IBM System Storage Support for Microsoft Volume Shadow
Copy Service and Virtual Disk Service
Version 4.5.0

User Guide

IBM

Edition notice

This publication applies to version 4.5.0 of the IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service and to all subsequent releases and modifications until otherwise indicated in a newer publication.

Contents

Figures

Tables

About this guide

The IBM® System Storage® Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service 4.5.0 User Guide contains configuration and user information.

Who should use this guide

The IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service 4.5.0 User Guide is intended for system administrators or others who install and use the Volume Shadow Copy Service and Virtual Disk Service.

Before installing and using the IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service 4.5.0, you should have an understanding of the Microsoft Windows Server environment, the VSS framework, the IBM SAN Volume Controller and DS8000® Storage Systems, the VMware environment, and Windows Hyper-V environment (if used).

Conventions used in this guide

These notices are used to highlight key information.

Note: These notices provide important tips, guidance, or advice.

Important: These notices provide information or advice that might help you avoid inconvenient or difficult situations.

Attention: These notices indicate possible damage to programs, devices, or data. An attention notice appears before the instruction or situation in which damage can occur.

CAUTION:
These notices indicate a situation that is potentially hazardous to people because of some existing condition or where a potentially dangerous situation might develop because of some unsafe practice.

DANGER

> **These notices indicate a situation that is potentially lethal or extremely hazardous to people. For example, after a computer side panel is removed, exposed high-voltage wires might be lethal.**

Related information and publications

You can find additional information and publications related to the IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service at the following websites.

- IBM Flex System™ Information Center
- IBM Storwize® V3500 Information Center
- IBM Storwize V3700 Information Center

- IBM Storwize V7000 Information Center
- IBM Storwize V7000 Unified Information Center
- IBM System Storage SAN Volume Controller Information Center
- IBM System Storage DS8000 Information Center
- VMware ESXi and ESX Information Center
- VMware Product Support for VMware vSphere, including support for ESX, ESXi, and vCenter.
- VMware knowledgebase
- Microsoft MSDN web page for Volume Shadow Copy Service
- Microsoft Windows Server Troubleshooting Center

Getting information, help, and service

If you need help, service, technical assistance, or want more information about IBM products, you can find various sources to assist you. You can view the following websites to get information about IBM products and services and to find the latest technical information and support.

- IBM website (ibm.com®)
- IBM Support Portal website (www.ibm.com/storage/support)
- IBM Directory of Worldwide Contacts website (www.ibm.com/planetwide)

Ordering publications

The IBM Publications Center is a worldwide central repository for IBM product publications and marketing material.

The IBM Publications Center website (www.ibm.com/shop/publications/order/) offers customized search functions to help you find the publications that you need. Some publications are available for you to view or download at no charge. You can also order publications. The publications center displays prices in your local currency.

Sending your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

Procedure

To submit any comments about this book or any other Host Solutions Group documentation:

- Go to the Feedback form on the IBM Storage Host Software Solutions Information Center . You can use this form to enter and submit comments.
- Send your comments by email to starpubs@us.ibm.com. Be sure to include the following information:
  - Exact publication title and version
  - Publication form number (for example, GA32-0770-00)
  - Page, table, or illustration numbers that you are commenting on
  - A detailed description of any information that should be changed

Chapter 1. Introduction

The Microsoft Volume Shadow Copy Service (VSS) can provide a point-in-time (shadow) copy of a Windows host volume while the volume is mounted and files are in use. The Microsoft Virtual Disk Service (VDS) provides a single vendor and technology-neutral interface for managing block storage virtualization, whether done by operating system software, RAID storage hardware, or other storage virtualization engines.

The IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service for DS8000 and SAN Volume Controller is a software module that runs as a service on Microsoft Windows Server and automatically creates snapshots of Windows-based applications. The module uses the Windows Server VSS framework for its management interface, and the DS8000 and SAN Volume Controller as the storage system on which snapshot data is stored and maintained.

Note: VSS providers must be installed and run as Administrator.

Chapter 2. Configuring in a physical environment

This section describes configuring the Volume Shadow Copy Service and Virtual Disk Service in a physical environment.

This includes:
- "Configuring VSS in a physical environment using Fibre Channel"
- "Configuring VSS in a physical environment using iSCSI"

Configuring VSS in a physical environment using Fibre Channel

Install the VSS provider in a physical environment using Fibre Channel (FC).

Procedure

1. Connect to the storage machine using CIMOM.
2. Create the free pool and reserved pool for VSS. Define the virtual hosts `VSS_FREE_POOL` and `VSS_RESERVED_POOL` on the storage system with the following fake WWPN: 5000000000000000 and 5000000000000001.

   Note: In a multiple hosts environment where hosts are connecting to the same storage, a common reserved pool and multiple free pools need to be created on the storage. Every host uses an individual free pool and the common reserved pool.
3. Use the following commands to set the fake WWPN of the free pool and the reserved pool: **ibmvcfg set vssFreeInitiator** and **ibmvcfg set vssReservedInitiator**.
4. Map source volumes to the physical machine by FC.
5. Map the target volumes to the free pool.

   Note: MPIO should be enabled with the appropriate vendor DSM if you configure multiple paths from the host to the storage array.

Configuring VSS in a physical environment using iSCSI

Install the VSS provider in a physical environment using iSCSI.

Procedure

1. Connect to the storage machine using CIMOM.
2. Create the free pool and reserved pool for VSS. Define the virtual hosts `VSS_FREE_POOL` and `VSS_RESERVED_POOL` on the storage system with the following fake WWPN: 5000000000000000 and 5000000000000001.
3. Use the following commands to set the fake WWPN of the free pool and the reserved pool: **ibmvcfg set vssFreeInitiator** and **ibmvcfg set vssReservedInitiator**.
4. Map source volumes to the physical machine by iSCSI.
5. Map the target volumes to the free pool.

Chapter 3. Configuring in a VMware environment

This section describes configuring the Volume Shadow Copy Service and Virtual Disk Service in a VMware environment.

This includes:
- "Prerequisites"
- "User Privileges" on page 6
- "Provider settings for VMware" on page 7
- "VMware advanced configuration" on page 11
- "Snapshots with various Storage Protocols" on page 14

Note: If the VMware virtual machine is not recognized as a virtual machine, ensure the `systeminfo` in the virtual machine is correct. See "VMware virtual machine not recognized as virtual machine" on page 27 for more information.

Prerequisites

This section lists the prerequisites for using and configuring the IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service in a VMware environment.

