syntax is:

```
Convert-VHD -Path <path and filename of the virtual hard disk to be replaced> -DestinationPath <path and filename of the new virtual hard disk> -VHDType Fixed
```

You can see an example of such a conversion in Figure 6.

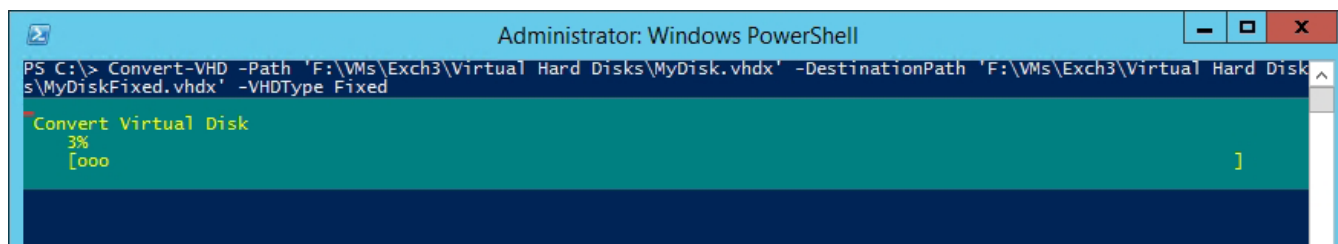


Figure 6. You can use the *Convert-VHD* cmdlet to convert a virtual hard disk.

Keep in mind however, that there is usually more to the process than simply converting the virtual hard disk. You will typically need to shut down the virtual machine, convert the virtual hard disk, and then remove the old virtual hard disk and replace it with the newly created virtual hard disk.

This process requires you to know the virtual hard disk's controller type, controller number, and controller location, so you will have to look this information up as a part of the process. The commands used in doing so are:

```
Stop-VM -Name <virtual machine name>
```

```
Convert-VHD -Path <path and filename of the virtual hard disk to be replaced> -DestinationPath <path and filename of the new virtual hard disk> -VHDType Fixed
```

```
Get-VMHardDiskDrive -VMName <virtual machine name>
```

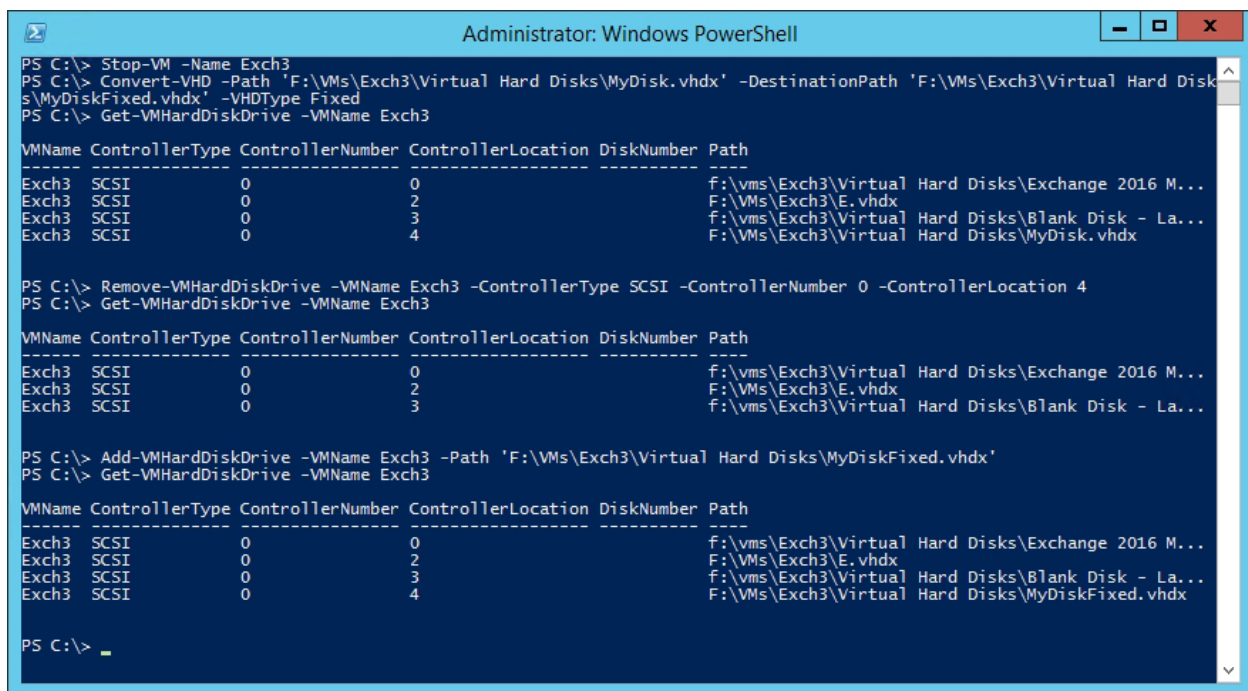
```
Remove-VMHardDiskDrive -VMName <virtual machine name> -  
ControllerType <IDE or SCSI> -ControllerNumber <disk controller  
number> -ControllerLocation <virtual hard disks location on the  
controller>
```

```
Get-VMHardDiskDrive -VMName <virtual machine name>
```

```
ADD-VMHardDiskDrive -VMName <virtual machine name> -Path  
<virtual hard disk path and filename>
```

```
Get-VMHardDiskDrive -VMName <virtual machine name>
```

You can see the entire process in action in Figure 7.



```
Administrator: Windows PowerShell  
PS C:\> Stop-VM -Name Exch3  
PS C:\> Convert-VHD -Path 'F:\VMs\Exch3\Virtual Hard Disks\MyDisk.vhdx' -DestinationPath 'F:\VMs\Exch3\Virtual Hard Disks\MyDiskFixed.vhdx' -VHDType Fixed  
PS C:\> Get-VMHardDiskDrive -VMName Exch3  
-----  
VMName ControllerType ControllerNumber ControllerLocation DiskNumber Path  
-----  
Exch3 SCSI 0 0 f:\vms\Exch3\Virtual Hard Disks\Exchange 2016 M...  
Exch3 SCSI 0 2 F:\VMs\Exch3\E.vhdx  
Exch3 SCSI 0 3 f:\vms\Exch3\Virtual Hard Disks\Blank Disk - La...  
Exch3 SCSI 0 4 F:\VMs\Exch3\Virtual Hard Disks\MyDisk.vhdx  
-----  
PS C:\> Remove-VMHardDiskDrive -VMName Exch3 -ControllerType SCSI -ControllerNumber 0 -ControllerLocation 4  
PS C:\> Get-VMHardDiskDrive -VMName Exch3  
-----  
VMName ControllerType ControllerNumber ControllerLocation DiskNumber Path  
-----  
Exch3 SCSI 0 0 f:\vms\Exch3\Virtual Hard Disks\Exchange 2016 M...  
Exch3 SCSI 0 2 F:\VMs\Exch3\E.vhdx  
Exch3 SCSI 0 3 f:\vms\Exch3\Virtual Hard Disks\Blank Disk - La...  
-----  
PS C:\> Add-VMHardDiskDrive -VMName Exch3 -Path 'F:\VMs\Exch3\Virtual Hard Disks\MyDiskFixed.vhdx'  
PS C:\> Get-VMHardDiskDrive -VMName Exch3  
-----  
VMName ControllerType ControllerNumber ControllerLocation DiskNumber Path  
-----  
Exch3 SCSI 0 0 f:\vms\Exch3\Virtual Hard Disks\Exchange 2016 M...  
Exch3 SCSI 0 2 F:\VMs\Exch3\E.vhdx  
Exch3 SCSI 0 3 f:\vms\Exch3\Virtual Hard Disks\Blank Disk - La...  
Exch3 SCSI 0 4 F:\VMs\Exch3\Virtual Hard Disks\MyDiskFixed.vhdx  
-----  
PS C:\> _
```

Figure 7. You can use PowerShell to convert and replace a virtual hard disk.

Checkpoints

The existence of checkpoints also impacts virtual hard disk performance. Furthermore, Microsoft advises against the use of checkpoints in production environments until the release of Windows Server 2016, which will feature a production checkpoint feature. The reason for this is because prior to the release of Windows Server 2016, the Hyper-V checkpoint feature (or snapshot feature as it was known in Windows Server 2008 and 2008 R2) was not application aware. As such, creating and then later applying a checkpoint on an application server had the potential to cause corruption or data loss. The Windows Server 2016 production checkpoint feature will utilize the Volume Shadow Copy Services (VSS) as a part of the checkpoint process, so as to ensure that VSS aware

applications can be safely check pointed. VSS is the same mechanism that backup applications use to safely back up Microsoft application servers.

Checkpoints don't usually have a major impact on write performance, assuming that the checkpoints are stored on a high speed volume. However, checkpoints can have a significant impact on read performance. A virtual machine's read performance tends to correspond directly to the number of checkpoints that exist for the virtual machine. The reason for this is that each checkpoint represents a differencing disk. When a virtual machine receives a read instruction, Hyper-V has to read each differencing disk in sequence, until it finds the requested data. You can remove unwanted checkpoints by completing these steps:

1. Open the Hyper-V Manager.
2. Select the virtual machine whose checkpoints you wish to remove.
3. Right click on a checkpoint that you intend to remove.
4. Select either the Delete Checkpoint or the Delete Checkpoint Subtree command from the shortcut menu, as shown in Figure 8.

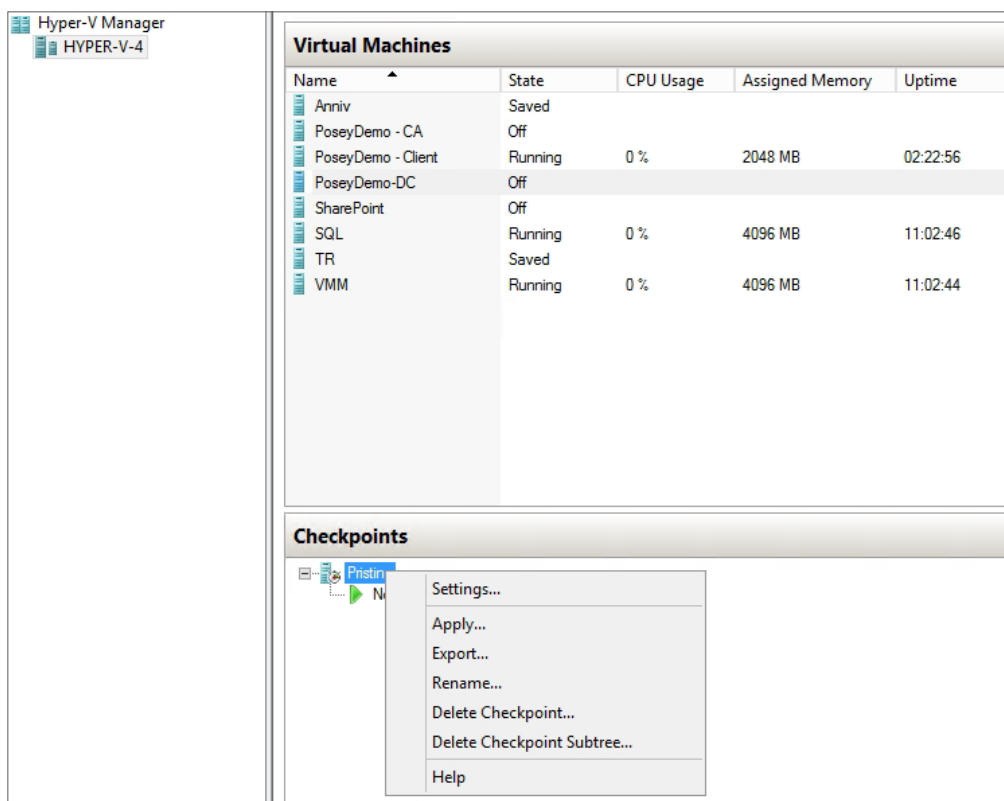


Figure 8. You can improve a virtual machine's read performance by removing unwanted checkpoints.

It is also possible to remove an unwanted virtual machine checkpoint by using PowerShell. To do so, you will have to use the Remove-VMSnapshot cmdlet. Checkpoints were referred to as snapshots prior to the release of Windows Server 2012, hence the reference to snapshots in the cmdlet.

Unless you know the name of the checkpoint that you want to remove, you will need to retrieve a list of checkpoints from the server. You can accomplish this task by using the Get-VMSnapshot cmdlet, and using the -VMName switch to provide the name of the virtual machine that you want to examine. The commands used to retrieve a list of checkpoints and then remove a specific checkpoint are:

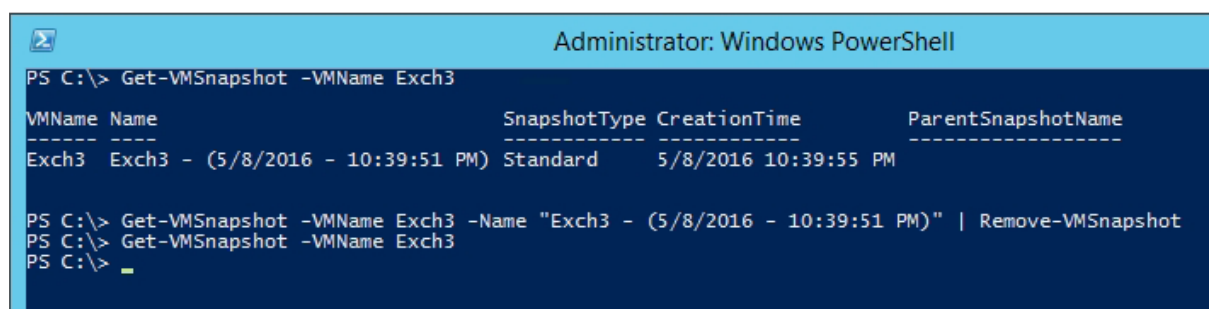
```
Get-VMSnapshot -VMName <virtual machine name>

Get-VMSnapshot -VMName <virtual machine name> -Name <checkpoint
name>

| Remove-VMSnapshot

Get-VMSnapshot -VMName <virtual machine name>
```

The last command in the code block above is not actually needed, but was included as a way of verifying the operation's success. You can see what these commands look like in Figure 9.



```
Administrator: Windows PowerShell
PS C:\> Get-VMSnapshot -VMName Exch3
VMName Name                SnapshotType CreationTime      ParentSnapshotName
-----
Exch3  Exch3 - (5/8/2016 - 10:39:51 PM) Standard          5/8/2016 10:39:55 PM

PS C:\> Get-VMSnapshot -VMName Exch3 -Name "Exch3 - (5/8/2016 - 10:39:51 PM)" | Remove-VMSnapshot
PS C:\> Get-VMSnapshot -VMName Exch3
PS C:\>
```

Figure 9. It is possible to use PowerShell to remove a checkpoint.

Incidentally, checkpoint files tend to grow over time. Believe it or not, this behavior is by design. When an administrator creates a checkpoint, Hyper-V creates a differencing disk. From that point on, all of the virtual machine's write operations are directed to the differencing disk, rather than to the virtual machine's original virtual hard disk. The

original virtual hard disk becomes read only, and is left in the state in which it existed when the checkpoint was created. It is this behavior that makes it possible to easily roll a virtual machine back to an earlier point in time. Because the original virtual hard disk becomes read only, and because all future write operations are directed to the differencing disk, the checkpoint's size will continue to grow until the checkpoint is either removed, or replaced with a newer checkpoint.

ISCSI MULTI-PATH NOT WORKING CORRECTLY

iSCSI storage is a popular choice for SMBs that want to create a cluster shared volume, without the cost or complexity of Fibre Channel. Although the iSCSI configuration process tends to be relatively straightforward, there are some common mistakes that can cause iSCSI multipath to not work correctly.

Microsoft Multi-Path I/O

The Windows Server operating system has built-in support for multi-path I/O for the purpose of providing high availability. Multi-path I/O works by enabling multiple connections (sessions) to a storage array. This makes it possible for each node in a Windows failover cluster to have its own connection to the storage hardware that hosts the cluster shared volume. As such, each node in the cluster has access to exactly the same storage resources.

Although this book addresses multi-path I/O from an iSCSI standpoint, it is important to understand that multi-path I/O is not unique to iSCSI. The Microsoft multi-path I/O implementation supports the use of iSCSI, Fibre Channel, and Serial Attached Storage (SAS).

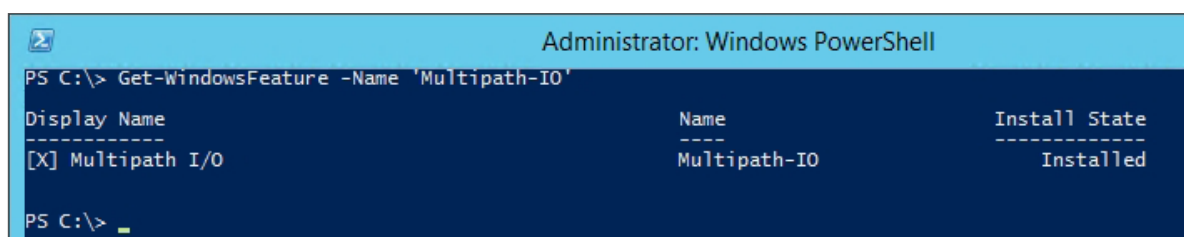
Microsoft's multi-path I/O feature uses a Device Specific Module (DSM) to provide support for storage arrays that natively support the Asymmetric Logical Unit Access (ALUA) model, as defined by SPC-3. Also supported are hardware arrays that adhere to the Active / Active controller model. Microsoft multi-path I/O feature also allows for hardware independent multi-path I/O at the iSCSI level.

Verifying Multi-Path I/O

The first step in troubleshooting any multi-path I/O related problem is to verify that Multi-Path I/O is enabled on the server. The easiest way to accomplish this is to use Windows PowerShell. To do so, open an elevated PowerShell window, and enter the following command:

```
Get-WindowsFeature -Name 'Multipath-IO'
```

As you can see in Figure 10, this command will show you the installation state for the Multi-Path I/O feature.



```
Administrator: Windows PowerShell
PS C:\> Get-WindowsFeature -Name 'Multipath-IO'
Display Name           Name           Install State
-----
[X] Multipath I/O      Multipath-IO   Installed
PS C:\> _
```

Figure 10. You can use the `Get-WindowsFeature` cmdlet to check whether or not the Multi-Path I/O feature is installed.

If you determine that the Multi-Path I/O feature is not installed, then you can easily install it from within PowerShell. Keep in mind that the Multi-Path I/O feature must be installed onto each server that will need multi-path access to the storage array. The command used to install the multi-path I/O feature is:

```
Enable-WindowsOptionalFeature -Online -FeatureName
MultiPathIO
```

You can see what this process looks like in Figure 11.

```
Administrator: Windows PowerShell
PS C:\> Get-WindowsFeature -Name 'Multipath-I/O'

Display Name          Name          Install State
-----
[ ] Multipath I/O    Multipath-IO  Available

PS C:\> Enable-WindowsOptionalFeature -Online -FeatureName MultiPathIO

Path          :
Online       : True
Restart Needed : False

PS C:\> Get-WindowsFeature -Name 'Multipath-I/O'

Display Name          Name          Install State
-----
[X] Multipath I/O    Multipath-IO  Installed

PS C:\> _
```

Figure 11. You can use PowerShell to enable multi-path I/O

The Multi-Path I/O Control Panel

Installing the multi-path I/O feature results in the Microsoft Device Specific Module (DSM) also being installed. In addition, Windows also installs the MPIO Control Panel, which allows administrators to configure MPIO functionality, create MPIO configuration reports, and install additional DSMs (to support additional storage products). You can access the MPIO Control Panel by navigating through the Windows Control Panel to System and Security \ Administrative Tools \ MPIO.

