# Preface

## Chapter 1 Introduction

### Introduction to VMware support

- Backup and Recovery types
- Guest based backup and recovery
  - Recommendations for NetWorker installed in a virtual machine
  - Advantages
  - Disadvantages
  - Installation
  - Configuration
  - Recovery
  - Recommendations and considerations for guest-based backup

### VADP based backup and recovery

- Advantages
- Disadvantages
- Software and hardware requirements
- Limitations to vCenter on non-English versions of Windows
- Limitations for VADP proxy host on non-English versions of Windows
- Transport modes
- Support for directives
- Incremental backups with image level backups
- Changed Block Tracking (CBT)
- Independent persistent disks are not backed up

### Licensing NetWorker support for VMware

- Virtual environments simplified licensing
- Using existing licenses to support VADP
- AMP virtual appliance
- Guest-based licensing
- VADP licensing

## Chapter 2 Upgrading

### Upgrading to vSphere 5.0

- Upgrading to 7.6 Service Pack 2 and later for VMware VADP backups
- Upgrade existing NetWorker server and VCB proxy
- Change vCenter role privileges after upgrading
- Upgrade only the proxy client to NetWorker 7.6 SP2 or later
- Upgrade to use vCenter if ESX/ESXi server was previously used for VM backups
- Space requirement changes on proxy for VADP vs VCB
- Post-upgrading steps for Virtual Center on a 64-bit Windows host

## Chapter 3 Managing and Monitoring Virtual Machines (VMs)

### Automatic discovery of VMware environments

- Performing on-demand auto-discovery of VMware environments
- Notifications of changes to VMware environments
Set up notifications ................................................................. 33
Monitor VMs ......................................................................... 34
Visual Representation of VMware environments ..................... 34
Virtualization node hierarchical display of the VMware environment .... 34
Graphical display of the VMware environment ......................... 35
Launch vSphere client from the NetWorker Console (Windows only) ..... 37

Chapter 4 Configuring NetWorker Clients for VADP Backup

Configuration options .............................................................. 40
Task 1: Configuring the VADP proxy host and Hypervisor resource 40
  Configure a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard ... 40
  Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows .............................. 43
Task 2: Configuring a virtual client for backup................................. 48
  Configure a virtual client if vCenter is configured and auto-discovery has been run ............................................................. 49
  Configure a virtual client manually by using the Client Properties window .. 51
Task 3: Creating a VADP User role in vCenter................................. 52
  Create a VADP Proxy role ......................................................... 52
  Assign the VADP User role to the user specified in the NetWorker Hypervisor resource: ......................................................... 53
  Minimum vCenter permissions needed to back up and recover using VADP 53
Task 4: Configuring Changed Block Tracking (CBT) ......................... 55
  Enable CBT using the command line ........................................... 55
  Enable CBT using the vSphere Client GUI ...................................... 56

Chapter 5 Recovering VADP Backups

File based recovery of a VM ......................................................... 58
  Perform a file based recovery on the local host......................... 58
  Perform a file based recovery using CIFS share ......................... 58
  Perform a file based recovery using directed recovery ............... 59
Image level (single step) recovery of a full VM ......................... 59
  Recommendations and considerations ........................................ 59
  Perform an image level recovery from the NetWorker User program ..... 60
  Perform an image level recovery from the command line .......... 62
  Recover VMs that have a mix of VADP image-level and traditional guest based backups ......................................................... 63
  Image level recovery to a different FARM or vCenter ................... 65
  Recovery of a VM using NBDSSL or hotadd transport mode .......... 65
  Recovery of a VM using SAN or hotadd transport mode on Windows 2008 .. 66
  Recovery of pre-NetWorker 7.6 SP2 VM backups ....................... 66

Chapter 6 VADP Planning and Best Practices

Recommendations and considerations for VADP backup and recovery...... 70
Application-level consistent backups ........................................ 71
  Option to enable or skip quiescing in the Application Information tab in NMC ................................................................. 71
  Advanced use and troubleshooting ............................................. 72
Contents

Selection of physical vs. virtual proxy .......................................................... 72
Backup targets for virtual proxy hosts.......................................................... 72
Proxy node sizing and performance considerations ............................... 73
VADP snapshot recommendations .............................................................. 73
Manually quiescing VADP snapshots.......................................................... 75
Recommendations for Data Domain systems............................................... 76
Network and Firewall port requirements ...................................................... 77
Memory requirements for the VADP proxy.................................................... 77
VADP mount point recommendations and space considerations........... 78
Support for tape drives in a VM ................................................................. 79
VMDirectPath requirements and recommendations ............................. 79
VMDirectPath restrictions...................................................................... 80
Considerations for VMDirectPath with NetWorker .............................. 80
Recommendations and considerations for transport modes ............... 81
SAN transport mode.............................................................................. 81
Hotadd transport mode ......................................................................... 81
NBD/NBDSSL transport mode .............................................................. 83
Performance optimization ...................................................................... 84
VADP proxy access to LUNs ................................................................. 85
SAN transport mode.............................................................................. 85
Hotadd transport mode ......................................................................... 86
NBD/NBDSSL transport modes............................................................. 86
Diskpart utility for SAN and hotadd transport modes ....................... 86

Glossary

Index
PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC representative if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. New versions of this document might be released on the EMC online support website. Check the EMC online support website to ensure that you are using the latest version of this document.

Purpose

This document describes the integration of VMware with NetWorker.

Audience

This guide is part of the NetWorker documentation set, and is intended for use by system administrators who are responsible for setting up and maintaining backups on a network. Operators who monitor daily backups will also find this guide useful.

Related documentation

The following EMC publications provide additional information:
- NetWorker Release 8.0 Administration Guide
- NetWorker Release 8.0 Installation Guide
- NetWorker Release 8.0 Cluster Installation Guide
- NetWorker Release 8.0 Release Notes
- NetWorker Avamar Integration Guide
- NetWorker Data Domain Deduplication Devices Integration Guide
- NetWorker License Manager 9th Edition Installation and Administration Guide
- NetWorker Licensing Guide
- NetWorker Release 8.0 Error Message Guide
- NetWorker Release 8.0 Performance Optimization Planning Guide
- NetWorker Release 8.0 Command Reference Guide
- NetWorker Management Console Online Help
- NetWorker User Online Help
Conventions used in this document

EMC uses the following conventions for special notices:

**NOTICE**

NOTICE is used to address practices not related to personal injury.

**Note:** A note presents information that is important, but not hazard-related.

**IMPORTANT**

An important notice contains information essential to software or hardware operation.

**Typographical conventions**

EMC uses the following type style conventions in this document:

**Normal**

Used in running (nonprocedural) text for:
- Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus
- Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities
- URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications

**Bold**

Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages

Used in procedures for:
- Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus
- What the user specifically selects, clicks, presses, or types

**Italic**

Used in all text (including procedures) for:
- Full titles of publications referenced in text
- Emphasis, for example, a new term
- Variables

**Courier**

Used for:
- System output, such as an error message or script
- URLs, complete paths, filenames, prompts, and syntax when shown outside of running text

**Courier bold**

Used for specific user input, such as commands

**Courier italic**

Used in procedures for:
- Variables on the command line
- User input variables

< > Angle brackets enclose parameter or variable values supplied by the user

[] Square brackets enclose optional values

| Vertical bar indicates alternate selections — the bar means “or”

{} Braces enclose content that the user must specify, such as x or y or z

... Ellipses indicate nonessential information omitted from the example
Where to get help

EMC support, product, and licensing information can be obtained as follows:

**Product information** — For documentation, release notes, software updates, or information about EMC products, licensing, and service, go to the EMC online support site (registration required) at:

http://support.EMC.com

**Technical support** — For technical support, go to EMC online support and select Support. On the Support page, you will see several options, including one to create a service request. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

BSGdocumentation@emc.com
Preface
CHAPTER 1
Introduction

This chapter covers these topics:

- Introduction to VMware support ................................................................. 12
- Guest based backup and recovery ............................................................... 13
- VADP based backup and recovery ............................................................... 15
- Licensing NetWorker support for VMware .................................................. 21
Introduction to VMware support

The NetWorker software provides support for backup and recovery of VMware virtual clients using traditional NetWorker file system backup and recovery or by using VMware backup technologies such as VCB or the vStorage APIs for Data Protection (VADP), which provide LAN-free backups of VMware virtual machines (VMs). Additionally, the NetWorker software provides automatic discovery of VMware environments and notification of changes to those environments, and provides both a graphical map and tabular view of VMware environments.

Backup and Recovery types

The following types are available:

- **Guest based backup and recovery** — Guest based backup involves installing a NetWorker client within each virtual machine host. This is still a popular way to protect VMs due to the same workflow implemented for a physical machine. This means backup configurations and recovery options follow traditional methods that administrators are already familiar with. There are no added configuration requirements however, there is a load consideration on the physical servers and resources. Therefore, care must be taken when considering operations on all VMs.

- **Image level backup and recovery** — Image backup and recovery uses VMware Consolidated backup (VCB) for pre-NetWorker 7.6 SP2 releases, or vStorage APIs for Data Protection (VADP) technology to offload backup processing from the server to a separate backup proxy host. With this option, challenges associated with resource utilization on the server can be avoided as the proxy host inherits the workload. However, this option is more complex to configure and requires additional hardware and infrastructure.

Note: Proxy hosts using NetWorker 7.6 SP2 and later use VADP only. For VCB support with a NetWorker 7.6 SP2 or later server, a NetWorker 7.6 SP1 proxy host is required.

Table 1 on page 12 provides a quick comparison between guest based and VADP based backup and recovery.

Table 1 Comparing Guest based versus Image backup and recovery

<table>
<thead>
<tr>
<th>Option</th>
<th>Guest based</th>
<th>Image (VCB or VADP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommend for</td>
<td>• Single file and database backups.</td>
<td>• LAN free backups</td>
</tr>
<tr>
<td></td>
<td>• Shared storage not available</td>
<td>• Disaster recovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Shared storage environments</td>
</tr>
<tr>
<td>VMDK level backups</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Individual file backups</td>
<td>Yes</td>
<td>Yes for Windows guest OS only</td>
</tr>
<tr>
<td>File level restore</td>
<td>Yes</td>
<td>Yes for Windows guest OS only</td>
</tr>
<tr>
<td>Deduplication supported</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Impact on virtual machine</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>
Introduction

Guest based backup and recovery operations are essentially the same as backing up and recovering a physical machine. Regardless of the virtualization technologies involved, VMs are complete OS installations hosted on virtualized hardware. These installations can be protected using the same basic techniques as their physical counterparts, that is, running a NetWorker client inside the virtual machine. The same OS support rules apply as they would to a physical machine.

Recommendations for NetWorker installed in a virtual machine

Consider the following recommendations when installing the NetWorker software on VMs:

- Have more CPU reservation and shares for the virtual machine hosting the NetWorker Server.
- Have more Memory reservation for the virtual machine hosting the NetWorker Storage Node.
- Set a high restart priority for the virtual machine hosting the NetWorker Server and Storage Node.
- Have the NetWorker Server, NetWorker Clients and NetWorker Storage Node connected to same virtual switch.
- Leverage the guest based deduplication for NetWorker clients.

Advantages

The following are advantages of guest-based backups:

- This is a simple and familiar implementation. Traditionally, most physical machine backups have been performed this way, which makes the transition to virtual machine backups using this technology a straight forward task.
- Database and application backups are supported as well. Configuration is as simple as installing and configuring the appropriate NetWorker database or application module. Note that application support is only available from within the client.
- Single file backup and restore is supported.
- All protected data is correctly referenced in the NetWorker server and client file index to the originating virtual machine.
- Restoring individual files directly to the virtual machine is supported.
- Incremental backups are easily configured.

<table>
<thead>
<tr>
<th>Option</th>
<th>Guest based</th>
<th>Image (VCB or VADP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact on ESX server</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Backup performance</td>
<td>Slower</td>
<td>High</td>
</tr>
<tr>
<td>Additional hardware requirements</td>
<td>No</td>
<td>Uses physical or virtual proxy, depending on implementation</td>
</tr>
</tbody>
</table>

Table 1: Comparing Guest based versus Image backup and recovery
Introduction

- Advanced VMware features and configurations, like Distributed Resource Scheduling (DRS) and VMotion, have no impact on the performance of NetWorker.
- In guest, host based source deduplication is available.
- Full directive support.

Disadvantages

The following are disadvantages of guest-based backups:

- Image level backup and recovery is not supported. Image level backup and recovery is mostly used to support disaster recovery.
- The backup processing load on one virtual machine will negatively impact system resources available to all VMs hosted on the same physical ESX server, even when source based deduplication is being used.
- Resource-intensive backups often place a heavy load on shared network and CPU resources.
- Client software installed on each virtual machine needs to be maintained and updated.
- The virtual machine must be powered on for backup processing to occur.

Installation

From an installation perspective, guest based backup and recovery is the most straightforward. A NetWorker client is installed on the virtual machine. The installation procedure for a virtual machine is the same as it would be for the operating system hosted on a physical machine.

Configuration

For standard file backups, the client configuration in the virtual machine is the same configuration procedure as for a physical machine.

Recovery

One advantage of this configuration is that recoveries are simple. This process is exactly the same as if the user was recovering files to a physical host, and allows individual users to perform their own recoveries.

Recommendations and considerations for guest-based backup

Guest based backup activities on a single virtual machine can create a significant load on the parent ESX Server and, therefore, indirectly impact every other virtual machine that is also hosted on the ESX Server. Backup policies should be defined to limit the number of simultaneous backup jobs that are running on each physical ESX Server. For example, you can use NetWorker backup groups to back up a selection of VMs across multiple ESX servers in order to minimize the impact on individual ESX servers and maximize the throughput of the backup.
NetWorker includes technology that can be used to minimize or eliminate full backups. If only incremental backups are performed, only the data that has changed since the previous backup is copied to the NetWorker storage node, which significantly decreases the I/O associated with backups and the amount of backup network traffic. As well, guest based deduplication can be leveraged to minimize the impact on the ESX servers shared resources, essentially eliminating the contention on CPU and memory.

This backup technique lends itself very well for database and application backups. Configuring a database or application backup in a virtual machine is essentially the same as configuring the same database and application backup on a physical machine. This technique can simplify and enhance database and application backups, often providing incremental capabilities and restores directly to the virtual machine. Guest based database deduplication is also supported for databases to help minimize impact on an ESX servers resources.

VADP based backup and recovery

NetWorker for VMware provides an alternate client backup technology for VMs in conjunction with vStorage APIs for Data Protection (VADP) technology from VMware.

VADP helps to perform backups from a VADP backup proxy server, which can be a physical or virtual machine, using the VMware snapshot technique (A point in time copy of the virtual machine). VADP can be used with a vCenter Server.

Advantages

The following are advantages of VADP backup and recovery:

- VADP backups offload backup processes from the ESX server to a VADP proxy server.
- Eliminates the need for a backup window by using VMware virtual machine snapshot technology.
- Supports backups of all files residing in VMs running a Microsoft Windows guest operating system using save set ALLVMFS.
- Supports backups of specific files or folders for VMs running a Microsoft Windows guest operating system.
- Supports incremental and non level-0 backups for VMs running on a Microsoft Windows guest operating system.
- Supports image level backups for VMs running any guest operating system supported by VMware.
- Supports the ability to recover individual files from an image level backup (Windows NTFS only).
- Supports deduplication across VMs and servers.
- Backup impact on the target virtual machine and other VMs hosted on the same server is minimized.
Introduction

◆ There is no need to install NetWorker software on each virtual machine.
◆ Provides LAN-Free backup because the VADP proxy server can be connected to the SAN through a fibre channel adapter.
◆ Advanced VMware features and configurations like Distributed Resource Scheduling (DRS) and VMotion do not have any impact on the performance of NetWorker.

Disadvantages

The following are disadvantages of VADP backup and recovery:
◆ File level recovery from Image level backup of non-NTFS system is not possible.
◆ Image recovery of an entire VM from an incremental CBT backup is not possible.

Software and hardware requirements

The software and hardware requirements for VADP include:
◆ One or more VADP proxy systems running any of the following operating systems (English versions only):
  • Windows Server 2003 SP1 (32-bit or 64-bit)
  • Windows Server 2003 R2 (32-bit or 64-bit)
  • Windows Server 2003 SP2 (32-bit or 64-bit)
  • Windows Server 2008 (32-bit or 64-bit)
  • Windows 2008 R2
◆ One or more vCenter/Virtual Center servers running any of the following versions:
  • vSphere 5 (instructions for updating to vSphere 5 are provided in the section “Upgrading to vSphere 5.0” on page 24)
  • vCenter Server versions: 4.1 or 4.0 managing ESX/ESXi 4.1, 4.0, and 3.5
    
    **Note:** VMware vCenter appliance is not currently supported by NetWorker.
  • VirtualCenter version 2.5 managing ESX/ESXi 3.5
    
    **Note:** NetWorker supports the backup/recovery of non-English versions of guest operating systems for the VMs. However, if using non-English versions of the Windows operating system for the vCenter or VADP proxy host, note the limitations in the sections "Non-English vCenter limitations" and "Non-English VADP proxy host limitations".
  
  ◆ Network connectivity must be available between the VADP proxy server and the vCenter Server managing the ESX Server cluster. It also needs to be connected to the ESX Server system.
  ◆ To connect to a Fibre Channel (FC) SAN, the VADP proxy needs a FC host bus adapter (HBA).
Introduction

- The NetWorker 7.6 Service Pack 2 or later client software must be installed on the VADP Proxy host.
- The NetWorker server should be running NetWorker 7.6 or later software.
- The NetWorker 7.6 Service Pack 2 or later client software must be installed on the vCenter server to enable autodiscovery.
- The VADP proxy host must have access to all LUNs on the ESX server that is hosting the VMs when used with SAN and hotadd transport modes. More information is provided in the section “VADP proxy access to LUNs” on page 85.
- VMware tools must be installed on the VM to ensure that backups are taken in a consistent state. Also, VMWare tools is needed for backups via FQDN/hostname.