This includes:
- "Supported VMware platforms"
- "Supported storage systems"
- "Installing VMware tools" on page 6
- "vSphere web Services" on page 6

Supported VMware platforms

The Volume Shadow Copy Service and Virtual Disk Service support the following VMware platforms:
- vSphere ESX Server 4.x
- vSphere ESXi Server 4.x
- vSphere ESX Server 5.0
- vSphere ESXi Server 5.0
- vSphere ESX Server 5.1
- vSphere ESXi Server 5.1
- vSphere vCenter Server 4.x
- vSphere vCenter Server 5.0
- vSphere vCenter Server 5.1

Supported storage systems

The Volume Shadow Copy Service and Virtual Disk Service support the following storage systems.

Table 1. Supported storage systems

Storage System	Microcode Version
DS8000	6.x, 7.0, 7.1
Storwize V3500	6.4.1, 7.1
Storwize V3700	6.4.1, 7.1
Storwize V5000	7.1
Storwize V7000	6.1, 6.2, 6.3, 6.4, 6.4.1, 7.1
SAN Volume Controller	5.1, 6.1, 6.2, 6.3, 6.4, 6.4.1. 7.1
Storwize V7000 Unified	1.3, 1.4, 1.4.1
IBM Flex System	6.4.1, 7.1

Installing VMware tools

VMware tools is required for communication between the ESX(i) Server web services and VM. VMware tools collects guest-related information such as the IP address and host name.

Procedure

To install the VMware tools:

1. Turn on the guest OS. From the VIClient menu for the specific guest, select **Install/Upgrade VMware Tools**.
2. Log on to the Windows Server (guest) and install the package.

vSphere web Services

vSphere web Services must be operational for the Volume Shadow Copy Service and Virtual Disk Service to work properly in the guest Windows Server. By default, vSphere web Services are on as ESX/ESXi OS loaded.

To check if vSphere web Services are online, use a web browser to access https://189.0.0.222 /mob

A prompt appears for the user credentials to log in the hosted web services. The "189.0.0.222" is an example of an ESX(i) server or a vCenter Server IP address.

User Privileges

The following user privileges are required for the Volume Shadow Copy Service and Virtual Disk Service VMware parameter:

- **Host** > **Configuration** > **Storage partition configuration**
- **Virtual machine** > **Configuration** > **Raw device**
- **Virtual machine** > **Configuration** > **Change resource**
- **Virtual machine** > **Configuration** > **Add or remove device**

If the Volume Shadow Copy Service and Virtual Disk Service communicate with the vCenter, the Read-Only role must be assigned to the data center to which the ESX(i) Server belongs. A role with the user privileges described in this section should be created. You can view the user privileges by accessing the vSphere client

and selecting the Permissions tab. Role settings in the vCenter lists the roles and permissions for the vCenter. In Table 2, the vSphere client is **ARCX3455GBXV3**.

Table 2. Role settings in the vCenter

File	Role Description	User Group	Role Value
ARCX3455GBXV3	Role for vCenter	vssuser	No access
ARCX3455GBXV3/test	Role for data center	vssuser	Read-only
ARCX3455GBXV3/test/ <IP address>	Role for ESX(i) Server	vssuser	vssrole
ARCX3455GBXV3/test/ <IP address>/NewVirtual Machine	Role for virtual machine	vssuser	vssrole
Note: In Role for data center, ensure the check-box **Propogate** is selected.			
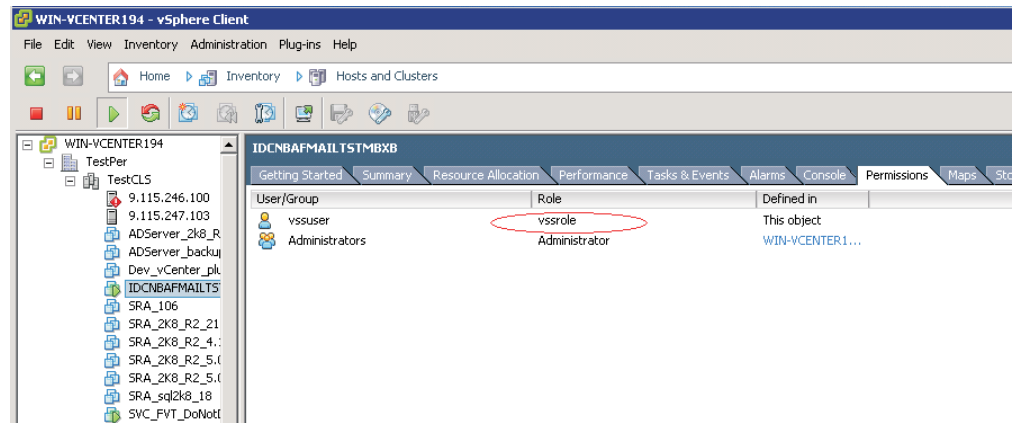
Figure 1. vSphere client - user privileges

Provider settings for VMware

Provider settings include Volume Shadow Copy Service and Virtual Disk Service parameters and a generated Java™ credentials keystore.

- "Provider parameters for VMware" on page 8
- "Generating the Java credential keystore" on page 9

Note: When configuring RDM, select **physical** in Select Compatibility Mode.
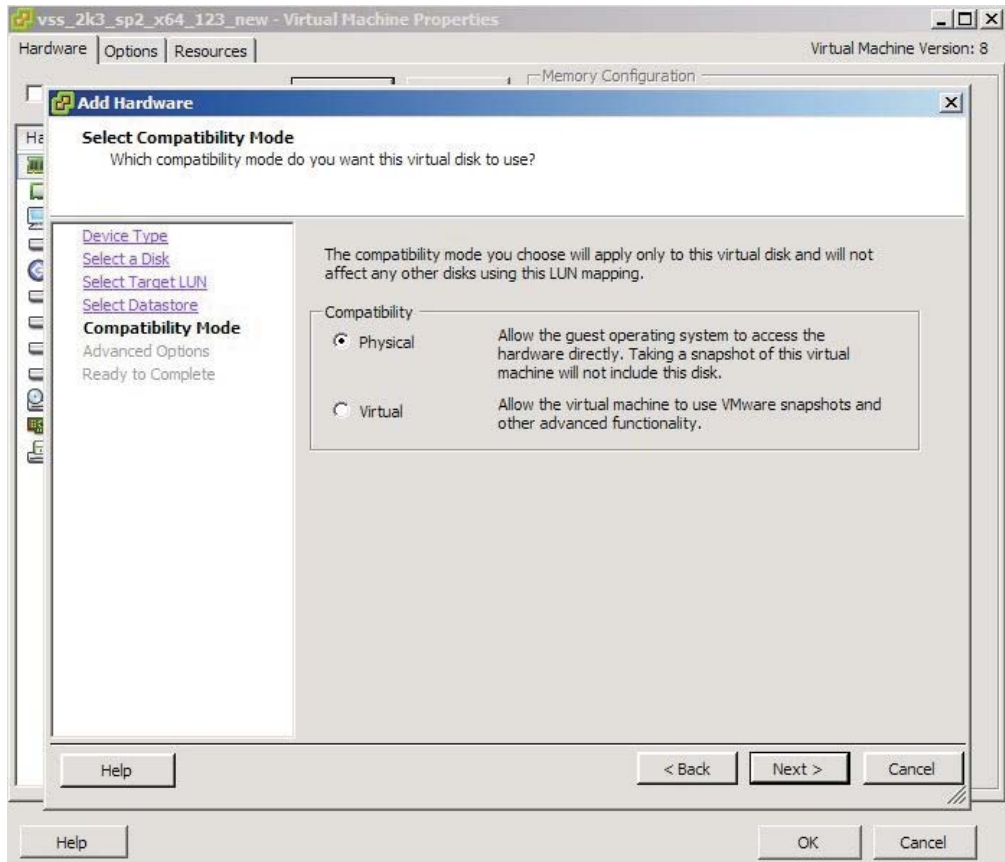
Figure 2. Select Compatibility Mode