NOTE: In a Server Core environment, you can launch the MPIO Control Panel by running MPIOCPL.EXE command.

The MPIO Control Panel, which you can see in Figure 12, is divided into four tabs – MPIO Devices, Discover Multi-Paths, DSM Install, and Configuration Snapshot.

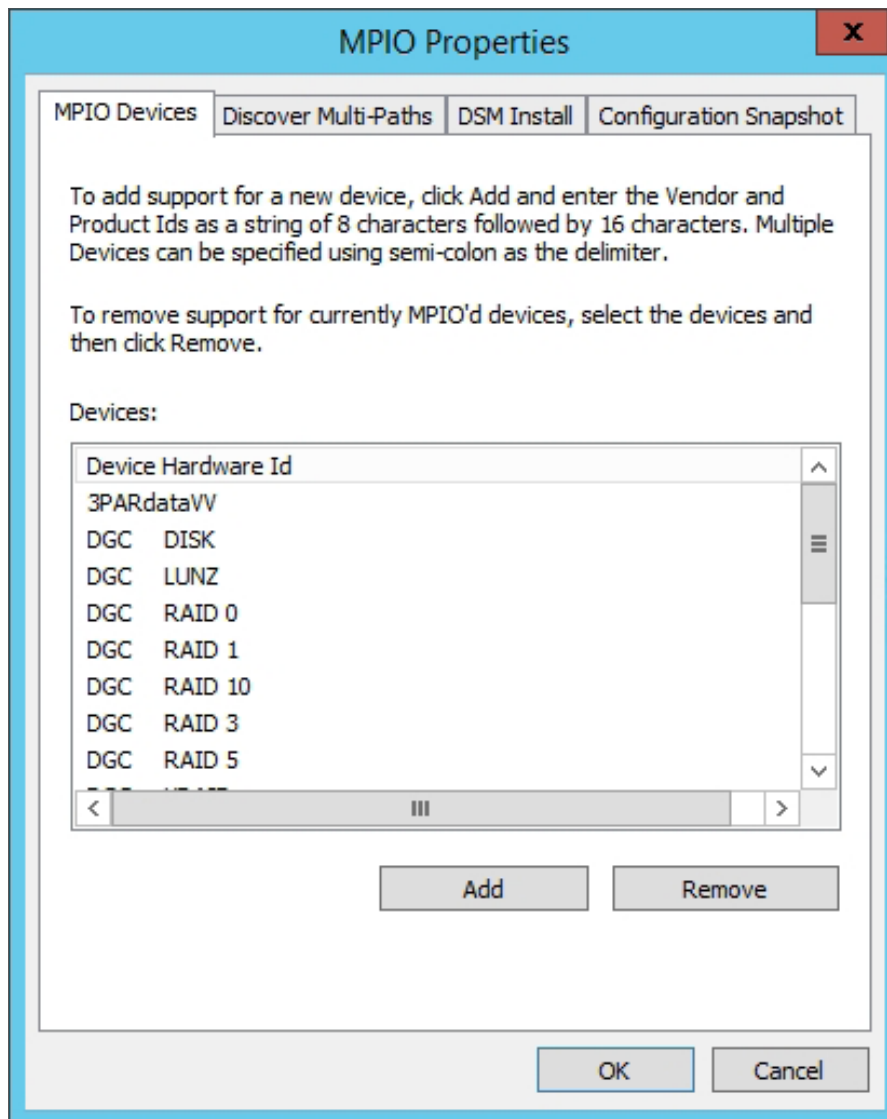


Figure 12. This is the MPIO Control Panel.

The MPIO Devices tab allows admins to add support for new storage devices. Simply click the Add button and enter the vendor and product IDs. The vendor ID is an eight-character string, and the product ID is a sixteen-character string. If you need to add multiple devices, you can do so by separating devices with a semi-colon.

The Discover Multi-Paths tab can be used to add device IDs for Fibre Channel devices that use Microsoft DSM. This tab can also be used to determine whether or not multiple instances actually point to a common Logical Unit Number (LUN).

The DSM Install tab is used to add support for storage devices that do not support the MPIO architecture. Most SPC-3 compliant arrays will work with the DSM provided by Microsoft, but some hardware vendors so provide their own DSM. You can add a third party DSM by using the Browse button to locate the corresponding .INF file, and then clicking the Install button.

The Configuration Snapshot tab exists primarily for troubleshooting purposes. By using this tab, administrators can save the MPIO configuration to a text file for review. You can see this tab and a configuration snapshot (taken from a system with no attached storage) in Figure 13.

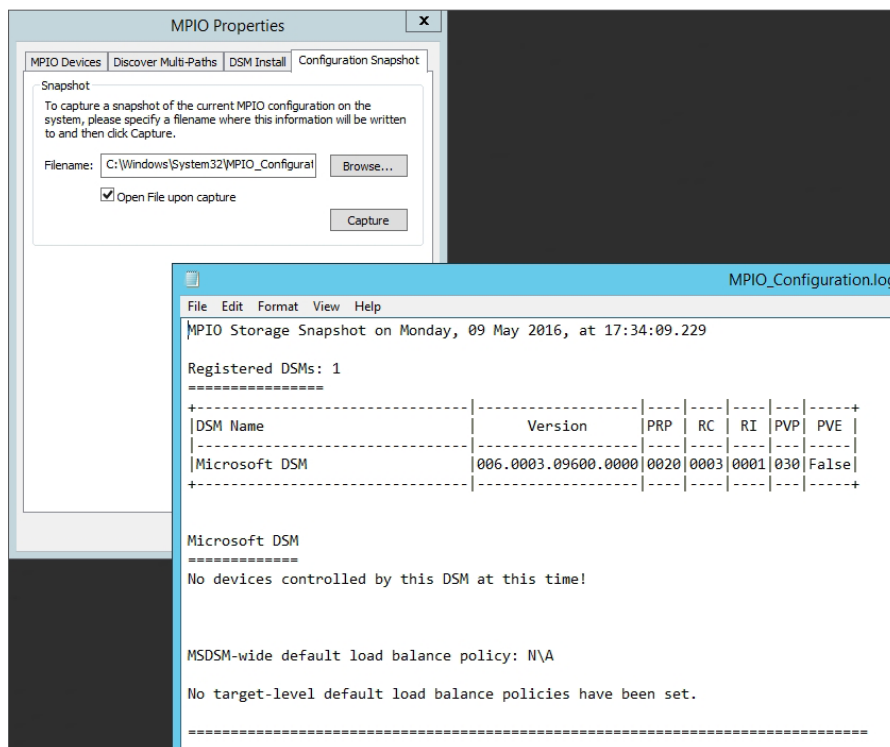


Figure 13. The Configuration Snapshot tab produces a report detailing registered DSMs, devices, and load balancing policies.

As you can see in the figure above, the MPIO Storage Snapshot report provides information about registered DSMs, controlled devices, and target load balancing policies. This report can be useful for troubleshooting, but the report tends to be even more useful if a comparison can be made between a report that was created when the system was functioning properly, and a report that was created after a problem started.

iSCSI Multipath Configuration Issues

The most common iSCSI configuration issues involve multipath not being enabled, and the iSCSI initiator not being allowed to access the iSCSI target. The iSCSI target configuration process varies by vendor, but typically the target is treated as being multipath enabled, so long as each of the iSCSI initiators have permission to access the

target. When the first iSCSI initiator establishes connectivity however, the initiator must be configured for multipath support. Otherwise, the other cluster nodes will be unable to connect to the iSCSI target.

As previously noted, the iSCSI configuration steps vary depending on which vendor's solution you are using. Assuming that you are using the Windows Server 2012 R2 iSCSI Initiator and iSCSI Target, you can verify the permissions required for multipath by completing these steps:

1. Open an iSCSI Initiator window, and select the Configuration tab.
2. Document the Initiator Name, as shown in Figure 14.
3. Repeat steps 1 and 2 for each node that will connect to the iSCSI target

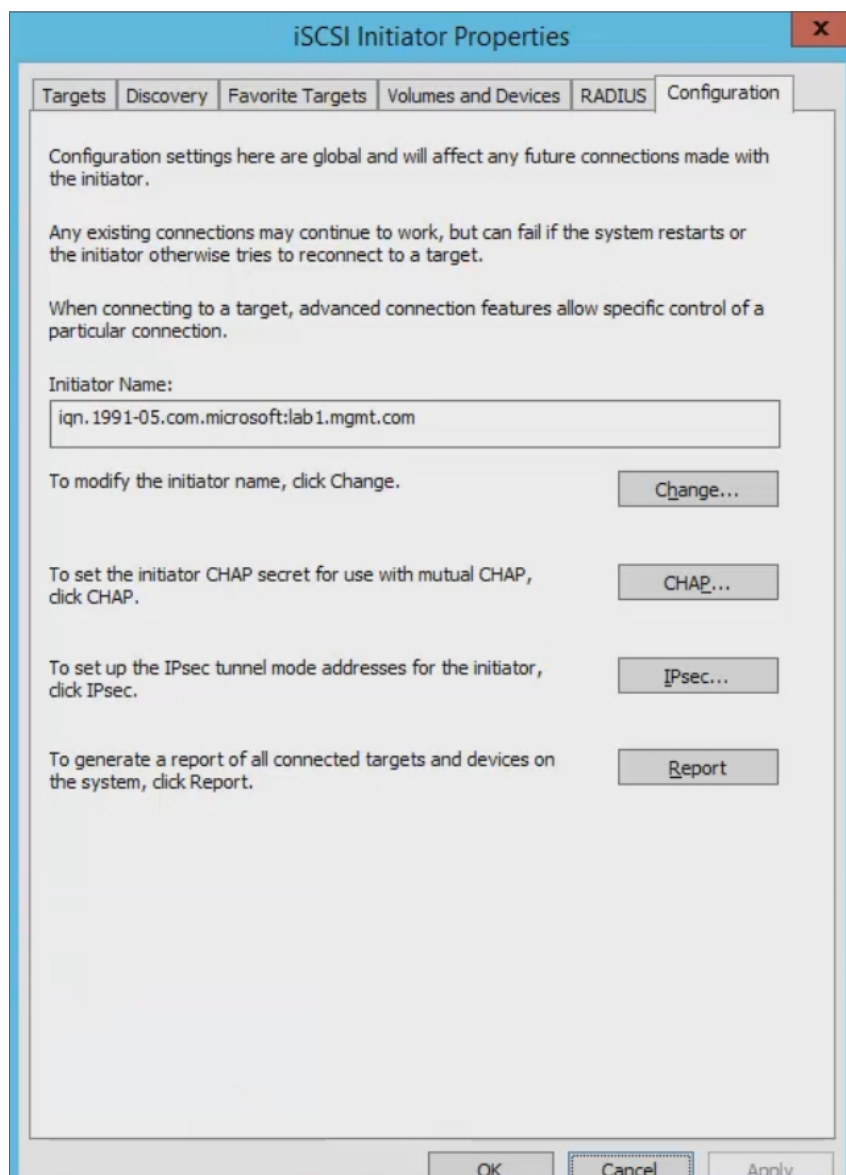


Figure 14. Document the name of each iSCSI Initiator.

4. Open the Server Manager and click on the File and Storage Services container.
5. Click on the iSCSI container.
6. Make note of the target's IQN so that you can connect to it.
7. Right click on the iSCSI target and choose the Properties command from the shortcut menu.
8. Select the Initiators container.
9. Add the IQN for each iSCSI initiator that will be connecting to the target, as shown in Figure 15. Each cluster node should have its own initiator.

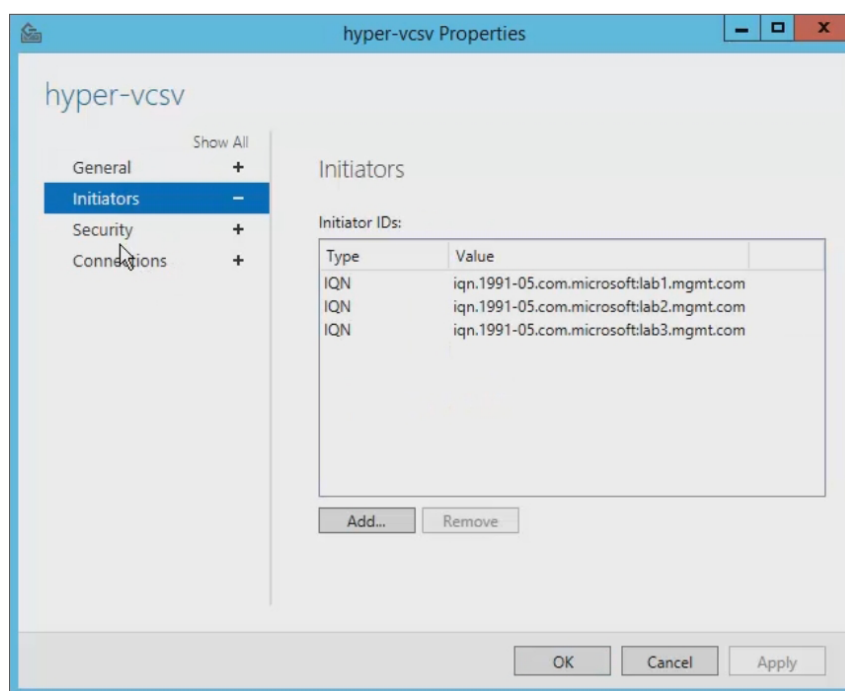


Figure 15. Each initiator must have permission to connect to the target.

10. Click on the Security tab and check to see if CHAP is enabled. If so, you will need to know the CHAP username and password.
11. Open the iSCSI Initiator on one of your cluster nodes.
12. If CHAP is being used, then go to the initiator's Configuration tab, click the CHAP button, and enter the CHAP credentials (also known as the CHAP secret).

13. Go to the Discovery tab.
14. Click the Discover Portal button.
15. Enter the DNS host name or IP address of the server that is acting as an iSCSI target.
16. Verify that the Port number is set to 3260, and that this port is open on your firewall.
17. Click OK.
18. Go to the initiator's Targets tab.
19. Verify that your iSCSI target is listed among the Discovered Targets.
20. Select the iSCSI target, and click Connect.
21. When Windows displays the Connect to Target dialog box, select the Enable multi-path check box, shown in Figure 16.
22. Click OK.
23. Repeat steps 11 to 22 on each remaining cluster node.

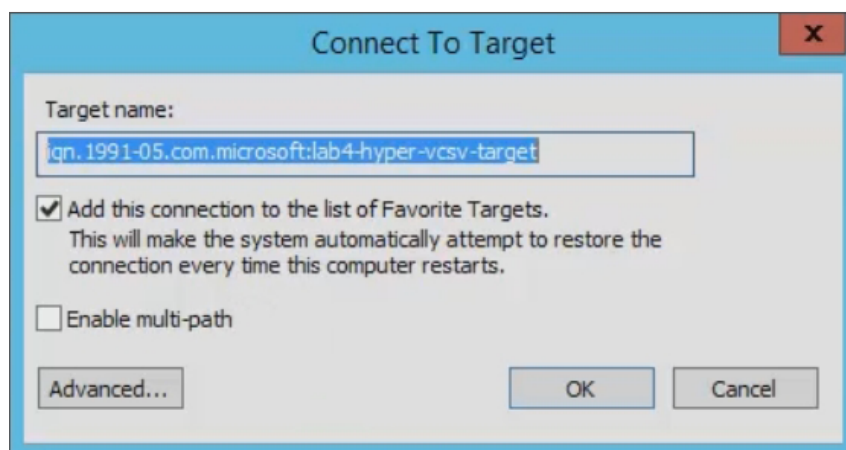


Figure 16. You must select the Enable Multi Path checkbox.

PAINFULLY SLOW FILE COPIES

One problem that many Hyper-V administrators have reported is that of extremely slow file transfers. In some situations, the file transfers can be so slow that the file copy process times out before the file transfer can be complete.

Before you begin diagnosing the file copy process, it is worth noting that the problem may not be related to Hyper-V itself. Slow file copy operations can be caused by any number of factors (such as resource contention, hypervisor level storage throttling, etc.), so it is important to use performance monitoring metrics to determine the underlying cause of the problem prior to trying to make any corrections.

If you do determine that a Hyper-V host or a virtual machine is the source of your file copy performance problems, then there are two things that you should check.

Check for Missing Patches

First, make sure that your Hyper-V servers are running all of the latest patches. Early on, Windows Server 2012 and Windows Server 2012 R2 were plagued by extremely slow file transfers (for certain hardware configurations). It was possible to work around these problems by disabling SMB signing, However, Microsoft eventually corrected that particular problem with a patch.

VMQ Needs to Be Disabled

Another common reason for extremely slow file copy is an incorrectly configured network adapter. In some situations, the Virtual Machine Queue (VMQ) may be enabled by default. When the VMQ feature is enabled, Hyper-V creates a dedicated queue on the physical network adapter for each virtual network adapter that requests a queue ([https://technet.microsoft.com/en-us/library/gg162704\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/gg162704(v=ws.10).aspx)).

According to Microsoft ([https://technet.microsoft.com/en-us/library/gg162704\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/gg162704(v=ws.10).aspx)), virtual machine queues should only be enabled for virtual machines that experience heavy volumes of inbound traffic. More importantly, Microsoft recommends that VMQ be disabled for 1 gigabit Ethernet NICs. Gigabit Ethernet NICs cannot derive any significant benefit from VMQ, and the use of VMQ on such NICs has sometimes been

known to performance and availability issues (<https://www.petri.com/hyper-v-network-issues-1-gbe-nics>).

It is important to note that even if you manually disable VMQ, some vendors automatically re-enable it as a part of the driver update process. Therefore, it is a good idea to check the VMQ status, even if VMQ was previously disabled.

A NIC's virtual machine queue can be disabled by completing the following steps:

1. Open the Device Manager on the Hyper-V Host Server.
2. Expand the Network Adapters container.
3. Right click on the network adapter, and select the Properties command from the shortcut menu, as shown in Figure 17. If the host contains multiple network adapters, then you will need to repeat this process for each adapter.
4. When Windows displays the adapter's Properties sheet, go to the Advanced tab.
5. Locate the setting for the Virtual Machine Queue, as shown in Figure 18, and make sure that the setting is disabled

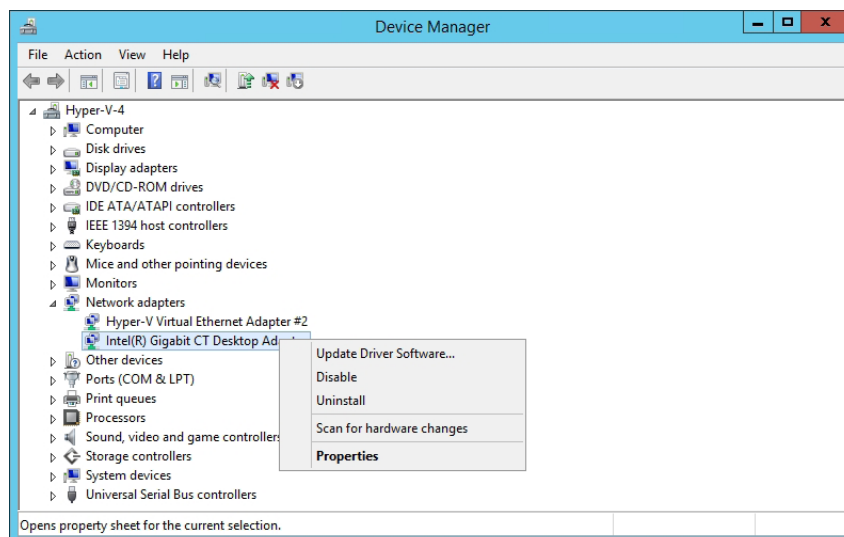


Figure 17. Locate the problematic network adapter within the Device Manager.