Note: The VMware tools installer contains a program, `comreg.exe`, which has a Windows 2008 R2 bug that prevents it from registering the VMware Snapshot Provider with VSS. VADP backups of a Windows Server 2008 R2 or Windows 7 VM may fail for certain versions of ESX 4.0.0 due to this issue.

Instructions for fixing this issue are provided at the following location:

To resolve this issue, upgrade to ESX 4.0 update 2 or ESX 4.1, or to upgrade your ESX 4.0.0 server with a VMware patch, go to the following link:
http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1013127

Limitations to vCenter on non-English versions of Windows

The following limitations apply to non-English versions of the Windows operating system using vCenter for VADP.

- The following names should always contain only English characters:
  - Backup VM display name in the left pane of vCenter
  - Backup VM hostname/FQDN
  - vCenter Datacenter name
  - vCenter Resource pool name
  - ESX datastore names containing the VM configuration files and virtual disks

- You can only restore VMs to the same language OS vCenter that was used during backup. For example, you cannot recover a VM backed up from a Japanese OS vCenter onto an English OS vCenter.

- VADP recovery can only be performed using the NetWorker User program. A command line recovery of the entire image will not work in cases where the backup was performed from a non-English vCenter.

Limitations for VADP proxy host on non-English versions of Windows

The following limitation applies to non-English versions of the Windows operating system for the VADP proxy host:
On the machine where the VADP recovery is launched, the NetWorker package should be installed in English only without any language packages (you must unselect all the other language packages explicitly during the NetWorker installation).

**Note:** Attempting to launch the VADP recovery dialog without following this procedure results in the overwriting of the local system files, which can lead to machine corruption.

### Transport modes

Advanced transport modes for image level recovery are supported for the VADP proxy host. The configured network transport mode can be set to the following values during backup or recovery:

- **SAN (Storage Area Network):** selecting this mode completely offloads the backup related CPU, memory or I/O load on the virtual infrastructure. The backup I/O is fully offloaded to the storage layer where the data is read directly from the SAN or iSCSI LUN.

  SAN mode requires a physical proxy with SAN access, and the VMs need to be hosted on either FibreChannel or iSCSI-based storage. The corresponding VMFS volumes must be visible in the Microsoft Windows Disk Management snap-in of the VADP proxy host.

- **Hotadd:** in this mode, the backup related I/O happens internally through the ESX I/O stack using SCSI hot-add technology. This provides better backup I/O rates than NBD/NBDSSL. However, selecting this mode places backup related CPU, memory and I/O load on the ESX hosting the VADP proxy.

  HOTADD mode requires a virtual proxy, and the ESX hosting the virtual proxy should have access to all the datastores where the VMs are hosted. So, if the datastores are SAN/iSCSI/NFS and if the ESX server where the VADP proxy resides is separate from the ESX server where the VMs are hosted, then:

  - In the case of SAN LUNs the ESX hosting the proxy and the ESX hosting the VMs should be part of the same fabric zones.
  - In the case of iSCSI LUNs the ESX hosting the proxy and the ESX hosting the VMs should be configured for the same iSCSI-based storage targets.
  - In the case of NFS datastores, the ESX hosting the proxy and the ESX hosting the VMs should be configured for the same NFS mount points.

- **NBD (Network Block Device):** in this mode, the CPU, memory and I/O load gets directly placed on the ESX hosting the production VMs, since the backup data has to move through the same ESX and reach the proxy over the network. NBD mode can be used either for physical or virtual proxy, and also supports all storage types.

- **NBDSSL (Network Block Device with SSL):** NBDSSL transport mode is the same as NBD except that the data transferred over the network is encrypted. Data transfer in NBDSSL mode can therefore be slower and use more CPU due to the additional load on the VADP host from SSL encryption/decryption.

  For recovery of VMs using NBDSSL mode, refer to the section “Recovery of a VM using NBDSSL or hotadd transport mode” on page 65.
You can set multiple transport modes to be used by the VADP proxy host using the pipe symbol “|” (for example, `san|nbd|nbdssl`).

By default, the transport mode field in the NetWorker User program is blank. Specify one transport mode to use for recovery.

More information on configuring transport modes is provided in “Task 1: Configuring the VADP proxy host and Hypervisor resource” on page 40. The transport modes are outlined in the table “Application information values” on page 45.

**Support for directives**

All local directives (.nsr file) are supported for ALLVMFS backups and specific save set backups.

VADP supports the following global directives:

- **Encryption directive** (for VADP enabled image level backups)
- **NT with Compression** (for VADP enabled image level backups)
- **VCB directive**

**Encryption directive**

The Encryption directive is supported only for Windows VMs with all attached disks having NTFS filesystem.

For the backup, the directive can be specified in the VM client properties.

- Encryption-*Encryption directive*

For the recovery of files or the entire VM from Encryption image backups with a pass phrase that is different than the current pass phrase (the current pass phrase is listed in the Datazone Pass Phrase attribute of the NetWorker server), use the following procedure:

- To recover AES encrypted data that was not encrypted with the current pass phrase, use the `-p` option with the command that is being used to recover data. For example:
  ```
  recover -p pass_phrase
  winworkr -p pass_phrase
  ```
- To enter multiple pass phrases with the `-p` option, type:
  ```
  recover -p pass_phrase1 -p pass_phrase2 -p pass_phrase3
  ```

**Note:** If an incorrect pass phrase or no pass phrase is entered, encrypted data is not recovered. Instead, the filenames will be created without data. However, if unencrypted data is also selected for recovery, it will be recovered.

**Compression directive**

The Compression directive is supported only for Windows VMs with all attached disks having NTFS filesystem.

For the backup, the directive Compression-*NT with compression directives* can be specified in the VM client properties.
For the recovery of files or recovery of the entire VM from Compression image backups, there is no change from the normal workflow.

**VCB directive**

The VCB directive is supported in the following two scenarios:

- When the save set is *FULL* and the backup level is incremental or any non level-0 backup.
- When the save set is ALLVMFS, regardless of the backup level.

**Note:** This directive is only applicable for VMs running Microsoft Windows.

For the backup, the directive can be specified in the VM client properties.

The VCB directive skips the following files and folders:

- pagefile.sys
- hiberfil.sys (Hibernation file)
- WINDOWS\system folder
- WINDOWS\System32 folder

**Incremental backups with image level backups**

For image level backups, an incremental backup of a VM is not supported after a hardware change, OS patch update, Service Pack update, drivers update and so on. Perform a full image level backup after every change made at the operating system and hardware level on the VM.

**Changed Block Tracking (CBT)**

VMs running on ESX 4.0 or later hosts with Virtual Hardware 7 can keep track of disk sectors that have changed. This feature is called Changed Block Tracking (CBT).

On a virtual machine, the virtual disk block changes are tracked from outside of the virtual machine in the virtualization layer. When a backup is performed, NetWorker uses CBT to determine which files have changed since the last backup, and backs up only those files.

Check if your virtual machine has CBT enabled, or enable CBT, by performing the steps outlined in “Task 4: Configuring Changed Block Tracking (CBT)” on page 55.

**Independent persistent disks are not backed up**

VADP does not support the backup and recovery of independent persistent disks. If such disks are detected during backup, they are skipped and a message is logged that indicates the disks were skipped. However, during an image level recovery, the disk is recovered without any data. If using independent persistent disks, you must use the traditional NetWorker style backup for protecting the data on the independent persistent disks via the backup client installed inside the VM.
Introduction

Licensing NetWorker support for VMware

The client license used for physical ESX hosts in non-VCB/VADP configurations is the Virtual Edition Client license. This license enables backup from any resident guest VM that has the NetWorker client software installed. For VMware environments being backed up via VADP or VCB, a single Virtual Edition Client license is required for each VADP/VCB proxy host. This license is sufficient to back up any number of VMs through that proxy host.

Virtual environments simplified licensing

NetWorker uses a simplified licensing model for virtualized environments. The EMC Software Compatibility Guide contains a list of supported server virtualization environments.

Two new attributes have been added to the General tab of the Client resource to identify the client as a virtual client:

- Virtual client. Set the attribute to Yes by selecting the Virtual Client attribute checkbox if the client is a virtual client.
- Physical host. If the client is a virtual client, set the attribute to the hostname of the primary/initial physical machine that is hosting the virtual client.

The NetWorker Licensing Guide provides more information on virtual licensing.

Using existing licenses to support VADP

When upgrading to NetWorker 8.0 from a release previous to NetWorker 7.6 SP2, note that the VADP proxy is used instead of VCB. The existing license used by the VCB proxy will automatically be migrated to support the VADP proxy.

AMP virtual appliance

The EMC Asset Management and Planning (AMP) appliance is a free, virtual appliance that can be downloaded from EMC Powerlink and installed on any VMware ESX server. The AMP appliance can be used to understand your software usage, measure the source capacity usage for the NetWorker software, plan future software investments and ensure license compliance. NetWorker leverages the EMC AMP to provide an estimate of the source capacity usage in a customer environment. Information on how to download, install and configure the EMC AMP appliance is provided in the NetWorker Licensing Guide.

Guest-based licensing

For guest based backups (not using VCB/VADP) with the NetWorker client installed on each physical host running a virtualization technology (Virtual Machine), only one Virtual Edition Client license is required per physical host. The Virtual Edition Client license backs up an unlimited number of VMs or guest host operating systems.

Guest based backups that use this license include:

- VMWare ESX servers
- Solaris zones
- LDOMs
Introduction

- LPARs
- nPARs
- VPARs
- Microsoft Hyper-V
- Xen and others

The following licensing model is used:

- One NetWorker Module license per application type, per physical host for non-VCB/VADP based backups.
- One client connection license per physical host for non-VADP based backups.
- When using VMotion, each ESX server that hosts the source Virtual Machine or destination Virtual Machine will require the virtual edition client license and the appropriate application module license.
- For ESX Servers using VMware Distributed Resource Scheduler (DRS) and VMware HA, a NetWorker Virtual Edition Client is required for each ESX Server in the ESX Cluster Farm. The appropriate number of module licenses depending upon the applications running in the farm.

For example, an environment has 60 VMs on 5 ESX Servers. Of the 60 VMs, 6 host SQL Server, 1 hosts Exchange and 1 hosts SharePoint. DRS and VMotion are used and the entire farm needs to be protected. The following licenses are needed:

- Qty 5 of NetWorker Virtual Edition Clients (1 for each ESX Server in the farm)
- Qty 7 of NMM licenses
  - For SQL, it would be Min (6, 5) = 5
  - For SharePoint, it would be Min (1, 5) = 1
  - For Exchange, it would be Min (1, 5) = 1
- For application backups, a NetWorker Virtual Edition Client and the appropriate NetWorker Application module is required for each physical server. One license is required for each application type (SQL, Exchange, SharePoint, Oracle, and SAP) used within all of the VMs on a single physical server. There are no changes to model codes for NetWorker Modules, so use the existing codes and license enablers.

For application protection, one NetWorker Module license is required per application type, per physical host for all virtualization technologies, including VMware ESX Server, IBM LPAR, and Solaris Domains.

For example, an ESX server hosting three (3) Exchange servers requires only a single NMM license. An ESX server hosting three (3) Exchange servers and a SharePoint server would require two NMM licenses; one license for the three Exchange servers and one license for the SharePoint server.

VADP licensing

For VADP backups of a VMware environment, one Virtual Edition Client license is required per VADP proxy host, regardless of the number of VMs and ESX servers configured to perform backups by using the proxy backup host.
CHAPTER 2
Upgrading

This chapter covers these topics:

◆ Upgrading to vSphere 5.0.......................................................... 24
◆ Upgrading to 7.6 Service Pack 2 and later for VMware VADP backups ................. 25
◆ Post-upgrading steps for Virtual Center on a 64-bit Windows host ......................... 29
Upgrading to vSphere 5.0

NetWorker releases previous to NetWorker 8.0 provided support for VADP with vSphere 4.1. VMware vSphere 5.0 is now available, which builds on the vSphere 4.1 release and continues to support VADP.

NetWorker release 7.6 SP2 and later can be used to backup and recover vSphere 5.0 VMs using VADP without any additional changes or updates, provided that the VMs are using VMFS v3.46 or earlier. For VMs that are using VMFS 5.0, support for VADP backups is limited to NBD/NBDSSL/hotadd transport mode unless the VDDK libraries are updated.

An update package is available for NetWorker 7.6 SP2 and later that updates the VDDK libraries from version 1.2.1 to version 5.0 to enable VMFS 5.0 support for VADP backups using all transport modes, including SAN and hotadd. This update must be applied to any NetWorker 7.6 SP2 and later VADP proxy that is expected to back up or recover VMs residing on VMFS 5.0. The update can be applied following the successful upgrade of the VCB proxy as detailed in the section “Upgrading to 7.6 Service Pack 2 and later for VMware VADP backups” on page 25, or following a new installation of NetWorker 7.6 SP2 and later.

This update is not included with the NetWorker package, but can be obtained from accessing the NetWorker Cumulative Releases document on Powerlink at Support > Software Downloads and Licensing > Downloads J-O > NetWorker, or from the following link:

http://powerlink.emc.com/km/live1/en_US/Offering_Basics/Articles_and_Announcements/NetWorker7_6_CumulativeHotFixes.pdf

To update the VDDK libraries from version 1.2.1 to version 5, perform the following steps:

1. Obtain the binaries from the link provided in the Cumulative Releases document. Separate binaries have been provided for x86 and x64. Run the binaries specific to your architecture.
2. Download the binaries to the following location:
   C:\nsr_migrate_vddk
3. Open a command prompt and CD to the following:
   
   If the proxy is x86:
   c:\nsr_migrate_vddk\nt86

   If the proxy is x64:
   c:\nsr_migrate_vddk\ntx64
4. Run nsr_migrate_vddk.exe.
5. Reboot the VADP proxy.

Note: Updates are not required for a NetWorker server or storage node that is not being used as a VADP proxy, or for guest-based VM clients and VCB proxy servers. This update is only required for VADP proxies that will be used for backup and recovery of vSphere 5.0 VMs residing in VMFS 5.0 datastores.
Upgrading to 7.6 Service Pack 2 and later for VMware VADP backups

NetWorker Release 7.6 Service Pack 2 introduced support for backup and recovery of VMware virtual clients using vStorage APIs for Data Protection (VADP). Prior to this release, virtual NetWorker clients were protected with VMware Consolidated Backups (VCB).

NetWorker 7.6 SP2 later later still support VCB-based backups with NetWorker 7.6 SP1 proxy servers. However, VADP-based backups must use a NetWorker 7.6 SP2 or later proxy server. A NetWorker 7.6 SP2 or later proxy cannot be used for VCB backups.

When upgrading the NetWorker software to release 7.6 SP2 or later, the upgrade tool must be run on the NetWorker server to transition to VADP backups. The following chapter provides information on upgrading the NetWorker software to release 7.6 Service Pack 2 or later to use VADP.

Upgrade existing NetWorker server and VCB proxy

After installing the NetWorker Release 7.6 SP 2 or later software on the NetWorker server and the VADP proxy server, run the `nsrvadpserv_tool` command on the NetWorker server. The `nsrvadpserv_tool` command updates pre-7.6 Service Pack 2 NetWorker virtual clients to use VADP for backup and recovery, converting all clients on a specified proxy. The `nsrvadpserv_tool` replaces the `nsrvcbserv_tool` that was used in NetWorker 7.6 SP1.

Be aware of the following when running this command:

- If you are upgrading from a pre-7.6 NetWorker installation, the Proxy Host client must be configured with Administrator privileges for the operating system. To ensure the Proxy Host is configured with Administrator rights:
  1. Connect to the NetWorker server by using NMC.
  2. Click Configuration.
  3. On the left pane, click Clients.
  4. Right mouse click on the Proxy client and select Properties.
  5. Click on the Apps & Modules tab.
  6. In the Remote User and Password fields, specify a user name and password for an account with Administrator rights on the Proxy server.

- By default, the `nsrvadpserv_tool` is located `c:\program files\legato\nsr\bin`.

- The NetWorker server and VCB Proxy host must be at NetWorker Release 7.6 Service Pack 2 and later.

- If the VCB_LOOKUP_METHOD is set to name, refer to the notes on page 27. Special consideration needs to be given if the VCB_LOOKUP_METHOD defined is set to IP rather than name.

To determine the Lookup Method on the Proxy Client resource, in the Application Information section, make note of the value for VCB_LOOKUP_METHOD. If the value is not set to name, manual steps detailed later in this procedure will need to be performed after the `nsrvadpserv_tool` is executed.
To update pre-7.6 Service Pack 2 NetWorker VMware virtual clients, type this command on the NetWorker server:

```
nsvadpserv_tool -p VM_proxy_hostname_or_IP_address
```

The `nsvadpserv_tool` does the following:

- **For pre-7.6 clients:**
  - Identifies the NetWorker clients that are VMs configured for the specified VADP proxy server.
  - Executes the `nsvadpctl_tool` on the NetWorker client configured as the VADP proxy server.
  - Reads the configuration file (config.js) and sends the information to the NetWorker server.
  - Updates the Application Information attribute of the NetWorker Client resource acting as the VADP proxy server with information from the config.js file.
  - Sets the backup command attribute in the NetWorker Client resource of all VMs configured for the specified VADP proxy server to `nsvadp_save`.
  - Creates the vCenter resource.

- **For 7.6 and 7.6 Service Pack 1 clients:**
  - Changes the backup command attribute in the NetWorker Client resource of all VMs from `nsrvcb_save` to `nsvadp_save`.
  - Updates the Application Information (APPINFO) attribute of the virtual Client resources so that “VCB” is replaced with “VADP” in all APPINFO variables. Examples are shown in Table 2 on page 26.