Provider parameters for VMware

Several Volume Shadow Copy Service and Virtual Disk Service parameters are specific to the VMware guest support feature. The parameters allow the Volume Shadow Copy Service and Virtual Disk Service to communicate with the ESX(i) Server web Services to manipulate the RDM disks during a snapshot.

You must set up the parameters for VMWare in the following two cases:
1. The snapshot disk is discovered by the ESX(i) Server through Fibre Channel and mapped to the virtual machine as the RDM disk.
2. The snapshot disk is discovered by the ESX(i) Server through software iSCSI and mapped to the virtual machine as the RDM disk.

The following Volume Shadow Copy Service and Virtual Disk Service parameters are available only in the VMware virtual platform:

vmhost
> The VMware web Service that is located on the ESX(i) Server or vCenter Server, such as: https://ESX_Server_IP/sdk

vmuser
> The user that has the access to the ESX(i) Server or vCenter Server with the authority to perform RDM disk operations

vmpassword
> The password for the vmuser to log on

vmcredential

The session credential store path for the ESX(i) Server or vCenter Server that is used by Java

You can use the IBM VSS configuration tool ibmvcfg to set the parameters. For example, type **ibmvcfg set vmhosst https://9.11.110.115/sdk**:

```
C:\Program Files\IBM\Hardware Provider for VSS-VSD>ibmvcfg set vmhosst
https://9.11.110.115/sdk
```

The vmcredential path is the full path name of the Java key file. See "Generating the Java credential keystore" for information about generating the Java keystore.

Generating the Java credential keystore

To generate the Java credential keystore, obtain the ESX(i) Server certificates and then set the credential as the keystore path.

Procedure

1. Obtain the ESX(i) Server or vCenter Server certificate using the vSphere client, the Secure Shell client application, or Internet Explorer. To obtain ESX(i) Server or vCenter Server certificates using the vSphere client, create a root-level directory for the certificates. For example, C:\VMware-Certs.

   a. Install the vSphere client if not already installed.

   b. Start the vSphere client and navigate to the ESX, ESXi, or vCenter Server web server. A message displays regarding the certifying authority for the certificate.

   c. Click **View Certificate** to display the certificate properties page.

   d. Click the **Details** tab.

   e. Click **Copy to File...** to start the Certificate Export wizard.

   f. Select **DER encoded binary X.509** (the default) and click **Next**.

   g. Click **Browse...** and navigate to the C:\VMware-Certs subdirectory.

   h. Enter a certificate name that identifies the server to which the certificate belongs. For example, (userinput) C:\VMware-Certs\<server name>.cer

2. To obtain server certificates using the Secure Shell client application, connect to the ESX system using an SSL client.

   Note: Remote connections to the ESX service console as root are effectively disabled. To obtain the certificate, you must connect as another user with privileges on the server.

Table 3. Server certificate file names and locations of the ESX(i) and vCenter servers

Server	Directory location for certificate	Certificate
ESX(i) 4.x, 5.0, 5.1	/etc/vmware/ssl/	rui.crt
vCenter Server 4.x, 5.0, 5.1	C:\Documents and Settings\All Users\Appications	rui.crt

   a. Copy the certificates from the server to the certificate subdirectory, using a unique file name for the certificate (assuming you are copying multiple default certificates from multiple ESX systems, for example).

3. To obtain server certificates using Internet Explorer, type the following URL to access the web service of the ESX(i) Server or vCenter Server: https://9.11.110.240/

    a. If you receive a message about the security certificate, select **Continue to this website (not recommended)**.

    b. On the toolbar, click **Certificate Error** and, in the Certificate Invalid window, click **View certificates**.

    c. In the Certificate window, select the **Details** tab.

    d. Click **Copy to File** and follow the Certificate Export Wizard with the default option to save the certificate.

    e. Create a directory for the Java keystore. For example, `C:\VMware`

    f. Use the Java keytool utility to import a certificate. The syntax is keytool **-import -file <certificate-filename> -alias <server-name> -keystore vmware.keystore** For example:

    ```
    C:\Program Files\IBM\Hardware Provider for VSS-vDS\jre\bin\keytool.exe -import -file
    C:\tools\rui.crt -keystore C:\VMware\vmware.keystore
    ```

    g. When prompted for a keystore password, type a password.

    h. The keystore utility displays the certificate information at the console. For example:

    ```
    Owner: OID.1.2.840.113549.1.9.2="1301079258,564d7761726520496e632e", CN=cimxa.ib
    m.com, EMAILADDRESS=ssl-certificates@vmware.com, OU=VMware ESX Server Default Ce
    rtificate, O="VMware, Inc", L=Palo Alto, ST=California, C=US
    Issuer: O=VMware Installer
    Serial number: 7730362f66385863
    Valid from: 3/25/11 7:54 PM until: 9/23/22 8:54 PM
    Certificate fingerprints:
            MD5:   58:A3:A3:D4:D8:E0:CE:63:6B:B7:7F:4E:3E:6B:71:9D
            SHA1: 8B:60:B9:08:32:33:06:11:47:7D:6D:B6:84:D1:D5:F9:78:D2:15:5F
            SHA256: 59:1B:A2:BE:D0:BC:04:1B:CE:62:B8:95:07:52:3E:54:69:76:10:A1:85:
    A6:A8:5A:C0:DB:45:79:46:FB:72:82
            Signature algorithm name: SHA1withRSA
            Version: 3
    ```

    Figure 3. Certificate information

    i. At the end of the certificate information, a prompt displays a request for confirmation that the certificate is trusted:

    ```
    Trust this certificate? [No}
    ```

    j. Type **yes** and press **<Enter>** to respond to the prompt and import the certificate into the `vmware.keystore` keystore. The console displays this message:

    ```
    Certificate was added to keystore
    ```

4. To set the vmcredential as the vmware.keystore path, type **ibmvcfg set vmcredential "C:\VMware\vmware.keystore**

5. Type **ibmvcfg showcfg** to verify that the configuration is correctly saved:

```
cimomHost:                     9.115.246.54
cimomPort:                     5989
username (cimom):              superuser
usingSSL:                      true
vssFreeInitiator:              50000000000000c0
vssReservedInitiator:          50000000000000c1
backgroundCopy:                50
targetSVC:
incrementalFC:                 false
timeout:                       0
rescanOnceArr:                 0
rescanOnceRem:                 0
rescanRemMin:                  0
rescanRemMax:                  45
storageProtocol:               auto
vmhost:                        https://9.115.247.103/sdk
vmusername:                    root
vmcredential:                  C:\vmware103.keystore
```

Figure 4. Verifying the configuration was saved

VMware advanced configuration

N_Port ID Virtualization (NPIV) is an extension to the Fibre Channel industry standard.