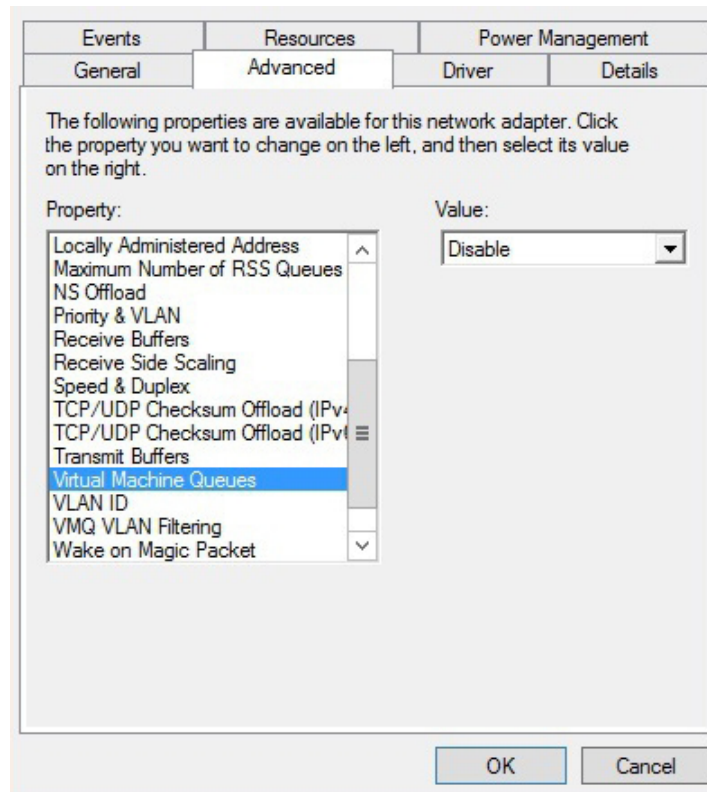


Figure 18 | Locate and disable the virtual machine queue.

If you prefer to use PowerShell, you can check to see whether VMQ is enabled on your network adapters by entering the following command:

`Get-NetAdapterVMQ`

This cmdlet will display the VMQ state for each network adapter, as shown in Figure 19.

If PowerShell reveals that VMQ is enabled for a particular network adapter, and you wish to disable VMQ, then you can do so by using the following command:

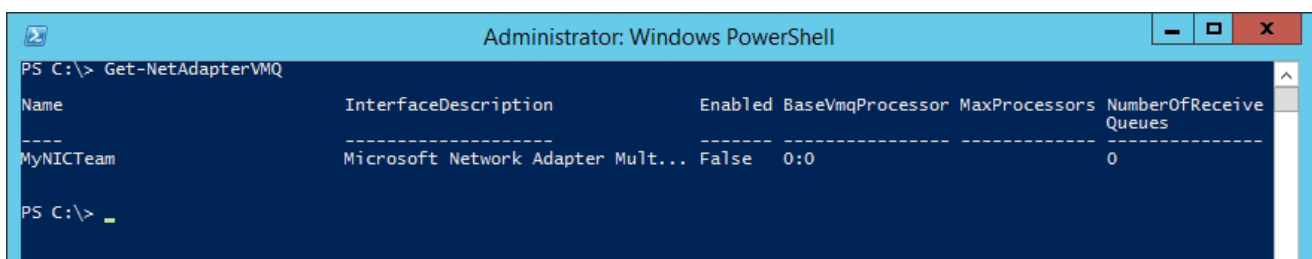
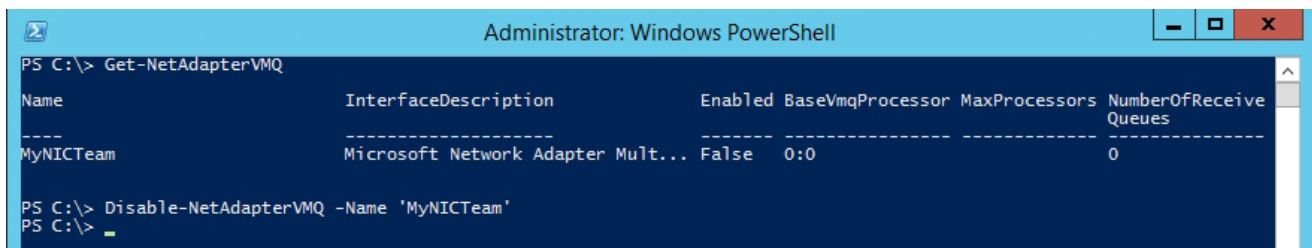


Figure 19. The Get-NetAdapterVMQ cmdlet will display the VMQ state for each network adapter.

```
Disable-NetAdapterVMQ -Name <network adapter name>
```

You will notice that this command requires you to supply the network adapter name. The name of each network adapter is revealed when you enter the Get-NetAdapterVMQ cmdlet. For example, the network adapter shown in the previous figure uses the name MyNICTeam, and that is the name that you would use if you were disabling VMQ for that particular network adapter. Figure 20 shows what this process looks like. In this case, VMQ is already disabled, but you can still see how to use the various commands.



```
Administrator: Windows PowerShell
PS C:\> Get-NetAdapterVMQ
Name                               InterfaceDescription             Enabled BaseVmqProcessor MaxProcessors NumberOfReceiveQueues
----                               -
MyNICTeam                          Microsoft Network Adapter Mult... False 0:0              0

PS C:\> Disable-NetAdapterVMQ -Name 'MyNICTeam'
PS C:\>
```

Figure 20. You can use the `Disable-NetAdapterVMQ` cmdlet to disable VMQ for a specified network adapter.

VIRTUAL MACHINES ARE LISTED AS BEING IN A CRITICAL STATE AND CANNOT BE POWERED ON

Another somewhat common problem that is often storage related involves a situation in which virtual machines cannot be powered on. Although this problem can sometimes be permissions related, it is more often related to the inability of Hyper-V to communicate with the storage on which virtual machine components reside. When this problem occurs, the Hyper-V Manager will hide the option to power on the virtual machine, and will also display a status message indicating that Hyper-V cannot connect to virtual machine storage. You can see an example of such a situation in Figure 21.

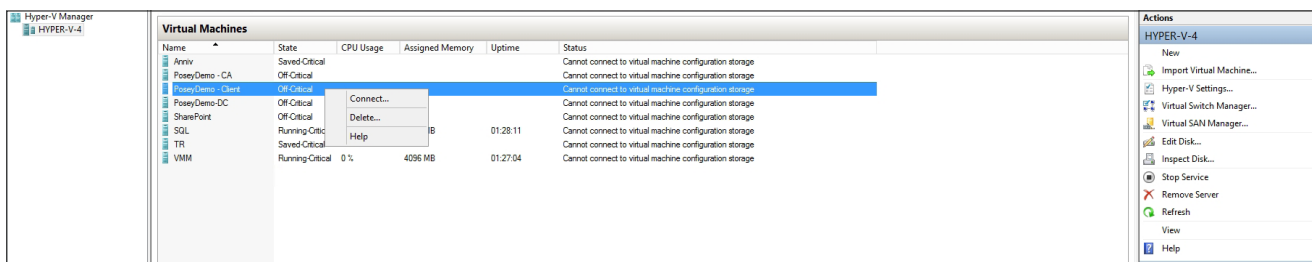


Figure 21. Virtual machines cannot be powered on.

As you look at the figure above, you will notice that some of the virtual machines are listed as being Off-Critical, while others have a state of Saved-Critical. You will also notice that the status indicates that Hyper-V cannot connect to virtual machine configuration storage. This problem can be caused by a storage failure, a storage disconnection, or by a change to a drive mapping. The problem can also stem from storage permissions being changed in a way that prevent Hyper-V from being able to read and write to the storage medium.

In this particular example, the problem was caused by a detached virtual disk within Windows Storage Spaces (not Hyper-V itself). Keep in mind however, that the same problem can occur even if you are not using Storage Spaces. Virtual machines that use Direct Attached Storage (DAS), iSCSI, Fibre Channel, etc., can all experience the same problem if a storage array or the connectivity to that array were to fail.

If you are using Windows Storage Spaces, then the Server Manager will often show you the cause of the problem. If you look at Figure 22 for example, you can see that the virtual disk is displaying a warning, and that right clicking on the disk provides the option to attach the virtual disk.

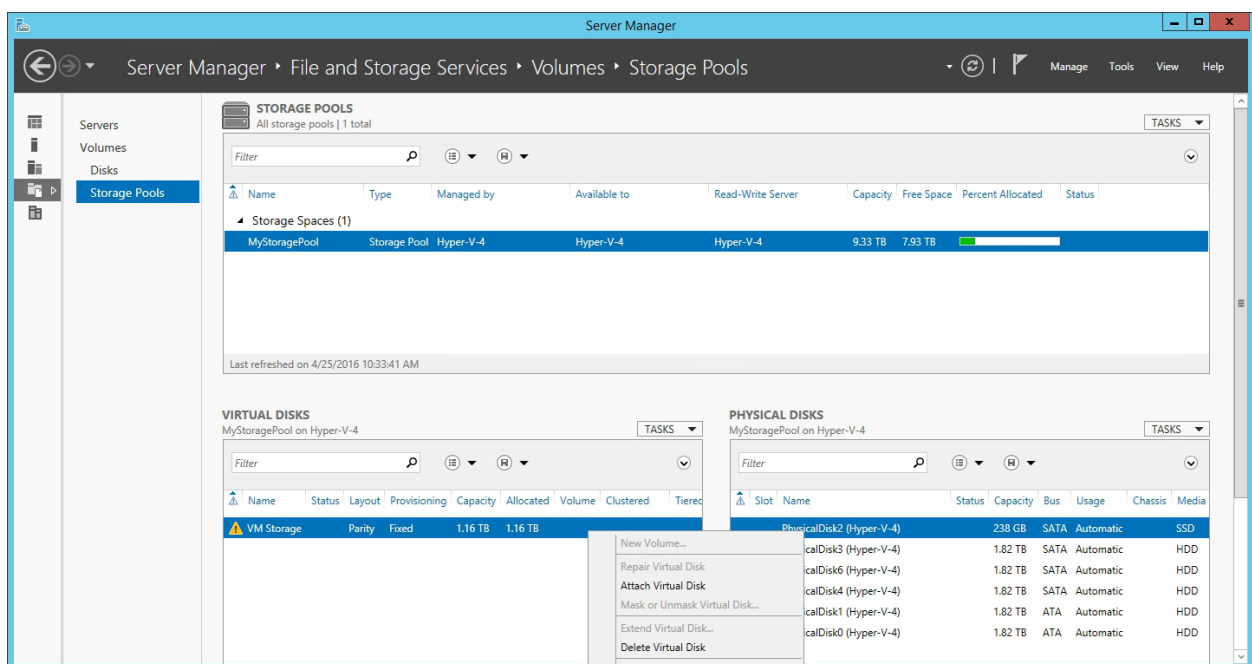


Figure 22. You can use the `Disable-NetAdapterVMQ` cmdlet to disable VMQ for a specified network adapter. The virtual disk that Hyper-V is using for virtual machine storage is detached.

It is worth noting that although a virtual disk can be attached within a matter of a couple of seconds, the Hyper-V virtual machines do not become immediately available. It can take a minute or two for Windows to re-establish the drive mappings for the recently attached virtual disk. Hyper-V will eventually recognize the change and make the virtual machines available (it can take up to about five minutes), but you may be able to speed things up by using the Refresh buttons found within Server Manager and Hyper-V Manager. Similar behavior can be expected when reattaching other forms of storage, even if Windows Storage Spaces is not used. It may take Hyper-V a few minutes to acknowledge that the problem has been fixed.

PERMISSIONS PROBLEMS

Often times problems that occur within Hyper-V can be attributed to permissions problems. These problems may result in Access Denied errors, and a variety of other error messages. In fact, there are too many different types of permissions related errors to be able to list them all here. Even so, the vast majority of these errors can be attributed to one of two things:

- A disconnect between a management tool and Hyper-V in which the management tool lacks the permission to perform the appropriate action
- A permissions problem in which Hyper-V lacks the required access to virtual machine resources.

AN ERROR OCCURRED WHILE ATTEMPTING TO CONNECT TO SERVER

The first type of error that you could potentially receive indicates that an error has occurred while attempting to connect to the server. The actual text of this error message can vary depending on the version of Windows that you are using and on the conditions that caused the error to be displayed, but you can see an example of such an error in Figure 23.

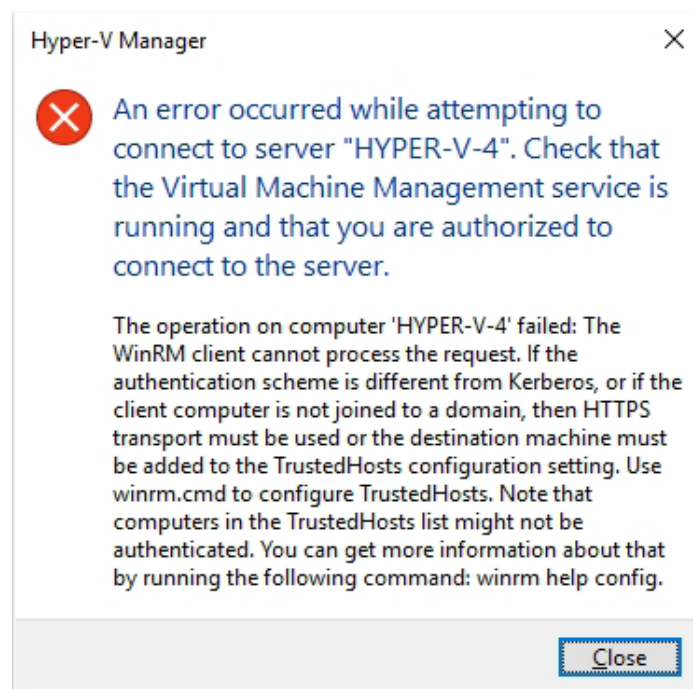


Figure 23. The Hyper-V Manager is unable to connect to Hyper-V.

This error usually occurs when an administrator attempts to access a remote Hyper-V server, but under the right circumstances, it can occur even if the Hyper-V Manager is being run directly on the Hyper-V Server. This error is often related to a permission problem. The administrator who is launching the Hyper-V Manager may lack permissions to the remote Hyper-V server. Before you can assume that a permissions problem is to blame however, you should check three things.

- First, check to be sure that DNS name resolution is working for the Hyper-V server. The client computer that is running the Hyper-V Manager should be able to resolve the remote Hyper-V server by its fully qualified domain name.
- Second, make sure that there are no firewall rules preventing the use of the Hyper-V Manager or System Center Virtual Machine Manager. A list of ports is provided in the next section.
- Third, verify that the Hyper-V Virtual Machine Management service is running on the Hyper-V Server. You can check the status of this service by entering Services.msc at the server's Run prompt. You can see what this looks like in Figure 24.

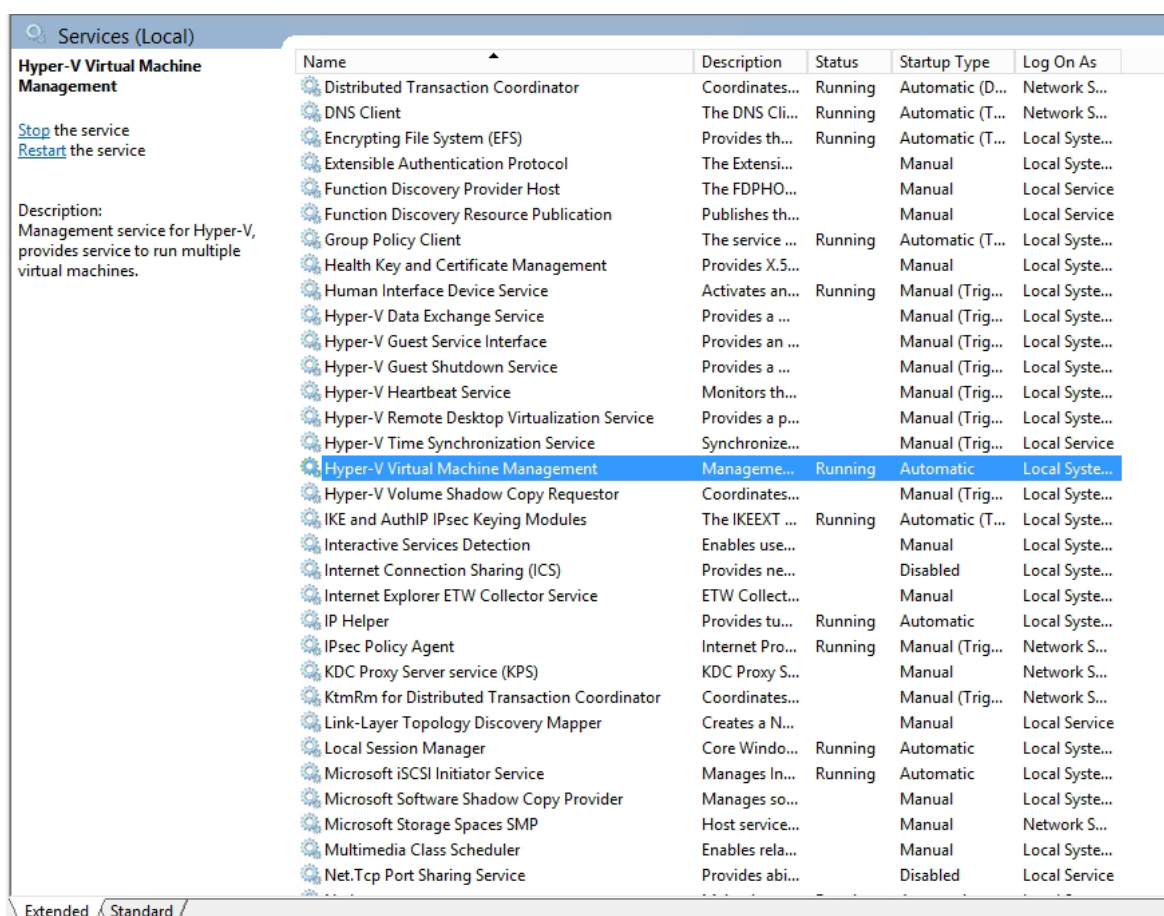


Figure 24. Make sure that the Hyper-V Virtual Machine Management Service is running.

If you prefer to check this service by using PowerShell, you can do so by entering this command:

```
Get-Service VMMS
```

If you find the service to be stopped, then you can start the service by entering this command:

```
Start-Service VMMS
```

You can see these commands being used in Figure 25.

```
PS C:\> Get-Service VMMS
Status      Name          DisplayName
-----
Stopped    VMMS          Hyper-V Virtual Machine Management

PS C:\> Start-Service VMMS
PS C:\> Get-Service VMMS
Status      Name          DisplayName
-----
Running     VMMS          Hyper-V Virtual Machine Management

PS C:\> _
```

Figure 25. You can use PowerShell to start the Hyper-V Virtual Machine Management Service.