**Note:** After upgrading the NetWorker server from 7.6 SP1 to 7.6 SP2 or later, the VM Client resource associated with the VCB proxy does not display the correct information in NMC. For example, if you are using both VADP and VCB proxies, VM Client resources that are still associated with VCB proxies will display the VADP proxy when viewing the VM resource in NMC. The correct information displays in the nsradmin output for the Client resource.

This issue is documented in the Release Notes under NW129735.

<table>
<thead>
<tr>
<th>Old APPINFO variable name</th>
<th>New APPINFO variable name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCB_MAX_BACKOFF_TIME=20</td>
<td>VADP_MAX_BACKOFF_TIME=20</td>
</tr>
<tr>
<td>VCB_TRANSPORT_MODE=nbd</td>
<td>VADP_TRANSPORT_MODE=nbd</td>
</tr>
<tr>
<td>VCB_HOST=10.31.78.120</td>
<td>VADP_HOST=10.31.78.120</td>
</tr>
<tr>
<td>VCB_BACKUPROOT=F:\mnt</td>
<td>VADP_BACKUPROOT=F:\mnt</td>
</tr>
<tr>
<td>VCB_MAX_RETRIES=10</td>
<td>VADP_MAX_RETRIES=10</td>
</tr>
<tr>
<td>VCB_LOOKUP_METHOD=name</td>
<td>removed</td>
</tr>
</tbody>
</table>
Upgrading to 7.6 Service Pack 2 and later for VMware VADP backups

Note:
The VADP_MAX_BACKOFF_TIME and VADP_MAX_RETRIES variables are removed if their values were set to 10 and 0 respectively, which are their default values.

The VADP_HYPERVISOR=VC_name variable is added to the APPINFO list of variables. This variable value is based on the VADP_HOST variable that is specified in the VADP proxy server’s Client resource.

If VM lookups are done by name instead of IP address, you must add the VADP_VM_NAME variable in the Application Information attribute of each NetWorker virtual Client resource. The variable format is entered as VADP_VM_NAME=vm1 where vm1 is the display name of the VM used in the vCenter.

VADP_VM_NAME is case-sensitive. For example, if the VM host name is upper-case (such as SUSE11-X86), the value of VADP_VM_NAME must be set to SUSE11-X86. Also, if the name entered for VADP_VM_NAME contains spaces, the name must be contained within quotation marks (for example, VADP_VM_NAME="this is my vm name")

Change vCenter role privileges after upgrading

The following steps are required if VCB backup/recovery was previously performed through NetWorker using a non-Administrator vCenter role.

In order to perform backups using VADP, the permissions associated with the non-Administrator role need to be modified in vCenter.

Task 1: Create a VADP User role

To create a VADP User role:

1. Log in to the vCenter server with Administrator privileges using vSphere Client.
2. From the vCenter server, select View › Administration › Roles.
3. Right-click the existing non-Administrator role that was previously used by NetWorker and select Clone. A new cloned role is created.
4. Rename the cloned role to VADP User.
5. Right-click the VADP User role and select Edit Role.
6. Assign the required permissions to the VADP User role. The section “Minimum vCenter permissions needed to back up and recover using VADP” on page 53 provides more information.

Task 2: Assign the VADP User role to the user specified in the NetWorker Hypervisor resource

1. Log in to the vCenter Server with Administrator privileges using vSphere Client.
2. In the left pane, select the vCenter server.
3. In the right pane, click the Permissions tab.
4. Right-click anywhere in the right pane and select Add Permission from the drop-down.
5. Add the NetWorker Hypervisor user and assign the VADP User role.

6. Ensure that Propagate to Child Objects is enabled, then click OK.

Note: The VMware Basic System Administration documentation and the Datacenter Administration Guide provide more information on assigning a role to a user. The VMware documentation is available at http://www.vmware.com/support/pubs/.

Upgrade only the proxy client to NetWorker 7.6 SP2 or later

If you only want to upgrade the NetWorker proxy client to 7.6 SP2 or later and do not want to upgrade the NetWorker server, a manual upgrade can be performed by using the following steps.

Note: The NetWorker server must be at a minimum of version 7.6. If the NetWorker server is not version 7.6 or 7.6 SP1, it will need to be upgraded prior to performing the proxy client upgrade.

A NetWorker 7.6 SP2 or later proxy can only be used for VADP based backups and should be used with a NetWorker 7.6 SP2 or later server.

Make the following changes to the APPINFO attribute of the Client resource for the proxy:

1. Change VCB_BACKUPROOT to VADP_BACKUP_ROOT.
2. Change VCB_HOST to VADP_HOST.
3. Change VCB_TRANSPORT_MODE to VADP_TRANSPORT_MODE.
4. If VCB_VM_LOOKUP_METHOD is set to ipaddr, remove that entry; if it is set to name, the Client resource of the virtual client must be changed. step 2 provides more information.
5. Remove VCB_PREEXISTING_MOUNTPOINT and VCB_PREEXISTING_VCB_SNAPSHOT.
6. Change VCB_MAX_RETRIES to VADP_MAX_RETRIES.
7. Change VCB_BACKOFF_TIME to VADP_BACKOFF_TIME.

The following attributes of the Client resource for the virtual client associated with the proxy need to be changed:

1. The Backup command needs to be changed from nsrvcb_save to nsrvadp_save.
2. If VCB_VM_LOOKUP_METHOD was set to name in the proxy Client resource, add VADP_VM_NAME to the virtual Client resource’s APPINFO attribute with the value of the VM Name that is known to the Virtual Center.

Note: The NMC Configuration wizards for NetWorker 7.6 SP2 or later will not work with a pre-7.6 SP2 server. Information must be entered manually in the Client resource, even for new proxy clients, until the server is upgraded to NetWorker 7.6 SP2 or later.
Upgrade to use vCenter if ESX/ESXi server was previously used for VM backups

The following upgrade steps must be performed if VM backups were previously configured directly to the ESX/ESXi server instead of going through the vCenter server.

Using a manual upgrade

If the nsrvadpserv_tool cannot be run (for example, if using a 7.6.1 or 7.6.0 NetWorker server instead of upgrading the server to 7.6 SP2), perform the following steps:

1. Follow the manual upgrade steps provided in the section “Upgrade only the proxy client to NetWorker 7.6 SP2 or later” on page 28.
2. Manually create a new Hypervisor resource for vCenter.
3. Update the proxy host with the appropriate VADP_HOST values.

Using the nsrvadpserv_tool

If the NetWorker server is being upgraded to 7.6 SP2 or later, perform the following steps:

1. Run the upgrade tool as outlined in the section “Upgrade existing NetWorker server and VCB proxy” on page 25.
2. Manually create a new Hypervisor resource for vCenter.
3. Update the proxy host with the appropriate VADP_HOST values.

Space requirement changes on proxy for VADP vs VCB

In NetWorker releases using VCB, extra space was required for the mount point on the VCB proxy for copy operations during backup and recovery. NetWorker releases using the VADP proxy require significantly less space (typically, around 10% of the VM data size).

Post-upgrading steps for Virtual Center on a 64-bit Windows host

The procedure described in this section is optional and applies only if your pre-7.6 Service Pack 2 VMware integration with NetWorker had a Virtual Center server installed on a 64-bit Windows host.

Prior to NetWorker 7.6 Service Pack 2, if the Virtual Center server was installed on a 64-bit Windows host, you had to create a "command host" on a 32-bit Windows host and then reference the command host in the Hypervisor resource that was set up for Virtual Center. This was required so that NetWorker could support automatic discovery of VMware environments. In NetWorker 7.6 Service Pack 2 and later, these additional steps are not required because NetWorker now supports automatic discovery directly on the 64-bit Virtual Center server.

To eliminate the need for a 32-bit command host when the Virtual Center is installed on a 64-bit host:

1. Install the NetWorker 7.6 Service Pack 2 or later client software on the 64-bit Virtual Center host.
2. Modify the Command Host attribute in the Hypervisor resource to specify the 64-bit Virtual Center server name.
   a. From the Administration window, click Configuration.
   b. In the expanded left pane, right-click Virtualization and then select Enable Auto-Discovery.
   c. In the Auto-Discovery dialog box, click Advanced.
   d. Delete the name of the 32-bit Windows computer that was in the Command Host field. When this field is empty, the name of the Virtual Center server is used as the Command Host.
   e. Ensure that the value in the Command Name field is nsrvim, then click OK.
This chapter covers these topics:

- Automatic discovery of VMware environments .......................................................... 32
- Automatic discovery of VMware environments .......................................................... 32
- Notifications of changes to VMware environments ..................................................... 33
- Visual Representation of VMware environments ......................................................... 34
Managing and Monitoring Virtual Machines (VMs)

Automatic discovery of VMware environments

The NetWorker software provides automatic discovery of VMware environments and notification of changes to those environments, and provides both a graphical map and tabular view of VMware environments.

Automatic discovery is performed by contacting one or more VMware vCenters that host a Web Services server. VMware vCenter is an infrastructure management tool that provides a central point for configuring, provisioning, and managing virtualized IT environments, and is part of the VMware Virtual Infrastructure package.

Auto-discovery of VMware environments within NetWorker requires VMware vCenter, and the NetWorker client software installed on a Windows system. VMware vCenter and the NetWorker client do not need to be installed on the same system to perform auto-discovery. The VMware Infrastructure documentation provides information about configuring VMware vCenter.

Note: NetWorker software supports auto-discovery via VMware vCenter only. It does not support auto-discovery via an ESX server. “Task 1: Configuring the VADP proxy host and Hypervisor resource” on page 40 describes how to enable auto-discovery.

A binary, nsrvim, is used to facilitate communication between the NetWorker software and the VMware vCenter. The nsrvim binary can communicate with the Web Services server on the VMware vCenter using the secure HTTPS protocol. The nsrvim binary is supported on NetWorker for Windows 32-bit and 64-bit installations. The nsrvim binary is also included in these installation packages.

All NetWorker servers regardless of platform must contact a NetWorker client running in a Windows environment for auto-discovery. By default, the NetWorker server contacts the NetWorker client running on the VMware vCenter.

The NetWorker software uses auto-discovery for two purposes:

◆ Notification of changes to the VMware environment.
◆ Creating and updating the visual view of the VMware environment.

The output of the nsrtask.raw file, located in the \Program Files\legato\nsr\logs directory, contains any errors that occur during auto-discovery.

Note: The NetWorker client must be installed on the vCenter Server in order to run auto-discovery in the default configuration

Performing on-demand auto-discovery of VMware environments

To perform an auto-discovery of VMware environments at any time, right-click the Virtualization node in the left pane of the Configuration screen and select Run Auto-Discovery. Individual elements in the Virtualization node can be selected to limit the auto-discovery task to the selected element.
After selecting **Run Auto-Discovery**, either from the right-click menu or from the Auto-Discovery dialog, the Running auto-discovery Now window allows you to monitor the auto-discovery process. Clicking the Stop Monitoring button will close the Running Auto-discovery Now window, but the auto-discovery process will continue.

**Note:** If auto discovery fails with the error, “Failing back to rsh, but RUSER not provided”, ensure that the NetWorker server can resolve the IP/FQDN of the Virtual Centre server, and that the Virtual Centre server can resolve the NetWorker server.

### Notifications of changes to VMware environments

After auto-discovery has been performed, if there are any new unprotected VMs, identified by vCenter, that do not have NetWorker Client resources associated with them, a notification will be triggered. A notification is also sent if auto-discovery fails.

### Set up notifications

A default Notification resource, named New Virtual Machine, is included with the NetWorker installation. You must modify the Action attribute of this Notification resource to specify the mailserver and email accounts to which these notifications will be sent. You can also create custom Notification resources by selecting Hypervisor for the Event attribute of the custom Notification resource.