In a server virtualization environment, NPIV allows each virtual machine to have a unique Fibre Channel (FC) World Wide Name (WWN), enabling multiple virtual machines to share a single physical host bus adapter (HBA) and switch port. This includes:

- "NPIV implementation requirements"
- "Server Administrator tasks" on page 12
- "Storage Administrator tasks" on page 12
- "Verifying NPIV configuration" on page 13
- "Snapshots with NPIV" on page 13

Note: NPIV is an optional advanced feature.

NPIV implementation requirements

To enable NPIV, ensure that the following hardware and software requirements are met.

- Switches: NPIV must be supported on the switch that is connected to the HBA.
- Host Bus Adapters: HBAs must support NPIV. The following HBA vendors and models are supported:
  - Brocade: Any 4 Gbit/sec or 8 Gbit/sec HBA
  - Emulex: 4Gbit/sec HBA running firmware level 2.70a5 or later. All Emulex 8 Gbit/sec HBAs running firmware 1.00a9 or later.
  - QLogic: Any 4 Gbit/sec or 8 Gbit/sec HBA
- Storage: Because NPIV is not apparent to storage arrays, no specific support is required.
- NPIV can be used only with Raw Device Mapping (RDM) disks. VMFS disks do not support NPIV. To implement NPIV, the physical HBAs port WWN on an ESX(i) Server host must have access to all LUNs that are to be accessed by virtual machines.

Note: NPIV is not necessary for RDM configuration.

- If you deploy a virtual machine from a template or a clone, the new virtual machine does not retain the WWN.

Server Administrator tasks

This section describes server administrator tasks while configuring NPIV.

Procedure

Note: When performing this procedure, ensure that your virtual machine is turned off.

1. Add an RDM disk to the virtual machine.
2. Enable NPIV with VI Client by assigning virtual WWPNs.
3. Record the Node WWN and the Port WWNs. Give this information to the storage administrator so that the administrator can zone and LUN-mask the back-end storage. See "Storage Administrator tasks" for information about the zone and LUN-mask procedures.
4. After the storage administrator completes zoning and configuration of the storage, you can safely turn on the VM.

Storage Administrator tasks

This section describes storage administrator tasks for configuring NPIV.

Procedure

1. Log on to the switch and create separate zones for the virtual port WWNs and physical HBA port WWNs. Zone all the physical HBA port WWNs in a single zone with the storage initiator, and then individually zone the virtual HBA port WWNs of each VM to a storage array port WWN.
2. On the storage subsystem, create separate hosts (SAN Volume Controller) or host connections (DS8000) with separate volume groups for physical HBA ports and virtual HBA ports. For example, in SAN Volume Controller 5.1.

   Create a host with physical HBA WWPNs. The result is:

```
node2:~ # svcinfo lshost 3
id 3
name ESX100
port_count 1
type generic
mask 1111111111111111111111111111111111111111111111111111111111111111
iogrp_count 4
status online
WWPN 21000024FF2FADE0
node_logged_in_count 1
state active
```

Figure 5. Host with physical HBA WWPNs

Create another host for VM with virtual HBA WWPNs. The result is:

You now have two hosts, one for the physical HBA port WWPNs, and one for the virtual port WWPNs. For example:

```
node2:~ # svcinfo lshost 32
id 32
name Win35npiv
port_count 1
type generic
mask 1111111111111111111111111111111111111111111111111111111111111111
iogrp_count 4
status online
WWPN 21050024FF2FAD75
node_logged_in_count 1
state active
```

Figure 6. Host with virtual HBA WWPNs

3. Map the LUN to both hosts so that the LUN can work through NPIV. For example:

```
node2:~ # svcinfo lsvdiskhostmap 22
id name      SCSI_id host_id host_name vdisk_UID                      IO_group_id IO_group_name
22 vm110npiv 0       3       ESX100    6005076802908168E000000000001D3C 0          io_grp0
22 vm110npiv 0       32      Win35npiv 6005076802908168E000000000001D3C 0          io_grp0
```

Figure 7. Map LUN to both hosts

The LUN 22 is mapped to physical HBA ports.

Verifying NPIV configuration

When you configure NPIV and turn on the virtual machine, the NPIV is functioning. To verify that I/O traffic is going through the virtual port (depending on the host HBA), create a Secure Shell connection to the physical ESX(i) Server.

Type one of the following commands, depending on your HBA vendor.

Note: Replace the number 1 at the end of the command with the number of your HBA.
- For a Brocade HBA, type **cat /proc/bfa/1**
- For a QLogic HBA, type **cat /proc/scsi/qla2300/1**
- For an Emulex HBA, **cat /proc/scsi/lpfc/1**

If the virtual WWNs (also known as vPorts) are listed, the virtual machine is functioning correctly.

Note: You can enable NPIV only after at least one RDM disk is attached to the virtual machine.

Snapshots with NPIV

The Volume Shadow Copy Service and Virtual Disk Service automatically detect whether the NPIV is enabled. If the NPIV is enabled and correctly functioning, the Volume Shadow Copy Service and Virtual Disk Service take the appropriate actions during the various snapshot stages.

The Volume Shadow Copy Service and Virtual Disk Service actions during the snapshot stages are as follows:
- "Creating a Snapshot" on page 14
- "Deleting a Snapshot" on page 14
- "Importing a Snapshot" on page 14
- "Masking a Snapshot" on page 14

Creating a Snapshot

During the snapshot-creation process, the Volume Shadow Copy Service and Virtual Disk Service map the snapshot target LUN to both the physical HBA WWPNs and virtual WWPNs.

The LUN is then assigned to the virtual machine from the ESX(i) Server as the RDM disk.

Deleting a Snapshot

The deletion of the snapshot is the opposite of the snapshot creation. During the deletion, the Volume Shadow Copy Service and Virtual Disk Service first unassign the RDM disk from the virtual machine.

The LUN is then masked from both physical HBA WWPNs and virtual WWPNs.

Importing a Snapshot

The import operation also uses NPIV if it is enabled and functioning.