Firewall Ports

As previously mentioned, an incorrectly configured firewall can make it impossible to remotely manage a Hyper-V host. The firewall ports that are required vary depending on whether you are using the Hyper-V Manager or System Center Virtual Machine Manager. The sections below list the required firewall ports.

Hyper-V Ports: Hyper-V uses the following firewall ports:

Hyper-V WMI (Async-In)	TCP	Any
Hyper-V WMI (DCOM-In)	TCP	135
Hyper-V WMI (TCP-In)	TCP	Any
Hyper-V (MIG-TCP-In)	TCP	6600
Hyper-V (REMOTE_DESKTOP_TCP_IN)	TCP	2179
Hyper-V (RPC)	TCP	RPC Dynamic Ports
Hyper-V (RPC-EPMAP)	TCP	RPC Endpoint Mapper
Hyper-V Management Clients – WMI (Async-In)	TCP	Any
Hyper-V Management Clients – WMI (DCOM-In)	TCP	135
Hyper-V Management Clients – WMI (TCP-In)	TCP	Any
Hyper-V Replica HTTP Listener (TCP-In)	TCP	80
Hyper-V Replica HTTPS Listener (TCP-In)	TCP	443

You can see a listing of Microsoft’s firewall rules for Hyper-V in Figure 26.

Hyper-V - WMI (Async-In)	Hyper-V	All	Yes	Allow	No	%system...	Any	Any	TCP	Any
Hyper-V - WMI (DCOM-In)	Hyper-V	All	Yes	Allow	No	%System...	Any	Any	TCP	135
Hyper-V - WMI (TCP-In)	Hyper-V	All	Yes	Allow	No	%System...	Any	Any	TCP	Any
Hyper-V (MIG-TCP-In)	Hyper-V	All	Yes	Allow	No	%system...	Any	Any	TCP	6600
Hyper-V (REMOTE_DESKTOP_TCP_IN)	Hyper-V	All	Yes	Allow	No	%system...	Any	Any	TCP	2179
Hyper-V (RPC)	Hyper-V	All	Yes	Allow	No	System	Any	Any	TCP	RPC Dynamic Ports
Hyper-V (RPC-EPMAP)	Hyper-V	All	Yes	Allow	No	System	Any	Any	TCP	RPC Endpoint Mapper
Hyper-V Management Clients - WMI (Async-In)	Hyper-V Management Clients	All	Yes	Allow	No	%system...	Any	Any	TCP	Any
Hyper-V Management Clients - WMI (DCOM-In)	Hyper-V Management Clients	All	Yes	Allow	No	%System...	Any	Any	TCP	135
Hyper-V Management Clients - WMI (TCP-In)	Hyper-V Management Clients	All	Yes	Allow	No	%System...	Any	Any	TCP	Any
Hyper-V Replica HTTP Listener (TCP-In)	Hyper-V Replica HTTP	All	Yes	Allow	No	System	Any	Any	TCP	80
Hyper-V Replica HTTPS Listener (TCP-In)	Hyper-V Replica HTTPS	All	Yes	Allow	No	System	Any	Any	TCP	443

Figure 26. These are the Hyper-V related firewall rules that exist within Windows Server 2012 R2.

System Center Virtual Machine Manager Ports: Microsoft defines a separate list of firewall ports for use with System Center 2012 R2 Virtual Machine Manager. These ports are outlined in a TechNet article at: <https://technet.microsoft.com/en-us/library/cc764268.aspx> The required ports are:

Connection type	Protocol	Default port
VMM server to VMM agent on Windows Server-based host (control)	WS-Management	80
VMM server to VMM agent on Windows Server-based host (file transfers)	HTTPS (using BITS)	443 (Maximum value: 32768)
VMM server to remote Microsoft SQL Server database	TDS	1433
VMM server to P2V source agent	DCOM	135
VMM Administrator Console to VMM server	WCF	8100
VMM Self-Service Portal Web server to VMM server	WCF	8100
VMM Self-Service Portal to VMM self-service Web server	HTTPS	443
VMM library server to hosts	BITS	443 (Maximum value: 32768)
VMM host-to-host file transfer	BITS	443 (Maximum value: 32768)
VMRC connection to Virtual Server host	VMRC	5900
VMConnect (RDP) to Hyper-V hosts	RDP	2179
Remote Desktop to virtual machines	RDP	3389
VMware Web Services communication	HTTPS	443
SFTP file transfer from VMWare ESX Server 3.0 and VMWare ESX Server 3.5 hosts	SFTP	22
SFTP file transfer from VMM server to VMWare ESX Server 3i hosts	HTTPS	443

Addressing Permissions Problems

Assuming that DNS name resolution is configured correctly, the correct firewall ports are open, and the Hyper-V Virtual Machine Management Service is running, then issues with accessing Hyper-V from the Hyper-V Manager are probably going to be permissions related. To correct the problem (in a non-domain environment), you will need to use the Component Services tool (Dcomcnfg.exe). The reason why you will need to use this tool is because permissions are applied at the Component Object Model (COM) level, and the Component Services tool allows you to modify COM level permissions.

You can modify the COM permissions by completing these steps:

1. Close the Hyper-V Manager.
2. On the client computer, open File Explorer and navigate to C:\Windows\System32.

3. Right click on the Dcomcnfg.exe file, and choose the Run as Administrator command from the shortcut menu. Remember that file extensions are hidden by default, so don't accidentally use the Dcomcnfg.exe.mui file. Provide administrative credentials if required.
4. When Windows launches the Component Services window, double-click the Computer container to reveal the My Computer container beneath it.
5. Right click on My Computer, shown in Figure 27, and select the Properties command from the shortcut menu.

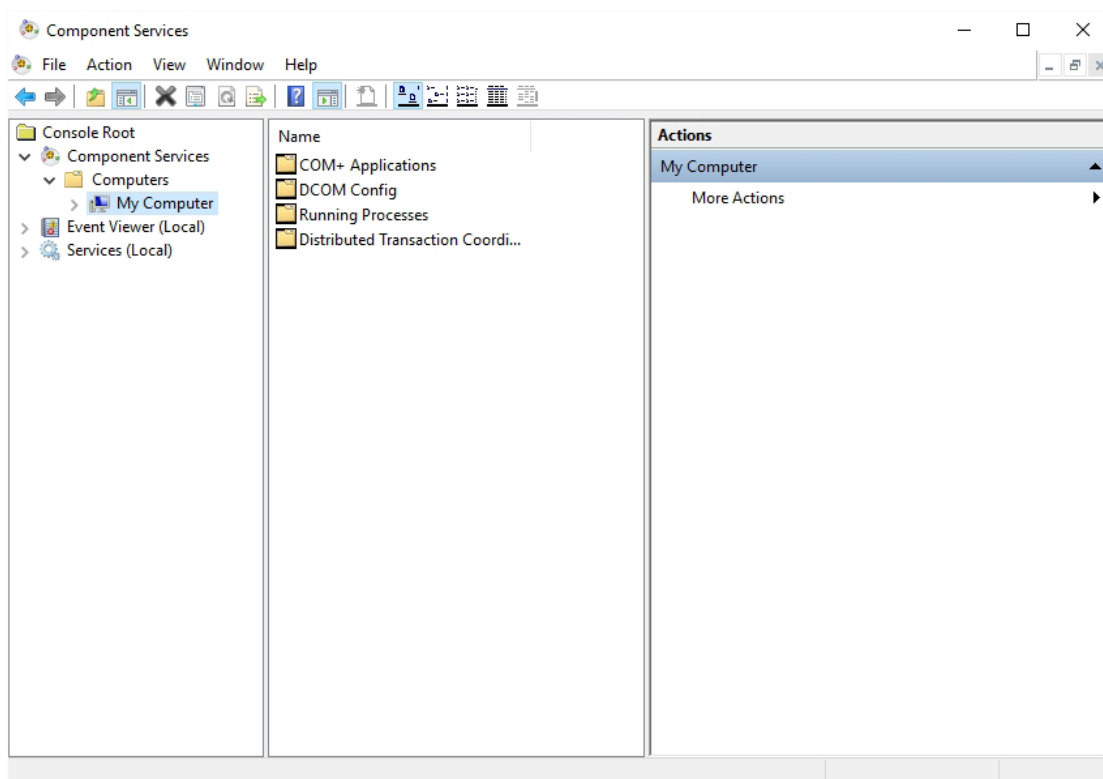


Figure 27. Right click on the My Computer container.

6. Select the COM Security tab.
7. Locate the Access Permissions section, and click the Edit Limits button, shown in Figure 28.

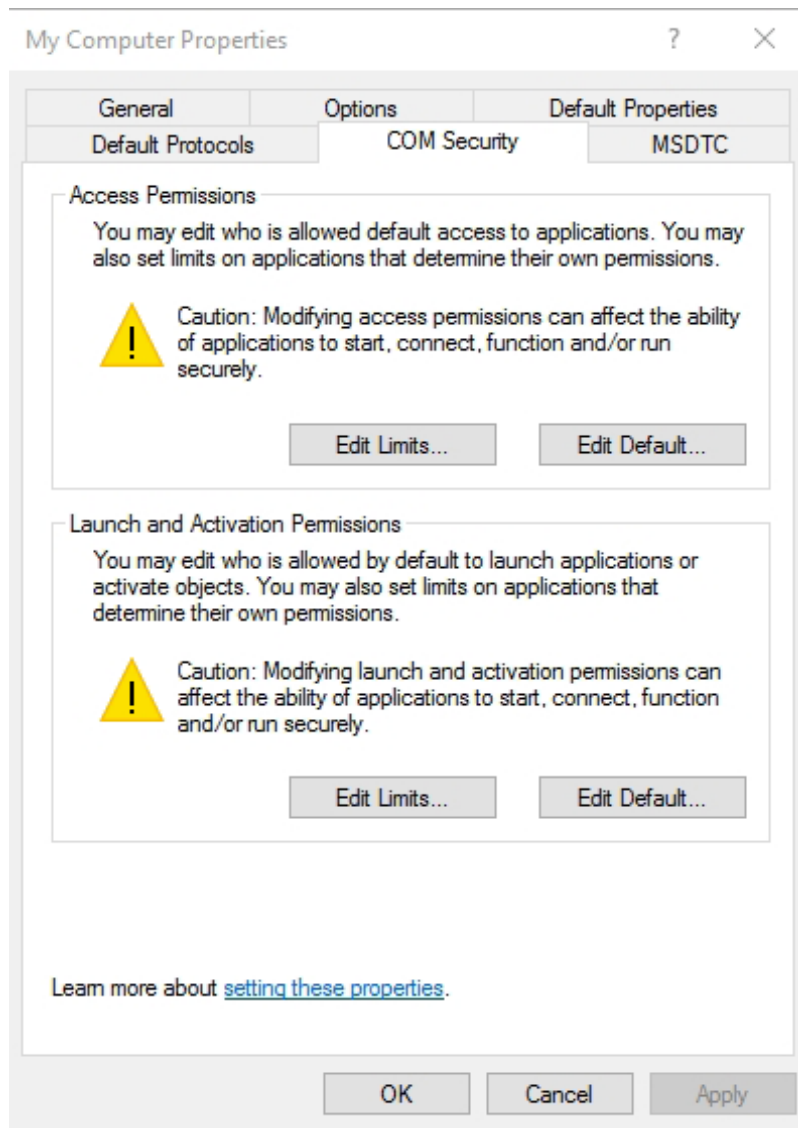


Figure 28. Locate the Access Permissions section, and click the Edit Limits button.

8. Check to see if Anonymous Login currently exists on the Default Security list. If it does not exist, then click the Add button, type Anonymous, and click OK
9. Select the Enable checkbox for Remote Access for Anonymous Logon option, as shown in Figure 29.
10. Click Apply, followed by OK.

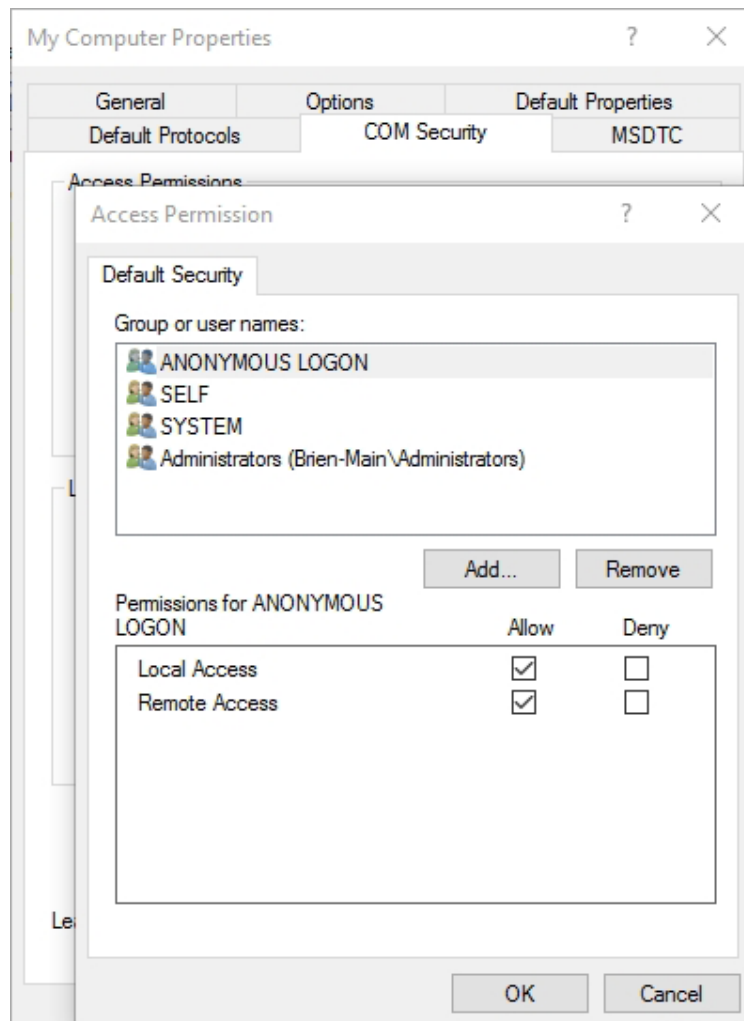


Figure 29. Enable anonymous remote access.

It is worth noting that although this technique works, it does decrease security. It is best to avoid using this technique if possible. For example, rather than running the Hyper-V Manager from a non-domain joined workstation (on which this fix would most likely be required), an administrator might instead opt to use a domain joined workstation, or establish an RDP session to a Hyper-V Server and run the Hyper-V Manager from there.

INADEQUATE RUNAS PERMISSIONS

If you are using System Center Virtual Machine Manager for Hyper-V Management, then access denied errors can sometimes occur as a result of a RunAs account that has been removed, disabled, or that lacks the appropriate permissions. When an administrator performs an action within System Center Virtual Machine Manager, the server treats the action as a scheduled job, even if the action is to occur immediately. As such, many actions require the use of a RunAs account. This account's permissions are used in place of the administrator's permissions. You can check for the existence of a RunAs account by completing these steps:

1. Open the Virtual Machine Manager console.
2. Select the Settings workspace.
3. Select the Run As Accounts container.
4. Verify that your RunAs account is listed, as shown in Figure 30. If the account is not listed, then click on the Create Run As Account icon, located on the toolbar, and follow the prompts to select an Active Directory account to be used as a RunAs account. If your RunAs account is already listed, but does not seem to be functioning correctly, then you might try removing the account from the list of RunAs accounts, and then adding it back.

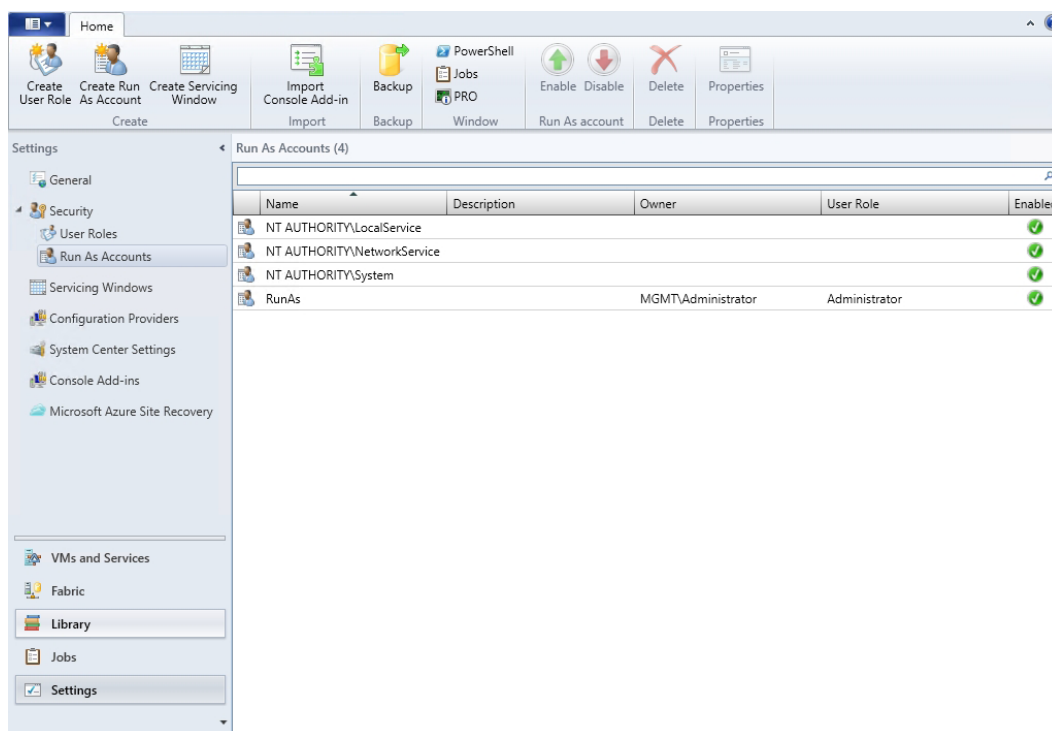


Figure 30. Make sure that your RunAs account appears on the list of RunAs accounts.

LIVE MIGRATION FAILURE

One of the more common Hyper-V problems involves the inability to live migrate a virtual machine from one host to another. There are countless issues that can cause live migrations to fail, but the three most common are:

- Missing permissions
- An Incorrect Authentication Protocol
- Mix Matched Configurations

MISSING PERMISSIONS

Administrators must give Hyper-V hosts permission to receive inbound live migrations. To verify that the necessary permissions are in place, complete the following steps:

1. Open the Hyper-V Manager on the receiving host.
2. Right click on the server name (within the console tree) and choose the Hyper-V Settings command from the resulting shortcut menu.
3. When Windows displays the Hyper-V Settings dialog box, select the Live Migrations container, shown in Figure 31.
4. Make sure that the Enable Incoming and Outgoing Live Migrations checkbox is selected.
5. Make sure that the Simultaneous Live Migrations number is set to an appropriate level, and that live migrations are not failing simply because too many concurrent live migrations are taking place.
6. Check the Incoming Live Migrations list for any restrictions that might cause live migrations to fail.
7. Repeat the process for the host containing the virtual machine that needs to be moved.