1. Connect to the NetWorker server via NMC
2. Click **Configuration**.
3. In the left hand side navigation pane, select **Notifications**.
4. Right click **New Virtual Machine** and select **Properties**.
5. In the Action field, remove nsrlog and specify the command appropriate for your NetWorker server’s operating system.
   a. For UNIX servers, the native mailer program will be used, refer to the appropriate operating system documentation for configuration details.
   b. For Windows servers, smtpmail, included with NetWorker can be specified. The action field would be:
      ```
smtplibmail -s subject -h mailhost recipient1@host.com
recipient2@host.com
```
      Where:
      - `subject` is the subject line of the email notification
      - `mailhost` is the fdqn of an email server which allows SMTP relaying.
      - `recipient1@host.com` is the email address that will receive the emails.

**Note:** For details regarding additional switches for the smtpmail command refer to esg116292 on http://powerlink.emc.com.
Monitor VMs

Monitoring of VMs, including notification when there is a new virtual machine, can be done through NMC in the same manner used to monitor other events. The NetWorker Administration Guide provides information on monitoring.

Visual Representation of VMware environments

After performing auto-discovery of VMware environments, the NetWorker console provides a graphical or tabular view of your VMware environments. This view is available in the right pane when the Virtualization node is selected in the left pane of the Configuration screen.

If auto-discovery has not been configured and the Virtualization node is selected, the right pane displays the Enable Auto-Discovery button. If auto-discovery has been configured and an auto-discovery has been performed, the right pane will display a graphical map of the VMware environment that was in place during the last auto-discovery. Automatic discovery is performed by contacting one or more VMware vCenters which host a Web Services server. VMware vCenter is an infrastructure management tool that provides a central point for configuring, provisioning, and managing virtualized IT environments, and is part of VMware Virtual Infrastructure package. For auto-discovery of VMware environments within NetWorker, VMware vCenters must also have NetWorker client software installed. See the VMware Infrastructure documentation for information about configuring VMware vCenter.

Virtualization node hierarchical display of the VMware environment

After an auto-discovery has been performed, the Virtualization node in the left pane of the Configuration screen can be expanded to provide a hierarchical display of the VMware environment. Four elements are displayed, in hierarchical view:

1. vCenters
2. DataCenters within the vCenter
3. Clusters within the DataCenter
4. ESX servers

VMs, NetWorker clients associated with those VMs, and NetWorker groups performing backups of those clients are not displayed in the Virtualization node hierarchical display. They are displayed in the right pane only.

Clicking on any element in the hierarchical tree will provide a detailed map view of that element and all of its children in the right pane. For example, selecting the top level virtualization node will display a complete view of your VMware environment across all vCenters that are configured for auto-discovery, while selecting an individual ESX server in the hierarchy will display all child elements associated with that ESX server including VMs, NetWorker clients associated with those VMs, NetWorker groups performing backups of those clients, and the proxy node for VMware clients.

Two right-click menu operations are available from the Virtualization node:

- Enable Auto-Discovery will open the Auto-Discovery dialog to configure auto-discovery, as described in “Performing on-demand auto-discovery of VMware environments” on page 32.
**Run Auto-Discovery** will perform an on-demand auto-discovery of your VMware environment. Individual elements in the Virtualization node can be selected to limit the auto-discovery task to the selected element.

**Graphical display of the VMware environment**

After an auto-discovery has been performed, elements of the VMware environment are displayed in the right “details” pane of the NetWorker Console. Objects displayed in the details pane vary depending on what is selected in the Virtualization node in the left pane. Several operations are available from the details pane, such as configuring new NetWorker clients to protect VMs.

**Note:** In order for a NetWorker Client resource to appear in the details pane, the name of the virtual machine and the name of the NetWorker Client resource must be identical.

Two views are available:

- **Map view**
- **Tabular view**

**Map view of the VMware environment**

Items displayed in the map view of the VMware environment will vary depending on what is selected in the Virtualization node in the left pane. If the Virtualization node is selected, the map view displays all vCenters that have had an auto-discovery performed and all child elements of those vCenters, beginning with vCenters on the left side of the pane. Lines connect each child element to its parent, with child elements proceeding hierarchically from left to right in the display, as illustrated in **Figure 1 on page 35**.

![Map view of the NetWorker Console](image)
Items displayed in the right details pane can be refined by selecting child elements in the Virtualization node hierarchy in the left pane. For example, if an individual ESX server is selected in the Virtualization node, only child elements associated with that ESX server are displayed.

**Displaying NetWorker clients associated with VMs**

By default, NetWorker clients associated with individual VMs are displayed. Rather, a Client icon will indicate whether the virtual machine has one or more NetWorker clients configured to protect it. NetWorker groups performing backups of those clients will be displayed with lines connecting the groups to the virtual machine.

If the virtual machine is being protected by the NetWorker software, you can double-click on the virtual machine to expand the display to view NetWorker clients configured to protect the virtual machine, with a line connecting the client to the NetWorker group that performs the backup of that client. You can also expand all VMs in the display by right-clicking anywhere in the right pane and selecting Expand All VMs.

**Creating new NetWorker clients for unprotected VMs**

If a virtual machine displayed in the right details pane is unprotected, this is indicated by the lack of a Client icon for that virtual machine. You can create a new NetWorker client for that virtual machine by right-clicking on the virtual machine and selecting Client Backup Configuration > New to open the Client Backup Configuration Wizard, or by selecting New to manually create a new client. “Task 2: Configuring a virtual client for backup” on page 48 provides information about creating clients to protect VMs.

**Other operations available from the map view**

You can also perform typical NetWorker operations on clients and groups from the map view. For example, by right-clicking on an existing NetWorker client, you can edit, delete, and copy clients, as well as initiating a recovery. You can also right-click on a NetWorker group displayed in the map view and perform typical group operations, such as editing or copying the group with all clients.

Unscheduled clients for backup are displayed in dotted-line within the configuration. Multiple instances of the same client within the savegroup are represented by their backup type, client name, and saveset name.

**Navigating within the Map view**

Several operations are available to facilitate navigation within the map view:

- **Zoom**: You can zoom in and out of the map view by selecting the zoom icons on the map view icon bar or by clicking on the right details pane and scrolling with the middle mouse wheel. You can also select an area to zoom into by selecting the Zoom Area button, or fit the entire display into the right details pane by selecting the Fit Content button. These operations are also available from the right-click menu in the details pane.

- **Moving the display**: You can move the graphical display by left-clicking in the details pane and dragging the mouse cursor.
Expanding and collapsing elements: You can expand or collapse any element in the map view to display or hide the child elements associated with the element by double-clicking the element. Additionally, you can expand or collapse all elements of a certain type by right-clicking anywhere in the details pane and selecting **Expand or Collapse**, and then selecting the element type.

Overview: You can open the Overview dialog by selecting the Overview icon on the map view icon bar or by right-clicking anywhere in the details pane and selecting Overview. The Overview dialog is particularly useful for large maps and allows you to quickly drill down to specific areas in the map.

Show and Find: The Show and Find functions allow you to limit items displayed in the map, and to search for specific items.

Tabular view: You can also switch to viewing the VMware environment in tabular view, rather than map view, by selecting the Table icon on the map view icon bar or by right-clicking anywhere in the details pane and selecting Table.

---

**Launch vSphere client from the NetWorker Console (Windows only)**

On supported Windows platforms, the vSphere client can be launched from the NetWorker Console's Configuration window, using the main menu or the map view.

To launch the vSphere client from the Console:

1. Start the Console, then click the **Configuration** tab.
2. Highlight the desired client in the left panel.
3. Launch the vSphere client by performing one of the following:
   - From the menu, select **Configuration > Launch vSphere Client**.
• From the map view, right-click the client and select **Launch vSphere Client** from the drop-down, as in **Figure 2 on page 38**.

*Figure 2* Launching the vSphere client from the Console (Windows only)
CHAPTER 4
Configuring NetWorker Clients for VADP Backup

This chapter covers these topics:

◆ Configuration options ........................................................................................................ 40
◆ Task 1: Configuring the VADP proxy host and Hypervisor resource .......................... 40
◆ Task 2: Configuring a virtual client for backup............................................................... 48
◆ Task 3: Creating a VADP User role in vCenter............................................................... 52
◆ Task 4: Configuring Changed Block Tracking (CBT) .................................................... 55
Configuration options

There are two options for configuring NetWorker clients for VADP backup. The configuration can be performed automatically by using the Client Backup Configuration wizard, or manually by using the Client Properties window:

◆ If using the Client Backup Configuration wizard, refer to “Configure a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard” on page 40.

◆ If using the Client Properties window, refer to “Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows” on page 43

Task 1: Configuring the VADP proxy host and Hypervisor resource

Backing up the VADP proxy host is not required. However, a NetWorker client must be created for the VADP proxy host before configuring the virtual clients. The VADP proxy NetWorker client will be referred to by VM clients during VADP backup and recovery operations.

You can create a NetWorker client for the VADP proxy host by using one of the following methods:

“Configure a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard” on page 40

“Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows” on page 43

Note: If multiple client instances of the same VADP proxy host exist in the NetWorker server, ensure that all the instances have the same application information attributes related to VADP. Manually copy the application information attributes into all the VADP proxy client instances.

Note, however, that when a virtual proxy is used, it cannot be created by copying the template of other VMs that are being protected.

Configure a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard

To create a NetWorker client for the VADP Proxy host by using the Client Backup Configuration Wizard:

1. From the Administration window, click Configuration.
2. In the expanded left pane, right-click Clients and select Client Backup Configuration > New.
The **Specify Client Name and Type** page displays, as in **Figure 3 on page 41**.

**Figure 3** Specify Client name and type

3. Type the name of the host machine in the **Client Name** field and select **VMware proxy host** and click **Next**.

4. Select the vCenter server associated with the Proxy host if present, otherwise:
   a. In the vCenter section, click **New** to create a new Hypervisor resource.
   b. In the vCenter field, specify the hostname of the vCenter.

   **Note:** There is no limit to the number of vCenter servers supported; however, each vCenter server must be created in the Hypervisor resource and each must be associated with the appropriate proxy/proxies in the environment.

   c. In the Username and Password field, type the username and password for an account with permission to perform backups, snapshots and registering/creating a new VM.

   If the user has non-administrative privileges on the vCenter server, follow the steps in the section “**Task 3: Creating a VADP User role in vCenter**” on page 52.

   d. Click **OK**.
5. In the Filesystem Mount Point Options section, specify the directory where all the VM backup jobs are supposed to reside in. The default value is `c:\mnt`. This option will set the `VADP_BACKUPROOT` variable in the Application Information properties of the Proxy host client in NetWorker.

Consider the following when defining this option:

- Ensure that the directory already exists, otherwise the VADP backup jobs will fail with “directory does not exist” error.
- The directory must be on a local disk and not on a CIFS share.
- This directory cannot be encrypted.
- For each backup job, a directory with a unique name derived from the * backup type and the VM name will be created here.

6. In the Retry Option selection, set the desired number of time to retry failures and the wait time in between retries. These options will set the `VADP_MAX_RETRIES` and `VADP_MAX_BACKOFF_TIME` variables respectively in the Application Information properties of the Proxy host client in NetWorker.

Consider the following:

- **VADP_MAX_RETRIES** - Use this option if you see a large number of backup jobs fail with “resource busy” errors. Usually, backup software will retry failed jobs, but it might be hours until the backup software retries.
- **VADP_MAX_BACKOFF_TIME** - If you change this default, also change the default for `MAX_RETRIES` (because this setting only applies if `MAX_RETRIES` is larger than 0).

7. In the Transport Mode Options section, select all desired modes in the Available Modes section and click the > button to add. Change the mode order if desired, the order in which modes are specified dictate the priority in which they are attempted. This option will set the `VADP_TRANSPORT_MODE` variable in the Application Information properties of the Proxy host client in NetWorker.

   **Note:** Each transport mode will be separated by a | when the variable is defined.

8. Click Next.

9. Click **Next** in the Specify the Proxy Host Backup option as it is not necessary to backup the Proxy host.

10. Click **Next** and review the Backup Configuration Summary.

11. Click **Create**.

12. Click **Finish**.
Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows

If vCenter is configured in the environment, there must be a Hypervisor resource for the vCenter server that hosts the VMs that use VADP. Before creating a Hypervisor resource for vCenter, ensure that the NetWorker client software is installed on the vCenter server to allow the Virtual Map of the environment to be generated with the auto-discovery feature.

**Note:** The NetWorker software supports auto-discovery of VMware environments with VMware vCenter only. It does not support auto-discovery with an ESX server.

If vCenter is not configured in the environment, there must be a Hypervisor resource created for each server in the environment. The NetWorker client on vCenter is only required if using the auto-discovery feature or the virtualization map feature.

VADP backups will work without the NetWorker client being installed on vCenter or VirtualCenter, however, the corresponding Hypervisor resource has to be created in the NetWorker server prior to starting the VADP backups.

To configure a Hypervisor resource:

1. From the Administration window, click Configuration.
2. In the expanded left pane, select Virtualization.
3. In the right pane, click Enable Auto-Discovery.
4. In the Auto-Discovery dialog box:
   a. In the Hostname field, enter the fully qualified domain name (FQDN) or IP address of the vCenter server.
   b. In the Username and Password fields, enter the credentials required to log onto the server. The username and password must belong to an account that has permission to perform VADP backups, snapshots and registering/creating a new VM. The user specified in the Hypervisor resource must also have administrative privileges on vCenter.
   c. To configure the vCenter server to use a port other than the default port for communications, click the Advanced tab and specify the correct port in the endpoint attribute of NSRhypervisor field.
      
      For example, if vCenter uses port 2000, define the endpoint attribute of NSRhypervisor attribute as:
      
      https://server_hostname:2000/sdk
      
      where server_hostname is the FQDN name of the vCenter host.
   d. When the vCenter server configuration is complete, right-click Virtualization and select Run Autodiscovery to generate the topology map.
Note: If auto discovery fails with the error “Falling back to rsh, but RUSER not provided,” ensure that the NetWorker server and the vCenter server can resolve each other’s IP / FQDN name.

e. Click OK.

To create a NetWorker client for the VADP Proxy host by using the Client properties windows:

1. From the Administration window, click Configuration.
2. In the expanded left pane, select Clients.
3. From the File menu, select New.
4. In the Name attribute, type the hostname of the Proxy client.
5. The browse and retention policy fields can remain empty, as they are set for the virtual clients.
6. If the Proxy client must be backed up, ensure that Scheduled Backups is selected.

Note: It is not mandatory to backup the Proxy client.

7. In the Save Set attribute, type the name of the files or directories to be backed up:
   a. To specify a file or directory for backup such as C drive, type \.
   b. To back up a specific directory such as Documents and Settings, type \Documents and Settings.
   c. To backup all file systems and VSS/System save sets, type ALL.

Note: If the Proxy client will not be backed up use the default selection.

8. In the Directive field, select a directive from the list, if needed.

VCB directive is applicable to VADP backups only and is supported in the following two scenarios:

- When file level incremental backups are performed instead of FULL image level backups.
- When FULL file level or incremental file level backups are performed when the save set is ALLVMFS.

The VCB directive skips the following files and folders:

- pagefile.sys
- hiberfil.sys (Hibernation file)
- WINDOWS\system folder
- WINDOWS\System32 folder
**Note:** The skips in the VCB directive are handled internally. An empty directive specification when viewing the directive resource in the NetWorker Console or the `nsradmin` interface is expected behavior.

9. Click **Apps and Modules**. The Create Client dialog displays, as shown in **Figure 4 on page 45**

![Figure 4 Apps and Modules tab in NMC](image)

10. In the Application Information field, add one line for each VC server hostname that is configured as part of the NSR Hypervisor resource:

   \[
   \text{VADP\_HOST=any.vc}
   \]

   where *any.vc* is the hostname of the vCenter server configured as the NSR Hypervisor resource.

11. The variables, described in **Table 3 on page 45**, can also be specified in the Application Information section.

**Table 3 Application information values (1 of 3)**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VADP_HOST</td>
<td>Specify the hostname of the VC server configured as part of the NSR Hypervisor resource. If there are multiple VC servers configured as part of the NSR hypervisor resource, specify their hostnames here. Example: VADP_HOST=any.vc VADP_HOST=another.vc</td>
<td></td>
</tr>
</tbody>
</table>
Table 3  Application information values (2 of 3)

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
</table>
| VADP_BACKUPROOT           | • Directory in which all of the VM backup jobs are supposed to reside. Ensure that the directory already exists or VADP backup jobs will fail with "directory does not exist" error.  
  • The directory must be on a local disk and not on a CIFS share.  
  • This directory cannot be encrypted.  
  • For each backup job, a directory with a unique name derived from the * backup type and the VM name will be created here.  
  • "If omitted, BACKUPROOT defaults to c:\mnt.  
  Example: VADP_BACKUPROOT=C:\mnt"                                                                                  | C:\mnt        |
| VADP_MAX_RETRIES          | Number of times an operation is re-tried after it fails. Use this option if you see a large number of backup jobs fail with "resource busy" errors. Usually, backup software will retry failed jobs, but it might be hours until the backup software retries.  
  Example VADP_MAX_RETRIES=1                                                                                           | 0             |
| VADP_MAX_BACKOFF_TIME     | Number of seconds to wait before retrying a failed operation. If you change this default, also change the default for MAX_RETRIES (because this setting only applies if MAX_RETRIES is larger than 0).  
  VADP_BACKOFF_TIME=20                                                                                                  | 10            |
| VADP_DISABLE_FLR          | If a virtual client is set up for image level backup and image level recovery (single step), setting this variable to YES will disable file level recoveries from the image backup. This variable only takes effect if the virtual client’s backup saveset is specified as *FULL*, which indicates an image level backup, and the backup level is full (0) with no incremental backup levels selected.  
  VADP_DISABLE_FLR=Yes                                                                                                  | No            |

**Note:** Setting this variable in the proxy application information and not specifying it at the virtual client level will disable file level recovery from all subsequent image backups done via the proxy
### VADP_TRANSPORT_MODE

Specify the transport mode to transfer data from a VMFS data store to a VADP proxy server. The following options are supported:

- **SAN** – Virtual disk data is read directly off a shared storage device that the virtual disk resides on. This requires VMFS storage on SAN or iSCSI and the storage device has to be accessible from both ESX and the VADP proxy.
- **hotadd** – This mode can be used when VADP is used in a virtual proxy. Because it uses the ESX I/O stack to move data, hotadd is more efficient than the transport mode NBD.
- **NBDSSL** – This mode is the same as "nbd" except that the data transferred over the network is encrypted. The data transfer in "nbdssl" mode can be slower and use more CPU than in the "nbd" transport mode. Also, for recovery of VMs using NBDSSL mode, refer to the section "Recovery of a VM using NBDSSL or hotadd transport mode" on page 65.
- **NBD** – VADP will use an over-the-network protocol to access the virtual disk. Data is read from the storage device by the ESX host and then sent across an unencrypted network channel to the VADP proxy. Please note that this mode does not provide the offload capabilities of the "san" mode (since data is still transferred from the ESX host across the network). However, "nbd" does not require shared storage and also enables VADP to be run inside a virtual machine.

*Example:* The following example displays all the possible attribute values used for a VADP configuration:

```
VADP_HOST=any.vc
VADP_HOST=another.vc
VADP_BACKUPROOT=G:\mnt
VADP_TRANSPORT_MODE=hotadd
VADP_MAX_RETRIES=2
VADP_MAX_BACKOFF_TIME=15
```

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VADP_TRANSPORT_MODE</td>
<td>Specify the transport mode to transfer data from a VMFS data store to a VADP proxy server. The following options are supported:</td>
<td>blank</td>
</tr>
<tr>
<td></td>
<td>• SAN – Virtual disk data is read directly off a shared storage device that the virtual disk resides on. This requires VMFS storage on SAN or iSCSI and the storage device has to be accessible from both ESX and the VADP proxy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hotadd – This mode can be used when VADP is used in a virtual proxy. Because it uses the ESX I/O stack to move data, hotadd is more efficient than the transport mode NBD.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NBDSSL – This mode is the same as &quot;nbd&quot; except that the data transferred over the network is encrypted. The data transfer in &quot;nbdssl&quot; mode can be slower and use more CPU than in the &quot;nbd&quot; transport mode. Also, for recovery of VMs using NBDSSL mode, refer to the section &quot;Recovery of a VM using NBDSSL or hotadd transport mode&quot; on page 65.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NBD – VADP will use an over-the-network protocol to access the virtual disk. Data is read from the storage device by the ESX host and then sent across an unencrypted network channel to the VADP proxy. Please note that this mode does not provide the offload capabilities of the &quot;san&quot; mode (since data is still transferred from the ESX host across the network). However, &quot;nbd&quot; does not require shared storage and also enables VADP to be run inside a virtual machine.</td>
<td></td>
</tr>
</tbody>
</table>

*Example:* If left blank, the default values are selected in the order of the description list. You can specify multiple modes by inserting a pipe (|) symbol between each value as shown in the following:

```
VADP_TRANSPORT_MODE=san hotadd nbdssl nbd
```

The order in which modes are specified dictate the priority in which they are attempted. In the above example, the san mode is attempted first; if that fails the hotadd mode is attempted, and so on.
Task 2: Configuring a virtual client for backup

You can configure a virtual client by using the Client Backup Configuration Wizard or by using the Client Properties window. Using either method, you can create a new Client resource or modify an existing one.

Complete the steps in one of the following topics depending on your environment:

◆ “Configure a virtual client if vCenter is configured and auto-discovery has been run” on page 49
◆ “Configure a virtual client manually by using the Client Properties window” on page 51

VMware clients can also be configured as deduplication clients. After creating a VMware client, follow the instructions in the NetWorker Data Domain Deduplication Devices Integration Guide or the NetWorker Avamar Integration Guide to configure the appropriate deduplication client.

After the virtual client has been backed up with the file level recovery option enabled, its client index can be browsed, and data can be recovered directly to the virtual client or data can be recovered onto a different virtual client using directed recovery.

Image level recovery of the full virtual machine using the full image can also be performed. It can be done to the same ESX server or to a different ESX server either within the same vCenter or a different vCenter.

Note: Since index entries are required for VADP image level restores, ensure that the browse policy is set appropriately. Index entries can still be created using the scanner command after the browse policy has expired.

Table 4 on page 48 lists the recovery options that are available based on the virtual client's configuration. Recovery steps are described in Chapter 5, “Recovering VADP Backups”.

Table 4  Recovery options that are available based on the virtual client configuration

<table>
<thead>
<tr>
<th>Backup Configuration</th>
<th>File level recovery</th>
<th>Image level (single step) recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual client with NTFS** OS and the ALLVMFS saveset is selected.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual client with NTFS** OS and the <em>FULL</em> saveset is selected.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual client with NTFS** OS and the <em>FULL</em> saveset is specified and the backup level is full (no incremental backups) and the VADP_DISABLE_FLR_APPINFO variable is set to Yes.*</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual clients that are not using the NTFS** OS and that have the <em>FULL</em> saveset selected.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
* The VADP\_DISABLE\_FLR variable does not apply to virtual clients that have the ALLVMFS saveset selected for backup. Additionally, if the VADP\_DISABLE\_FLR variable is specified on both the virtual client and on the VADP proxy, the setting on the virtual client takes precedence.

** NTFS implies NTFS of the following operating systems:
- Windows 2003
- Windows 2008
- Windows 2008 R2
- Windows Vista
- Windows XP
- Windows 7

Configure a virtual client if vCenter is configured and auto-discovery has been run

To configure a virtual client if vCenter is configured:

1. In the Virtualization map, right click on the Virtual Machine and select Client Backup Configuration -> New.

2. In the Specify the Client Name page, confirm that the client name field is populated and VMware client is enabled. Click Next.

   **Note:** The specified client name should be a recognized hostname/alias in a name service and/or FQDN. If the VM display name appears in the field, this entry must be changed to the hostname or FQDN or client creation will fail.

3. In the Specify the VMware Physical Host and Backup Type page, the Physical Host field will be populated with the Physical Host for the Virtual Machine.

4. Select VMware Proxy backup and from the Proxy host list, select the name of the Proxy Host VC Server. The VC names are taken from the multiple VADP\_HOST values set on the Application Information section of the proxy Client resource. Click Next.

5. In the Specify the Backup Options page, complete the following optional sections if required:
   - **Deduplication** — Select Data Domain if this client is being used with the DD Boost option that is available in NetWorker 7.6 SP1 and higher. Select Avamar deduplication backup and the corresponding Avamar server from the list if this client is using Avamar deduplication. Select None if no deduplication is being used.
   - **Target Pool** — Select a pool, from the list, to which data from this client’s backup will be directed. If a pool is selected, this value will override any other pool selection criteria that is associated with the client’s backup group or the client’s save sets. This field is most often used when backing up to a NetWorker 7.6 SP1 or higher Data Domain device.

6. Click Next to display the Specify the Proxy Backup Options page.
7. (Optional) In the **Virtual Machine Name** field, type the display name of the VM used in the vCenter. If a value is not entered, backups for this virtual machine will be done by IP address.

If a name is entered in this field, the name must match the display name as seen in vCenter Administrator, otherwise the backup will fail.

**Note:** This name is case-sensitive. Also, if the name of the VM contains spaces, then the name should be enclosed in double quotes "".

8. In the Backup Type section, specify the desired backup:

- Image level backup (this is equivalent to saveset *FULL*).
- Backup all files (this is equivalent to saveset ALLVMFS).
- Backup Specific files and folders.
  - To specify a file or directory for backup such as C: drive, enter c:\ or c\.
  - To back up a specified directory, such as Documents and Settings, enter c:\Documents and Settings.

**Note:** Due to limits with VADP, only one entry is allowed for the Save Set attribute.

9. Click **Next**.

10. In the Select NetWorker Client Properties section, select the **Browse** and **Retention** policies from the drop down menus.

11. If desired, select the **Backup Schedule** for this client.

**Note:** If a backup schedule is also defined for the backup group that this client will be added to, the group schedule will override the client schedule.

12. Type a description of the client in the **Client Comment** field, if desired.

13. If the NetWorker server and VADP proxy client are two different machines, in the Remote access field specify:

```
user=system, host=VADP proxy host
```

Where *system* is the system account of the Windows VADP proxy and *VADP proxy host* is the name of the Proxy host.

14. Click **Next**.

15. In Specify the NetWorker Backup Group, choose the desired group or select **Create a new group** and provide a group name and desired number of client retries.

16. If a new group is created, in the Schedule Options section, specify the desired time for the group to start in the **Schedule backup start time** field and enable **Automatically start the backup at the scheduled time**.

17. Click **Next**.

18. In the **Backup Storage Nodes** section, select the storage nodes that contain the devices to which the backups will be directed.
19. In the **Recovery Storage Nodes** section, select the storage nodes whose available devices will be used for recovery operations.

20. Click **Next**.

21. Review the backup configuration summary and click **Create**.

   You can now enable a directive on the VM:

22. Click **Clients**, right-click the newly created VM client, and select **Properties**.

23. From the **Directive** list, select **VCB directive**, **Encryption directive**, or **NT with compression directive**.

24. Click the **Apps and Modules** tab and ensure that `nsrvadp_save` is in the **Backup command** field.

25. Click **OK**.

More information on directives is provided in the *NetWorker Administration Guide*.

### Configure a virtual client manually by using the Client Properties window

To configure a virtual client by using the Client Properties window:

1. From the **Administration** window, click **Configuration**.

2. In the expanded left pane, select **Clients**.

3. From the **File** menu, select **New**.

4. In the **Name** attribute, type the hostname of the client.

5. In the **Browse Policy** field, select a browse policy from the list.

   **Note:** If the browse policy is set at the client level, it will override the browse policy specified for any groups to which this client is a member.

6. In the **Retention Policy** field, select a retention policy from the list.

   **Note:** If the retention policy is set at the client level, it will override the retention policy specified for any groups to which this client is a member.

7. Ensure **Scheduled Backups** is selected.

8. In the **Save Set** attribute, type the name of the files or directories to be backed up.

   **Note:** Due to limitations with VADP, only one entry is allowed for the Save Set attribute.

   a. To specify a file or directory for backup such as C drive, type `c:\`

   b. To back up a specific directory such as Documents and Settings, type `c:\Documents and Settings`.

   c. To backup all virtual machine file systems, type `ALLVMFS`.

   d. To backup up the entire VM image, type `*FULL*`.

9. From the **Directive** attribute, select a directive from the list, if desired.
10. Click the **Apps and Modules** tab.

11. In the **Backup Command** field, type `nsrvadp_save`.

12. In the **Application Information** field add a value `VADP_HYPERVERVISOR` to indicate which vCenter server to use for communication. For example:

   ```
   VADP_HYPERVERVISOR=vCenter1
   ```

   Where `vCenter1` is the name of the vCenter server.

   Also add this value for the `VADP_VM_NAME` attribute.

   **Note:** `VADP_VM_NAME` is case-sensitive, so the VM host name must be entered as it is displayed (for example, `SUSE11-X86`). Also, if the name of the VM contains spaces, then the `VADP_VM_NAME` should be enclosed in double quotes "".

13. Select **VADP** for the **Proxy backup type** field.

14. If the NetWorker Server and VADP proxy client are on two different machines:
   a. Click on the **Globals (2 of 2)** tab.
   b. In the **Remote access** field specify:

      ```
      user=system, host=VADP proxy host
      ```

      Where `system` is the system account of the Windows VADP proxy and `VADP proxy host` is the name of the Proxy host.

15. Click **OK**.

---

**Task 3: Creating a VADP User role in vCenter**

The following section provides the steps required to create a VADP User role in the vCenter server. Although it is possible to run VADP backup/recovery using Administrator privileges on vCenter, this is not recommended from a security perspective. It is recommended to create a new role specific to VADP in the vCenter server and assign it to the user specified in the Hypervisor resource.

**Create a VADP Proxy role**

1. Log in to the vCenter Server with Administrator privileges using vSphere Client.

2. From the vCenter Server, select **View > Administration > Roles**.

3. Click **Add Role**.

4. Name the role **VADP User**.

5. Assign the required permissions to the **VADP User** role and click **OK**.

   The section “Minimum vCenter permissions needed to back up and recover using VADP” on page 53 provides more information.
Assign the VADP User role to the user specified in the NetWorker Hypervisor resource:

1. Log in to the vCenter Server with Administrator privileges using vSphere Client.
2. Select the vCenter server in the left pane.
3. Click the Permissions tab in the right pane.
4. Right-click inside the right pane and select Add Permission.
5. Add the NetWorker Hypervisor user and assign the VADP User role.
6. Ensure Propagate to Child Objects is enabled and click OK.

**Note:** Refer the appropriate VMware Basic System Administration or Datacenter Administration Guide documentation for steps to assign a role to user.

VMware documentation can be found at [http://www.vmware.com/support/pubs/](http://www.vmware.com/support/pubs/)

**Minimum vCenter permissions needed to back up and recover using VADP**

It is recommended to create a single VADP User role with the backup and recovery privileges specified in Table 5 on page 53 and Table 6 on page 54. You can then use the associated user for VADP backup and recovery operations.

**Table 5  VADP backup privileges**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Privileges</th>
</tr>
</thead>
</table>
| Virtual machine > Configuration| • Add existing disk
|                                 | • Add or Remove device
|                                 | • Change Resource
|                                 | • Disk Change Tracking
|                                 | • Disk Lease
|                                 | • Raw device
|                                 | • Remove disk
|                                 | • Settings                                      |
| Virtual machine > Provisioning | • Allow disk access                             |
|                                 | • Allow read-only disk access                   |
|                                 | • Allow virtual machine download               |
| Virtual machine > State         | • Create snapshot                               |
|                                 | • Remove snapshot                               |
| Datastore                       | • Browse datastore                               |
|                                 | • Low level file operations                     |
### Table 5 VADP backup privileges

<table>
<thead>
<tr>
<th>Setting</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session</td>
<td>• Validate session</td>
</tr>
<tr>
<td>Global</td>
<td>• Cancel task</td>
</tr>
<tr>
<td></td>
<td>• Licenses</td>
</tr>
<tr>
<td></td>
<td>• Log Event</td>
</tr>
<tr>
<td></td>
<td>• Settings</td>
</tr>
<tr>
<td>Tasks</td>
<td>• Create task</td>
</tr>
<tr>
<td></td>
<td>• Update task</td>
</tr>
</tbody>
</table>

### Table 6 VADP recovery privileges (1 of 2)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>• Cancel task</td>
</tr>
<tr>
<td></td>
<td>• Licenses</td>
</tr>
<tr>
<td></td>
<td>• Log Event</td>
</tr>
<tr>
<td></td>
<td>• Settings</td>
</tr>
<tr>
<td>Resource</td>
<td>• Assign virtual machine to resource pool</td>
</tr>
<tr>
<td>Datastore</td>
<td>• Allocate space</td>
</tr>
<tr>
<td></td>
<td>• Browse datastore</td>
</tr>
<tr>
<td></td>
<td>• Low level file operations</td>
</tr>
<tr>
<td></td>
<td>• Remove file</td>
</tr>
<tr>
<td></td>
<td>• Update virtual machine files (only found in 4.1)</td>
</tr>
<tr>
<td>Virtual machine &gt; Inventory</td>
<td>• Create new</td>
</tr>
<tr>
<td></td>
<td>• Register</td>
</tr>
<tr>
<td></td>
<td>• Remove</td>
</tr>
<tr>
<td></td>
<td>• Unregister</td>
</tr>
<tr>
<td>Virtual machine &gt; Configuration</td>
<td>• Add existing disk</td>
</tr>
<tr>
<td></td>
<td>• Add new disk</td>
</tr>
<tr>
<td></td>
<td>• Add or Remove device</td>
</tr>
<tr>
<td></td>
<td>• Advanced</td>
</tr>
<tr>
<td></td>
<td>• Change CPU count</td>
</tr>
<tr>
<td></td>
<td>• Change Resource</td>
</tr>
<tr>
<td></td>
<td>• Disk change Tracking</td>
</tr>
<tr>
<td></td>
<td>• Disk Lease</td>
</tr>
<tr>
<td></td>
<td>• Extend virtual disk</td>
</tr>
<tr>
<td></td>
<td>• Host USB device</td>
</tr>
<tr>
<td></td>
<td>• Memory</td>
</tr>
<tr>
<td></td>
<td>• Modify device setting</td>
</tr>
<tr>
<td></td>
<td>• Raw device</td>
</tr>
<tr>
<td></td>
<td>• Reload from path</td>
</tr>
<tr>
<td></td>
<td>• Remove disk</td>
</tr>
<tr>
<td></td>
<td>• Rename</td>
</tr>
<tr>
<td></td>
<td>• Reset guest information</td>
</tr>
<tr>
<td></td>
<td>• Settings</td>
</tr>
<tr>
<td></td>
<td>• Swapfile placement</td>
</tr>
<tr>
<td></td>
<td>• Swapfile placement</td>
</tr>
<tr>
<td></td>
<td>• Upgrade virtual hardware</td>
</tr>
</tbody>
</table>
Task 4: Configuring Changed Block Tracking (CBT)

You can check if your virtual machine has CBT enabled or enable/disable CBT using the command line executable, `nsrvadp_modify_vm.exe`.

**Note:** When Changed Block tracking (CBT) is enabled, incremental and differential backups are supported only for Windows VMs, and all attached disks must be NTFS file systems. Note also that CBT-based incremental backups are always file based. Image level recovery from a CBT-based incremental backup is not supported.

Enable CBT using the command line

From the command line, the executable `nsrvadp_modify_vm.exe` allows you to enable CBT, disable CBT, or view the CBT properties for a specified VM. The VM can be specified using either the IP, DNS or VM name. If the VM is running when the executable is run, then a snapshot will be created and deleted so that any changes made to CBT can take effect.

From the command line, specify the following format:

```
directory\nsrvadp_modify_vm.exe -H vCenter server -P protocol -u user -p password -l lookup method -k lookup key -c command
```

where:
- `directory` is the location of the executable (for example, `c:\bin\nw762\nsr\bin`).
- `vCenter server` is the vCenter server hostname
- `protocol` is the protocol to use with the web service. Can be one of the following:
  - http
  - https

---

Table 6 VADP recovery privileges (2 of 2)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine &gt; Interaction</td>
<td>• Power Off&lt;br&gt;• Power On&lt;br&gt;• Reset</td>
</tr>
<tr>
<td>Virtual machine &gt; Provisioning</td>
<td>• Allow disk access&lt;br&gt;• Allow read-only disk access&lt;br&gt;• Allow virtual machine download</td>
</tr>
<tr>
<td>Virtual machine &gt; State</td>
<td>• Create snapshot&lt;br&gt;• Remove snapshot&lt;br&gt;• Revert to snapshot</td>
</tr>
<tr>
<td>Network</td>
<td>• Assign network&lt;br&gt;• Configure</td>
</tr>
<tr>
<td>Session</td>
<td>• Validate session</td>
</tr>
<tr>
<td>Tasks</td>
<td>• Create task&lt;br&gt;• Update task</td>
</tr>
</tbody>
</table>
Configuring NetWorker Clients for VADP Backup

- **user** is the vCenter user name
- **password** is the vCenter user password
- **lookup method** is the lookup method to use. Can be one of the following:
  - vm-name
  - ip-addr
  - dns-name
- **lookup key** is the lookup key to use
- **command** is where you specify one of the following CBT options:
  - cbt-disable
  - cbt-enable
  - info

In the following example, the command line interface is used to enable CBT on a VM **vm31-w2k3x64**:

```
c:\bin\nw_762\nsr\bin>nsrvadp_modify_vm.exe -H 10.13.187.212 -P https -u administrator -p password1 -l vm-name -k vm31-w2k3x64 -c cbt-enable
```

**Enable CBT using the vSphere Client GUI**

It is recommended to use the command line tool to enable CBT. If, however, the command line tool does not work properly, CBT can be enabled using the vSphere Client GUI. The VMware vSphere documentation provides more details.
CHAPTER 5
Recovering VADP Backups

This chapter covers these topics:

- File based recovery of a VM ................................................................. 58
- Image level (single step) recovery of a full VM ........................................ 59
- Recovery of pre-NetWorker 7.6 SP2 VM backups .................................... 66
File based recovery of a VM

File-level recovery is supported only on VMs that have a Windows operating system with the NTFS file system.

Perform a file based recovery on the local host

File based recovery on the local host running a VM client requires that the NetWorker client is installed on the VADP proxy.

To perform a file based recovery on the local host:

1. Launch the NetWorker User program on the VM client.
2. Follow the procedure outlined in the NetWorker Administration Guide's Recovery chapter. Make sure to specify the restore path using the Recover Options dialog, illustrated in Figure 5 on page 58.

Perform a file based recovery using CIFS share

To perform a file based recovery using the CIFS share:

1. Launch the NetWorker User program on the NetWorker server or VADP proxy.

   **Note:** The remote access list of the VM client must include either user@server or user@proxy.

2. Browse the file system for the VM client and select file to recover, as outlined in the NetWorker Administration Guide's Recovery chapter.
3. Set the destination directory to the CIFS share of the VM client.
4. Recover the files onto the CIFS share.
5. At the VM client, move the files from the CIFS share to the appropriate directory.

**Perform a file based recovery using directed recovery**

File based recovery using directed recovery requires that the NetWorker client is installed on the VM client.

1. Launch the NetWorker User program on the NetWorker server or VM client.

   **Note:** The user must have the Remote Access All Clients privilege.

2. Select the VM client as the source client.

3. Select the target client as VM-client.

4. Select a destination folder.

5. Follow the procedure in the NetWorker Administration Guide's Recovery chapter to select files for recovery and perform the recovery.

**Image level (single step) recovery of a full VM**

This section describes how to perform an image level recovery (disaster recovery) of the full virtual machine. There are two methods of recovering a full virtual machine:

- “Perform an image level recovery from the NetWorker User program” on page 60
- “Perform an image level recovery from the command line” on page 62

**Recommendations and considerations**

The following considerations apply when performing an image level recovery of a full VMware virtual machine:

- For a remote VADP proxy client, image level recovery requires the members of the VADP proxy client’s administrator group to be part of the remote access list of the VM clients or the member should have the “Remote access all clients” privilege.

- The user must have VMware privileges to register or create VMs.

- Recovery of the full virtual machine is only supported using save set recovery.

- Only level FULL of FULLVM save sets are supported for VM image recovery.

- The VMware converter must be installed on the VADP proxy host machine if you need to recover backups made prior to NetWorker 7.6 Service Pack 2. If the VMware converter is not installed, the save set of the full virtual machine (FULLVM save set) can be recovered using a traditional NetWorker recovery.

**Note:** Image level recovery is only supported with VMware stand-alone converter version 3.0.3.

- The VADP proxy system must be running one of the following:
  - Microsoft Windows 2003 (with at least SP1 installed)
  - Microsoft Windows 2003 R2
• Microsoft Windows 2008
• Microsoft Windows 2008 R2

If any hardware level changes such as a new disk partition, are made to the virtual machine, you must perform a level full backup before you can perform an image level recovery of the full virtual machine.

The virtual machine can recover to the same VMware ESX server or VMware vCenter (VC) taken at the time of backup or to a different ESX or VC. Recovery to different resource pools and different datastores are also supported. A different datastore can be specified for each disk and a configuration datastore can be specified to restore the configuration files.

A recover of the virtual machine will fail if the virtual machine already exists in the specified ESX or VC server. Also, the original virtual machine name’s folder should not exist in the datastores selected for recovery.

If you do not want to delete the original VM, remove the VM from the inventory (right click the VM name in the vCenter GUI and select Unregister the VM), then rename the datastore folders associated with the VM by using the Datastore window in the vCenter GUI.

During the recovery of a full virtual machine (FULLVM save set), the recovered virtual machine will start in forceful powered off state because of a VADP snapshot limitation.

For non-Windows VMs: If using traditional NetWorker client-based backups along with VADP image based backups for the same VM client, ensure that the browse policy for the client-based backups does not exceed the frequency of VADP image based backups. This practice is recommended because the indices of client-based backups may have to be removed prior to image-level recovery. The section “Image level recovery to a different FARM or vCenter” on page 65 provides more details.

For example, a Linux client has a schedule of daily level FULL client-based backups along with monthly VADP image based backups. In this case, it is recommended to set the browse policy of the client-based backups to a maximum of 1 month.

Perform an image level recovery from an encrypted backup

If the image level backup of the VM being recovered was performed with the Encryption directive, the following step applies:

By default, the current Datazone pass phrase is automatically used to recover the VM image. If the current Datazone pass phrase was created after a password-protected backup was performed, you must provide the password that was in effect when the VM image was originally backed up.

Perform an image level recovery from the NetWorker User program

This procedure is supported on Windows XP and later Windows platforms only.

To perform an image level recovery of a full VMware virtual machine (VM) to the VMware ESX server or VMware vCenter server:

1. Launch the NetWorker User program on the NetWorker client or VADP proxy.
2. From the Operation menu, select Save Set Recover.
3. In the **Source Client** dialog box, select the virtual machine client from where the save set originated and click **OK**.

4. In the **Save Sets** dialog box, select the Save Set name for the full virtual machine backup client (FULLVM) and select a level **FULL** backup. Click **OK**.

**Note:** Only level full of FULLVM save sets are supported for VM image restore.

5. In the **VADP Restore** dialog box, type the following information depending on the type of recovery and then click the **Start** button.

**Restore to VMware vCenter (VC):**

- **VM DISPLAY NAME** - Specify a new VM name to restore the backed up VM.
- **vCenter Server** - Specify the fully qualified domain name (FQDN) or the IP address of the VC server.
- **Data Center Name** - Specify the name of the Data Center to use.
- **ESX Server** - Specify the fully qualified domain name (FQDN) or the IP address of the ESX Server on which to perform the restore. By default, the source ESX server is displayed in this field.
- **Config Data Store** - Specify the name of the datastore to which the VM configuration data will be restored.
- **Resource Pool Name** - Specify the resource pool to use for the restore. Leave this field empty to use the default pool.
- **Transport Mode** - Specify the transport mode for recovery (SAN, hotadd or NBD).

**Note:** NBDSSL mode fails for recovery of VMs in NetWorker. The transport mode hotadd fails for ESX 5.0 and with VC 5.0. “Recovery of a VM using NBDSSL or hotadd transport mode” on page 65 provides a workaround to this issue.

- **Data Store** — Specify the name of the datastore for each disk on the VM.

Figure 6 on page 61 depict a VADP Restore dialog box that is set up for a VMware vCenter restore.

![Figure 6 VMware vCenter restore](image-url)
Perform an image level recovery from the command line

To perform a command line recover of a full VMware virtual machine to the VMware ESX server or VMware vCenter (VC) server:

1. Use the `mminfo` command to determine the save set ID of the level FULL FULLVM backup, for example:

   ```bash
   mminfo -avot -q "name=FULLVM,level=full"
   ```

   **Note:** Only level FULL of FULLVM save sets are supported for VM image recovery.

2. Recover the full VMware virtual machine using the `recover` command, for example:

   ```bash
   recover -S ssid [-d staging-location] -o VADP:host=VC hostname[:port];VADP:transmode=transport mode;VADP:datacenter=datacenter name;VADP:resourcepool=resource pool name; VADP:hostsystem=ESX hostname;VADP:datastore=datastores
   ```

   where

   - `ssid` is the save set identifier of the FULLVM.
   - `staging-location` is the staging location path to recover the FULLVM image to the proxy. This value is needed only for a recovery to staging location and applies only to backups taken before NetWorker release 7.6 Service Pack 2.
   - `VC hostname` is the VMWare VC name that is used to perform the restore.
   - `port` is the port used to log in to the web server of the VC host. If no value is entered, the default port number is used.
   - `transport mode` is the transport mode to use for recovery. For example:
     - `SAN`
   - `datacenter name` is the data center name where the VM is restored to.
   - `resource pool name` is the resource pool name that the VM restored is connected to.
   - `ESX hostname` is the VMWare ESX server machine name where the VMWare virtual machine needs to be restored.
   - `datastores` is the list of datastores that need to be associated with the configuration and the disks of the virtual machine that is being restored. They are name / value pairs separated with hash (#) symbols. For example:
     ```bash
     VADP:datastore="config=stor1#disk1=stor2#disk2=stor3"
     ```

   The following command depicts a command to recover the FULLVM with a ssid of 413546679. The recovery is directed to the ESX server named esxDemo1.emc.com. Default values are used for the datacenter, resource pool, and datastores.
Recovering VADP Backups

recover.exe -S 413546679 -o
VADP:host=esxDemo1.emc.com;
VADP:transmode=hotadd

Recover VMs that have a mix of VADP image-level and traditional guest based backups

If your VMs have a mix of both VADP image level backups and traditional guest based (also known as client based) backups, you may have to use one of the following recovery procedures depending on the build number of your NetWorker software:

- “Image-level recoveries of non-Windows VMs” on page 63
  This issue applies only to NetWorker 7.6.2 build 631 or earlier.
- “Unable to browse guest based backups on non NTFS filesystems” on page 64
  This issue applies only to NetWorker 7.6.2.1 build 638 or later.

Image-level recoveries of non-Windows VMs

The following considerations apply to NetWorker releases 7.6.2 build 631 and earlier when recovering non-Windows VMs that have a mix of VADP image-level and guest based (client based) backups.

If using traditional NetWorker guest based backups along with VADP image-based backups for the same VM client, then you must first remove the indices of the previous traditional save sets before you can perform an image-level recovery of the full virtual machine, otherwise the image-level recovery will fail. The only indices that need to be removed are those indices of the traditional save sets whose backups were performed prior to the VADP image-level backup that you have selected for restore.

Run the following command on the NetWorker server to mark the browsable save sets corresponding to the traditional backup as recoverable save sets.

```
nsrim -c client_name -N traditional_saveset_name -l
```

The last parameter in the command is a lower-case L.

This command removes the oldest full save and all dependant save sets from the online index. You may need to run the command multiple times for every level FULL browsable traditional save set and for every traditional save set name.

After removing the indices, you can perform the image-level recovery using either the NetWorker User program or the command line.

**Example**

For example, a Linux client mars has a mix of both VADP image-level and traditional backups as seen in the following output:

```
C:\>mminfo -avot -q "client=mars, volume=delve.001"
volumetypeclient date time size ssid fl lvl name
delve.001 adv_file mars 4/14/2011 10:01:35 PM 103 MB 3953675679 cb incr /usr
delve.001 adv_file mars 4/14/2011 10:07:10 AM 15 GB 4104550902 cb full FULLVM
delve.001 adv_file mars 4/14/2011 2:55:31 PM 3481 MB 4003904887 cb full /usr
delve.001 adv_file mars 4/14/2011 3:03:18 PM 103 MB 3903242058 cb incr /usr
delve.001 adv_file mars 4/14/2011 3:28:30 PM 15 GB 3852911942 cb full FULLVM
```
If you want to recover the latest image-level backup (in the above example, SSID=3852911942), first remove all the indices of browsable save sets that are from the previous traditional backups.

In this case, because there are two instances of browsable level FULL of the save set name /usr that need to be removed, the following command must be run twice on the NetWorker server:

```
nsr -c mars -N /usr -l
```

If you want to recover from the second last image-level backup, (for example, from SSID=4104550902), first remove all the indices of browsable save sets which are from the previous traditional backups.

In this case, since there is one instance of browsable level FULL for the save set name /usr that needs to be removed, the following command must be run once on the NetWorker server:

```
nsr -c mars -N /usr -l
```

**Note:** Browsable recovery of the traditional backup save sets will no longer be possible once the respective indices are removed. If the traditional backup indices are still needed, they can be restored once the image-level recovery is complete by running the following command on the NetWorker server:

```
scanner -c <client name> -i <device path>
```

For example: `scanner -c mars -i c:\device2`

### Unable to browse guest based backups on non NTFS filesystems

The following issue applies to NetWorker releases 7.6.2.1 build 638 and later. Traditional guest based (client based) backups are not browsable in the recovery GUI for VMs that are running a non NTFS filesystem and that have a mix of VADP and guest based backups. This issue does not apply to Windows VMs that are using NTFS. Additionally, save set recoveries are not affected and can be performed in the usual way.

To work around the issue, a command line recovery that specifies the backup time must be performed. Run the following commands from a command line on the VADP proxy or the VM:

To find the backup time:

```
mminfo -av -s networker_server -q "client=virtual_client"
```

To perform the recovery:

```
recover -t backup_time -s networker_server -c virtual_client
```

**Example**

The following VM (host name mars) has a mix of both VADP and traditional guest based backups. This example shows how to recover a traditional backup save set on the VM by first locating the time of the backup save set using the `mminfo` command and then by using that time with the `recover` command. The host name of the NetWorker server in this example is jupiter.

```
C:\mminfo -av -s jupiter -q "client=mars"
volume type client date time size ssid fl lvl name
```
Recovering VADP Backups

kuma-6 Data Domain mars 5/24/2011 10:59:22 PM 5243 MB 1440475890 cb full FULLVM

C:\recover -t "5/24/2011 10:38:39 PM" -s jupiter -c mars

Notice that in the previous example output from the mminfo command, the first two lines listed are for traditional backup and the last two lines are for a VADP backup, which is denoted with the save set name, FULLVM. The NetWorker Command Reference Guide provides more information about using the recover command to mark (select) files and to perform the recovery.

Image level recovery to a different FARM or vCenter

When recovering to a different server within the same vcenter environment, or when recovering to a different server within a different vcenter environment, you must select whether to keep the same UUID, or create a new UUID.

When you start a VM that was restored to a new location, the following message displays:

In ESX/ESXi 3.x:

The virtual machine's configuration file has changed its location since its last poweron. Do you want to create a new unique identifier (UUID) for the virtual machine or keep the old one?

* Create  
* Keep  
* Always Create  
* Always Keep

If you choose to keep the UUID, select Keep, then click OK to continue starting the virtual machine.

If you choose to create a new UUID, Select Create, then click OK to continue powering on the virtual machine.

In ESX/ESXi 4.x:

Question (id = 0) : msg.uuid.altered:This virtual machine might have been moved or copied.
In order to configure certain management and networking features, VMware ESX needs to know if this virtual machine was moved or copied.

* Cancel  
* I moved it  
* I copied it

If you choose to keep the UUID, select I moved it, then click OK to continue starting the virtual machine.

If you choose to create a new UUID, Select I copied it, then click OK to continue powering on the virtual machine.

Recovery of a VM using NBDSSL or hotadd transport mode

Recovery of a VM in NetWorker fails for the transport mode NBDSSL and for hotadd mode for ESX 5.0 and with VC 5.0. Use the following steps to work around the issue:
Recovering VADP Backups

**Note:** Before performing the following steps, ensure that you delete any snapshots that are active on the VM. Do not power on the VM until these steps have been performed.

1. Right click the VM and select **Edit settings**.
2. Select the virtual hard disk and select **Remove** but do not delete the VMDK. Click **OK**.
3. Return to the **Edit settings** menu and select **Add**.
4. Choose **Hard Disk** and use an existing virtual disk.
5. Associate the new hard disk with the VMDK file, then click **OK**. For example, use the **Add disk** pop-up window and add the hard disks by pointing them to the correct VMDK file in the datastore.
6. Power on the VM.

**Recovery of a VM using SAN or hotadd transport mode on Windows 2008**

When recovering a VM using either the **san** or **hotadd** transport mode on a Windows 2008 system, perform the following one-time configuration on the proxy host before initiating the recovery:

1. Open a command prompt on the proxy host.
2. Run the following command:
   ```
   DISKPART
   ```
3. Enter **SAN** and check for the SAN policy.
4. If the policy indicates **offline**, enable the policy by entering the following:
   ```
   SAN POLICY=OnlineALL
   ```
   **Note:** After the recovery is successful, **SAN POLICY** can be changed back to the default value (**SAN POLICY=offline** or **SAN POLICY=offlineshared**).
5. Restart the proxy for the change to take effect.

You can now initiate the VM recovery using **san** or **hotadd** mode.

**Note:** If recovery is initiated from a Windows machine other than the proxy, these steps need to be performed on the machine where the recovery is initiated.

**Recovery of pre-NetWorker 7.6 SP2 VM backups**

To recover backups of VMs that were performed via VCB, install **VMware Converter 4.0.1** on the machine where the restore will be initiated. This allows you to perform a 2-step recovery (for example, first to a staging location, and then manually through the VMware Converter 4.0.1).

**Note:** Single Step recovery of VCB backups can only be performed when VMware Converter 3.0.3 is installed, however, due to the incompatibility of this Converter version with vSphere 4.0/4.1, it is recommended not to use Single Step recovery when recovering old
VCB backups to a vSphere host.
Note also that VMware Converter 4.0.1 is the last version that supports VCB. VMware Converter 4.1 does not support VCB recovery. The following article provides more information:
Recovering VADP Backups
CHAPTER 6
VADP Planning and Best Practices

This chapter covers these topics:

◆ Recommendations and considerations for VADP backup and recovery ............... 70
◆ Application-level consistent backups ..................................................................... 71
◆ Selection of physical vs. virtual proxy ................................................................. 72
◆ VADP snapshot recommendations ........................................................................ 73
◆ Recommendations for Data Domain systems ........................................................ 76
◆ Network and Firewall port requirements ............................................................... 77
◆ Memory requirements for the VADP proxy .......................................................... 77
◆ VADP mount point recommendations and space considerations ................................ 78
◆ Support for tape drives in a VM ............................................................................ 79
◆ Recommendations and considerations for transport modes ............................... 81
◆ Performance optimization .................................................................................... 84
◆ VADP proxy access to LUNs .................................................................................. 85
Recommendations and considerations for VADP backup and recovery

Be aware of the following recommendations and considerations before implementing VADP backup and recovery.

- Ensure that VC and ESX/ESXi are updated to the latest released update.
- VADP supports backup and recovery via VMware VirtualCenter or vCenter. The section "Software and hardware requirements" on page 16 provides more information on supported vCenter versions.

**Note:** Backup and recovery directly to a standalone ESX/ESXi host is not supported. The ESX/ESXi must be connected to either VirtualCenter or vCenter to perform backup and recovery operations.

- VADP does not support IPv6. Instructions for disabling IPv6 and using IPv4 are provided in the section “Network and Firewall port requirements” on page 77.
- Ensure that the client parallelism on the VADP proxy machine is set to the maximum number of VM backups to be run concurrently. The section “Recommendations and considerations for transport modes” on page 81 provides information on the maximum supported concurrent backups for each transport mode.

For example if running 10 VM backups simultaneously, ensure that the client parallelism in the VADP proxy Client resource is set to 10.

- It is recommended to keep the vCenter and VADP proxy as separate machines to avoid contention of CPU and memory resources.
- In previous NetWorker releases using VCB, extra space was required for the mount point on the VCB proxy for copy operations during backup and recovery. NetWorker releases using the VADP proxy require significantly less space. The section “VADP mount point recommendations and space considerations” on page 78 provides more information.
- Ensure the path specified in VixDisklib and VixMountAPI config files are enclosed in double quotes as below:

```
tmpDirectory="C:\Program Files\Legato\nsr\plugins\VDDK\tmp"
```

These files are stored in the following location by default:

`<NetWorker install folder>\nsr\plugins\VDDK`  

**Note:** Double quotes should be specified in the path even though the path is already present.

- EMC recommends using the VADP proxy host as the storage node. This provides the optimal configuration for any given transport mode as data transfer occurs directly from the ESX/ESXi datastore to the storage node.
Application-level consistent backups

Performing a backup using VMware VADP creates a crash-consistent snapshot of a virtual machine image. However, advanced VMware functionality allows a backup application using VADP to achieve application-level consistent backups.

When performing a full VMware backup using VADP, in addition to VM quiescing, vSphere version 4.1 and later provides application quiescing using VSS on Windows 2008 and later platforms. This functionality requires that VMware tools is installed on the VM guest. If VMware tools is not installed, there is no backup integration with the VSS framework and backups are considered crash-consistent.

If the VM was created using a Windows 2008 template, then no additional configuration is required. If the VM was created using a non-standard template, or the configuration was manually modified, you must enable application-consistent quiescing by modifying the following line in the VM’s configuration file (.vmx): 

disk.EnableUUID = "true"

Further information is provided in the following VMware knowledge base article:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1028881

The only VSS backup type supported by vSphere is VSS_BT_COPY. As a result, the application backup history will not be updated and no additional application integration (such as Exchange log truncation) will be performed. Further details on backup type VSS_BT_COPY and its use in different applications is provided in the MSDN documentation.

Note: Due to the number of issues related to VMware Tools, for VSS integration the minimum recommended version of VMware is ESX 4.1 Update 1.

Option to enable or skip quiescing in the Applicaiton Information tab in NMC

An option is available in the Application Information tab in NMC to enable or skip quiescing during VADP backup.

To control the quiesce options that NetWorker passes to the VC/ESX during VADP backup, specify the VADP_QUIESCE_SNAPSHOT attribute in the Application Information tab NMC as follows:

- If VADP_QUIESCE_SNAPSHOT=Yes, then quiesced snapshots for VM clients are initiated
- If VADP_QUIESCE_SNAPSHOT=No, then non-quiesced snapshots for VM clients are initiated. In this case, the snapshot will not be application consistent. EMC does not recommend setting this option.

If this attribute is not specified, then NetWorker initiates quiesced snapshots for VM clients by default.
Note: The attribute VADP_QUIESCE_SNAPSHOT can be applied either at the VM level or proxy level. If applied at the VADP proxy level, all the VMs that use this VADP proxy will be affected.

Advanced use and troubleshooting

VMware VADP backups also support custom pre-and-post processing scripts inside the Windows VM guest for applications that do not have full VSS support.

The VMware knowledge base article 1006671 provides information on how to configure custom quiescing scripts inside the virtual machine is:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1006671

The VMware knowledge base article 1031200 provides information on how to instruct backup processes to skip VSS quiesce for only specific VSS writers:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1031200

The VMware knowledge base article 1018194 provides information on troubleshooting quiesce issues around VSS on the VM:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1018194

The VMware knowledge base article 1007696 provides troubleshooting of Volume Shadow Copy (VSS) quiesce related issues inside the VM:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1007696

Selection of physical vs. virtual proxy

NetWorker supports the use of both physical proxy hosts and virtual proxy hosts for backup of VMware environments. Whether to use a physical or virtual proxy should be determined based on performance requirements, the choice of backup targets, and available hardware.

Backup targets for virtual proxy hosts

The following are considerations of backup targets for virtual proxy hosts:

- If the backup is directed to disk (either AFTD or DDBoost), there are no special configuration requirements.
- If the backup is directed to tape drives, then review the requirements and limitations of using tape drives inside a VM in the section “Support for tape drives in a VM” on page 79.

Note: This requires that data transport is set to NBD/NBDSSL mode since VMware does not allow hotadd mode in conjunction with VMDirectPath.
Proxy node sizing and performance considerations

The following proxy node sizing and performance considerations apply when using physical and virtual proxies:

**Note:** There are no observed performance differences between physical and virtual proxies when running on similar hardware.

- The maximum number of concurrent sessions when using a physical proxy is higher than that of a virtual proxy. The section “Recommendations and considerations for transport modes” on page 81 provides more information on concurrent sessions for specific transport modes.
- Recommendations for a physical proxy is 4 CPU cores with 8GB of RAM. Recommendations for a virtual proxy is 4 vCPUs and 8GB vRAM per proxy, where each vCPU is equal to or greater than 2.66 GHz.
- NetWorker supports up to 12 parallel sessions using a single virtual proxy. This refers to the number of virtual disks processed in parallel, so if a single VM contains multiple virtual disks, this must be taken into account.
- Number of virtual proxies per ESX host depends only on the type of hardware on which the ESX has been installed.
- For lower-end ESX hosts, it is recommended not to mix I/O load on ESX (with the virtual proxy and backup VMs residing on a single ESX), but to have a separate ESX for the virtual proxy.
- For high-end ESX hosts, it is recommended to have a maximum of 5 virtual proxies concurrently running on a single ESX host.
- Optimal CPU load and performance when using DDBoost devices is observed with 4 concurrent backups per device. Lower number of parallel sessions to a single device does not achieve full performance while higher number increases CPU load without additional performance gain. Based on the CPU load, there is typically no performance improvement from adding more than 3 DDBoost devices per proxy node.

VADP snapshot recommendations

The following are recommendations for VADP snapshots:

- Schedule backups when very little I/O activity is expected on the virtual machine datastore, as this can impact the time required for taking the snapshot or removing the snapshot.
- It is recommended to keep at least 20% free space on all datastores for snapshot management.

**Note:** When the datastore is almost out of space, VMware creates a snapshot named Consolidate Helper while attempting to delete snapshots. This snapshot cannot be automatically deleted by the backup application. To remove the Consolidated Helper snapshot, the VM must be shut down and the snapshot manually deleted from vCenter before the next backup. Otherwise, change files may accumulate on the datastore. The accumulation of such files can affect both the backup performance and
the I/O performance of the virtual machine. Information about deleting the Consolidate Helper snapshot is provided in the following VMware knowledge base article:

http://kb.vmware.com/kb/1003302

To avoid this issue, ensure that there is always sufficient space available for snapshots.

- In the case of VMs that have a large amount of change rate during backups, the snapshots can grow in size considerably while the backup is running. Therefore, ensure that the snapshot working directory on the VMFS datastore has enough space to accommodate the snapshot during the backup.

- In the case of VMs that use virtual compatibility RDM disks, if the RDM disk is larger than the maximum VMDK size of the datastore that holds the VM’s configuration file, performing a snapshot on the VM with an RDM will fail. Therefore, ensure that the datastore that holds the VM’s configuration file has the appropriate VMFS block size to support the size of the RDM disk.

**Note:** VMs with physical compatibility RDM disks are not supported for VADP backups, because VM snapshots cannot be applied to such VMs.

- VMware snapshots by default reside on the datastore where the VM configuration files are located. Therefore, ensure that the snapshot working directory supports the size of all the disks attached to a given VM.

Starting with version 4.0, ESX and ESXi will compare the maximum size of a snapshot redolog file with the maximum size of files on the datastore. If the file could grow beyond the maximum size, ESX cancels the Create Snapshot operation and displays the following error:

File is larger than the maximum size supported by datastore.

**Example**

For example, if VM01 has the following disk layout:

- Disk01 - 50GB stored on VMFS01 datastore with a 1MB Block size
- Disk02 - 350GB stored on VMFS02 datastore with a 4MB Block size

Attempting to take a snapshot of this VM would fail with the error indicated above. This is because VMFS01 contains the working directory of the VM01, and snapshots get stored in the working directory. In the case of Disk02, this may indicate that the redolog file has grown beyond VMFS01’s maximum file limit of 256GB, which is where it will be stored.

To resolve this issue, either change the location of the virtual machine configuration files, or change the working directory to a datastore with enough block size.

To move the virtual machine configuration files, use Storage VMotion or Cold migration with relocation of files. More information is provided in the VMware KB article at the following link:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1004040
To change the `workingDir` directory to a datastore with enough block size, refer to the VMware KB article at the following link:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1002929

Table 7 on page 75 indicates the maximum virtual disk file size corresponding to block sizes on a datastore in ESX/ESXi 4.0:

**Table 7 Maximum virtual disk file size and corresponding block size for ESX/ESXi 4.0**

<table>
<thead>
<tr>
<th>Block Size</th>
<th>Maximum File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 MB</td>
<td>256 GB - 512 Bytes</td>
</tr>
<tr>
<td>2 MB</td>
<td>512 GB - 512 Bytes</td>
</tr>
<tr>
<td>4 MB</td>
<td>1024 GB - 512 Bytes</td>
</tr>
<tr>
<td>8 MB</td>
<td>2048 GB - 512 Bytes</td>
</tr>
</tbody>
</table>

Table 8 on page 75 identifies the maximum virtual disk file size corresponding to block sizes on a datastore in ESX/ESXi 4.1:

**Table 8 Maximum virtual disk size and corresponding block size for ESX/ESXi 4.1**

<table>
<thead>
<tr>
<th>Block Size</th>
<th>Maximum File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 MB</td>
<td>256 GB</td>
</tr>
<tr>
<td>2 MB</td>
<td>512 GB</td>
</tr>
<tr>
<td>4 MB</td>
<td>1024 GB</td>
</tr>
<tr>
<td>8 MB</td>
<td>2048 GB - 512 Bytes</td>
</tr>
</tbody>
</table>

**Manually quiescing VADP snapshots**

Issues on the virtual machine may prevent the successful completion of quiescing VSS prior to snapshot creation. The following VMware knowledgebase article provides details on troubleshooting quiesce issues around VSS on the virtual machine:


As a workaround, non-quiesced snapshots can be configured. This configuration will apply to all snapshots and will require a reboot of the virtual machine. VMware recommends scheduling downtime before performing this action:

1. Uninstall VMware Tools from the VM.
2. Reboot the system.
3. Reinstall VMware Tools. Ensure to select **Custom Install**.
4. Deselect **VSS**.
Recommendations for Data Domain systems

The following are recommendations for deploying NetWorker and Data Domain systems to back up the virtualized environment.

◆ For DD Boost enabled VADP backups:
  
  • The best CPU load and performance is observed with 4 concurrent backups per device.
  
  • Setting a lower number of parallel sessions to a single device does not result in optimal performance.
  
  • Setting a higher number of parallel sessions to a single device increases the CPU load without any improvements to performance.
  
  • It is recommended to have at least 400MB to 500MB of RAM for each VM being backed up if small to medium sized VMs are in use (VMs with less than 100GB virtual disks attached). If the largest VM being backed up has more than 100GB of virtual disks attached, the RAM can be further increased.

  More information on calculating the optimal memory for a given proxy is provided in the section “Memory requirements for the VADP proxy” on page 77.

◆ Better throughput is observed with DD Boost when there is less commonality between the VMs being backed up. As a best practice, it is recommended that VMs related to the same parent VM template/clone should be part of different backup groups, and these backup groups should have different start times.

◆ In the case of both hotadd and SAN modes, a 20-40% improvement is observed in the backup throughput for every additional proxy, provided the backend storage where the VMs reside is not a bottleneck.

◆ If using hotadd mode:
  
  • Refer to the section “Recommendations and considerations for transport modes” on page 81 for memory requirements. These requirements may increase depending on the size of the VM virtual disks, as described in the RAM recommendation above and the section “Memory requirements for the VADP proxy” on page 77.
  
  • Virtual proxy parallelism should not be set to a value greater than 12. This limit can further be decreased if the VMs have more than one disk attached. More information related to best practices when using hotadd mode is provided in the section “Recommendations and considerations for transport modes” on page 81.
  
  • In the case of multiple virtual proxies, it is recommended to consolidate all virtual proxies under dedicated ESX/ESXi host(s) in the environment to minimize the impact on production VMs during the backup window. These ESX/ESXi hosts should not be running any other VMs.
  
  • A maximum of 5 virtual proxies per one standalone ESX is recommended.
  
  • A maximum of 3 virtual proxies per ESX is recommended in a DRS cluster for proxies.
Network and Firewall port requirements

Be aware of the following firewall and network requirements:

- If there is a firewall between the VADP proxy host and the servers that run VMs that you plan to back up from the VADP proxy host, ensure that bi-directional TCP/IP connections can be established on port 902 between the VADP proxy host and the servers.

- If the Virtual Center or vCenter server uses a port other than the default port of 443, specify the port in the endpoint attribute of NSRhypervisor field. "Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows" on page 43 provides more information.

- VADP does not support IPv6. If vCenter is installed in a Windows 2008 system with IPv6 enabled (IPv6 is enabled by default) and the same system is also used as the VADP proxy, VADP backups will hang.

Ensure that IPv6 is disabled on the following:

- vCenter
- ESX/ESXi
- VADP-Proxy

**Note:** ESX/ESXi above refers to the actual host system and not the VMs to be backed up.

Disable IPv6 using Network Connections in the Control Panel, then add an IPv4 entry like the following to the hosts file on the system where vCenter is installed:

`<IPv4 address> <vCenter FQDN> <vCenter hostname>`

After this entry has been added, run the following command in the VADP proxy host to verify that the IPv4 address is being resolved:

`C:\Users\Administrator\ping <vCenter hostname>`

Memory requirements for the VADP proxy

The following NetWorker processes are related to VADP backup operations:

- `nsrvadp_save`
- `nsrvddk`
- `save`

The first two of these processes get spawned for each VM backed up. A save process gets spawned for each VM being backed up only if the backup is FLR-enabled.

**Note:** Once the backup of the VM completes, all the above processes exit, releasing the memory consumed on the proxy host.
Memory sizing requirements for the VADP proxy are as follows:

- For Linux VMs or FLR-disabled Windows backups, approximately 200MB per VM is required.
- For FLR-enabled Windows backups, use the following information to calculate the memory required:
  
  - When VADP backups are running, `nsrvadp_save`, which runs on the VADP proxy machine, consumes up to 2MB for every 1GB of virtual disk.
  
  - The `nsrvddk` and `save` processes consume approximately 200MB of memory per VM.

As an example, if you are running backups for a maximum of 4 VMs concurrently, then take the 4 Windows VMs with the largest disk sizes in the environment; in this example, if each VM has the following disk layout:

- VM1: Windows= Disk1-50GB, Disk2-100GB, Disk3-512GB
- VM2: Windows=Disk1-50GB, Disk2-512GB, Disk3-1TB
- VM3: Windows=Disk1-50GB, Disk2-100GB, Disk3-256GB
- VM4: Windows=Disk1-100GB, Disk2-1.5TB

The memory consumed by VADP processes on the proxy would then be:

- VM1: (Maximum sized disk in GB for VM* 2 MB) + 200 MB** = 1224 MB
- VM2: (Maximum sized disk in GB for VM* 2 MB) + 200 MB** = 2248 MB
- VM3: (Maximum sized disk in GB for VM* 2 MB) + 200 MB** = 712 MB
- VM4: (Maximum sized disk in GB for VM* 2 MB) + 200 MB** = 3272 MB

Therefore, the total memory needed on the proxy for VADP processes would be 7456 MB.

**Note:** **200 MB** is the memory needed per Windows VM for the `nsrvddk` and `save` processes.

- If the proxy is also being used as storage node, the following nsrmmd overhead needs to be included in the total memory requirement:
  
  - DD BOOST per device memory usage- approximately 500MB
  - backup to disk per device memory usage- approximately 50MB

**VADP mount point recommendations and space considerations**

Note the following recommendations for the VADP mount point (VADP_BACKUPROOT):

- Ensure the mount point is not located in the system folder (for example, `c:/Windows/temp`) as this folder is skipped during backup. Having the mount point in this folder may result in backup failures or backups that skip data due to directives that are applied during VADP backups.
Do not use any special characters (for example, *, # and so on) in the VM name or the name of the datastore associated with the VM. If these names contain special characters, the mount operation fails.

The VADP mount point cache requires space equal to at least 5-10% of the total amount of data being backed up in the case of Windows VMs. This space is required for temporarily storing the VMDK index during the backup, and is cleaned up once the backup completes. In the case of Linux or FLR-disabled Windows VMs, minimal space is required as indicated in the note below.

**Example**

As an example of how much space is required for a Windows VM:

If the proxy client parallelism is set to 5 so that a maximum of 5 Windows VMs are backed up concurrently, then calculate the total used disk space for the 5 largest Windows VMs in the environment. Allocate at least 10% of this total used space for the VADP_BACKUPROOT mount point.

So, if each VM in the above example has around 2 disks and each disk has 40GB used space:

- Total amount of data being backed up = 40GB * 2 * 5 = 400GB
- Total amount needed for mount point = 400 * 10% = 40GB

In this case, ensure that the drive specified for VADP_BACKUPROOT has at least 40GB of free space.

**Note:** This mount point space is only needed when performing FLR-enabled image level backups of Windows VMs. It is otherwise very minimal (in the order of a few MB per VM) when performing image level backups of Linux VMs or FLR-disabled image level backups of Windows VMs.

### Support for tape drives in a VM

In order to use tape drives (physical and virtual tape drives) in a VM, specific compatible hardware and VMware ESX/ESXi versions are required, and the drives must be configured using VMDirectPath.

VMDirectPath allows device drivers in guest operating systems to directly access and control physical PCI and PCIe devices connected to the ESX host in a hardware pass-through mode, bypassing the virtualization layer.

The VMDirectPath feature is available in VMware ESX/ESXi 4.0 Update 2 or later versions of Hypervisor. The following section assumes that the reader has a working knowledge of VMware vSphere ESX/ESXi and virtual machine configuration.

### VMDirectPath requirements and recommendations

The following requirements and recommendations apply when using VMDirectPath:

- VMDirectPath requires Intel Virtualization Technology for Directed I/O (VT-d) or AMD IP Virtualization Technology (IOMMU). You may need to enable this option in the BIOS of the ESX/ESXi system.
- The ESX/ESXi version should be 4.0 Update 2 or later version.
The VM should be Hardware version 7. For example, vmx-07.

The optimal VMDirectPath PCI/PCIe devices per ESX/ESXi host is 8.

The optimal VMDirectPath PCI/PCIe devices per virtual machine is 4.

VMDirectPath restrictions

The following restrictions apply during the configuration of VMDirectPath:

- The ESX host must be rebooted after VMDirectPath is enabled.
- The VM must be powered down when VMDirectPath is enabled in order to add the PCI/PCIe device directly to the VM.
- Using fiber channel tape drives in a VM is not supported without VMDirectPath in production environments due to the lack of SCSI isolation. Tape drives can be configured and used without VMDirectPath, but the support is limited to non-production environments.

The VMware knowledge base article esg1010789 provides information on configuring VMDirectPath:

http://kb.vmware.com/kb/1010789

The following features are not available for a VM configured with VMDirectPath, as the VMkernel is configured without the respective device under its control when passed to a virtual machine:

- vMotion
- Storage vMotion
- Fault Tolerance
- Device hot add (CPU and memory)
- Suspend and resume
- VADP hotAdd transport mode (when used as virtual proxy)

Note: If using VMDirectPath in a NetWorker VADP virtual proxy host, then the transport modes are limited to either NBD or NBDSSL. This is due to a VMware limitation.

Additional information on VMDirectPath is available in the following VMware technical note:


Considerations for VMDirectPath with NetWorker

The following are considerations apply when using VMDirectPath with NetWorker:

- For virtual environments that must run backups to fiber channel connected tape devices where there is a large amount of data in the VM, VMDirectPath can be used with NetWorker.
1 vCPU is sufficient to process 500 GB of data as long as the other VMs are not sharing the physical core on the underlying ESX/ESXi hardware, and the vCPU has exclusive access to the single core.

If other VMs that reside on the same ESX/ESXi are sharing the underlying hardware (physical CPU), it may be required to add more vCPU and dedicating underlying hardware by using CPU affinity settings.

To achieve optimal performance, it is recommended that the guest VM acting as the DSN has a minimum of 4 GB of memory available with 2 vCPUs allocated.

If multiple target sessions are needed in each device and 4 or more vCPUs are assigned to the VM, ensure that there are enough devices available for backup operations. An insufficient amount of devices can result in less throughput due to CPU scheduling overhead of the Hypervisor.

Ensure that the device drivers for the HBA are updated on the guest operating system.

Recommendations and considerations for transport modes

Following are recommendations for SAN, hotadd and NBD/NBDSSL transport modes.

SAN transport mode

The following recommendations and considerations apply when one of the VADP transport modes is set to SAN (VADP_TRANSPORT_MODE=SAN):

- Prior to connecting the VADP proxy host to the SAN fabric, perform the steps in the section “Diskpart utility for SAN and hotadd transport modes” on page 86.
- Memory usage per DD BOOST device should be approximately 500MB.
- A maximum of 50 concurrent backups should be performed per proxy when using a backup-to-disk device.
- A maximum of 100 concurrent backups should be performed per proxy when using a DDBost device.
- A maximum of 100 concurrent backups can be run at any given time against a given VC.

Hotadd transport mode

The following recommendations and considerations apply when one of the VADP transport modes is set to hotadd (VADP_TRANSPORT_MODE=hotadd):

- Prior to running VADP backups using the virtual proxy host, perform the steps in the section “Diskpart utility for SAN and hotadd transport modes” on page 86.
- A minimum of 4 vCPUs must be allocated per virtual proxy, with 8GB vRAM per proxy and each vCPU equal to or greater than 2.66 GHz.
- Memory usage per DD BOOST device should be approximately 300MB.
- The ESX server must be running ESX 3.5 update 4 or later.
Client parallelism on the VADP virtual proxy should not be set to a value greater than 12 where the VMs being backed up have a maximum of 1 disk per VM in the environment.

If the VMs in the environment have more than 1 disk per VM but less than 12 disks per VM, then the maximum client parallelism value on the VADP virtual proxy should not exceed \( N \), where \( N \) is based on the following calculation:

Maximum of \( N \) number of disks can be backed up by the virtual proxy provided this is equal to the number of free scsi controller slots in the first SCSI controller (for example, SCSI controller #0), and that \( N \) does not exceed 12.

For example, if a maximum of 6 VMs backups are to be run concurrently, then take the 6 VMs with the largest number of attached virtual disks in the environment and calculate the total number of disks:

- If the 6 VMs have a total of 12 virtual disks (i.e. 2 disks per VM), set the parallelism on the virtual proxy client to a maximum of 6 (which will in turn perform a concurrent backup of a maximum of 12 disks being attached to the virtual proxy).
- If the 6 VMs have a total of 18 virtual disks (i.e. 3 disks per VM), set the parallelism on the virtual proxy client to a maximum of 4 (which will in turn perform a concurrent backup of a maximum of 12 disks being attached to the virtual proxy).

**Note:** If the VMs in the environment have more than 12 disks attached per VM, then use NBD or NBDSSL mode instead of hotadd mode.

The virtual proxy can only back up those VMs whose virtual disk size does not exceed the maximum size supported by the VMFS datastore where the configuration files of the virtual proxy reside.

As a best practice, always place the configuration files of the virtual proxy on a datastore that has a block size of 8MB. This will ensure that the virtual proxy can back up all of the supported virtual disk sizes.

The datastore for the VADP proxy virtual machine must have sufficient free space before the hotadd backup begins.

If there are multiple virtual proxies, it is recommended to host all the virtual proxies in a dedicated ESX/ESXi server. This would keep the virtual proxy resource consumption of CPU and memory isolated within that ESX/ESXi environment without impacting the production VMs.

VMs having IDE virtual disks are not supported for hotadd mode. Instead, nbd mode is recommended for these.

The virtual machine to back up and the virtual machine that contains the hotadd VADP proxy host must reside in the same VMware datacenter. This requirement also applies to virtual machine restore -- the virtual machine to restore and the virtual machine where the restore is initiated must reside in the same VMware datacenter.

If a backup failure occurs, the virtual proxy may sometimes fail to unmount hotadded disks. In such cases, you must manually unmount the hotadded disks from the virtual proxy. If any of the client VM disks are still attached to the virtual proxy, perform the following:

1. Right-click the virtual proxy and go to **Edit Settings**.
2. Select each of the hotadded disks and choose **Remove**.

**Note:** Ensure that you select "Remove from virtual machine" and not "Remove and delete..." when unmounting.

**NBD/NBDSSL transport mode**

The following recommendations and considerations apply when one of the VADP transport modes is set to NBD or NBDSSL (i.e., VADP_TRANSPORT_MODE=NBD):

- If NBDSSL mode fails for recovery of VMs, apply the workaround in the section "Recovery of a VM using NBDSSL or hotadd transport mode" on page 65.

- One can only run a concurrent backup of 20 virtual disks against a given ESX/ESXi. The limit refers to the maximum number of virtual disks and is per ESX/ESXi host, irrespective of the number of proxies being used in the environment.

Due to this limitation, it is recommended to apply the following best practices:

- If the ESX is not part of a VMware cluster or is part of a DRS-disabled VMware cluster, then apply one of the following:
  - When using a single proxy to backup a given ESX via NBD/NBDSSL, set the client parallelism of the VADP proxy Client resource such that the limit of 20 concurrent disk connections per ESX host is not exceeded.
  - When using multiple proxies to backup a given ESX via NBD/NBDSSL, then the client parallelism on each VADP proxy should be calibrated such that the total concurrent disk connections per ESX host does not exceed 20.

- If ESX is part of a DRS-enabled VMware cluster, then apply one of the following best practices:
  - When using a single proxy to backup via NBD/NBDSSL, set the client parallelism of the VADP proxy Client resource such that the limit of 20 concurrent disk connections per cluster is not exceeded.
  - When using multiple proxies to backup via NBD/NBDSSL, then the client parallelism on each VADP proxy should be calibrated such that the total concurrent disk connections per cluster does not exceed 20.

**Note:** In the following examples, the backup group parallelism would take effect only if the VADP proxy host client parallelism is set to an equal or higher number.

**Example 1** One proxy in the environment, all VMs on the same ESX (no cluster)

In the following example, there is a single proxy in the environment and 11 VMs need to be backed up via NBD/NBDSSL. All 11 VMs are hosted on the same ESX, which is not part of a cluster, and both of these jobs have to be run at the same time:

- 8 VMs from ESX contains 2 disks disk.
- 3 VMs from same ESX contains 3 disks each.

Use one of the following best practices:
Set the client parallelism of the proxy to 8.

Create a single backup group containing all 11 VMs from the given ESX and set the group parallelism to 8.

Either of the above would ensure that at any given time, the maximum number of disks being backed up from that ESX will not exceed 20.

**Example 2  Two proxies in the environment, all VMs on the same ESX on DRS-disabled cluster**

In the following example, there are two proxies in the environment to back up 11 VMs via NBD/NBDSSL. All 11 VMs are hosted on the same ESX, which is part of a DRS-disabled cluster, and both of these jobs have to be run at the same time:

- Proxy1 has been assigned to backup 8 VMs, each VM contains 2 disks.
- Proxy2 has been assigned to backup 3 VMs, each VM contains 3 disks.

Use one of the following best practices:

- Set the client parallelism of Proxy1 and Proxy2 to 5 and 2 respectively.
- Create a single backup group containing all 11 VMs from the given ESX and set the group parallelism to 8.

Either of the above would ensure that at any given time, the maximum number of disks being backed up from that ESX will not exceed 20.

**Example 3  Two proxies in the environment, all VMs hosted on DRS-enabled cluster**

In the following example, there are two proxies in the environment to back up 11 VMs via NBD/NBDSSL. All 11 VMs are hosted on one DRS-enabled cluster:

- Proxy1 has been assigned to backup 8 VMs, each VM contains 2 disks.
- Proxy2 has been assigned to backup 3 VMs, each VM contains 3 disks.

Both these jobs have to be run at the same time.

Use one of the following best practices:

- Set the client parallelism of Proxy1 and Proxy2 to 5 and 2 respectively.
- Create a single backup group containing all 11 VMs from the given cluster and set the group parallelism to 8.

Either of the above would ensure that at any given time, the maximum number of disks being backed up from that cluster will not exceed 20.

**Performance optimization**

The following section provides recommendations for optimizing VADP performance.

- The success of the VADP snapshot creation and deletion is based on two things:
  - The amount of I/O occurring on the virtual machine datastore during snapshot creation.
  - The design of the I/O substructure associated with each datastore.
To avoid snapshot-associated issues, backups should be scheduled during times of relatively low I/O activity on the virtual machine. Reducing the number of simultaneous backups can also help with this.

The use of multiple backup proxy servers is supported with NetWorker. Depending on the number of VMs/ESX servers in use, another backup proxy can be added to increase backup throughput capacity.

During VADP backups, the backup proxy server performs a significant amount of backup processing. Proper sizing of the backup proxy server can help ensure maximum backup performance of the virtual machine environment. In some instances, a physical proxy may be preferable.

The capacity of the backup proxy can be broken down into two main areas:

1. VADP data path:
   This is the path that the backup data created by VADP will follow during the backup lifecycle. The VADP proxy server accesses backup data using the configured network transport mode. The configured transport mode can be set to the following values:
   - SAN (Storage Area Network)
   - Hotadd
   - NBD (Network Block Device)
   - NBDSSL (Network Block Device with SSL)

2. NetWorker data path:
   The VADP proxy can also be a NetWorker server, client or storage node. To maximize backup throughput, the VADP proxy should be configured as a storage node so that client data is written directly to the backup media.

The overall backup performance of VADP Proxy will be defined by the slowest component in the entire backup data path. These components are:

- VADP transport mode used
- VADP Proxy system resources such as the CPU, internal bus, and RAM
- VADP snapshot creation time
- I/O load at the time of creation

**VADP proxy access to LUNs**

The following considerations apply when using the following transport modes to access LUNs.

**SAN transport mode**

For SAN mode backups, the VADP proxy requires read access to the SAN LUNs hosting the VMs.

For image recovery via SAN mode, ensure that the VADP proxy has read-write access to the SAN LUNs hosting the VMs. To ensure read-write access, add the VADP proxy to the same fabric zones to which the ESX server system belongs.
Hotadd transport mode

For hotadd mode, the ESX server (where the VADP proxy virtual machine resides) must have access to the datastores of the VMs that you want to back up. For example, if the datastores are from SAN LUNs and the ESX server where the VADP proxy resides is separate from the ESX server where the VMs are located, then the ESX hosting the proxy should be part of the same fabric zones to which the ESX hosting the VMs belongs.

NBD/NBDSSL transport modes

For nbd/nbdssl, no zoning is required since access to the datastore is always by way of LAN. Only network connectivity to ESX/ESXi is required for access to the datastore.

Diskpart utility for SAN and hotadd transport modes

When an RDM NTFS volume is being used for any of the VMs on the VADP proxy host, Windows will automatically attempt to mount the volume and assign drive letters to VM disks during backup. This may lead to data corruption on the VMs.

To prevent Windows from automatically assigning drive letters to the RDM NTFS, perform the following steps.

**Note:** Steps 1 and 2 are only applicable in the case of SAN transport mode where SAN fabric zoning is already in place such that the VADP proxy host is already displaying the SAN LUNs in Windows disk management. If this does not apply, skip to Step 3.

1. Shut down the Windows proxy.
2. Disconnect the Windows proxy from the SAN or mask all the LUNs containing VMFS volumes or RDM for VMs.
3. Start the proxy and log into an account with administrator privileges.
4. Open a command prompt and run the diskpart utility by entering the following:
   ```
   diskpart
   ```
   The diskpart utility starts and prints its own command prompt.
5. Disable automatic drive letter assignment to newly discovered volumes by entering the following in the diskpart command prompt:
   ```
   automount disable
   ```
6. Clean out entries of previously mounted volumes in the registry by entering the following in the diskpart command prompt:
   ```
   automount scrub
   ```
This glossary contains terms related to disk storage subsystems. Many of these terms are used in this manual.

A

B

backup An operation that saves data to a volume.

Backup proxy The system designated as the off-host backup system. This is a host with NetWorker client package installed and the VADP software.

C

changed block trackingIntroduced with vSphere 4, changed block tracking provides a true block level incremental backup technology for ESX 4 virtual machines (VMs).

client A computer, workstation, or fileserver whose data can be backed up or recovered.

client file index A database that tracks every database object, file, or file system that is backed up. The NetWorker server maintains a single client index file for each client.

Console Server NetWorker servers and clients are managed from the NetWorker Console server. The Console server also provides reporting and monitoring capabilities for all NetWorker servers and clients.

D

E

F

file index See "client file index."

G

Guest OS An operating system that runs on a virtual machine.

H

I

image level backup and recovery Used in the case of a disaster recovery

inactivity timeout The number of minutes to wait before a client is considered to be unavailable for backup.
JAR (Java Archive)  
A file that contains compressed components needed for a Java applet or application.

L  
label  
A NetWorker assigned label that uniquely identifies a volume. Templates can be used to define label parameters.

managed application  
A program that can be monitored and/or administered from the Console server.

media database  
Indexed entries about the location and the life cycle status of all data and volumes that the NetWorker server manages.

metadata  
VSS-defined information that is passed from the writer to the requestor. Metadata includes the writer name, a list of VSS components to back up, a list of components to exclude from the backup, and the methods to use for recovery. See "writer." See "VSS component."

NetWorker client  
See "client."

NetWorker Console server  
See "Console Server."

NetWorker Management Console  
See "Console Server."

NetWorker server  
The host running the NetWorker server software, which contains the online indexes and provides backup and recovery services to the clients on the same network. See also "online indexes."

NetWorker Administrator  
A default NetWorker server user group that can add, change, or delete NetWorker server user groups.

NetWorker storage node  
See "storage node."

online indexes  
Databases on the NetWorker server that contain information about client backups and backup volumes. See "client file index." See "media database."

recover  
To restore files from a backup volume to a client disk.
**Glossary**

**S**
- **save**
  The command that backs up client files and makes entries in the online index.
- **save set**
  A group of files or a file system that is backed up on storage media.
- **single step backup and recovery**
  See "image level backup and recovery."
- **storage node**
  A storage device physically attached to another computer whose backup operations are controlled by the NetWorker server.

**T**

**U**
- **update enabler**
  A code that updates software from a previous release. Like other temporary enabler codes, it expires after 45 days.

**V**
- **VADP**
  An acronym for vStorage APIs for Data Protection. VADP supersedes the VCB framework for VMware backups.
- **vCenter**
  An infrastructure management tool that provides a central point for configuring, provisioning, and managing virtualized IT environments, and is part of the VMware Virtual Infrastructure package.
- **Virtual machine**
  Software that creates a virtualized environment between the computer platform and its operating system, so that the end user can install and operate software on an abstract machine.
- **VM**
  An acronym for virtual machine.
- **VMDK**
  A designation specific to the files that comprise a VMware virtual machine. These files are commonly called VMDK files because of the .vmdk extension that VMware adds to these files.
- **VMware Tools**
  Installed inside each virtual machine, VMware Tools enhance virtual machine performance and add additional backup-related functionality.
- **VSS (Volume Shadow Copy Service)**
  Microsoft technology that creates a point-in-time snapshot of a disk volume. NetWorker software backs up data from the snapshot. This allows applications to continue to write data during the backup operation, and ensures that open files are not omitted.
- **VSS component**
  A subordinate unit of a writer. See "writer."

**W**
- **writer**
  A database, system service, or application code that works with VSS to provide metadata about what to back up and how to handle VSS components and applications during backup and restore. See "metadata" and "VSS component."
INDEX

A
Application Information attributes 26, 45

C
Changed Block Tracking (CBT) 20
configure 55

D
Directives
compression 19
encryption 19
support for directives 19
VCB 20, 44

E
EMC online support website 7

G
Guest based backup and recovery 12, 13
Advantages 13
comparison with Image level backup and recovery 12
Configuration 14
Disadvantages 14
Installation 14
licensing 21
Recommendations and considerations 14
Recommendations for NetWorker installed in a virtual machine 13
Recovery 14

H
Hypervisor resource
automatic configuration 41
configuring 40
manual configuration 43

I
Image level backup and recovery 12
comparison with Guest based backup and recovery 12
incremental backups 20
recovery 59
recovery to a different FARM or vCenter 65

N
nsrvadp_save 84
nsrvadpserv_tool 25, 29

R
Recovery
File-based 58

Image level 59
pre-NetWorker 7.6 SP2 VM backups 66

T
Transport modes 18, 47
Hotadd 18
NBD 18
recovery using SAN or hotadd mode 66
SAN 18

U
Upgrading to NetWorker 7.6 SP2 25
ESX/ESXi server 29
Post-upgrade steps for 64-bit Virtual Center on Windows 29
upgrading only the proxy client 28

V
VADP backup and recovery 15, 70
Advantages 15
Disadvantages 16
independent persistent disks 20
licensing 22
network and firewall port requirements 77
performance optimization 84
Recommendations and considerations 70
Software and hardware requirements 16
VADP for VMware 12, 25
VADP proxy host
automatic configuration 40
configuring 40
manual configuration 43
VADP User
assign VADP user role 27
backup privileges 53
create VADP User role 27, 52
recovery privileges 54
vCenter permissions 53
vCenter
changing role priviliges after upgrading 27
Virtual client backup 48
automatic configuration 49
manual configuration 51
virtual clients 12, 25
Automatic discovery 32
Virtualization 34
VMware 12
Automatic discovery of VMware environments 32
Configuring a NetWorker client 48
graphical display of the VMware enviroment 35
Licensing 21
Notification of changes to VMware environment 33
setting up notifications in NMC 33
Index

virtualization node hierarchical display 34
Visual representation of environment 34
vSphere Client
launching from NMC 37
vStorage APIs for Data Protection (VADP) 12, 25