The process is similar to the snapshot-creation process. The Volume Shadow Copy Service and Virtual Disk Service first map the snapshot target LUN to both the physical HBA WWPNs and virtual WWPNs of the destination server. The LUN is assigned to the virtual machine from the ESX(i) Server as the RDM disk.

Masking a Snapshot

Similar to the deletion of the snapshot, the mask operation causes the RDM disk to be removed from the virtual machine.

The LUN is then masked from both the physical HBA WWPNs and the virtual WWPNs.

Snapshots with various Storage Protocols

Because SAN Volume Controller version 5.1 or later also provides iSCSI protocol, the Volume Shadow Copy Service and Virtual Disk Service support both the FC and iSCSI protocols for snapshots, starting from version 4.2. The VSS configuration tool provides an option for choosing the protocol to use if more than one protocol is available. You can choose auto, FC, or iSCSI.

For example:

```
cimomHost:              9.115.246.54
cimomPort:              5989
username (cimom):       superuser
usingSSL:               true
vssFreeInitiator:       50000000000000c0
vssReservedInitiator:   50000000000000c1
backgroundCopy:         50
targetSVC:
incrementalFC:          false
timeout:                0
rescanOnceArr:          0
rescanOnceRem:          0
rescanRemMin:           0
rescanRemMax:           45
storageProtocol:        fc
vmhost:                 https://9.115.247.103/sdk
vmusername:             root
vmcredential:           C:\vmware103.keystore
```

Figure 8. VSS configuration tool

Note: If you choose auto, the Volume Shadow Copy Service and Virtual Disk Service select the protocol to use.

For additional information, see "Storage Protocol Priority."

Storage Protocol Priority

If several protocols coexist, define a priority that determines which protocol is used during the snapshot.

The following cases require a decision on which protocol to use:
- ESX(i) Server has FC HBA and also with software iSCSI enabled.
- ESX(i) Server software has iSCSI enabled, and virtual machine software iSCSI installed.
- ESX(i) Server has FC HBA and with software iSCSI enabled, along with virtual machine software iSCSI installed.

The protocol to be used depends on the storageProtocol parameter of the Volume Shadow Copy Service and Virtual Disk Service configuration and which protocols are available. The priority among the various protocols is as follows:
- ESX(i) Server FC has the highest priority. If the storageProtocol parameter is set to auto, the Volume Shadow Copy Service and Virtual Disk Service first check if ESX(i) Server FC is available. The Volume Shadow Copy Service and Virtual Disk Service try other protocols only when the FC protocol is not available.
- Virtual machine software iSCSI has a higher priority to software iSCSI. If the storageProtocol parameter is set to auto or iSCSI and FC protocol is not available (no HBA or WWPNs not defined on storage), the Volume Shadow Copy Service and Virtual Disk Service first check if iSCSI is enabled on the virtual machine. The Volume Shadow Copy Service and Virtual Disk Service try ESX(i) Server software iSCSI only when the virtual machine software iSCSI is not available.

Special cases and exceptions

The Volume Shadow Copy Service and Virtual Disk Service offer the option to choose the storage protocol.

You responsible for ensuring that changing the storage protocol and Volume Shadow Copy Service and Virtual Disk Service settings for VMware does not affect the previously created snapshots.

Example of a special case that causes problems

This example illustrates a special case that can cause some problems. The procedure in this example is as follows:
1. Create a snapshot with the FC protocol.
2. Change the protocol setting to virtual machine iSCSI.
3. Incorrectly modify or clear the VMware settings.
4. Delete the previous created snapshot.

In this case, the FlashCopy® map is removed on storage and the target LUN is unmapped from the hosts. However, the RDM file remains on the ESX(i)(i) Server because the VMware settings (vmhost, vmuser, vmpassword, or vmcredential) were incorrectly set. This leaves the Volume Shadow Copy Service and Virtual Disk Service unable to communicate with the ESX(i) Server.

If the VMware settings are correct, the deletion process can still be successful with RDM file removal.

If this example case occurs, a warning message displays when the user tries to change the VMware settings using **ibmvcfg**.

It is not necessary to configure the Volume Shadow Copy Service and Virtual Disk Service parameters (such as vmhost and vmuser) for VMware. If you decide to use the virtual machine software iSCSI protocol, all processes are performed using Ethernet protocol.

Chapter 4. Configuring Hyper-V

With the Volume Shadow Copy Service and Virtual Disk Service, you can take shadow copies in the Hyper-V guest OS.

If you installed the software ISCSI initiator in the guest OS and you do not plan to use FC protocol or ISCSI protocol on the host, the configuration is the same as physical host.

Because the guest OS does not support an FC HBA, Volume Shadow Copy Service and Virtual Disk Service serve as a bridge to associate the FC HBA on the host to the guest OS when creating and deleting a shadow copy. VSS VDS also supports the host ISCSI, depending on host and provider settings. Privileges to access the host WMI are required to support this feature.

VSS VDS cannot support the hardware information of a virtual hard disk. Therefore, VSS VDS supports shadow copies only on pass-through disks in the guest OS. The VSS VDS automatically attaches the target LUN of the volume shadow copy to the guest OS as a pass-through disk.

Hyper-V basic configuration

Basic configuration enables you to create shadow copies in the Hyper-V guest OS.

Basic configuration includes:
- "Hyper-V requirements"
- "Configuring the Host (Hyper-V) Server"
- "Configuring Volume Shadow Copy Service and Virtual Disk Service using Hyper-V" on page 18
- "Configuring source volumes using Hyper-V" on page 19
- "Taking snapshots using Hyper-V" on page 19

Hyper-V requirements

The following requirements must be met to configure the Hyper-V guest OS.
- Volume Shadow Copy Service and Virtual Disk Service 4.5.0.
- Server Hardware: Microsoft recommended server configuration for Microsoft Windows Server 2008 Hyper-V.
- Microsoft Windows Server 2008 Hyper-V.
- Multipathing I/O (MPIO) software. Available from your storage array vendor.

Configuring the Host (Hyper-V) Server

Configure the host server to create shadow copies in the Hyper-V guest OS.

Procedure
1. Install one of the following:
   - Microsoft Windows Server 2008 x64
   - Windows Server 2008 R2
   - Microsoft Windows server 2012

2. Install the Hyper-V role on the Windows Server using the Server Manager, and then reboot the server.

3. Disable automount for the disks on the host. Type the following commands:
```
C:\>diskpart
C:\>diskpart>automount disable
```

4. To allow for remote administration on the physical host, enable the Windows Firewall: `netsh firewall set service RemoteAdmin enable`.

5. Install the Multipath I/O (MPIO) driver that ships with Windows 2008.

6. Install the MPIO driver that your storage vendor supplied.

7. Install and configure the Hyper-V guest OS using the Hyper-V Manager. The guest OS should be Windows 2003 R2 or later.