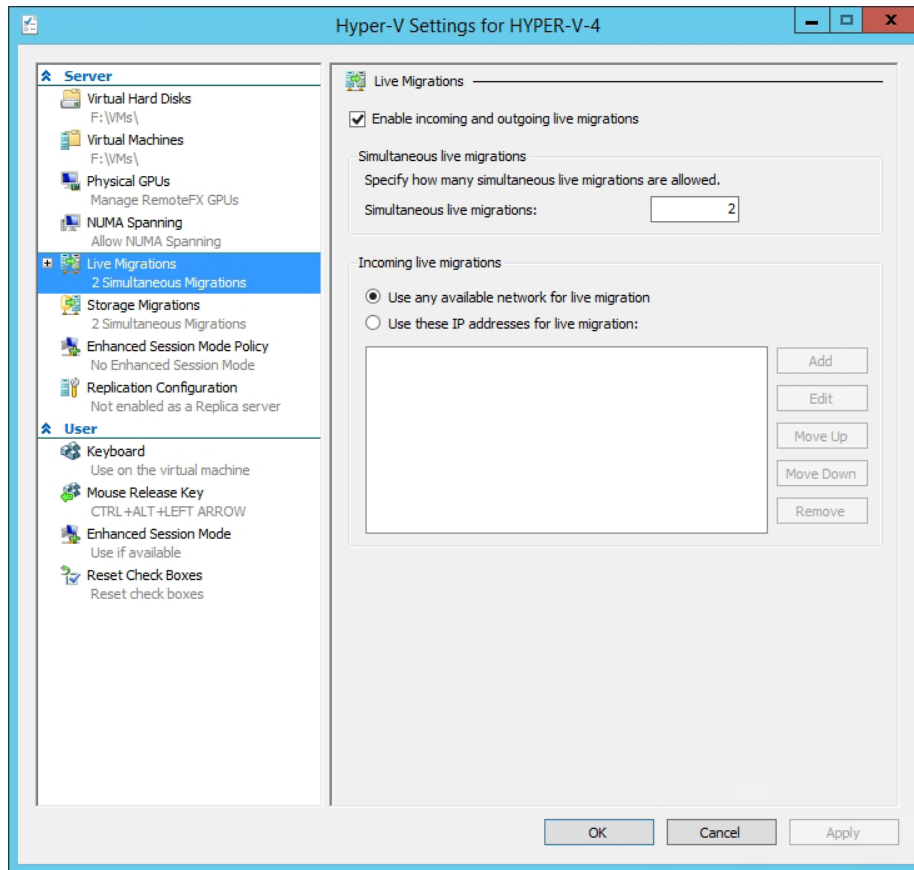


Figure 31. Make sure that live migrations are enabled.

As an alternative, you can use PowerShell to check to see if live migration is enabled. The command used for doing so is:

```
(Get-VMHost <virtual machine name>).  
VirtualMachineMigrationEnabled
```

If live migration is enabled, then this command should return a value of True, as shown in Figure 32.

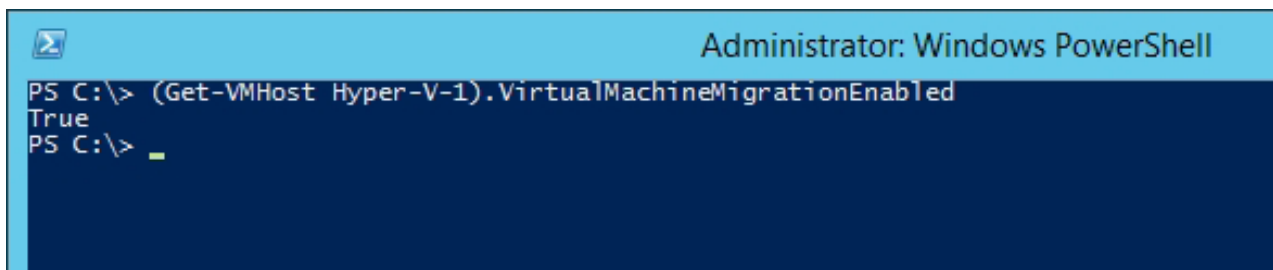


Figure 32. You can use PowerShell to check to see if live migration is enabled for a host.

If you need to enable live migration, you can do so by using the Enable-VMMigration cmdlet. You will typically also need to configure the migration network and the migration protocol (the migration protocol will be discussed in the next section). The commands used for these steps are:

```
Enable-VMMigration
Set-VMMigrationNetwork <network IP>
Set-VMHost -VirtualMachineMigrationAuthenticationType
<authentication protocol>
```

AN INCORRECT AUTHENTICATION PROTOCOL

An administrator's choice of authentication protocol can cause live migrations to fail. The source and destination servers must use the same authentication protocol, but there is more to it than that.

Hyper-V gives you two authentication protocol choices – CredSSP and Kerberos. The CredSSP protocol has a hop count limit of one. This limitation means that if the CredSSP protocol is being used, then you must be initiating the live migration locally on the Hyper-V server that contains the virtual machine that you want to live migrate. If you are using CredSSP and initiate live migration from another host, then the live migration will fail.

The Kerberos protocol is much more flexible, and more secure. However, Microsoft recommends enabling constrained delegation if you are going to use Kerberos. You can verify a Hyper-V server's live migration authentication protocol by completing these steps:

1. Open the Hyper-V Manager.
2. Right click on the Hyper-V server within the console tree, and choose the Hyper-V Settings command.
3. When Windows opens the Hyper-V Settings dialog box, select expand the Live Migrations container.

4. Select the Advanced Features container, as shown in Figure 33.
5. Make note of the authentication protocol that is being used, and change the protocol if necessary

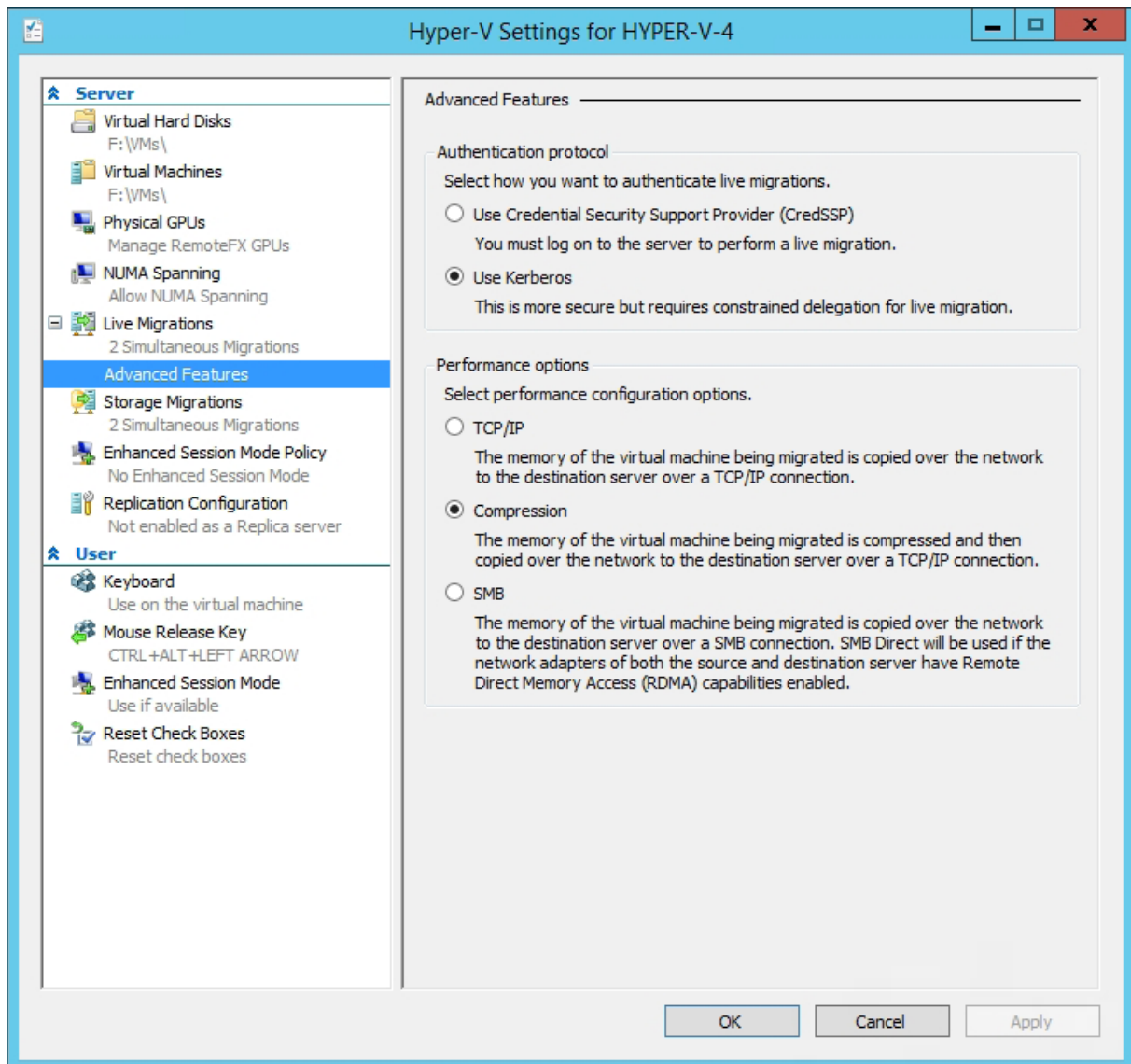
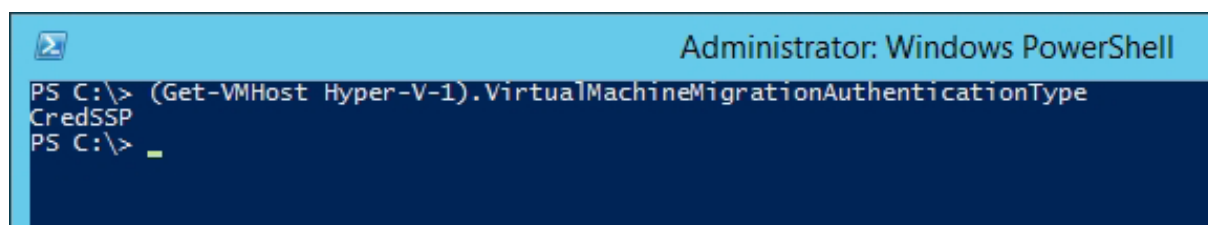


Figure 33. The Authentication Protocol options exist on the Advanced Features container.

If you prefer, you can verify the live migration authentication type using PowerShell. The command for doing so is:

```
(Get-VMHost <virtual machine name>).  
VirtualMachineMigrationAuthenticationType
```

As you can see in Figure 34, this command causes the authentication protocol to be displayed.



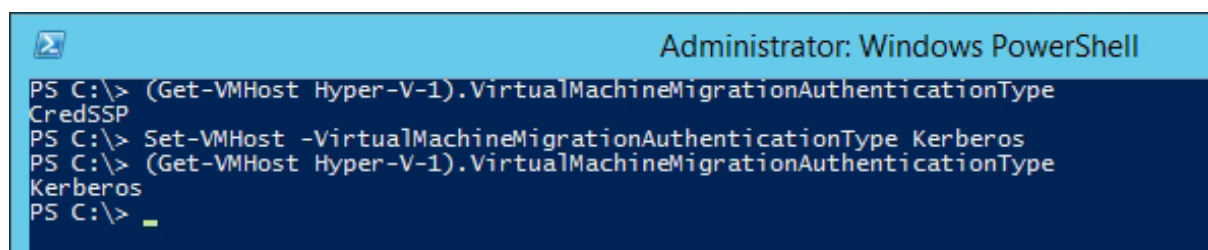
```
Administrator: Windows PowerShell
PS C:\> (Get-VMHost Hyper-V-1).VirtualMachineMigrationAuthenticationType
CredSSP
PS C:\> _
```

Figure 34. PowerShell can tell you which authentication protocol is being used for live migrations.

If you need to switch to a different authentication protocol, then you can do so by using this command:

```
Set-VMHost -VirtualMachineMigrationAuthenticationType
<authentication protocol>
```

Figure 35 shows the process of switching from CredSSP authentication to Kerberos authentication.



```
Administrator: Windows PowerShell
PS C:\> (Get-VMHost Hyper-V-1).VirtualMachineMigrationAuthenticationType
CredSSP
PS C:\> Set-VMHost -VirtualMachineMigrationAuthenticationType Kerberos
PS C:\> (Get-VMHost Hyper-V-1).VirtualMachineMigrationAuthenticationType
Kerberos
PS C:\> _
```

Figure 35. You can use PowerShell to change the live migration authentication type.

MISMATCHED CONFIGURATIONS

There is no rule that says that your Hyper-V servers must be identical in every way, but if you are going to be performing a live migration then the source and destination must be similar enough to allow for a successful migration.

CPU Mismatches

The hardware component that tends to cause the most problems with live migrations is the CPU. If your source and destination servers contain different CPU architectures, then you can sometimes force a live migration to succeed by disabling advanced CPU features. Depending on the hardware that you are using, it may be possible to re-enable the advanced CPU features once the live migration is complete.

You can disable a virtual machine's advanced CPU features by following these steps:

1. Open the Hyper-V Manager.
2. Right click on a virtual machine and choose the Settings command from the shortcut menu.
3. Expand the Processor container.
4. Select the Compatibility container.
5. Select the Migrate to a Physical Computer with a Different Processor Version checkbox, as shown in Figure 36

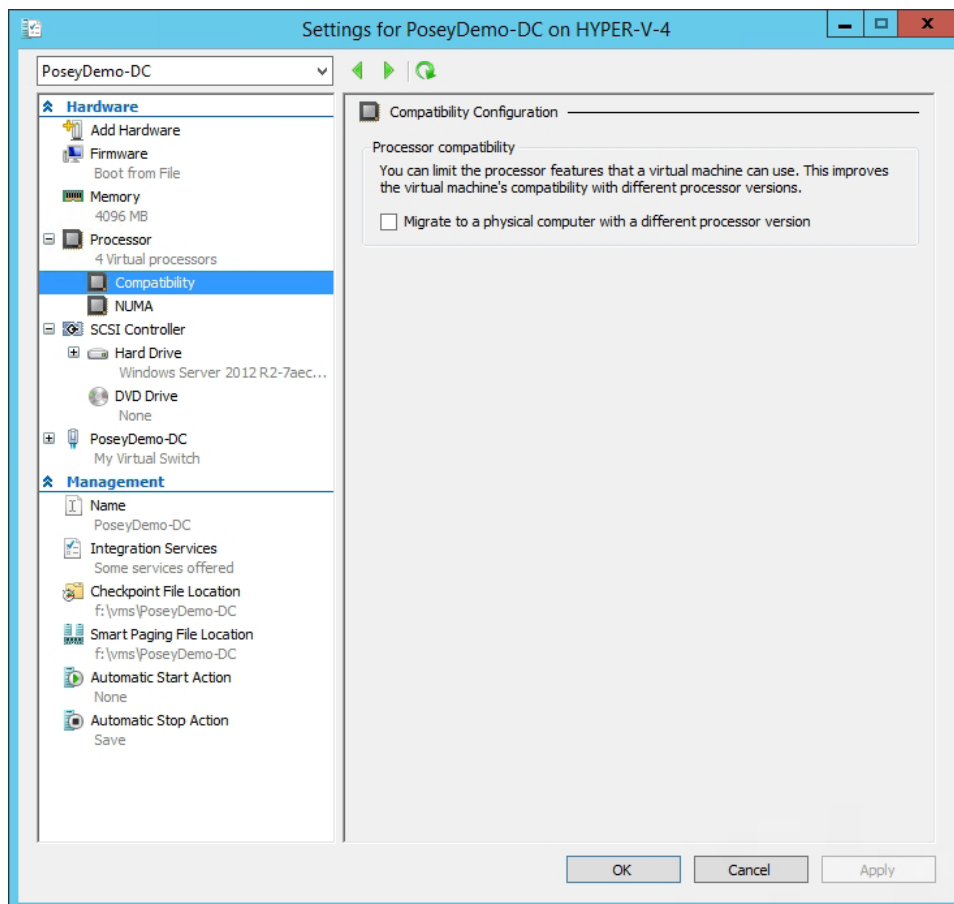


Figure 36. Select the Migrate to a Physical Computer with a Different Processor Version checkbox to disable the CPU's advanced features.

Virtual Switch Mismatches

Depending on which tool is being used to perform a live migration, live migrations can also fail if the source and destination servers do not contain identically named virtual switches. You can verify a virtual machine's virtual switch name by completing these steps:

1. Open the Hyper-V Manager.
2. Right click on a virtual machine and choose the Settings command from the shortcut menu.
3. Select the Network Adapter tab, shown in Figure 37.
4. Make note of the virtual switch name.
5. Create an identically named virtual switch on the destination host if necessary.

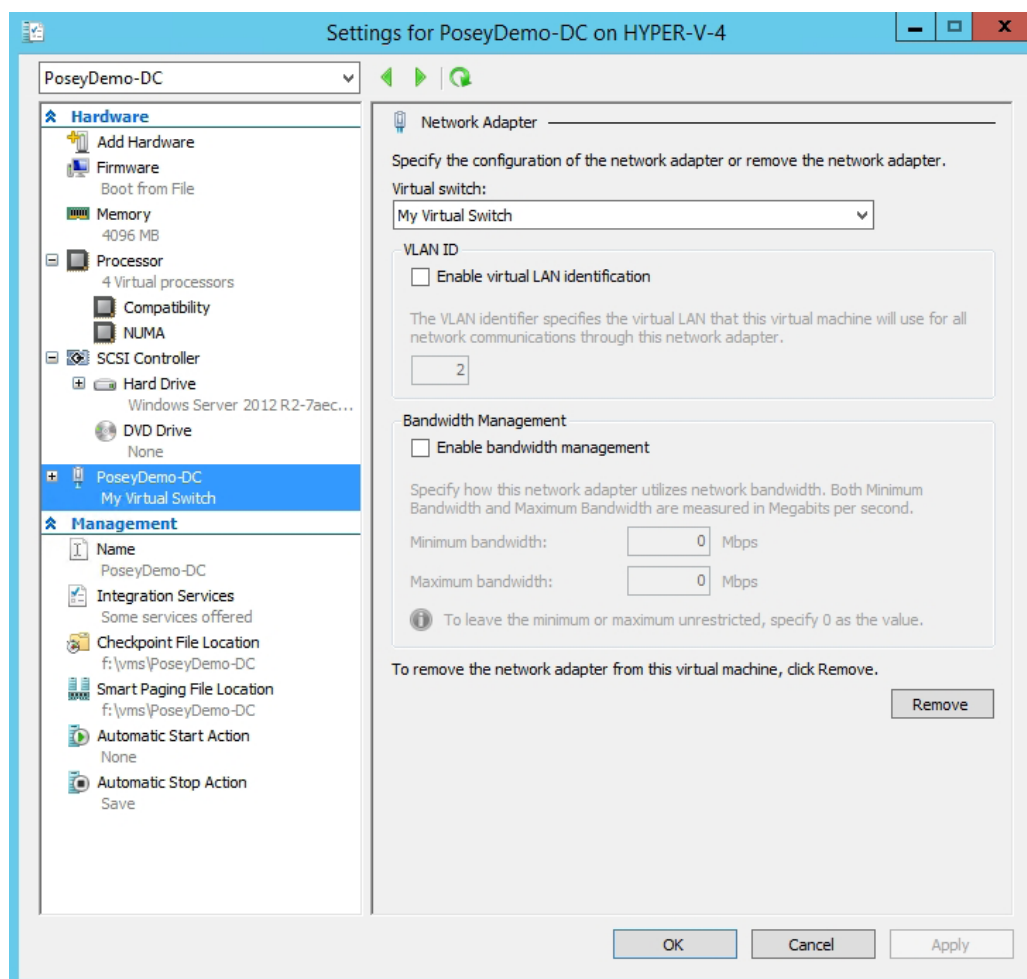
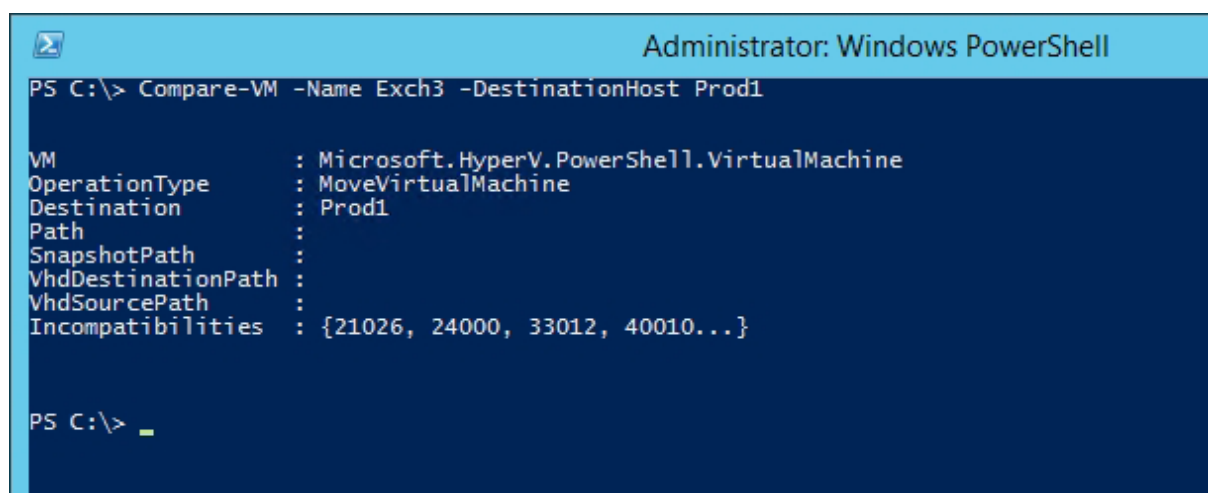


Figure 37. Make note of the virtual switch name, and create an identically named virtual switch on the destination host if necessary.