8. Download and install Microsoft Visual C++ 2008 SP1 Redistributable Package on physical host. The package can be download from the Microsoft website:
   - Microsoft Visual C++ 2008 SP1 Redistributable Package (x64)
   - Microsoft Visual C++ 2008 SP1 Redistributable Package (x86)

   Note: The x86 and x64 versions must both be installed.

Configuring Volume Shadow Copy Service and Virtual Disk Service using Hyper-V

Configure the Volume Shadow Copy Service and Virtual Disk Service using the Hyper-V guest OS.

Procedure

1. Log on to the Hyper-V guest OS.

2. Install the Volume Shadow Copy Service and Virtual Disk Service.

3. Copy the `ibmrescan.exe` file from the installation directory to the physical host.

4. Set the parameters to access the host server. For this step, you need the host server IP address, domain, user name, and password. The following list provides information about settings and the relevant commands.
   - To set the IP address of the Host Server, type: **ibmvcfg set vmhost <hyper-V host IP address>**
   - To set the user name, type: **ibmvcfg set vmusername <hyper-V host user name which can manage hyper-V>**
   - To set the password, type: **ibmvcfg set vmpassword <hyper-V host user password>**
   - To set the domain, type: **ibmvcfg set vmdomain <hyper-V host user domain>**
   - To set the command to rescan devices on physical host, type: **set rescandevicecmd <command on host to rescan device>**

     For example, **set rescandevicecmd "C:\ibmrescan.exe"**

   To view the configuration settings, type **ibmvcfg showcfg**

   a. Provide the following privileges for the user:
      - Access WMI on the host Server
      - Query WMI objects in the following name spaces: `root/cimv2`, `root/wmi`, `root/default` and `root/virtualization`.
      - Create a process with class `Win32_Process` in `root/cimv2`.
      - Manage the resources in the `root/virtualization` name space.

   b. Set the domain as the host name if the user does not belong to a Windows domain.

Configuring source volumes using Hyper-V

Because the Volume Shadow Copy Service and Virtual Disk Service support taking shadow copies only for volumes that are based on disks from SVC or DS8000, the disks must be assigned to the guest OS by the pass-through mode.

Procedure

1. Shut down the guest OS and add SCSI Controller to the guest OS.
2. Add the pass-through disk drive to the guest OS.

   Note: The guest OS can be in the running state, but the disks should be the offline state on the host, so that they can appear in the physical hard box combo box.
3. Log on to the guest OS, create a volume on the newly added hard disk, and assign a drive letter or mount point to the volume.

Taking snapshots using Hyper-V

You need to configure LUNs with the same size as the source LUNs as snapshot targets in the free pool on storage.

Before taking a snapshot for the volume on the guest OS, type the following command to check if the configuration is correct.

Note: The command supports one or more drive letters or mount points. In the example command, X: is the driver letter or mount point to take the snapshot.
`ibmvcfg testsnapshot X:`

The procedures to take, delete, mask, resynchronize, and import snapshots are the same as the procedures for the physical host. Provider attaches the target LUNs to the physical host and then assigns it to the guest OS as a pass-through disk when taking or importing a snapshot. When deleting or masking a snapshot, IBM VSS Hardware Provider removes the target LUN from the guest OS before detaching it from the physical host.

See "Snapshots with NPIV" on page 13 for information on these tasks.

Hyper-V advanced configuration

Advanced configuration includes NPIV(N_Port Virtualization) configuration and storage protocol priority support in the Volume Shadow Copy Service and Virtual Disk Service.
- "Creating a virtual port with Microsoft Windows 2012 Virtual HBA"
- "Configuring NPIV with Hyper-V" on page 20
- "Setting the storage protocol" on page 22

Creating a virtual port with Microsoft Windows 2012 Virtual HBA

Before configuring the Hyper-V guest OS, it is necessary to configure the Microsoft Windows 2012 virtual HBA.

Before you begin

The following requirements are necessary to configure Microsoft Windows 2012 Virtual HBA with Hyper-V:

- NPIV-enabled FC adapter
- NPIV-enabled FC Switch
- Microsoft Windows server 2012
- NPIV WMI provider that is installed on the host. (Most of the FC drivers implement this provider.)

Procedure

1. Click **Virtual SAN Manager** in the right panel of the Windows 2012 Hyper-V Manager.
2. Create a virtual SAN and select the HBA to be virtualized.
3. In the Hyper-V guest OS settings, add a Fibre Channel adapter. Specify the virtual SAN created in 2.
4. In the Open Switch Administration panel, double-check the WWPN of the virtual HBA from the name server. Typically, it should share a port with the physical HBA.
5. Modify the zone configuration to make the virtual HBA visible to the storage port.

Creating a zone with Microsoft Windows 2012 Virtual HBA

This section describes creating a zone with Microsoft Windows 2012 Virtual HBA.

Procedure

1. Create a zone using NPIV.
2. Create an alias and zone with the virtual port that you created in "Creating a virtual port with Microsoft Windows 2012 Virtual HBA" on page 19. However, do not add the host WWN to the zone.

   Note: The zone contains the new virtual port that you created and the storage. It is not necessary to reboot the host to make the NPIV port available.

Configuring storage with Microsoft Windows 2012 Virtual HBA

This section describes configuring storage with Microsoft Windows 2012 Virtual HBA.

Procedure

Add the virtual port to the LUN that will contain the guest.

Note: It is not necessary to add the physical port to the LUN.

Taking a snapshot with Microsoft Windows 2012 Virtual HBA

This section describes taking a snapshot with Microsoft Windows 2012 Virtual HBA using Hyper-V.

The procedure for taking a snapshot is the same as "Creating a Snapshot" on page 14. The provider automatically attaches the LUN to the guest OS through a virtual port.

Configuring NPIV with Hyper-V

Advanced configuration includes NPIV(N_Port Virtualization) configuration and storage protocol priority support in Volume Shadow Copy Service and Virtual Disk Service.

Note: The following sections do not apply to the ISCSI protocol.
- "Requirements for configuring NPIV with Hyper-V"
- "Creating a virtual port"
- "Creating a zone"
- "Configuring storage"
- "Configuring the host disk"
- "Deploying guests" on page 22
- "Configuring source volume" on page 22
- "Verifying NPIV configuration" on page 22
- "Taking a snapshot" on page 22

Requirements for configuring NPIV with Hyper-V
This section describes requirements for configuring NPIV with Hyper-V.
- NPIV-enabled FC Adapter
- NPIV-enabled FC Switch
- FC HBA Manager and Agent with V-Port creation feature
- NPIV WMI provider installed on host. (Most of the FC drivers implement this provider.)

Creating a virtual port
Create a virtual port using the FC HBA Manager GUI.

Procedure
1. Open FC HBA Manager GUI.
2. Select a physical port and create a virtual port on it.

Creating a zone
Create a zone using NPIV.

Create an alias and zone with the virtual port that you created in "Creating a virtual port" but do not to add the host WWN to the zone.

Note: The zone contains only the new NPIV port that you created and the storage. You do not need to reboot the host to make the NPIV port available.

Configuring storage
Add the virtual port to the LUN that will contain the guest.

You do not need to add the physical port to the LUN.

Configuring the host disk
For virtual disks, bring the new LUN online and initialize it. Assign drive letters to the volume to contain the guest OS configuration files and VHDs. A volume with a mount point is not supported by Volume Shadow Copy Service and Virtual Disk Service NPIV.

For pass-through disks, two LUNs per guest are required. One LUN is required for the configuration files, and the other LUN is required to install the OS. The volume that contains configuration files must be assigned a drive letter. Make sure that the disk is offline when you install the OS.

Deploying guests

You can use Hyper-V Manager or Microsoft System Center Virtual Machine Manager to deploy guests.

Deploying with Hyper-V Manager

1. Open Hyper-V Manager.
2. Click **New** > **Virtual Machine...** in the Actions panel.
3. When you are prompted for a location for the virtual machine, choose the volume that is on the LUN that you created in "Configuring storage" on page 21.

After memory and networking configurations, specify the name and location of the hard disk where you want to install the guest OS. If you are using a virtual hard disk, locate the hard disk on a volume that is on the LUN through the virtual port. If you are using a pass-through disk, the disk should be from the virtual port, should be offline, and should be configured as MBR disk type. A pass-through disk does not support GPT and dynamic disk types. If the disk is previously configured as GPT or dynamic, you must bring the disk online and convert it, in which case you need to shut down the guest.

Deploying with SCVMM

If the host is managed by Microsoft System Center Virtual Machine Manager (SCVMM), you can create a virtual machine through SCVMM. When you are prompted for the host on which to place the guest, select the host that has the virtual port active. When you are prompted for a location for the files, click **Browse** and select the LUN that you created. If you do not see the LUN, refresh the disks or check the host to make sure the disk is online and formatted. .

Configuring the disk to install the guest OS is the same as configuring Hyper-V Manager to install the guest OS.

Configuring source volume

The procedure for configuring the source volumes is the same as in "Configuring source volumes using Hyper-V" on page 19 except the LUN is through the virtual port.

Verifying NPIV configuration

Verify the NPIV configuration using the FC HBA Manager.

To make sure that a LUN is from virtual port, you can open FC HBA Manager and verify that the LUN is under the virtual port (some of the FC HBA Managers do not support this feature).

Taking a snapshot

The procedure for taking a snapshot is the same as in "Taking snapshots using Hyper-V" on page 19, except provider automatically attaches the LUN to the host through a virtual port.

Setting the storage protocol

Because the Volume Shadow Copy Service and Virtual Disk Service support the ISCSI feature for SAN Volume Controller 5.1 or later, the storage protocol setting is determined by the protocol that attached the target LUNs to the host.

The following options are available for this setting:

Auto   Volume Shadow Copy Service and Virtual Disk Service automatically choose the appropriate protocol. If no protocol is available on the host, the snapshot fails.

FC   Volume Shadow Copy Service and Virtual Disk Service choose the Fibre Channel protocol. If the FC protocol is not available, the snapshot fails.

ISCSI   Volume Shadow Copy Service and Virtual Disk Service choose the ISCSI protocol. If the ISCSI protocol is not available, the snapshot fails.

Use the following command to set the storage protocol: `ibmvcfg set storageprotocol <auto, fc, iscsi>`

If more than one storage protocol is installed on the host and guest OS, Volume Shadow Copy Service and Virtual Disk Service follow an algorithm to choose the correct protocol. The protocol is as follows:

1. Protocol setting is auto
   - If FC and ISCSI coexist, choose FC before ISCSI.
   - If ISCSI installed on both guest and host, choose ISCSI on guest before on host.
2. Protocol setting is FC
   - If FC protocol is available, choose uses FC protocol on host.
3. Protocol setting is ISCSI
   - Ignore FC configuration with this setting.
   - If ISCSI is installed on both guest and host, choose ISCSI on guest before on host.

Priorities for storage protocol settings lists the protocol settings and their priorities.

Table 4. Summary table of protocol selections

Protocol Setting	Guest OS	Host	Using
Auto	None	FC, ISCSI	FC on Host
	ISCSI (software initiator)	FC	FC on Host
		ISCSI	ISCSI on host
		None	ERROR
		FC, ISCSI	FC on Host
		FC	FC on Host
		ISCSI	ISCSI on Guest
		None	ISCSI on Guest
FC	None	FC, ISCSI	FC on Host
		FC	FC on Host
		ISCSI	ERROR
		None	ERROR
	ISCSI (software initiator)	FC, ISCSI	FC on Host
		FC	FC on Host
		ISCSI	ERROR
		None	ERROR

Table 4. Summary table of protocol selections (continued)

Protocol Setting	Guest OS	Host	Using
ISCSI	None	FC, ISCSI	ISCSI on host
		FC	ERROR
		ISCSI	ISCSI on host
		None	ERROR
	ISCSI (software initiator)	FC, ISCSI	ISCSI on Guest
		FC	ERROR
		ISCSI	ISCSI on Guest
		None	ERROR

Chapter 5. Best Practices

Use these best practices while configuring the Volume Shadow Copy Service and Virtual Disk Service.

- "Limitations"
- "Troubleshooting" on page 26

Limitations

The topics in this section describe limitations related to Volume Shadow Copy Service and Virtual Disk Service support.

Ensuring that no shadow copy exists before you change settings that are related to FC/ISCSI initiators

If you configured Volume Shadow Copy Service and Virtual Disk Service to attach target LUN to the guest OS through the host FC/ISCSI when creating or importing a shadow copy, you must delete or mask the shadow copy with the same configuration.

Ensure that no shadow copy exists before you change settings that are related to FC/ISCSI initiators.

The **ibmvss** settings are as follows:

- **storageProtocol**
- **VMHost**
- **Vmusername**
- **vmpassword**
- **vmdomain**

The hardware or OS settings are as follows:

- enable/disable host FC/ISCSI HBA
- enable/disable host software ISCSI
- enable/disable guest OS software ISCSI

Incremental FlashCopy mapping persists

Incremental FlashCopy copies only the changes to either the source or target data since the last FlashCopy operation. It is designed to enable completion of point-in-time online backups much more quickly than using traditional FlashCopy.

In IBM VSS Hardware Provider, to enable incremental FlashCopy mapping, type: **ibmvcfg.exe set incrementalFC Yes**.

Once set to incremental, all FlashCopy created is incremental until you return to regular FlashCopy by typing **ibmvcfg.exe set incrementalFC No**.