If you prefer to use PowerShell, then you can use the Compare-VM cmdlet to test the suitability of a Hyper-V host to receive a particular virtual machine. This cmdlet requires you to provide the virtual machine name and the name of the destination host. The syntax for this command is:

```
Compare-VM -Name <virtual machine name> -DestinationHost  
<destination Hyper-V host server name>
```

Figure 38 shows an example of how this command can be used.



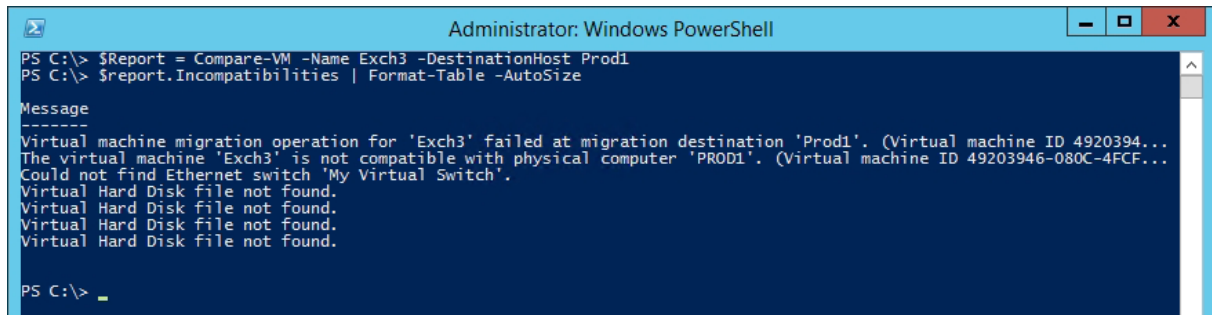
```
Administrator: Windows PowerShell  
PS C:\> Compare-VM -Name Exch3 -DestinationHost Prod1  
  
VM : Microsoft.HyperV.PowerShell.VirtualMachine  
OperationType : MoveVirtualMachine  
Destination : Prod1  
Path :  
SnapshotPath :  
VhdDestinationPath :  
VhdSourcePath :  
Incompatibilities : {21026, 24000, 33012, 40010...}  
  
PS C:\> _
```

Figure 38. You can use the Compare-VM cmdlet to check Hyper-V's ability to live migrate a virtual machine.

As you can see in the figure above, Compare-VM reported some errors, but those errors are in numerical form, and require further explanation. To get an explanation of errors that you might receive, enter the following commands:

```
$Report = Compare-VM -Name <virtual Machine Name>  
-DestinationHost <Hyper-V Destination Host Server>  
$Report.Incompatibilities | Format-Table -AutoSize
```

You can see an example of the output from these commands in Figure 39. In this particular case, there are two main problems occurring. First, the destination server does not contain a virtual switch with a name that matches that of the virtual switch that is currently being used by the VM. Second, four virtual hard disks cannot be found. The virtual hard disk errors are occurring because some of the virtual hard disks that the virtual machine is configured to use have been intentionally deleted for the sake of demonstration.



```
Administrator: Windows PowerShell
PS C:\> $Report = Compare-VM -Name Exch3 -DestinationHost Prod1
PS C:\> $report.Incompatibilities | Format-Table -AutoSize

Message
-----
Virtual machine migration operation for 'Exch3' failed at migration destination 'Prod1'. (Virtual machine ID 4920394...
The virtual machine 'Exch3' is not compatible with physical computer 'PROD1'. (Virtual machine ID 49203946-080C-4FCF...
Could not find Ethernet switch 'My Virtual Switch'.
Virtual Hard Disk file not found.
Virtual Hard Disk file not found.
Virtual Hard Disk file not found.
Virtual Hard Disk file not found.
PS C:\> _
```

Figure 39. This is what an incompatibility report looks like.

BACKUP RELATED PROBLEMS

Many of the commonly reported Hyper-V problems are related to an inability to back up Hyper-V virtual machines. Hyper-V can be backed up at the host level or at the guest level. Host level backups are generally the preferred method of backing up Hyper-V, because they occur at the Hyper-V Layer, which allows for more efficient backup operations, and removes the need for software agents. However, It is worth noting, that it is still relatively common to see backup vendors still focused on backing up Hyper-V virtual machines from within the guest, via a software agent. Let's cover each scenario briefly

Guest level backups are made at the virtual machine level, and usually involve installing a backup agent directly onto the virtual machine. Although guest level backups do have their place, there are also some disadvantages to using them. One disadvantage is that guest level backups can be more difficult to manage than host level backups, because most organizations have far more virtual machines than Hyper-V hosts.

A second disadvantage to guest level backups is that the backup application backs up the virtual machine contents, not the full virtual machine. In other words, the backup application will back up the contents of the virtual machine's virtual hard disk, but does not back up external virtual machine components such as checkpoints or hardware configurations. The reason for this is that the backup agent is running inside of a virtual machine, and is therefore unaware of that the operating system is running on virtual hardware.

When a backup application performs a host level backup, there are two methods that are commonly used to back up the virtual machines. One method is known as the saved state method. The backup application momentarily places the virtual machine into a saved state and then creates a checkpoint. Once the checkpoint has been created, the virtual machine is returned to a running state and a backup is created. The checkpoint allows the backup software to back up the virtual machine without having to worry that the virtual hard disk contents will be modified before the backup can be completed. After the backup completes, the checkpoint is deleted.

The other backup method is known as the Child VM Snapshot Method. This method also relies on the use of checkpoints, but is the preferred backup method because it does not require the virtual machine to be placed into a saved state. This method uses the Volume Shadow Copy Services (VSS) to back up a virtual machine. VSS will be discussed in the next section.

It is worth noting that a backup operator will not typically be asked to choose between backup methods. The backup software examines each virtual machine to see if it meets the criteria for a Child VM Snapshot Backup. If the criteria cannot be met, then a Saved State backup is created instead. It is normal for some virtual machines to be backed up using the Child VM Snapshot Method while others are backed up using the Saved State method.

There are a number of criteria that must be met if a virtual machine is to be backed up using the Child VM Snapshot Method:

- The Backup (Volume Checkpoint) Integration Service must be running on the virtual machine. The Integration Services are a collection of drivers that allow the virtual machine to communicate with the hypervisor. The Integration Services can be enabled or disabled individually, as shown in Figure 40.

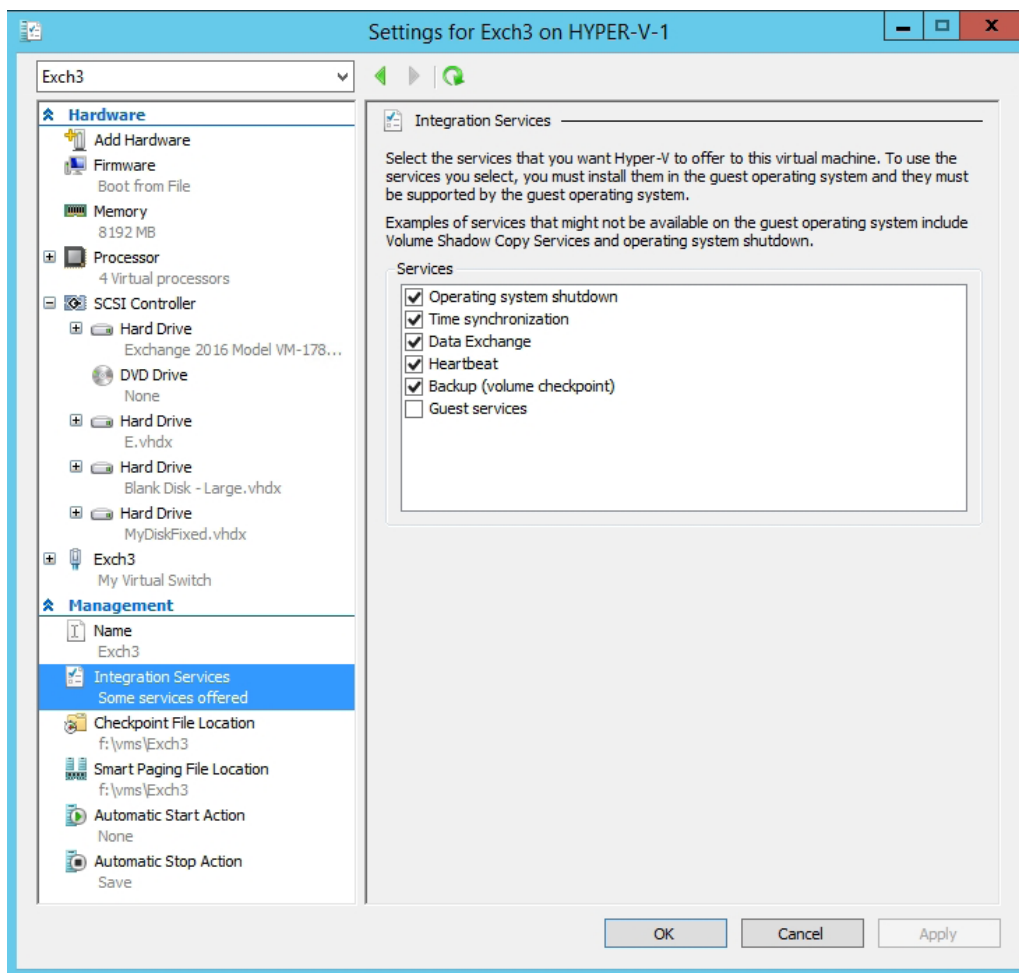


Figure 40. The Backup (Volume Checkpoint) integration service must be enabled.

- The virtual machine must be configured to store checkpoints on the same physical volume as the virtual machine's virtual hard disk. As you can see in the previous figure, each virtual machine's Settings dialog box includes a Checkpoint File Location container. You can compare this container's location to that of the virtual machine's virtual hard disk.
- The virtual machine must be configured to treat its storage as basic disks rather than dynamic disks. The virtual machine's virtual hard disks must also be formatted using a file system such as NTFS that supports the use of checkpoints. This requirement isn't a reference to dynamic disks or to thin provisioning, but rather to the way that the guest operating system uses the virtual hard disk. If you enter the DiskMgmt.msc command at a guest operating system's Run prompt, Windows will open the Disk Management Console. This console shows you whether each disk is configured as Basic or Dynamic, as shown in Figure 41. As you can see in the figure, the Disk Management Console also shows the file system that is being used on each volume.
- The virtual machine must be in a running state. If the virtual machine is paused or powered off, then a Saved State backup will be created.

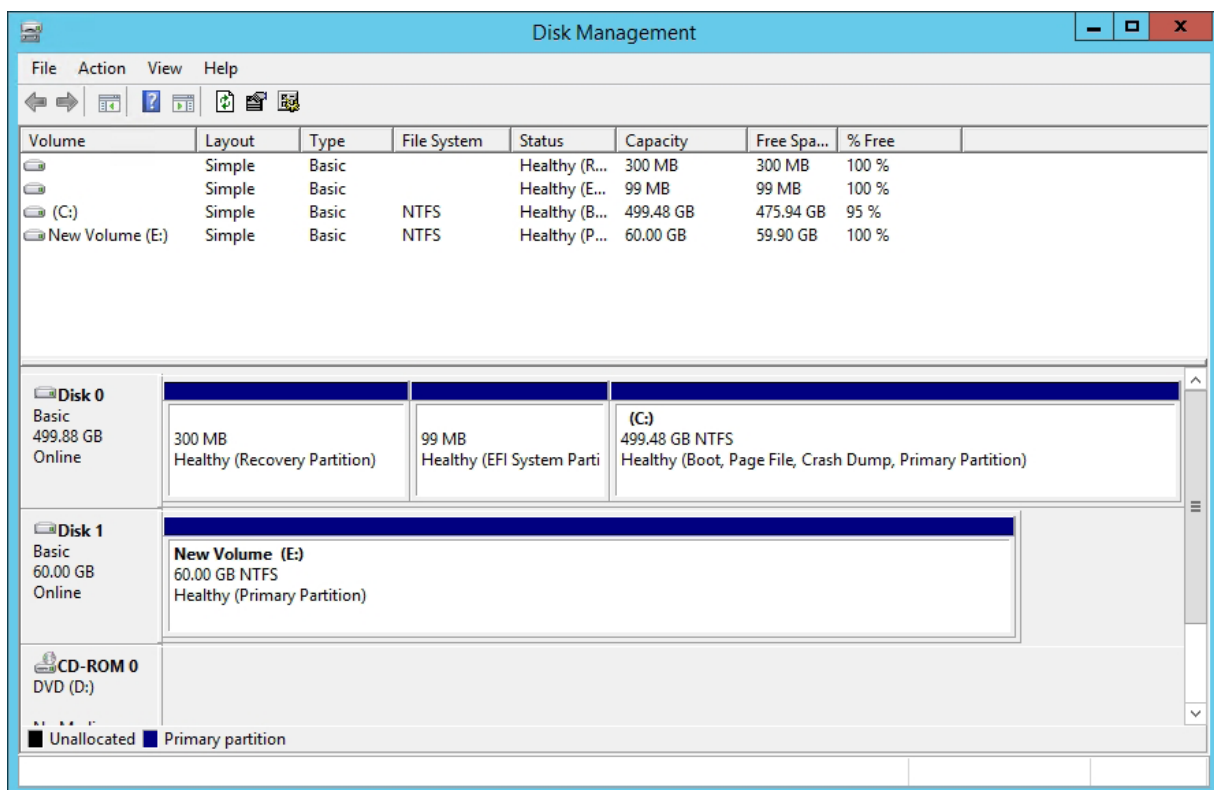


Figure 41. The Disk Management Console will show you the guest operating system's storage configuration.

The Anatomy of the Volume Shadow Copy Service

The Volume Shadow Copy Services (VSS), which is the mechanism used to create Child VM Snapshot Backups, make use of three main parts. These parts include:

- The VSS Writer- Each VSS aware application includes its own VSS writer. The VSS writer is the component that tells the backup software how to back up the application.
- The VSS Requestor – The VSS requestor is the component that initiates the backup process. The VSS requestor is almost always integrated into a backup application.
- The VSS Provider – The VSS Provider is provider functions similarly to a device driver, in that it allows the VSS process to work with the system’s hardware and operating system. Windows allows for the use of operating system providers and hardware providers.

The VSS Requestor (the backup application) initiates the backup process. The requestor announces to the server that it needs to create a snapshot. It then queries the server to determine which VSS writers are installed. Each VSS aware application has its own writer. The requestor then instructs each writer to prepare for a backup. The writers perform a quiescence, in order to in order to get the data ready to be backed up. Once this process is complete, the VSS requestor instructs each writer to create a snapshot. Once this process has finished, the provider tells the requestor where to locate the data for use in the backup process. When the backup finishes, the VSS requestor informs the VSS writers that the backup is complete, and the writers will then perform any required post-backup tasks, and then allow the server to resume normal operations. You can see a diagram of this process in Figure 42.