Assume an Incremental FlashCopy mapping called "fcmap1" has been created, where F1 is the source volume mapped to host and F2 is the target volume. Then F1 can be used as a source volume in only one FlashCopy mapping. If the FlashCopy mapping is deleted from IBM VSS Hardware Provider, the target

volume F2 returns to the free pool, but the FlashCopy mapping still exists in storage. When a new incremental FlashCopy using F1 as the source volume is created later, F2 and fcmap1 are reused.

Deleting and restoring cascaded FlashCopy mappings

SAN Volume Controller and Storwize 7000 can minimize the overhead required to maintain multiple snapshots of the same source volume by putting the target volumes into a cascade where each target is dependent on changes recorded in target volumes of subsequent snapshots.

For example, assume that four VSS snapshots are created of a source volume, where S is the source volume and T1 through T4 are the targets, T1 being first chronologically and T4 the last. The following cascade occurs: **S** > **T4** > **T3** > **T2** > **T1**

With this type of cascade relationship, a copy-on-write process is needed only between the source volume and the latest FlashCopy target. Any blocks that remain unchanged on the source volume are not copied at all.

In IBM VSS Hardware Provider, to enable cascading FlashCopy mapping, type `ibmvcfg.exe set backgroundCopy 0`.

To disable cascading FlashCopy mapping, type `ibmvcfg.exe set backgroundCopy <n>` where <n> is a number in the range 1–100.

When enabling cascading, sequentially create the FlashCopy mappings: **S** > **T1**, **S** > **T2**, **S** > **T3**, and **S** > **T4**.

If you delete mapping **S** > **T2**, then **S** > **T1** is also deleted, and only **S** > **T3** and **S** > **T4** exist.

If you later restore mapping **S** > **T2**, then **S** > **T3** and **S** > **T4** are deleted, and only **S** > **T1** and **S** > **T2** exist.

Troubleshooting

The topics in this section provide troubleshooting information that is related to Volume Shadow Copy Service and Virtual Disk Service support for Hyper-V.

Provider cannot find FC or ISCSI initiator

1. Verify the FC and ISCSI configurations on the host, SAN, and storage. Make sure that at least one initiator is installed on the host or the guest OS.
2. Verify the settings for Hyper-V. Ensure that the IP address, user name, password, and domain are set correctly, that the user is authorized to access WMI on the host, and that the domain is set as the host's computer name if it is not the domain user.
3. Ensure that the storage protocol setting and the existing initiator configuration are not in conflict.

Volume not supported by Volume Shadow Copy Service and Virtual Disk Service

Verify that the volume on the disk is supported by the Volume Shadow Copy Service and Virtual Disk Service. The disk must be from SAN Volume Controller or

DS8000 and must be added to the guest OS as a pass-through disk. Virtual hard disks are not supported by the Volume Shadow Copy Service and Virtual Disk Service, although they may be supported on the LUN from SAN Volume Controller or DS8000.

Importing a shadow copy failed or locating a LUN failed while taking the shadow copy

Either the guest OS has no SCSI controller or the address on the SCSI controller on the guest OS is insufficient. Shut down the guest OS and add the SCSI controller to the guest OS.

Target LUNs are not attached to the host through the virtual port

1. Verify the virtual port configuration on the host, SAN, and storage.
2. Verify that the guest OS configuration files are on the LUN through the virtual port. The volume on the LUN must be assigned a drive letter. A mount point is not supported.
3. Ensure that the storage protocol is not set to ISCSI.

VMware virtual machine not recognized as virtual machine

The VMware virtual machine is not recognized as a virtual machine because the **systeminfo** in the VM is incorrect.

The correct **systeminfo** is:
- `System Manufacturer: VMware, Inc`
- `System Model: VMware Virtual Platform`

If the option `SMBIOS.reflectHost = "TRUE"` in the virtual machine's configuration file (vmx) is added, the **systeminfo** is changed.

For example:
- `System Manufacturer: IBM`
- `System Model: Custom_`

Note: If the VM is converted by the VMware vCenter Converter, the option is added automatically.

To correct this, do the following:
1. Shut down the virtual machine.
2. Delete the option.
3. Turn on the virtual machine.

Notices

The legal notices pertain to IBM storage product documentation.

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Almaden Research
650 Harry Road
Bldg 80, D3-304, Department 277
San Jose, CA 95120-6099
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

This section describes trademark information.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of the International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Copyright and trademark information website at:

http://www.ibm.com/legal/us/en/copytrade.shtml

VMware, the VMware logo, ESX, ESXi, vSphere, and vCenter are trademarks or registered trademarks of VMware Corporation in the United States, other countries, or both.

Microsoft, Windows Server, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Other product and service names might be trademarks of IBM or other companies.

Index

A
about this document
    sending comments   x

B
best practices   25
    troubleshooting   26

C
comments, sending   x
configuration   6, 7, 8, 9, 17
    Hyper-V   17, 18
        configuring source volumes   19
        Microsoft Windows 2012 virtual
         HBA   19
        NPIV   21
        requirements   17, 21
    NPIV   11, 21
        server administration tasks   12
        storage administration tasks   12
        verify   13
    physical environment   3
    VMware environment   5
    VSS Hardware Provider   18
configuring Microsoft Windows 2012
  virtual HBA   19
creating
    NPIV   14

D
deleting
    NPIV   14
deploying guests   22
documentation
    improvement   x

G
generating JAVA credential keystore   9

H
host
    configuration
        Hyper-V   17
host disk
    configuration   21
Hyper-V   17, 21
    advanced configuration   19
    basic configuration   17
    configuration   17
        configuring source volumes   19
        VSS Hardware Provider   18
    configuring Microsoft Windows 2012
      virtual HBA   19

Hyper-V *(continued)*
    configuring NPIV
        requirements   21
    requirements   17, 19

I
importing
    NPIV   14
installation
    using Fibre Channel   3
    using iSCSI   3
introduction   1

L
limitation   25

M
masking
    NPIV   14

N
NPIV
    configuration   11, 12, 13
        Hyper-V   21
        verify   22
    configuration requirements   21
    requirements   11
    server administration tasks   12
    snapshot   22
    storage administration tasks   12
    verify   13

P
physical environment
    installation   3
prerequisites
    supported platforms   5
Prerequisites
    VMware Tools
        installing   6
    vSphere Web Services   6
provider parameters for VMware   8
provider settings for VMware   7

R
reader feedback, sending   x

S
sending
    comments   x
snapshot   22

snapshots   14
    NPIV   13
    storage protocols   14
    using Hyper-V   19
source volume
    configuring   22
storage
    configuring   21
storage protocol priority   15
    special cases and exceptions   15
Storage Protocol setting   23

U
user privileges   6

V
verify NPIV configuration   22
virtual port
    create   21
VMware Tools
    installing   6
vSphere Web Services   6

Z
zoning
    create   21

IBM ®

Printed in USA