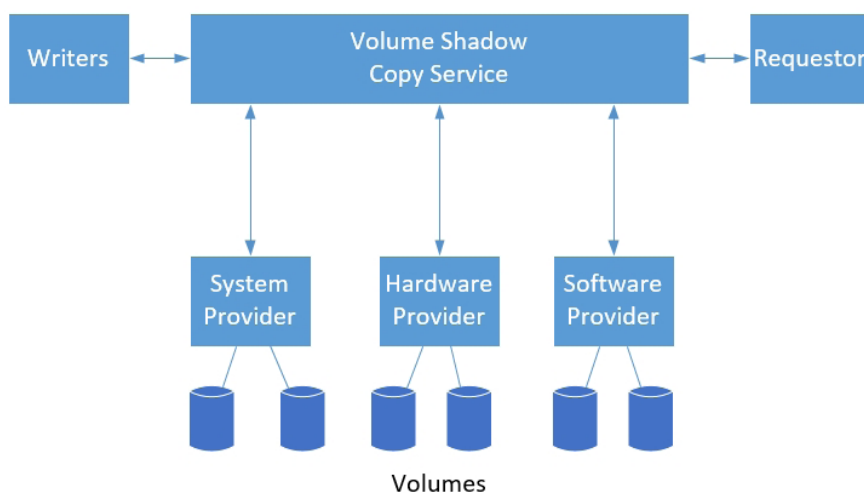
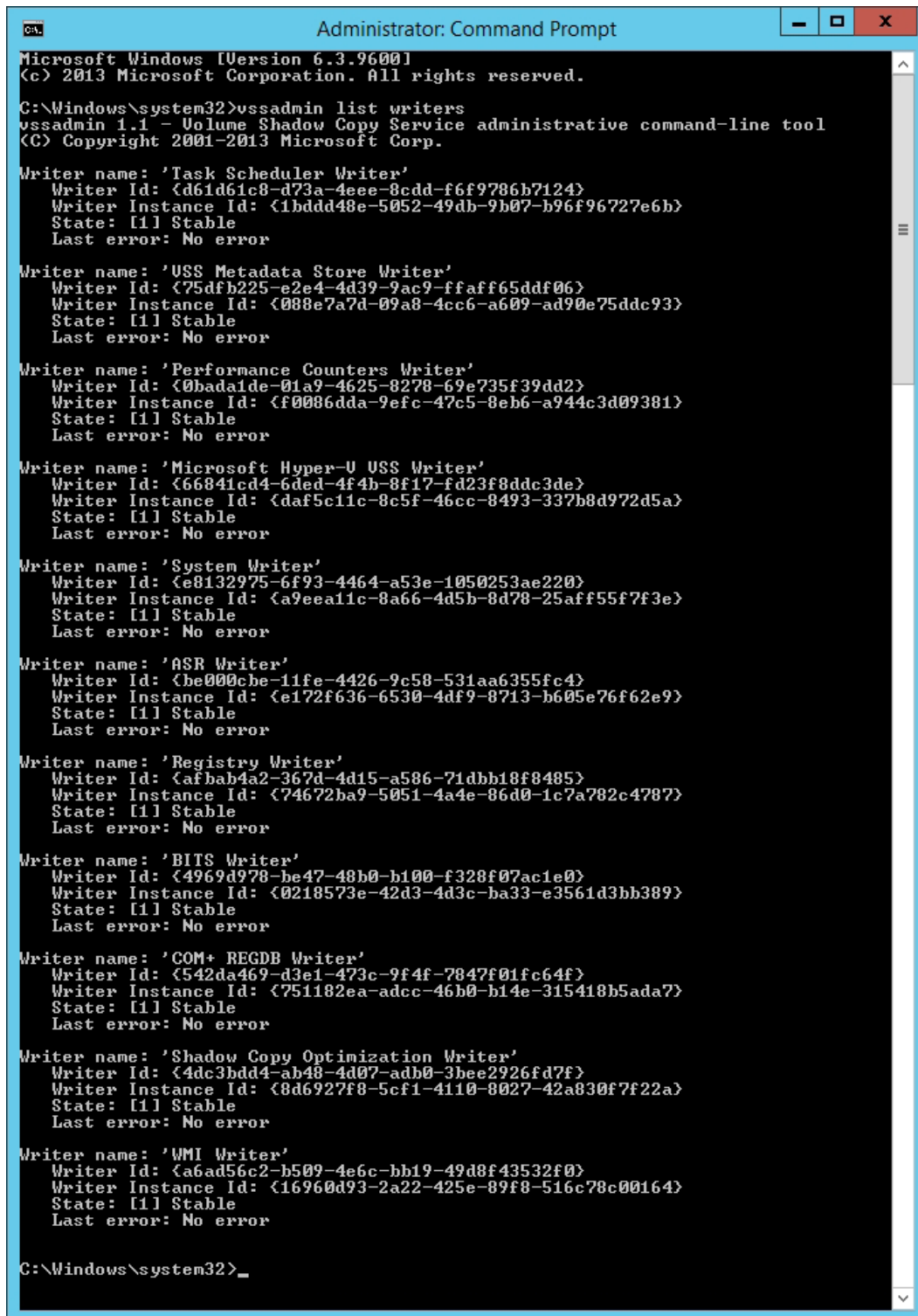


Figure 42. These are the primary VSS components.

Troubleshooting the Volume Shadow Copy Service:

The primary tool for diagnosing VSS problems is a command line tool called VSSAdmin. You can for example, use the VSSAdmin List Writers command to verify that each of the writers is stable, and is not in an error condition. You can see an example of this in Figure 43. You can see other VSSAdmin command line switches by entering the VSSAdmin /? command.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Writer name: 'Task Scheduler Writer'
  Writer Id: {d61d61c8-d73a-4eee-8cdd-f6f9786b7124}
  Writer Instance Id: {1bddd48e-5052-49db-9b07-b96f96727e6b}
  State: [1] Stable
  Last error: No error

Writer name: 'VSS Metadata Store Writer'
  Writer Id: {75dfb225-e2e4-4d39-9ac9-ffaff65ddf06}
  Writer Instance Id: {088e7a7d-09a8-4cc6-a609-ad90e75ddc93}
  State: [1] Stable
  Last error: No error

Writer name: 'Performance Counters Writer'
  Writer Id: {0bada1de-01a9-4625-8278-69e735f39dd2}
  Writer Instance Id: {f0086dda-9efc-47c5-8eb6-a944c3d09381}
  State: [1] Stable
  Last error: No error

Writer name: 'Microsoft Hyper-U VSS Writer'
  Writer Id: {66841cd4-6ded-4f4b-8f17-fd23f8ddc3de}
  Writer Instance Id: {daf5c11c-8c5f-46cc-8493-337b8d972d5a}
  State: [1] Stable
  Last error: No error

Writer name: 'System Writer'
  Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
  Writer Instance Id: {a9eea11c-8a66-4d5b-8d78-25aff55f7f3e}
  State: [1] Stable
  Last error: No error

Writer name: 'ASR Writer'
  Writer Id: {be000cbe-11fe-4426-9c58-531aa6355fc4}
  Writer Instance Id: {e172f636-6530-4df9-8713-b605e76f62e9}
  State: [1] Stable
  Last error: No error

Writer name: 'Registry Writer'
  Writer Id: {afbab4a2-367d-4d15-a586-71dbb18f8485}
  Writer Instance Id: {74672ba9-5051-4a4e-86d0-1c7a782c4787}
  State: [1] Stable
  Last error: No error

Writer name: 'BITS Writer'
  Writer Id: {4969d978-be47-48b0-b100-f328f07ac1e0}
  Writer Instance Id: {0218573e-42d3-4d3c-ba33-e3561d3bb389}
  State: [1] Stable
  Last error: No error

Writer name: 'COM+ REGDB Writer'
  Writer Id: {542da469-d3e1-473c-9f4f-7847f01fc64f}
  Writer Instance Id: {751182ea-adcc-46b0-b14e-315418b5ada7}
  State: [1] Stable
  Last error: No error

Writer name: 'Shadow Copy Optimization Writer'
  Writer Id: {4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
  Writer Instance Id: {8d6927f8-5cf1-4110-8027-42a830f7f22a}
  State: [1] Stable
  Last error: No error

Writer name: 'WMI Writer'
  Writer Id: {a6ad56c2-b509-4e6c-bb19-49d8f43532f0}
  Writer Instance Id: {16960d93-2a22-425e-89f8-516c78c00164}
  State: [1] Stable
  Last error: No error

C:\Windows\system32>
```

Figure 43. You can use the VSSAdmin List Writers command to verify writer health.

Hopefully, your writers are in a healthy state and no errors are reported. If however, errors are shown, then Dell provides guidance for correcting the problem at: <https://support.software.dell.com/kb/117647>

In a Hyper-V environment, VSS-based host level backups of virtual machines are made possible through the Hyper-V Integration Services. If a Windows virtual machine is not being backed up correctly, then it is a good idea to make sure that the Backup Integration Service is enabled for the virtual machine. You can do so by completing these steps:

1. Open the Hyper-V Manager.
2. Right click on the virtual machine that you are having trouble backing up, and select the Settings command from the resulting shortcut menu.
3. When Windows displays the Settings dialog box, select the Integration Services container.
4. Verify that the Backup (Volume Checkpoint) integration services are enabled, as shown in Figure 44.

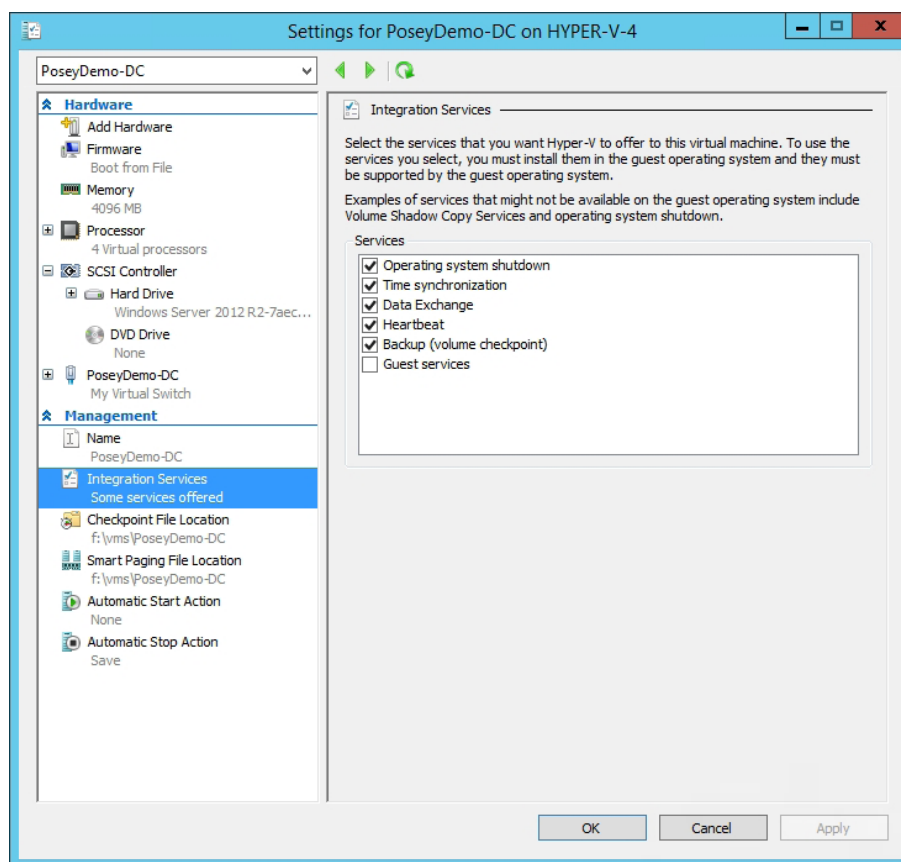
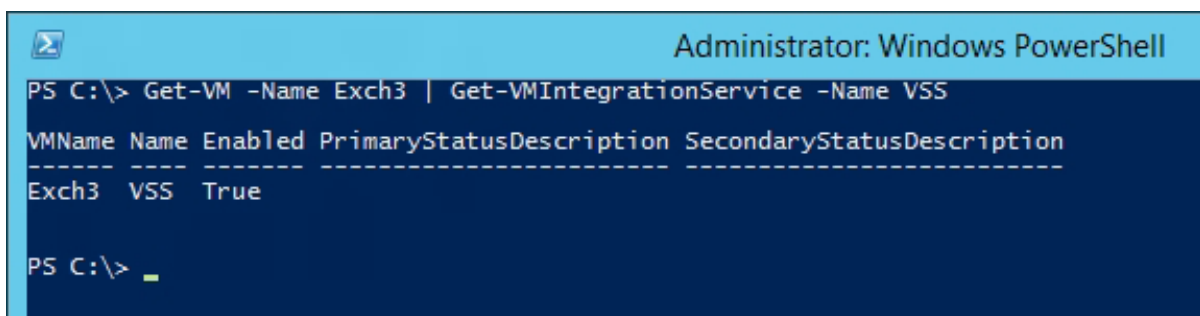


Figure 44. Make sure that the Backup (Volume Checkpoint) integration service is enabled.

If you would like to use PowerShell to check to see whether the Backup (Volume Checkpoint) integration Service is enabled, you can do so by entering the following command:

```
Get-VM -Name <virtual machine name> | Get-VMIntegrationService -Name VSS
```

You can see what this command looks like in Figure 45. In this case, the Enabled column shows a value of True, indicating that the Backup (Volume Checkpoint) integration service is enabled.



```
Administrator: Windows PowerShell
PS C:\> Get-VM -Name Exch3 | Get-VMIntegrationService -Name VSS
VMName Name Enabled PrimaryStatusDescription SecondaryStatusDescription
-----
Exch3  VSS  True
```

Figure 45. You can use PowerShell to test whether the Backup (Volume Checkpoint) integration service is enabled.

One of the nice things about PowerShell is that it makes it easy to verify the existence of the Backup (Volume Checkpoint) integration service across a large number of virtual machines. If for example, you wanted to check the status of the Backup (Volume Checkpoint) integration service for every virtual machine on a particular host, you could do so by using the following command:

```
Get-VM | Get-VMIntegrationService -Name VSS
```

You can see the command's output in Figure 46.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.MGMT> Get-VM | Get-VMIntegrationService -Name VSS

VMName           Name Enabled PrimaryStatusDescription SecondaryStatusDescription
-----
Anniv            VSS   True
PoseyDemo - CA   VSS   True
PoseyDemo - Client VSS   True
PoseyDemo-DC     VSS   True
SharePoint       VSS   True
SQL              VSS   True
TR               VSS   True
VMM              VSS   True

PS C:\Users\Administrator.MGMT> _
```

Figure 46. You can check the integration services on multiple virtual machines.

BACKUP RELATED CHECKPOINTS THAT CANNOT BE DELETED

Another problem that Hyper-V administrators sometimes encounter is that the backup process creates checkpoints (snapshots), and these checkpoints do not always go away when the backup completes.

Dealing with a lingering backup checkpoint requires extreme caution. Typically, if a checkpoint remains following a backup, it means that the backup application is still using the checkpoint, or that a failure occurred within a backup, even if that failure was unreported. Although it is possible to manually delete a backup checkpoint, you should always contact your backup vendor's support department first, in an effort to confirm that it is safe to remove the checkpoint. Otherwise, removing the checkpoint could break the backup application.

In order to understand why this problem happens, and how the fix works, it is necessary to understand how checkpoints are used by the backup process. A checkpoint is really nothing more than a differencing disk that has a parent / child relationship with a virtual machine. When you back up a virtual machine, Hyper-V may (depending on the type of backup that you are creating) create a differencing disk. This differencing disk intercepts any write operations that might occur during the backup process. That way, Hyper-V does not have to worry about the virtual hard disk's contents being modified during the backup process. After the backup process completes, then the differencing disk's contents are merged with the primary virtual hard disk, and the differencing disk is deleted. At least that's the way that the process is supposed to work. If the backup fails, then the checkpoint can remain in place.

Unfortunately, there is no easy way of removing this checkpoint. Most of the time, the only real option is to delve into PowerShell.

To remove the unwanted checkpoint, complete these steps:

1. Open an administrative PowerShell window on the Hyper-V Server that contains the virtual machine that is experiencing the problem.
2. Enter the Get-VM cmdlet. This causes PowerShell to produce a list of the virtual machines that reside on the server. This step is important, because you will need to know the virtual machine's virtual machine name, which can be different from its computer name. You can see an example of such a list in Figure 47.

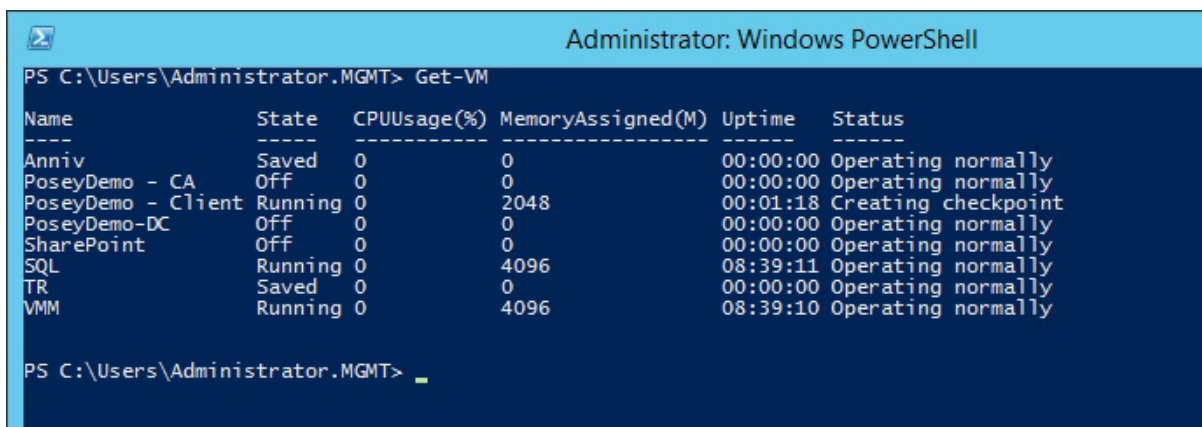


Figure 47. The Get-VM cmdlet displays a list of the virtual machines that exist on the host.

3. Enter the following command: `Get-VMSnapshot -VMName <virtual machine name> | FL` This command will return information about the checkpoint, as shown in Figure 48. It is worth noting that this figure displays a standard checkpoint, rather than a checkpoint from a failed backup. However, the general concepts remain the same.


```

PS C:\Users\Administrator.MGMT> Get-VMSnapshot -VMName "PoseyDemo - Client" | FL

SnapshotType           : Standard
VMId                   : dac2050b-b3a3-4172-b279-0fe798d1b510
VMName                 : PoseyDemo - Client
State                  : Off
Key                    : Microsoft.HyperV.PowerShell.SnapshotObjectKey
IsDeleted              : False
ComputerName           : HYPER-V-4
Id                     : 92770ac6-297e-4415-9f21-606081fd9b23
Name                   : PoseyDemo - Client - (4/25/2016 - 7:27:15 PM)
Version                : 5.0
Notes                  : #CLUSTER-INVARIANT#: {89b4c0e8-84e5-4769-a5f8-07d32cb2c1ad}
Generation            : 2
Path                   : f:\vms\PoseyDemo - Client
CreationTime           : 4/25/2016 7:28:04 PM
IsClustered           : False
SizeOfSystemFiles     : 75144
ParentSnapshotId      :
ParentSnapshotName     :
MemoryStartup         : 2147483648
DynamicMemoryEnabled  : False
MemoryMinimum         : 536870912
MemoryMaximum         : 1099511627776
ProcessorCount        : 4
RemoteFxAdapter       :
NetworkAdapters       : {PoseyDemo - Client}
FibreChannelHostBusAdapters : {}
ComPort1              : Microsoft.HyperV.PowerShell.VMComPort
ComPort2              : Microsoft.HyperV.PowerShell.VMComPort
FloppyDrive           :
DVDDrives             : {DVD Drive on SCSI controller number 0 at location 1}
HardDrives            : {Hard Drive on SCSI controller number 0 at location 0}
VMIntegrationService  : {Time Synchronization, Heartbeat, Key-Value Pair Exchange, Shutdown...}

PS C:\Users\Administrator.MGMT>

```

Figure 48. PowerShell returns information about the snapshot.

4. Enter the following command: `Get-VMSnapshot -VMName <virtual machine name> | Remove-VMSnapshot` This command removes the checkpoint.
5. Verify that the checkpoint has been removed by running the following command: `Get-VMSnapshot -VMName <virtual machine name> | FL` The checkpoint should no longer exist, as shown in Figure 49.

```

PS C:\Users\Administrator.MGMT> Get-VMSnapshot -VMName "PoseyDemo - Client" | FL

SnapshotType           : Standard
VMId                   : dac2050b-b3a3-4172-b279-0fe798d1b510
VMName                 : PoseyDemo - Client
State                  : Off
Key                    : Microsoft.HyperV.PowerShell.SnapshotObjectKey
IsDeleted              : False
ComputerName           : HYPER-V-4
Id                     : 92770ac6-297e-4415-9f21-606081fd9b23
Name                   : PoseyDemo - Client - (4/25/2016 - 7:27:15 PM)
Version                : 5.0
Notes                  : #CLUSTER-INVARIANT#: {89b4c0e8-84e5-4769-a5f8-07d32cb2c1ad}
Generation            : 2
Path                   : f:\vms\PoseyDemo - Client
CreationTime           : 4/25/2016 7:28:04 PM
IsClustered           : False
SizeOfSystemFiles     : 75144
ParentSnapshotId      :
ParentSnapshotName     :
MemoryStartup         : 2147483648
DynamicMemoryEnabled  : False
MemoryMinimum         : 536870912
MemoryMaximum         : 1099511627776
ProcessorCount        : 4
RemoteFxAdapter       :
NetworkAdapters       : {PoseyDemo - Client}
FibreChannelHostBusAdapters : {}
ComPort1              : Microsoft.HyperV.PowerShell.VMComPort
ComPort2              : Microsoft.HyperV.PowerShell.VMComPort
FloppyDrive           :
DVDDrives             : {DVD Drive on SCSI controller number 0 at location 1}
HardDrives            : {Hard Drive on SCSI controller number 0 at location 0}
VMIntegrationService  : {Time Synchronization, Heartbeat, Key-Value Pair Exchange, Shutdown...}

PS C:\Users\Administrator.MGMT> Get-VMSnapshot -VMName "PoseyDemo - Client" | Remove-VMSnapshot
PS C:\Users\Administrator.MGMT> Get-VMSnapshot -VMName "PoseyDemo - Client" | FL
PS C:\Users\Administrator.MGMT>

```

Figure 49. The checkpoint no longer exists.

HIGH AVAILABILITY ISSUES

Although Hyper-V can be run on a standalone server, Hyper-V servers are often configured to use the Windows Failover Clustering feature, so as to make virtual machines highly available. This section discusses some of the more common issues that occur in clustered deployments.

VIRTUAL MACHINES DO NOT FAIL OVER TO ANOTHER CLUSTER NODE

Although some organizations create single server Hyper-V deployments, production Hyper-V deployments need to be clustered. The reason for this is simple. A production Hyper-V host typically hosts multiple production workloads. If that host server were to fail, then all of the virtual machines that are running on the host would also fail, resulting in a major outage.

One somewhat common problem that Hyper-V administrators encounter is that clusters do not behave as expected. Virtual machines may for example, fail to failover to another Hyper-V host. There are a number of different things that can cause this problem.

The Virtual Machine is not Defined as a Clustered Role

One common cause of this problem is that the virtual machines have not been made highly available. It isn't enough to deploy the Windows Failover Clustering Feature onto your Hyper-V Servers. You must make the individual virtual machines highly available by configuring the virtual machines to act as a clustered role. You can determine whether or not a virtual machine has been made highly available by completing these steps:

1. Open the Failover Cluster Manager.
2. Expand the listing for your cluster, and select the Roles container.
3. Verify that your virtual machines are listed as clustered roles, as shown in Figure 50.

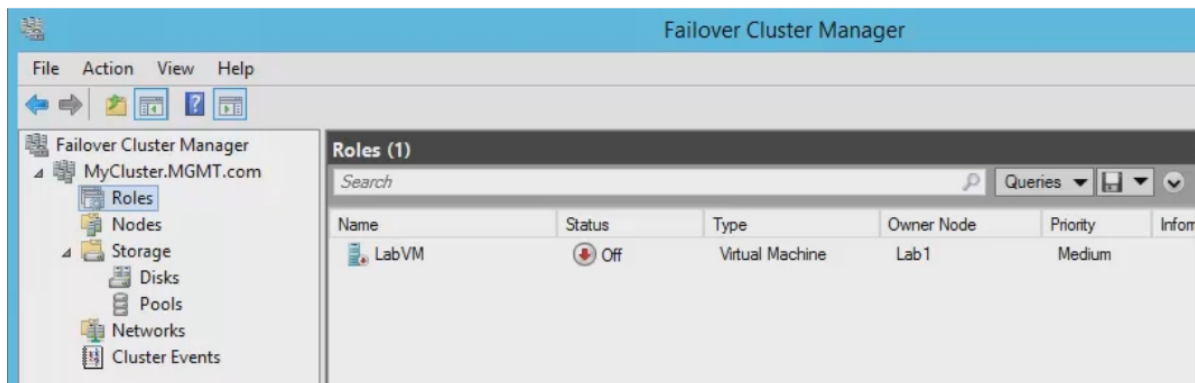


Figure 50. Make sure that your virtual machines are listed as clustered roles.

If you discover that your virtual machines are not listed, then you can click on the Configure Role link, found in the console's Actions pane. This will cause Windows to Launch the High Availability Wizard. Now, you must simply follow the wizard's prompts and choose Virtual Machine as the role type and then choose the virtual machine that you wish to make highly available.

If you work through the High Availability Wizard and discover that the virtual machines that you wish to make highly available are not listed, then there are a couple of possible things to check. Make sure that the virtual machine resides on a Hyper-V server that acts as a part of the cluster.

INADEQUATE RESOURCES

Even if a failover cluster is configured correctly, and virtual machines have been configured to be highly available, the failover process can still fail if there are not sufficient system resources available on the destination host. The destination host must have adequate CPU, memory, and other hardware resources available if it is to be able to run virtual machines that were previously running on a different host. This can be a problem for organizations that attempt to maximize virtual machine density, because the Hyper-V servers may already be running so many virtual machines that they simply do not have the resources to accommodate other virtual machines in the event of a failover.

Even if the destination host has plenty of resources available for running some of the virtual machines from the failed host, those resources might not be adequate for hosting every virtual machine that was previously running on the failed host.

One way to check for this condition is to examine the host's event log entries. Windows Server stores log entries related to virtual machine high availability in the Microsoft-Windows-Hyper-V-High-Availability event log. You can access this event log by opening the Event Viewer and navigating to Application and Service Logs \ Microsoft \ Windows \ Hyper-V-High-Availability.

One event to watch out for is:

```
Event ID: 21502
Source: Microsoft-Windows-Hyper-V-High-Availability
Type: Error
Description: Virtual Machine <virtual machine name>
live migration did not succeed at the source. Migration
failed.
```

This error can occur if there isn't enough physical memory on the destination host to accommodate the virtual machine that is being migrated. Memory is often the limiting resource when it comes to live migrations or failovers.

In situations in which the destination host does not have adequate resources to accommodate all of the inbound virtual machines, you can prioritize virtual machine failovers based on each individual virtual machine's importance.

To configure a priority for a virtual machine, complete these steps:

1. Open the Failover Cluster Manager.
2. Select the Roles container.
3. Right click on the virtual machine that you wish to prioritize, and then select the Properties command from the shortcut menu.
4. Choose a priority for the virtual machine, as shown in Figure 51.
5. Click OK.

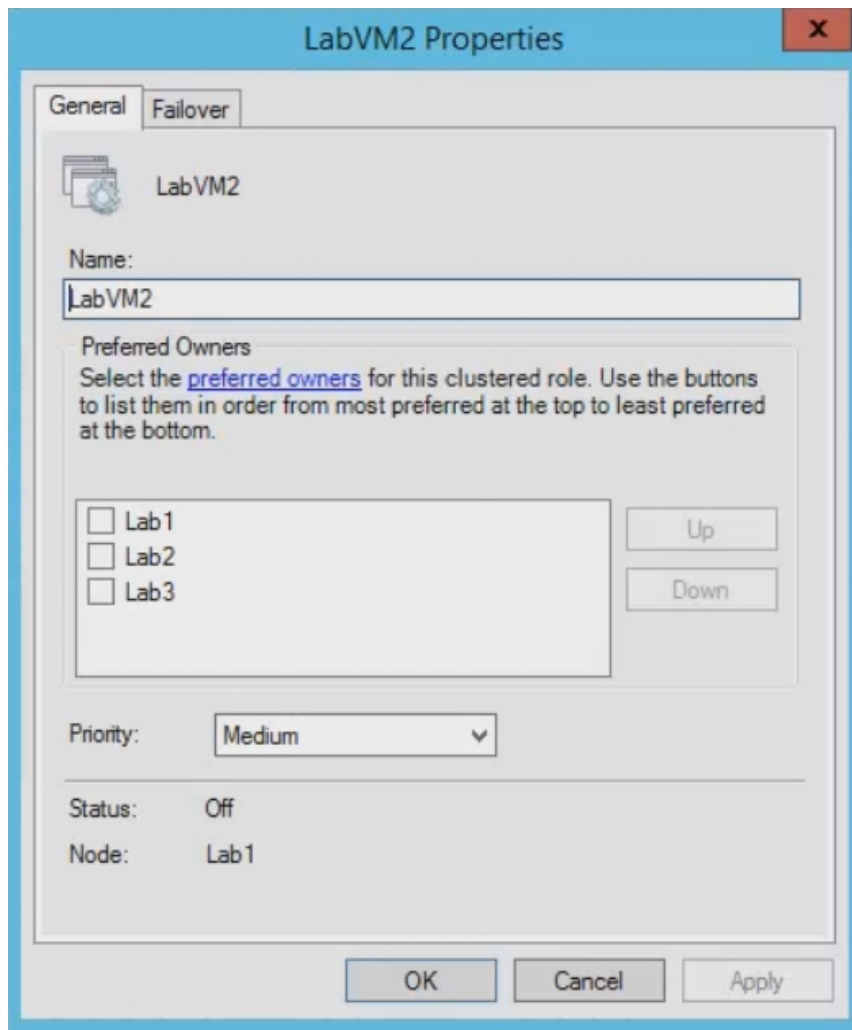


Figure 51. Set a priority for the virtual machine and click OK.

Virtual machines can also be prioritized through the Virtual Machine Manager console. To do so, follow these steps:

1. Open the Virtual Machine Manager Console.
2. Select the VMs and Services workspace.
3. 3. Right click on the virtual machine that you wish to re-prioritize, and choose the Properties command from the shortcut menu.
4. 4. When the virtual machine’s Properties dialog box appears, select the Availability container.
5. 5. Choose the priority that you want to assign to the virtual machine, as shown in Figure 52. You can only prioritize highly available virtual machines, which is why the priorities are greyed out in the figure.

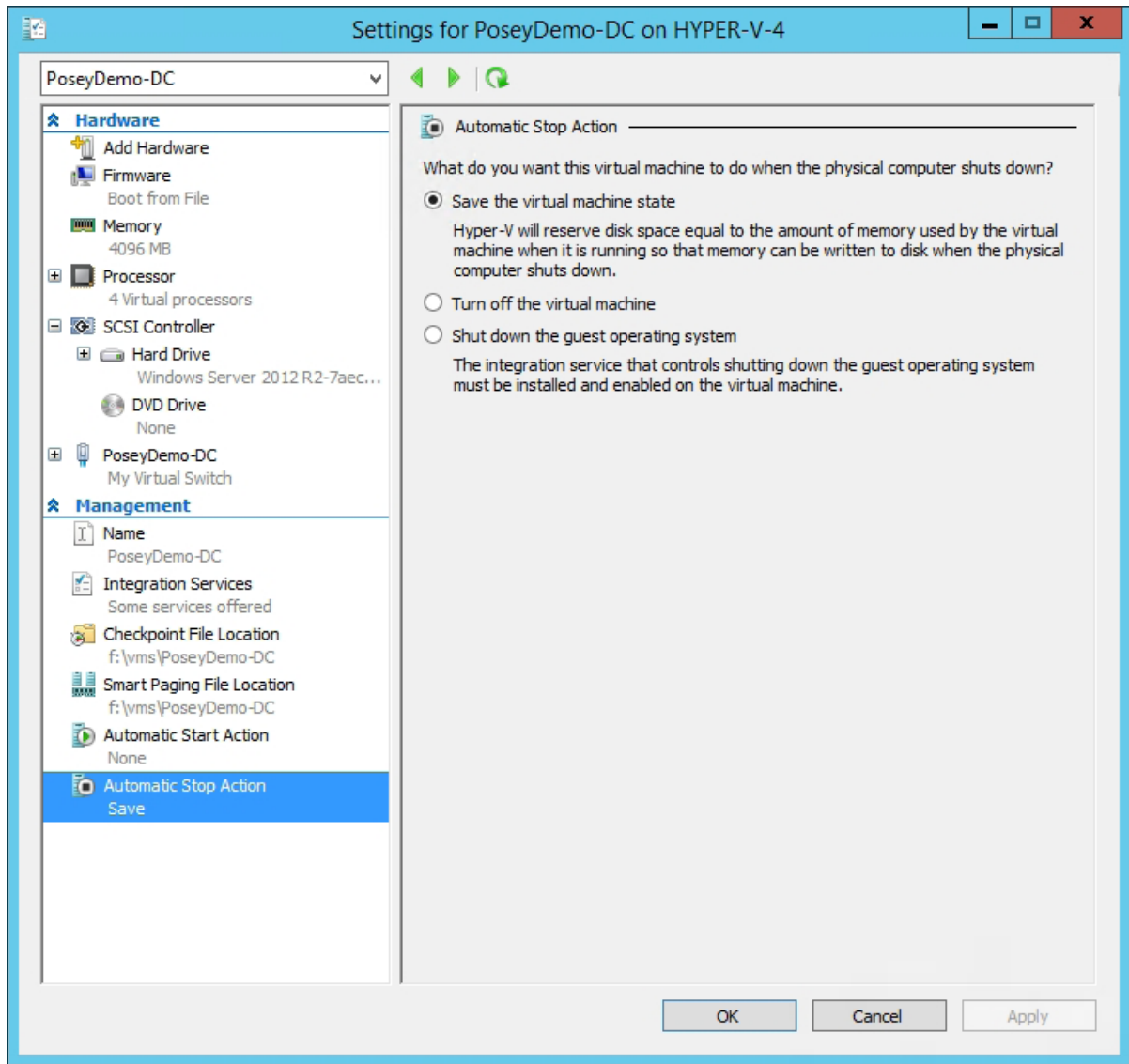


Figure 52. You can configure virtual machine priorities through the Virtual Machine Manager console.

CONCLUSION

Hyper-V is a very stable and reliable, enterprise class hypervisor. Even so, problems can, and sometimes do occur. In many cases, these problems are caused by simple configuration issues. In other cases, problems may be attributed to resource contention.

If you experience Hyper-V problems that have not been discussed in this book, then you might consider looking at Microsoft's Hyper-V resources on TechNet: [https://technet.microsoft.com/en-us/library/mt169373\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/mt169373(v=ws.11).aspx). For more serious problems, you can contact Microsoft Support (<https://technet.microsoft.com/en-us/windowsserver/hh553005.aspx>).

ABOUT ALTARO

Altaro Software (www.altaro.com) is a fast growing developer of easy to use backup solutions used by over 30,000 customers to back up and restore both Hyper-V and VMware-based virtual machines, built specifically for Small and mid-market business with up to 50 host servers. Altaro take pride in their software and their high level of personal customer service and support, and it shows; Founded in 2009, Altaro already service over 30,000 satisfied customers worldwide and are a Gold Microsoft Partner for Application Development and Technology Alliance VMware Partner.

ABOUT ALTARO VM BACKUP

Altaro VM Backup is an easy to use backup software solution used by over 30,000 Small and mid-market business customers to back up and restore both Hyper-V and VMware-based virtual machines. Eliminate hassle and headaches with an easy-to-use interface, straightforward setup and a backup solution that gets the job done every time.

Altaro VM Backup is intuitive, feature-rich and you get outstanding support as part of the package. Demonstrating Altaro's dedication to Hyper-V, they were the first backup provider for Hyper-V to support Windows Server 2012 and 2012 R2 and also continues support Windows Server 2008 R2.

For more information on features and pricing, please visit:

<http://www.altaro.com/vm-backup>

Don't take our word for it – Take it for a spin!

[DOWNLOAD YOUR FREE COPY OF ALTARO VM BACKUP](#)

and enjoy unlimited functionality for 30 days. After your 30-day trial expires you can continue using the product for up to 2 VMs for free, forever. No catch!

Altaro VM Backup - Trusted by over 30,000 SMBs

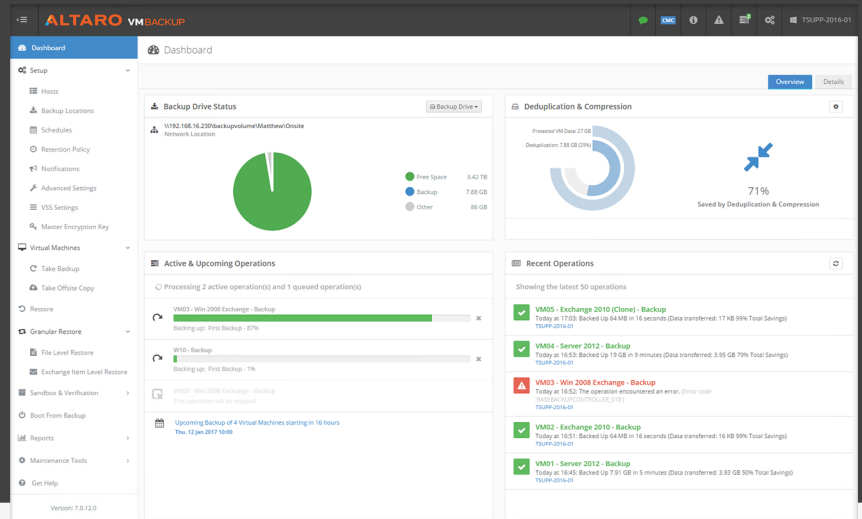
New v7! Altaro VM Backup for Hyper-V & VMware. Hassle-free and affordable VM backup software. Grab your free copy for 2 VMs now!

- ✓ Hassle-free and effective
- ✓ Unbeatable Value
- ✓ Outstanding Support

Free for 2 VMs, forever.

Back up unlimited VMs for 30 -days. After 30-days you get 2 VMs for free, forever. Download now!

Backup Now!

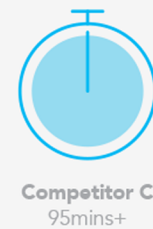
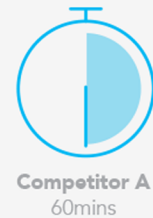


Up and running quickly, without the need for complex configurations!

With Altaro VM Backup, you can install and run your first virtual machine (VM) backup in less than 15 minutes. Get up and running quickly, without the need for complex configurations or software dependencies.

Altaro VM Backup is designed to give you the power you need, without the hassle and steep learning curve.

- **Easy to use, intuitive UI** - making it easy to implement a rock solid backup strategy
- **Managing and configuring backup/restore jobs across multiple hosts has never been simpler**
- **Full control & scalability** - Monitor and manage all your Hyper-V and VMware hosts from a single console



Virtual machine backup software packed with powerful features for Hyper-V and VMware.

[View Features](#)

ABOUT BRIEN M. POSEY



Brien Posey is a 14 time Microsoft MVP with over two decades of IT experience. Prior to going freelance, Brien worked as CIO for a national chain of hospitals and healthcare facilities. He has also served as a network engineer for the United States Department of Defense at Fort Knox and as a network administrator for some of the country's largest insurance companies. In addition to his work in IT, Brien is currently training to be a civilian astronaut. For more information visit brienposey.com or twitter.com/BrienPosey

FOLLOW ALTARO

Like our eBook? **There's more!**

Subscribe to our Hyper-V blog <http://www.altaro.com/hyper-v> and receive best practices, tips, free Hyper-V PowerShell scripts and more here: <http://www.altaro.com/hyper-v/sign-up>

Follow Altaro at:



 **SHARE THIS RESOURCE!**

Liked the eBook? Share it now on:

