Veritas NetBackup™ for VMware Administrator's Guide

Release 9.1

VERITAS™

Veritas NetBackup™ for VMware Administrator's Guide

Last updated: 2021-06-07

Legal Notice

Copyright © 2021 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party (“Third-party Programs”). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

https://www.veritas.com/about/legal/license-agreements

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas Technologies LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1 Introduction 13

About NetBackup for VMware 13
About the virtual machine backups that include database data 14
About the NetBackup appliance as a VMware backup host 14
NetBackup for VMware components 15
Appliance as backup host: component overview 18
Media servers as backup or discovery hosts 18
Overview of the VMware backup process 20
NetBackup for VMware terminology 20

Chapter 2 Required tasks: overview 24

Overview of VMware tasks 24
Overview of NetBackup tasks 25

Chapter 3 Notes and prerequisites 26

NetBackup for VMware prerequisites 26
NetBackup for VMware: notes and restrictions 27
Notes on VMware Virtual Volumes (VVols) 33
NetBackup IPv6 parameter required for backups in VMware IPv6 environments 34
NetBackup for VMware: notes on Linux virtual machines 34
Notes on the NetBackup appliance as a VMware backup host 35
NetBackup for VMware support for SAN multi-pathing 35
NetBackup for VMware support for fault tolerant VMs 37
NetBackup character restrictions for the Primary VM identifier 37
In the policy Query Builder, display names, resource pool names, and vApp names are case-sensitive 39
Notes on the hotadd transport mode 40
Notes and limitations for tag usage in VMware Intelligent Policy queries 41
Notes and limitations for the backup and restore of VMware tag associations 42

Chapter 4 Configure NetBackup communication with VMware 44

Adding the VMware backup host to NetBackup 44
Adding NetBackup credentials for VMware 45
Using the VMware Managed Object Browser to verify the server name 49
Changing the host name of a VMware server in NetBackup 50
Setting privileges for posting events to vCenter 51
Authentication token for the NetBackup vSphere plug-ins 51
Setting global limits on the use of VMware resources 51
Validating VMware virtualization server certificates in NetBackup 54
ECA_TRUST_STORE_PATH for NetBackup servers and clients 58
ECA_CRL_PATH for NetBackup servers and clients 59
ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients 60
ECA_CRL_CHECK for NetBackup servers and clients 61
VIRTUALIZATION_HOSTS_CONNECT_TIMEOUT for servers and clients 62
VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED for servers and clients 63
VIRTUALIZATION_CRL_CHECK for NetBackup servers and clients 64
VMWARE_TLS_MINIMUM_V1_2 for NetBackup servers and clients 65

Chapter 5 Configure NetBackup policies for VMware 67

Configuring a VMware policy from the Policy Wizard 68
Configuring a VMware policy from the Policies utility 68
Limit jobs per policy on the Attributes tab (for VMware) 72
Backup options on the VMware tab 73
VMware backup host 73
Optimizations options (VMware) 74
Primary VM identifier options (VMware) 76
Existing snapshot handling options (VMware) 77
Transport modes options (VMware) 78
Application protection options (VMware) 79
VMware - Advanced Attributes dialog 81
About the Post vCenter events option (VMware Advanced Attributes) 85
Exclude Disks tab 86
About the exclude disk options for virtual disk selection 88

Exclude disks from backups: an example to avoid 90
Restoring data from the backups that excluded the boot disk or data disks 91
Browse for VMware virtual machines 91
Limiting the VMware servers that NetBackup searches when browsing for virtual machines 95
Virtual machine host names and display names should be unique if VMs are selected manually in the policy 97
Primary VM identifier option and manual selection of virtual machines 98
About incremental backups of virtual machines 99
Configuring incremental backups 99
Storage Foundation Volume Manager volumes in the virtual machine 100

Chapter 6 Configure a VMware Intelligent Policy 101

About automatic virtual machine selection for NetBackup for VMware 102
Support and use of VMware tag associations 103
The basics of a NetBackup query rule 104
Important notes on automatic virtual machine selection 105
NetBackup requirements for automatic virtual machine selection 107
Automatic virtual machine selection: Task overview 108
Options for selecting VMware virtual machines 109
Configuring automatic virtual machine selection 111
Editing an existing query in Basic Mode 115
Using the Query Builder in Advanced Mode 116
AND vs. OR in queries 117
Examples for the NetBackup Query Builder 118
The IsSet operator in queries 120
About selecting virtual machines by means of multiple policies 121
Order of operations in queries (precedence rules) 123
Parentheses in compound queries 124
Query rules for resource pools 125
Query rules for datacenter folders (host folder) 126
Query rules for duplicate names 127
Query rules for tags 128
Query Builder field reference 129
Test Query screen for VMware 141
Test Query: Failed virtual machines 143
Effect of Primary VM identifier parameter on Selection column in Test Query results 144

Effect of Primary VM identifier parameter on VM Name column in Test query results 146
Refreshing the display of virtual environment changes in the Query Builder 147
Reducing the time required for VM discovery in a large VMware environment 148

Chapter 7 Reduce the size of backups 150

About reducing the size of VMware backups 150
Block-level backup (BLIB): full vs incremental 151
Deleting a vSphere Client snapshot 152

Chapter 8 Back up virtual machines 154

Backing up virtual machines 154
Using the Activity Monitor to monitor virtual machine backups 156
Restarting jobs individually in the Activity Monitor 158
Viewing NetBackup activity in vSphere Web Client or vSphere Client (HTML5) 158
Using OpsCenter to report on virtual machine backups 160

Chapter 9 Use Accelerator to back up virtual machines 161

About the NetBackup Accelerator for virtual machines 161
Accelerator: full vs. incremental schedules 162
How the NetBackup Accelerator works with virtual machines 163
Accelerator notes and requirements for virtual machines 163
Accelerator forced rescan for virtual machines (schedule attribute) 165
Accelerator requires the `OptimizedImage` attribute 166
Accelerator backups and the NetBackup catalog 166
Accelerator messages in the backup job details log 167
NetBackup logs for Accelerator with virtual machines 167
About reporting the amount of Accelerator backup data that was transferred over the network 168
Replacing the Accelerator image size with the network-transferred data in NetBackup command output 171

Chapter 10 Restore virtual machines 175

Restore notes and restrictions 175
Restore notes and restrictions on Linux 179
Restoring the full VMware virtual machine 181

Virtual Machine Recovery dialog boxes (restore to original location) 182
Virtual Machine Recovery dialogs boxes (restore to alternate location) 188
About VMware virtual machine disk restore 196
Restoring VMware virtual machine disks by using Backup, Archive, and Restore 197
Select Virtual Disks panel 199
Recovery Destination panel 200
Virtual Disk Destination panel 201
Storage Destination panel 203
Recovery Summary panel 203
Restoring VMware virtual machine disks by using NetBackup commands 204
Determining the backup image ID from which to restore a VMware virtual machine disk 205
Creating the VMware virtual machine disk restore file 206
Modifying the virtual machine disk restore file 208
Validating the virtual machine disk restore file 212
Restoring the virtual machine disk or disks by using the `nbrestorevm` command 213
VMware virtual machine disk restore file 214
About restore of individual files 223
Restoring individual files 224
Setting up NetBackup Client Service for restore to a Windows shared virtual machine drive 227
Restore Marked Files dialog for restore of VMware files 227
How NetBackup handles VMware tag associations at restore 230
Browse and search virtual machines for restore 232
Search Virtual Machines for Restore dialog 233
Browse the vCloud or vSphere view for virtual machine clients 235
Search results dialog 236
If the recovery host is not at the same NetBackup release level as the backup host 236

Chapter 11 Restore virtual machines with Instant Recovery 237

About Instant Recovery for VMware 237
Task overview for Instant Recovery for VMware 239
Performance recommendations for Instant Recovery for VMware 240
Requirements for Instant Recovery for VMware 241

Notes on Instant Recovery for VMware 242
Restarting the Client for NFS service on a Windows restore host 243
Instant Recovery options on the nbrestorevm command 244
Restoring a virtual machine with Instant Recovery for VMware 249
Restoring a virtual machine to a different location with Instant Recovery for VMware 253
Restoring individual files with Instant Recovery for VMware while the current virtual machine is running 256
Job types for Instant Recovery for VMware 259
Reactivating a restored virtual machine with Instant Recovery for VMware 260

Chapter 12 Use NetBackup for vCloud Director 262

About NetBackup for vCloud Director 262
Notes on creating a NetBackup policy for vCloud 263
Notes on restoring virtual machines into vCloud Director 264
Restoring virtual machines into vCloud Director 265
Reducing the time required for VM discovery in a large vCloud environment 270
Virtual machine recovery dialog boxes for vCloud Director 275
Recovery Destination dialog box 275
Recovery Options dialog box (vCloud Director) 276
Recovery vApp Options for vCloud Director dialog box (restore to original location) 276
Virtual Machine Options dialog box for vCloud Director 276
Perform Recovery dialog box for vCloud Director 277
Recovery Options dialog box for vCloud Director (restore to alternate location) 277
Recovery vApp Options for vCloud Director dialog box (restore to alternate location) 278
Select a vApp dialog box 279
Recovery Destination Options for vCloud Director dialog box (restore to alternate location) 279
Virtual Machine Options (restore to alternate location) 280
Network connections (restore to alternate location) 280
Perform Recovery dialog box for vCloud Director (restore to alternate location) 280

Chapter 13 Best practices and more information 281

NetBackup for VMware best practices 281
NetBackup for VMware with deduplication 282
Best practices for VMware tag usage 282

Further assistance with NetBackup for VMware 284

Chapter 14 Troubleshooting 285

Notes on troubleshooting NetBackup for VMware 286
Beware of unsupported backup host 287
How to determine the ESX network that NetBackup used for the backup or restore 287
NetBackup logging for VMware 288
Configuring VxMS logging 290
Format of the VxMS core.log and provider.log file names 293
Configuring the VDDK logging level 294
Preventing browsing delays caused by DNS problems 295
Changing the browsing timeout for virtual machine discovery 297
Changing timeout and logging values for vSphere 298
Credentials for VMware server are not valid 300
Snapshot error encountered (status code 156) 301
The origin of the snapshot failure: NetBackup or VMware? 304
Conflict between NetBackup and VMware Storage vMotion with vSphere 5.0 or later 304
Incremental backups of the VM may fail if the NTFS file system in the guest OS is corrupted and the backup uses MSDP storage 305
The restore fails when you restore individual files to a virtual machine that has NetBackup client software 306
Backup or restore job hangs 306
VMware SCSI requirements for application quiesce on Windows 307
Mount point missing on a restored Windows virtual machine 308
Mount points not available when restoring files from a Linux virtual machine 308
Invalid client error when you restore files using NetBackup BAR interface installed on the virtual machine 308
VMware virtual machine does not restart after restore 309
A restored VM may not start or its file system(s) may not be accessible 309
NetBackup job fails due to update tasks on the VMware server 309
The vSphere interface reports that virtual machine consolidation is needed 310
The Enable file recovery from VM backup option does not work if a volume disk set contains a mixture of disk types 310
Linux VMs and persistent device naming 311
For a VMware virtual machine with Windows dynamic disks, a restore from incremental backup fails with a Windows restore host and the hotadd transport mode 312

Simultaneous hotadd backups (from the same VMware backup host) fail with status 13 314
Troubleshooting VMware tag usage 315
Ensuring that guest customizations can be restored in vCloud Director 317
Troubleshooting vmdk restore to existing VM 318
Errors for backups of virtual machines on Virtual Volumes (VVols) 319
Issues with the CA certificate during installation of the NetBackup client on VMware Cloud (VMC) 321

Appendix A NetBackup commands to back up and restore virtual machines 323

Using NetBackup commands to create a VMware policy 323
Notes on creating a VMware policy for vCloud Director 327
VMware policy: bpplinfo options and keywords 327
bpplinclude options for modifying query rules in a VMware policy 330
Using the nbdiscover command to search the virtual environment 332
Using the nbrestorevm command to restore virtual machines into vSphere 333
Using the nbrestorevm command to restore virtual machines into vCloud Director 338
Using the nbrestorevm command to restore virtual machines with Instant Recovery 343
Using the nbrestorevm command to restore virtual machine disks 343
The `nbrestorevm -R` rename file for restoring virtual machines 343
Logs for troubleshooting the nbrestorevm command 346
Query format and examples for searching virtual machine backups 347
Allowing other servers or clients to restore virtual machines 350

Appendix B Configuring services for NFS on Windows 352

About installing and configuring Network File System (NFS) for Granular Recovery Technology (GRT) 352
About configuring services for NFS on Windows 2012 or 2016 (NetBackup for VMware) 353
Enabling Services for Network File System (NFS) on a Windows 2012 or 2016 media server (NetBackup for VMware) 353

Enabling Services for Network File System (NFS) on a Windows 2012 or 2016 restore host (NetBackup for VMware) 357
Disabling the Server for NFS (NetBackup for VMware) 360
Disabling the Client for NFS on the media server (NetBackup for VMware) 362
Configuring a UNIX media server and Windows backup or restore host for Granular Recovery Technology (NetBackup for VMware) 364
Configuring a different network port for NBFSD (NetBackup for VMware) 365

Appendix C The Reuse VM selection query results option 366

About the Reuse VM selection query results option 366
The effect of virtual machine discovery on vCenter 367

Appendix D Backup of VMware raw devices (RDM) 369

About VMware raw device mapping (RDM) 369
Configurations for backing up RDMs 370
About alternate client backup of RDMs 370
Requirements for alternate client backup of RDMs 370
Configuring alternate client backup of RDMs 371

Index 374

Chapter 1

Introduction

This chapter includes the following topics:

- About NetBackup for VMware
- About the virtual machine backups that include database data
- About the NetBackup appliance as a VMware backup host
- NetBackup for VMware components
- Appliance as backup host: component overview
- Media servers as backup or discovery hosts
- Overview of the VMware backup process
- NetBackup for VMware terminology

About NetBackup for VMware

NetBackup for VMware provides backup and restore of the VMware virtual machines that run on VMware ESX servers. NetBackup for VMware takes advantage of VMware vStorage APIs for data protection. The backup process is off-loaded from the ESX server to a VMware backup host.

NetBackup for VMware does the following:

- Performs off-host backup of virtual machines (NetBackup client software is not required on the virtual machine). Off-host backup reduces the backup processing load on the VMware host.
- Increases the backup speed as compared to standard file-order backup methods, if the virtual machine is heavily populated with small files.

- Automatically creates quiesced snapshots using VSS (Windows only). Creates quiesced snapshots on Linux if snapshot quiesce is enabled in the Linux guest OS.
- Uses snapshot technology to keep virtual machines 100% available to users.
- Supports VMware vSphere and vCloud Director.
- Performs full backups and incremental backups, including block-level incrementals.
- Backs up the full virtual machine.
- Backs up the virtual machines even when they are turned off.
- Can restore selected files from the backup.

About the virtual machine backups that include database data

When NetBackup backs up a VMware virtual machine, database data in the virtual machine is backed up with the rest of the virtual machine. NetBackup allows the recovery of individual database files from the backup. This feature supports Microsoft Exchange Server, SQL Server, and SharePoint Server.

Note the following:

- To enable restore of individual database files, a NetBackup Windows client must be installed in the virtual machine during the backup.
- NetBackup uses Windows Volume Shadow Copy Service (VSS) to quiesce the database before it creates a snapshot of the virtual machine.
- A full backup is performed of the database data with each backup job, even if the policy schedule is incremental.

See “Application protection options (VMware)” on page 79.

About the NetBackup appliance as a VMware backup host

The NetBackup appliance uses the VMware policy type to back up VMware virtual machines.

The following topics contain notes on the appliance as the backup host:

- For an overview of the appliance as backup host in a virtual environment:
  See “Appliance as backup host: component overview” on page 18.

- For configuration tasks:
  See “Overview of VMware tasks” on page 24.
  See “Overview of NetBackup tasks” on page 25.
- For a list of requirements and limitations:
  See “Notes on the NetBackup appliance as a VMware backup host” on page 35.
- For log files:
  See “NetBackup logging for VMware” on page 288.

NetBackup for VMware components

Table 1-1 describes the components that NetBackup for VMware uses.

Table 1-1 Components of NetBackup for VMware

Component	Description
Backup host	NetBackup for VMware uses a special host that is called a VMware backup host (formerly called the VMware backup proxy server). The backup host is a NetBackup client that performs backups on behalf of the virtual machines. The backup host must have access to the datastores of the virtual machines. The backup host is the only host on which NetBackup client software is installed. No NetBackup client software is required on the VMware virtual machines. Note that the backup host is referred to as the recovery host when it performs a restore. The backup host can be configured in any of the following ways: ■ As a NetBackup client (Windows or Linux) with a connection to separate primary and media servers. The primary servers and media servers can be Windows, UNIX, or Linux. ■ As a NetBackup client that is installed on the media server (see Backup media server). ■ The NetBackup client and primary and media server can all reside on the same host (Windows or Linux). For a list of supported platforms for the backup host, see the *NetBackup Enterprise Server and Server OS Software Compatibility List* available from the following location: NetBackup Primary Compatibility List
Discovery host	Used for the automatic selection of virtual machines for backup. This host discovers virtual machines and filters them by means of the selection rules in the policy Query Builder. The resulting list determines which virtual machines are backed up. The discovery host can be on any platform that NetBackup supports for primary or media servers. It can also be the same host as the backup host. You specify this host on the policy **Clients** tab: Click **Select automatically through VMware Intelligent Policy query**, then **NetBackup host to perform automatic virtual machine selection**.

Table 1-1 Components of NetBackup for VMware *(continued)*

Component	Description
Access host	A VMware Access host is another term for a NetBackup client that acts as a backup host or a recovery host.
Backup media server	A media server that can operate as the backup host. See "Media servers as backup or discovery hosts" on page 18.
NetBackup client	Installed on the backup host.
NetBackup primary server	Manages the backups of virtual machines, by means of the NetBackup client that is installed on the backup host.
NetBackup media server	Performs the backups to storage on behalf of the NetBackup client.
Virtual machine	Virtual machines provide complete guest operating systems on virtualized hardware. In a NetBackup policy, a virtual machine is configured as a NetBackup client, even though NetBackup client software is not installed on the virtual machine.
ESX server	The VMware ESX server presents a virtualized hardware environment to multiple virtual machines; each virtual machine runs an independent operating system. Users can run applications in the virtualized OS as if the OS was installed in its own physical computer.
vCenter Server	The VMware vCenter Server (or VirtualCenter server) coordinates multiple ESX servers and workloads. It can migrate virtual machines from one ESX server to another. It also provides the ability to back up the virtual machines that are turned off. The vCenter Server is optional in the NetBackup for VMware environment.

Figure 1-1 shows a NetBackup for VMware environment on a local network. The backup host accesses the VMware datastore through the ESX servers.

Figure 1-1 NetBackup for VMware: components on local network

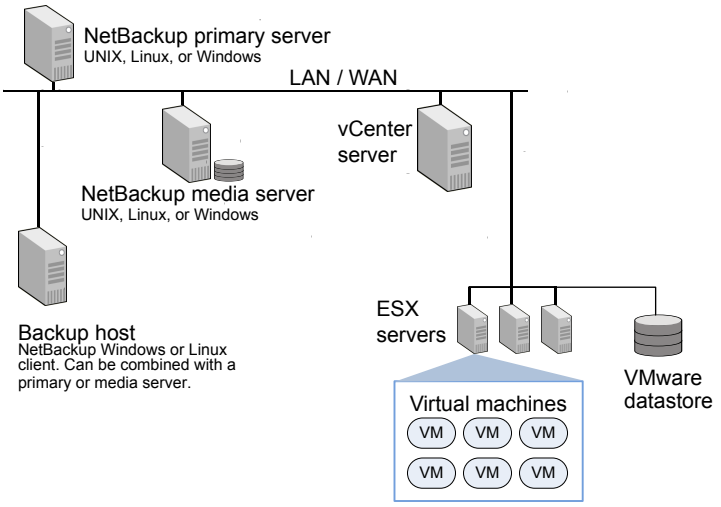
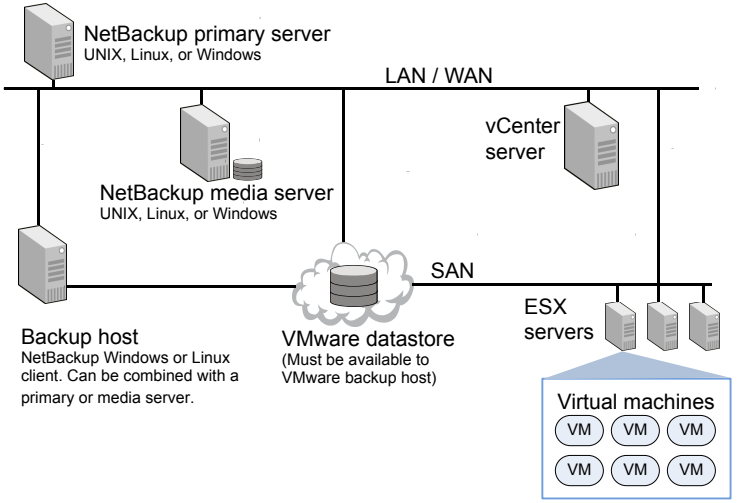


Figure 1-2 shows a NetBackup for VMware environment on a SAN. The backup host accesses the VMware datastore directly over the SAN.

Figure 1-2 NetBackup for VMware: components on SAN

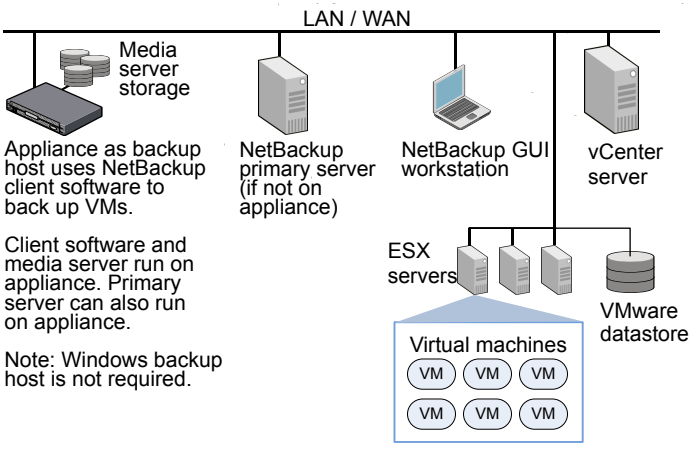


Appliance as backup host: component overview

As Figure 1-3 shows, the appliance can operate as the VMware backup host. A separate Windows backup host is not required.

The appliance as backup host can also run the NetBackup media server and primary server.

Figure 1-3 NetBackup for VMware with appliance as backup host



The NetBackup environment can also be on a SAN:

See Figure 1-2 on page 17.

Further information is available on the appliance as backup host:

See “Notes on the NetBackup appliance as a VMware backup host” on page 35.

Media servers as backup or discovery hosts

NetBackup for VMware uses a special host that is called a VMware backup host. The backup host is a NetBackup client that performs off-host backups of the virtual machines. The backup host must have access to the datastores of the virtual machines. The backup host reads the data from the datastore and sends it over the network to the media server. The media server backs up the data to storage.

NetBackup also uses a discovery host. For the policies that automatically select virtual machines, the discovery host filters virtual machines according to the rules in the policy Query Builder. The discovery host returns a list of virtual machines to be selected for backup.

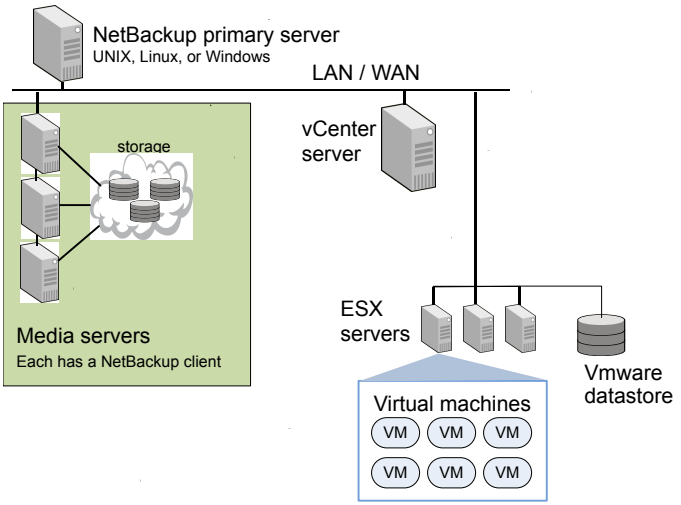
NetBackup can use media servers as backup hosts and as discovery hosts.

Media servers acting as backup or discovery hosts can provide the following advantages:

- Host redundancy: If one media server goes down, another media server takes over.
- Faster backup: The media server can read the data from the datastore and send the data straight to the storage device. Without media server access to storage devices, an ordinary backup host must send the backup data over the local network to the media server.

Figure 1-4 shows a group of media servers that can also act as backup or discovery hosts. The media servers can discover virtual machines for automatic selection, and perform off-host backups and send the backup data directly to storage.

Figure 1-4 Backup media servers



You can combine the flexibility of backup media servers with a standard feature of NetBackup: storage unit groups. Create a storage unit group that contains the storage units that your media servers can access. Any of the media servers can operate as a backup host.

Note the following requirements:

- To configure media servers as backup hosts: Set the policy **VMware backup host** field on the **VMware** tab to **Backup Media Server**.
  See "VMware backup host" on page 73.

- To configure media servers as discovery hosts: Set the policy **NetBackup host to perform automatic virtual machine selection** field on the **Clients** tab to **Backup Media Server**.
  See "Options for selecting VMware virtual machines" on page 109.

Overview of the VMware backup process

The following table describes the phases in the NetBackup backup process.

Table 1-2 NetBackup backup process

Phase	Description
Phase 1	The NetBackup primary server initiates the backup.
Phase 2	The NetBackup client on the VMware backup host initiates a VMware snapshot on the virtual machine.
Phase 3	Windows: VSS synchronizes the file system on the virtual machine. Linux: If snapshot quiesce is enabled in the Linux guest OS, the file system is synchronized on the virtual machine. (Contact your operating system vendor and VMware for additional information on how to enable snapshot quiesce.)
Phase 4	The VMware server creates a snapshot on the virtual disk datastore.
Phase 5	The NetBackup client reads the snapshot from the datastores and writes the data to the NetBackup storage unit.

NetBackup for VMware terminology

Table 1-3 lists the terminology that is used in NetBackup for VMware.

For further explanations of VMware terminology, refer to your VMware documentation.

Table 1-3 NetBackup for VMware terms

Term	Definition
backup host	The backup host is a NetBackup client that performs backups on behalf of the virtual machines. (This host was formerly known as the VMware backup proxy server.) The backup host is the only host on which NetBackup client software is installed. As an option, the backup host can also be configured as a NetBackup primary server or media server. The backup host is referred to as the recovery host when it performs a restore. See "NetBackup for VMware components" on page 15.
backup media server	A media server that operates as a backup host.
datastore	In NetBackup for VMware, the datastore is a disk that contains the virtual machines files.
datastore cluster	A collection of datastores that can be managed as a single unit. VMware Storage DRS manages the storage resources of the cluster.
discovery host	Discovers the virtual machines, filters them by the rules in the Query Builder, and returns a list of virtual machines to be selected for backup. The discovery host is used only for automatic selection of virtual machines. Can be the same host as the VMware backup host. See "NetBackup for VMware components" on page 15.
guest OS	An operating system that runs on a virtual machine.
hotadd	The backup or restore transport mode when the backup host is installed in a virtual machine.
hypervisor	A software virtualization layer that lets different operating systems run simultaneously on the same physical computer. The VMware hypervisor is vSphere, which runs on the ESX server host.

Table 1-3 NetBackup for VMware terms *(continued)*

Term	Definition
independent disk	A virtual disk that cannot be captured with a snapshot. An independent disk can be configured as either persistent or temporary. **Note:** NetBackup for VMware cannot back up the data on an independent disk. The backup succeeds but the backup image contains no data for the independent disk. If you restore the disk from the backup, the independent disk is restored to its original allocation size but contains no data. For example, the Windows swap file can reside on an independent disk, and is consequently not included in the virtual machine backup. To back up the data on an independent disk, install a NetBackup client on the virtual machine. See "NetBackup for VMware: notes and restrictions" on page 27.
query	The combination of rules in the policy's Query Builder, by which NetBackup selects virtual machines for backup. A query consists of one or more rules.
Query Builder	For creating filtering rules for automatic selection of virtual machines for backup. The Query Builder is on the **Clients** tab of the NetBackup policy.
query rule	A single statement in a query, by which NetBackup selects virtual machines for backup. An example of a query rule is: `Displayname Contains "finance"`
Raw device mapping (RDM)	Allows a virtual machine to directly access physical disks (on Fibre Channel or iSCSI). RDM allows the OS and applications in the virtual machine to have pass-thru access to raw devices. NetBackup for VMware cannot back up an RDM disk. NetBackup client software must be installed in the virtual machine. See "About VMware raw device mapping (RDM)" on page 369.
recovery host	See backup host.
transport mode	Determines how the snapshot data travels between the VMware datastore and the backup host. See "Transport modes options (VMware)" on page 78.

Table 1-3 NetBackup for VMware terms *(continued)*

Term	Definition
virtual machine	An execution environment that the hypervisor creates for the computer hardware. The resulting virtualized environment allows different operating systems to run simultaneously on the same physical computer.
virtual network	A logical network that allows the exchange of data between virtual machines. A virtual network uses a virtual switch (VMware vSwitch). A virtual network can be connected to a physical network.
vmdk file	In a VMware ESX server, one or more vmdk files make up the disk image or virtual drive in a virtual machine. The `.vmdk` files contain the operating system, applications, and data in the virtual machine.
VMware Tools	Installed inside each VMware virtual machine. Enhances the virtual machine performance and adds backup-related functionality.
vmx datastore	Sometimes called the vmx directory or configuration datastore. Contains the configuration files that describe the virtual machine, such as vmx files. During a backup of a virtual machine snapshot, vmdk writes are also cached on this datastore. Note that a separate vmx datastore is not a VMware requirement.
vStorage	VMware vStorage APIs enable data protection features for more efficient use of storage capacity. NetBackup can use vStorage to back up the latest vSphere environments as well as to back up earlier VMware environments.

Chapter 2

Required tasks: overview

This chapter includes the following topics:

- Overview of VMware tasks
- Overview of NetBackup tasks

Overview of VMware tasks

The VMware components including ESX servers and virtual machines must be set up before you configure NetBackup.

Table 2-1 VMware tasks

Sequence	Tasks
Phase 1	Ensure that the hardware and the SAN are configured properly. The VMware datastore where the target virtual machine files exist must be accessible to the VMware backup host. A SAN connection between the backup host and the datastore is optional if you use the NBD transfer type or NBDSSL transfer type. To use the SAN transport type, set up the datastore on Fibre Channel or iSCSI. In this configuration, the VMware backup host must be able to access the datastore over the SAN.
Phase 2	Install the VMware ESX server and virtual machines.
Phase 3	Install VMware Tools on the virtual machines that you plan to back up. VMware requires that ESX server names resolve to an IP address. It is highly recommended that you use DNS for the naming resolution among VMware servers.
Phase 4	Optional: install a vCenter (or VirtualCenter) server.

Overview of NetBackup tasks

Table 2-2 lists the NetBackup configuration tasks for VMware. These tasks are described in other NetBackup topics and guides, as indicated.

Table 2-2 NetBackup tasks

Sequence	Tasks
Phase 1	Install the NetBackup primary server and media server. See the *NetBackup Installation Guide*. It is recommended that the NetBackup media server and the VMware backup host be installed on the same host.
Phase 2	Install the NetBackup Enterprise Client license on the primary server, and install NetBackup client software on the VMware backup host. NetBackup for VMware requires an Enterprise Client license for each ESX Server. To protect an application or database, note: an additional license for the appropriate NetBackup package is needed for each ESX server that hosts the application or database.
Phase 3	Add the VMware backup host to your NetBackup configuration. See "Adding the VMware backup host to NetBackup" on page 44. **Note:** This step is not required on the appliance: the backup host is already installed on the appliance.
Phase 4	Enter NetBackup access credentials as needed: for VMware vCenter, for vCloud Director, and for individual ESX servers. See "Adding NetBackup credentials for VMware" on page 45. **Note:** The NetBackup primary server must have network access to the VMware servers that NetBackup has credentials for.
Phase 5	Create a NetBackup policy for VMware. See "Configuring a VMware policy from the Policies utility" on page 68.
Phase 6	Perform a backup. See "Backing up virtual machines" on page 154.

Chapter 3

Notes and prerequisites

This chapter includes the following topics:

- NetBackup for VMware prerequisites
- NetBackup for VMware: notes and restrictions
- Notes on VMware Virtual Volumes (VVols)
- NetBackup IPv6 parameter required for backups in VMware IPv6 environments
- NetBackup for VMware: notes on Linux virtual machines
- Notes on the NetBackup appliance as a VMware backup host
- NetBackup for VMware support for SAN multi-pathing
- NetBackup for VMware support for fault tolerant VMs
- NetBackup character restrictions for the Primary VM identifier
- In the policy Query Builder, display names, resource pool names, and vApp names are case-sensitive
- Notes on the hotadd transport mode
- Notes and limitations for tag usage in VMware Intelligent Policy queries
- Notes and limitations for the backup and restore of VMware tag associations

NetBackup for VMware prerequisites

The following prerequisites apply to NetBackup for VMware:

- The VMware components including ESX servers and virtual machines must be set up before you configure NetBackup.
  See “Overview of VMware tasks” on page 24.

- The NetBackup Java Runtime Environment (JRE) must be installed on the discovery host and the recovery host. Install the NetBackup Remote Administration Console to install NetBackup Java.
- The VMware backup host must run on Windows or Linux. The supported hardware types are the same as for any NetBackup client. For the supported platforms for the backup host, see the *NetBackup Enterprise Server and Server OS Software Compatibility List* available from the following location:
  NetBackup Primary Compatibility List
- To use the hotadd transfer type for backup or restore, the VMware backup or restore host is installed in a virtual machine.
  See "Notes on the hotadd transport mode" on page 40.

NetBackup for VMware: notes and restrictions

Note the following about NetBackup for VMware:

- For information on supported VMware versions and on supported platforms for the backup host, see the *NetBackup Enterprise Server and Server OS Software Compatibility List* available from the following location:
  NetBackup Primary Compatibility List
  For additional support information on NetBackup for VMware, see *Support for NetBackup in virtual environments*:
  http://www.veritas.com/docs/000006177
- NetBackup for VMware supports FIPS mode for SSL communication when using VDDK. This can be enabled by adding the `VDDK_FIPS_MODE = ENABLED` entry to the `bp.conf` file on VMware access hosts.
- NetBackup for VMware does not support the **Retain snapshot for Instant Recovery or SLP ...** option on the policy **Attributes** tab of the NetBackup Administration Console.

  NetBackup supports these features as follows:

  - For Instant Recovery, use the `nbrestorevm` command.
    See "About Instant Recovery for VMware" on page 237.
  - For SLP management of snapshots, use Replication Director.
    For more information, see the *NetBackup Replication Director Solutions Guide*.
- NetBackup allows up to 31 snapshots per virtual machine. If the virtual machine has more than 31 snapshots, the backup may fail with status 13. Messages similar to the following appear in the NetBackup job details:

```
10/18/2012 4:56:59 PM - Critical bpbrm(pid=4604)from client
Umesh_w2k3_hypervm33: FTL - vSphere_freeze: Unable to remove
existing snapshot, too many existing snapshots (91).
10/18/2012 4:56:59 PM - Critical bpbrm(pid=4604) from client
Umesh_w2k3_hypervm33: FTL - VMware_freeze: VIXAPI freeze
(VMware snapshot) failed with 26: SYM_VMC_REMOVE_SNAPSHOT_FAILED
```

As a reminder to consolidate or delete snapshots, the NetBackup detailed status provides the following message when the number of snapshots exceeds 15:

```
Umesh_w2k3_hypervm33: WRN - vSphere_freeze: VM has 16 existing
snapshots. Snapshots may start failing if this number exceeds 32
```

To back up a virtual machine that has more than 31 snapshots, consolidate or delete the existing snapshots. Then rerun the backup.

Note: Replication Director backups allow more than 31 snapshots per virtual machine.

- If the number of snapshot delta files for a VM's vmdk exceeds 32, snapshot creation fails. A message similar to the following appears in the NetBackup detailed status:

  ```
  Umesh_w2k3_hypervm33: FTL - vSphere_freeze: Unable to
  proceed with snapshot creation, too many existing delta files(50).
  ```

  As a reminder to consolidate or delete snapshots, the NetBackup detailed status provides the following message when a vmdk's delta files exceed 16:

  ```
  Umesh_23k3_hypervm33: WRN - vSphere_freeze: VM has 17 existing
  delta files for vmdk Umesh_23k3_hypervm33.vmdk. Snapshots may start
  failing if this number exceeds 31
  ```

  Delta files can accumulate if the VM's snapshots are not deleted or consolidated. Consolidate or delete the existing snapshots, then rerun the backup.

- NetBackup for VMware cannot back up the data on an independent disk, because an independent disk cannot be captured with a snapshot. The backup succeeds but the backup image contains no data for the independent disk.
  To back up the data on an independent disk, install a NetBackup client on the virtual machine. You can configure NetBackup to back up the virtual machine and any independent disks as if the client was installed on a physical host. You can restore the virtual machine and then restore the independent disk as a separate job.

- NetBackup for VMware does not back up standard iSCSI LUNs that are connected to the virtual machine. If the virtual machine has an iSCSI LUN, the backup succeeds but the drive that represents the LUN is not backed up.
  Note: NetBackup for VMware supports datastores over iSCSI.
- Several notes and limitations apply to Linux virtual machines.
  See "NetBackup for VMware: notes on Linux virtual machines" on page 34.
- If a Windows virtual machine includes Veritas Storage Foundation volumes, the **Enable file recovery from VM backup** option is not supported.
  See "Storage Foundation Volume Manager volumes in the virtual machine" on page 100.
- During an incremental backup with the **Enable file recovery from VM backup** option (with or without block-level incremental backup), any files that had been moved or renamed are not backed up. Those files are not available when you browse to restore individual files from that incremental backup.

  Note: When you restore the entire VM from a block-level incremental backup, the file metadata is updated and the moved or renamed files reflect the updated metadata.

- VMware virtual machine templates are for cloning virtual machines: They cannot be turned on and used as functioning VMs. As a result, VMware has imposed the following restrictions on backup and restore of virtual machine templates:
  - A virtual machine template cannot be captured in a snapshot. NetBackup backs up the template to the designated storage unit.
  - Block level incremental backup (BLIB) cannot be used when backing up a virtual machine template.

    Note: As a result of this restriction, NetBackup Accelerator cannot be used to back up VMware virtual machine templates.

  - A virtual machine template cannot be backed up over a SAN. You must configure the NetBackup policy to use a local network transfer type, such as **nbd**. Likewise, the restore of a template must be conducted over a local network.

    Note: You can use the Query Builder in the NetBackup policy to create rules for automatic selection of virtual machine templates.

- NetBackup supports non-ASCII characters in virtual machine objects, as follows:
  - The NetBackup primary server, the backup host, and the restore host must run NetBackup 8.1 or later. The backup host and the restore host may be the same computer.
  - Windows operating systems on the NetBackup primary server, the backup host, and the restore host do not assume non-ASCII characters in VM display name if the system locales of Windows hosts are not set to UTF-8. Even if the system locale is not set to UTF-8, a backup of the VMware virtual machine whose display name contains non-ASCII character may work. However, a restore from the VMware virtual machine backup that has non-ASCII characters in its display name needs a Linux or UNIX restore host which uses UTF-8 character encoding.
  - The UNIX and Linux operating systems on the NetBackup primary server, the backup host, and the restore host must use UTF-8 character encoding. The backup host and the restore host may be the same computer.
  - The name that NetBackup uses to select a VM for backups cannot contain non-ASCII characters. The **Primary VM identifier** field in the backup policy identifies the name type that NetBackup uses to select VMs. For example, if you specify **VM display name** as the **Primary VM identifier**, the display name of each VM that you back up cannot contain non-ASCII characters.
    See "Primary VM identifier options (VMware)" on page 76.
    VM BIOS UUID and **VM instance UUID** names never contain non-ASCII characters.
  - For security purposes, VM names have some restrictions.
    See "NetBackup character restrictions for the Primary VM identifier" on page 37.

  Examples of objects are file and folder names, annotations, floppy image name, parallel port or serial port file name, CD-ROM ISO name, and so on.
- For dual-boot virtual machines, NetBackup does not support the following policy options:
  - **Enable file recovery from VM backup**
  - **Exclude deleted blocks**
  - **Exclude swap and paging files**
  - **Exclude boot disk**
  - **Exclude all data disks**
- To support the following exclude disk options, the backup host must be at release level 8.1 or later:

- **Perform custom attribute based exclusion**
  Custom Attribute based disk exclusion requires that you enter in NetBackup the credentials for the vCenter server or servers that host the VMs. ESXi server credentials are not sufficient.
  See "Adding NetBackup credentials for VMware" on page 45.
- **Specific disk(s) to be excluded**

- NetBackup does not support the following exclude disks options for Replication Director backups:
  - **Exclude boot disk**
  - **Exclude all data disks**
  - **Perform custom attribute based exclusion**
  - **Specific disk(s) to be excluded**
- If you remove a disk from exclusion, the individual files that were last modified before the most recent backup cannot be restored. To restore those files, restore the entire virtual disk or the virtual machine. After the next full backup, those files are available to restore individually.
- NetBackup fails the backups of virtual machines that are empty. A VM may be empty because all of its disks are empty or because disk exclusion excludes all disks.
- To back up a virtual machine while Storage vMotion migrates its files, NetBackup must conduct the backup through the vCenter server.
  See "Conflict between NetBackup and VMware Storage vMotion with vSphere 5.0 or later" on page 304.
- Several notes and limitations apply to the automatic selection of virtual machines for backup (Virtual Machine Intelligent Policy).
  See "NetBackup requirements for automatic virtual machine selection" on page 107.
- For hotadd backup or restore: The virtual machine to back up (or restore) and the virtual machine that contains the hotadd backup host must reside in the same VMware data center.
- Note the following information about NetBackup for VMware compression and encryption:
  - NetBackup's compression or encryption options
    NetBackup for VMware does not support NetBackup's compression or encryption options (in the NetBackup policy attributes).
  - Granular file recovery/SFR on the VM

NetBackup for VMware granular file recovery/SFR supports Windows NTFS file compression but the restored file or folder will be uncompressed.

NetBackup for VMware granular file recovery/SFR supports file-level compression (such as zip or lzh), and the file or folder will be restored as the original compressed file.

NetBackup for VMware granular file recovery/SFR does not support Windows NTFS file encryption nor any type of encryption that is set in the guest OS (such as BitLocker).

- VM volume recovery

  NetBackup for VMware VM volume recovery supports any type of compression or encryption that they are set in the guest OS (such as BitLocker).

- Storage optimization cannot be used if a snapshot exists on the virtual machine when VMware Changed Block Tracking is turned on.
  See "About reducing the size of VMware backups" on page 150.
- If the policy's **Primary VM identifier** option is set to **VM hostname**, note: NetBackup cannot select a VMware virtual machine for backup if it cannot obtain an IP address for the virtual machine.
- For Exchange, SharePoint, and SQL applications, NetBackup for VMware supports Granular Recovery Technology (GRT) restores from full backups only.
- See "Restore notes and restrictions" on page 175.
- If a policy is changed from manual selection to Intelligent policy (or vice versa), the next backup of the VM is a regular full backup, even if a backup already exists for that VM.

  For example:

  - In a new VMware policy, the **Select manually** option on the **Clients** tab is used to select a VM. The first backup from the policy runs.
  - In the policy, an Intelligent Policy query is used to select the same VM, and the VM is backed up a second time. Because of the switch from manual selection to query-based selection, this second backup is a regular full backup. Note that for a policy that uses **Enable block-level incremental backup** (BLIB) or BLIB plus Accelerator, the backup processing is not limited to changed blocks only.

    For the second backup, the Detailed status log includes a message similar to the following:

    ```
    There is no complete backup image match, a regular full backup
    will be performed.
    ```

The same backup behavior occurs if the policy's VM selection is switched from query-based to manual selection: The second backup is a regular full backup.

- For the virtual machines that vSphere 6.5 hosts, NetBackup fails the backup if a snapshot exists while NetBackup tries to enable VMware Change Block Tracking. Because the VMware Change Block Tracking API behavior changed beginning in vSphere 6.5, NetBackup fails the backup.
  NetBackup enables CBT on a VM if **Block Level Incremental Backups** is enabled in the backup policy and CBT is not enabled already on the VM.
- In vSphere, if your virtual environment has IPv6 addresses, use only fully qualified domain names (FQDNs) that are mapped to IPv6 addresses on the DNS server.
- The Test query operation fails for a VMware policy in the following condition:
  There is no direct connectivity between the NetBackup primary server and the ESX server (for example, ESX server in NAT environment) where a virtual machine is to be backed up and the **NetBackup host to perform automatic virtual machine selection** option is set to Backup Media Server (for example, NAT media server).

Notes on VMware Virtual Volumes (VVols)

NetBackup supports backup and restore of the virtual machines that are configured on Virtual Volumes (VVols).

- Ensure that you have the required snapshot license from the array vendor.
- Consult the storage array documentation from the vendor for space requirements.

Configuring backup and restore of virtual machines with VVols is the same as for virtual machines without VVols, with these exceptions:

- To restore a virtual machine with the hotadd transport mode: VMware requires that the virtual machine and the restore host virtual machine reside on the same VVol datastore. Otherwise, the restore must use a different transport mode (not hotadd).
- For a restore to standard (non-VVol) datastores, the NetBackup job creates a vSphere snapshot of the virtual machine while NetBackup restores the data. Note: For a restore to a VVol datastore, NetBackup restores the data to the virtual machine without creating a vSphere snapshot.

NetBackup IPv6 parameter required for backups in VMware IPv6 environments

For backups and restores of VMware virtual machines in an IPv6 environment, you must configure the IPv6 support on the following NetBackup hosts:

- The primary server
- The backup host

The **Both IPv4 and IPv6** option of the **IP Address Family Support** host property configures IPv6 support. The **IP Address Family Support** host property is on the **Network Settings** host properties dialog box.

If the NetBackup primary server and the backup host are the same host, configure the support on that host only. If the NetBackup primary server and the backup host are separate hosts, configure the support on each host.

For more information about the **IP Address Family Support** host property, see the *NetBackup Administrator's Guide, Volume I*:

http://www.veritas.com/docs/DOC5332

NetBackup for VMware: notes on Linux virtual machines

The following notes apply to virtual machines with Linux guest operating systems:

- NetBackup cannot exclude unused or deleted blocks from the backup if the virtual machine is configured with software RAID volumes. The policy's **Exclude deleted blocks** option is not supported.
- If snapshot quiesce is enabled in the Linux guest OS, NetBackup for VMware synchronizes the guest OS file system before it takes the snapshot. Contact your operating system vendor and VMware for additional information on enabling snapshot quiesce. Note: If snapshot quiesce is not enabled, NetBackup cannot guarantee that data in the file system is in a consistent state when the snapshot occurs.
- Unmounted LVM2 volumes must start with /dev
  If the path of an unmounted LVM2 volume does not start with /dev, the backup of the virtual machine fails. Note: The path of the volume is set with the `dir` parameter on the LVM volume configuration file. An example of this configuration file is /etc/lvm/lvm.conf.
- For Linux files or directories, NetBackup for VMware has the same path name restriction as NetBackup on a Linux physical host. Files or directories with path

names longer than 1023 characters cannot be individually backed up or restored. Such files can be restored when you restore the entire virtual machine from a full virtual machine backup.

- The Linux ext4 file system includes a persistent pre-allocation feature, to guarantee disk space for files without padding the allocated space with zeros. When NetBackup restores a pre-allocated file (to any supported ext file system), the file loses its preallocation and is restored as a sparse file. The restored file is only as large as the last byte that was written to the original file. Subsequent writes to the restored file may be non-contiguous.

  Note: The restored file contains all of its original data.

- The NetBackup policy's **Enable file recovery from VM backup** option is not supported for the disks inside a Linux guest OS that are configured as follows:
  - The disks are divided into logical volumes by means of the Linux Logical Volume Manager (LVM), and
  - The LVM volumes were created with thin-provisioning.
- See "Restore notes and restrictions on Linux" on page 179.

Notes on the NetBackup appliance as a VMware backup host

Note the following requirements and limitations for the appliance as the backup host:

- The appliance must be version 2.5 or later.
- You must use the VMware policy type.
- The appliance supports iSCSI connections. Refer to the *NetBackup Appliance iSCSI Guide* for more information.

NetBackup for VMware support for SAN multi-pathing

NetBackup for VMware on Windows supports dynamic multi-pathing (DMP) between the vSphere ESXi storage and the NetBackup for VMware agent (Windows backup host). Dynamic multi-pathing can provide SAN I/O high-availability and improved backup throughput.

For NetBackup for VMware on a Linux backup host, the following items describe the support for dynamic multi-pathing in a SAN environment:

NetBackup appliance

The NetBackup appliance (beginning with the 2.6.0.2 release) supports SAN dynamic multi-pathing for VMware backups. I/O is redirected through the volume manager dynamic multi-pathing node.

For more information, see the *NetBackup Appliance Administrator's Guide* for version 2.6.0.2 and later:

http://www.veritas.com/docs/DOC2792

Non-appliance Linux host

NetBackup supports backups and restores for multi-pathing under the following conditions:

- The virtual disk SAN transport allowed list specifies the device node paths that you want to use for multipathing. The virtual disk `vixDiskLib.transport.san.allowed list` API function defines the allowed list. For NetBackup purposes, Veritas recommends that you include the DMP nodes in the allowed list; the following is an example:

  ```
  vixDiskLib.transport.san.allowed list = /dev/vx/dmp/
  hitachi_usp-v0_00a0,/dev/vx/dmp/hitachi_usp-v0_00
  a0s1,/dev/vx/dmp/hitachi_usp-v0_00a0s2,/dev/vx/dm
  p/hitachi_usp-v0_00a0s3,/dev/vx/dmp/hitachi_usp-v
  0_00a0s4,/dev/vx/dmp/hitachi_usp-v0_00a0s5
  ```

- The virtual disk SAN transport blocked list specifies the device node paths you want to exclude from multipathing. The virtual disk `vixDiskLib.transport.san.blocked list` API function defines the blocked list. For NetBackup purposes, Veritas recommends that you set the blocked list to `all`; the following is an example:

  ```
  vixDiskLib.transport.san.blocked list = all
  ```

Specify the allowed list and the blocked list in the following file on the backup host:

```
/usr/openv/lib/shared/vddk/lib64/vixDiskLib.ini
```

For more information about the allowed list and the blocked list, see the appropriate VMware documentation. For example, for Virtual Disk Development Kit 6.0 the allowed list and the blocked list function descriptions are in the VMware *Virtual Disk Programming Guide*.

Note: This support or limitation does not affect NetBackup support for VMware's Native Multipathing, which is multi-pathing between the ESXi host and storage.

This support or limitation does not affect NetBackup for VMware on Windows backup hosts. The Windows operating system has integrated multi-pathing support. The following Microsoft guide contains more information:

http://microsoft.com/mpio

NetBackup for VMware support for fault tolerant VMs

NetBackup supports backing up and restoring primary fault tolerant virtual machines on vSphere 6.0 and later. (NetBackup does not backup or restore the secondary VMs.) If you choose to overwrite the VM during the restore, NetBackup deletes both the primary and the secondary VMs during the restore process. NetBackup then restores the primary VM.

Fault tolerance is not enabled on the restored VM. After the restore has completed, you can turn on fault tolerance.

For information about how to turn on fault tolerance, see the VMware documentation for your version of vSphere.

NetBackup character restrictions for the Primary VM identifier

For VMware virtual machines in a NetBackup policy, certain characters are not allowed in their names. The backup policy **Primary VM identifier** field identifies the name type that NetBackup uses to select VMs.

See "Primary VM identifier options (VMware)" on page 76.

If the name contains disallowed characters, backups or restores may fail.

The following table describes the characters and strings that NetBackup does not allow for backup or restore in the **Primary VM identifier**, except where noted.

Table 3-1 Disallowed characters and strings in the primary VM identifier

Character/string	Description	Notes
"	Quotation mark, unicode x22.	
$	Dollar sign, unicode x24.	

Table 3-1 Disallowed characters and strings in the primary VM identifier *(continued)*

Character/string	Description	Notes
'	Apostrophe, unicode x27.	
*	Asterisk, unicode x2A.	
,	Comma, unicode x2C.	
:	Colon, unicode x3A.	
;	Semi-colon, unicode x3B.	
?	Question mark, unicode x3F.	
@	At sign, unicode x40.	
|	Vertical line, unicode x7C.	
`	Grave accent, unicode x60.	
´	Acute accent, unicode xB4.	
%	Percent sign, unicode x25.	Disallowed in the virtual machine display name for application-aware VMware backups for SharePoint, allowed elsewhere. In VIP query and VM search results, NetBackup converts % in the display name of **Included** VMs to the literal string **%25**. When you specify a display name in a query, replace the % character with **%25**.
&	Ampersand sign, unicode x26.	
<	Less than sign, unicode x3C.	
>	Greater than sign, unicode x3E.	
-	Hyphen-minus, unicode x2D.	Disallowed in the first position only.
/	Solidus, unicode x2F.	Disallowed in VM display name, allowed in other objects.
\	Reverse solidus, unicode x5C.	Disallowed in VM display name, allowed in other objects.

Table 3-1 Disallowed characters and strings in the primary VM identifier *(continued)*

Character/string	Description	Notes
.	Full stop (period), unicode x2E.	Disallowed in VM display name when in the last position, allowed in other objects.
□	Space, unicode x20.	In VIP query and VM search results, NetBackup converts a space character in the display name of **Included** VMs to the literal string **%20**. When you specify a display name in a query, replace the space character with **%20**.
Unicode characters greater than x7F (non-ASCII)		Disallowed when the backup policy specifies the VM display name as the primary VM identifier.
%2f	Literal string, not a unicode character definition.	Disallowed in VM display name, allowed in other objects.
%5c	Literal string, not a unicode character definition.	Disallowed in VM display name, allowed in other objects.

Additional character restrictions for VM names can be found in the *NetBackup Cloud Administrator's Guide*, available from this location:

http://www.veritas.com/docs/000003214

In the policy Query Builder, display names, resource pool names, and vApp names are case-sensitive

In VMware vSphere, virtual machine display names, resource pool names, and vApp names are case-sensitive. For example, a virtual machine with the name "vm1" is a different virtual machine from one that is named "VM1."

The VMware virtual machines with the name values that do not exactly match the query string case are not returned in the result set. Backups for those virtual machines are missed.

For example, for the following virtual machines:

```
vmware-ted
VMware-charles
VMWARE-john
vmWARE-jason
```

A query specifying `Displayname Contains "vmware-"` returns `vmware-ted` but not the other virtual machines.

Notes on the hotadd transport mode

NetBackup supports several transport modes for sending snapshot data between the VMware datastore and the VMware backup host during a backup or restore. One of those transport modes (**hotadd**) is used when the VMware backup host is installed in a virtual machine.

Note the following about the hotadd transport mode:

- The VMware backup host must be installed in a virtual machine.
- The following is a VMware requirement: The virtual machine to back up and the virtual machine that contains the hotadd backup host must reside in the same VMware datacenter. The same VMware requirement applies to virtual machine restore: The virtual machine to restore and the virtual machine that contains the hotadd restore host must reside in the same VMware datacenter.
  For hotadd backup, it is recommended at least one hotadd backup host for each datacenter.
- NetBackup does not support IDE disks on the virtual machine.
- On the virtual machine to back up, no two disks should have the same name. (Identical names can occur if the disks reside on different datastores.)
- The ESX server (where the backup-host virtual machine resides) must have access to the datastore of the virtual machines that you want to back up.
- The datastore for the backup-host virtual machine must have some free space before the hotadd backup begins. Otherwise, the backup may fail.
- Restores that use the hotadd or SAN transport modes do not include the VM's metadata changes in the restore. The status log of the NetBackup job contains messages similar to the following:

```
07/25/2013 12:37:29 - Info tar (pid=16257) INF - Transport Type
= hotadd
07/25/2013 12:42:41 - Warning bpbrm (pid=20895) from client
<client_address>: WRN - Cannot set metadata (key:geometry.
biosSectors, value:62) when using san or hotadd transport.
```

Retry the restore with a different transport mode (**nbd** or **nbdssl**).
This problem is a known VMware issue..

- Locking timeouts in the VMware VDDK may cause simultaneous hotadd backups from the same VMware backup host to fail.
  See “Simultaneous hotadd backups (from the same VMware backup host) fail with status 13” on page 314.
- For a list of VMware restrictions on the hotadd transport mode, refer to VMware’s documentation.

Notes and limitations for tag usage in VMware Intelligent Policy queries

- NetBackup does not support the selection of virtual machines based on the category.
- NetBackup uses tags for virtual machine selection independent of the tag's category. The VMware vSphere Web Client can create tags in two different categories with the same tag name. In the example, both virtual machines are selected if the policy is configured to include virtual machines with the “HR” tag.
  Example:
  - `Virtual_Machine_1` has a user-specified tag `HR` in the category `Production`
  - `Virtual_Machine_2` has a user-specified tag `HR` in the category `Test`
- NetBackup only recognizes the tags that are associated with virtual machines, not other vCenter objects such as Datastores.
- vCenter Server 6.0 or later is required.
- Any Windows host with only the NetBackup Client Software installed that is also defined in the VMware policy's **Client** tab as the **NetBackup host to perform automatic virtual machine selection** must have NetBackup Java installed. Install the NetBackup Remote Administration Console to install NetBackup Java.
- Be aware of a known bug in vSphere 6.0 when the system time of the discovery host and the vCenter Server are not synchronized. This issue is known to cause backups to fail with a NetBackup Status Code 4263.
  VMware knowledge base article: http://kb.vmware.com/kb/2125193
- If you use block-level incremental backups (BLIBs) with a VMware VIP policy, understand the effect of changing the VMware discovery host setting. After this policy change, subsequent incremental backups will back up the full data, not only the changed data, because the policy execution manager loses the backup references. If the discovery host must be changed, a full schedule backup is

needed after the policy change to allow subsequent incremental backups to back up the changed data.

- In large VMware environments, consider increasing the **Maximum bearer token lifetime** from the default value. Veritas has observed issues with discovery jobs timing out because the default value is too small. The **Maximum bearer token lifetime** is a vCenter Server setting. More information on this issue is available. See "Troubleshooting VMware tag usage" on page 315.

Notes and limitations for the backup and restore of VMware tag associations

- Tag associations are part of the metadata of the virtual machine. NetBackup considers virtual machine tag association protection a best effort backup. Any tag collection errors are shown in the Activity Monitor for the virtual machine snapshot jobs.
  If for any reason NetBackup is unable to back up tag associations, the job completes successfully with a NetBackup Status Code 0. Any failures to retrieve tag associations in the backup are, however, reported in the job details in the Activity Monitor.
- vCenter Server 6.0 or later is required.
- VMware tag associations are only backed up when you use VMware Intelligent Policies.
- NetBackup backs up tag associations with virtual machines. NetBackup does not back up tag associations with other vCenter Server objects, such as datastores or folders.
- Tag associations for all virtual machines are retrieved during the discovery job. The tag associations are, however, stored in the backup image for each individual virtual machine. Be aware there is a time difference between the discovery job time and the backup job. If tag associations are changed between these times, the changes are not backed up.
- If tag associations of a virtual machine were successfully backed up, then NetBackup attempts to recreate tag associations with the restored virtual machine. If the recovery host version is incompatible, NetBackup completes the recovery of the virtual machine and sets the job status to 0. The recovery job details, however, provide information on the failure to recreate the tag associations.
- If tag associations of a virtual machine were not backed up successfully, then NetBackup does not attempt to recreate tag associations with the restored Virtual Machine. NetBackup completes the recovery of the virtual machine and sets

the job status to 0. The recovery job details provide information on the failure to collect the tag associations that occurred at the time of backup.

- When Replication Director for VMware is used to protect your virtual machines, tag associations are backed up only when Application Consistent protection is enabled. When Application Consistent protection is disabled, NetBackup does not protect tag associations.

Chapter 4

Configure NetBackup communication with VMware

This chapter includes the following topics:

- Adding the VMware backup host to NetBackup
- Adding NetBackup credentials for VMware
- Changing the host name of a VMware server in NetBackup
- Setting privileges for posting events to vCenter
- Authentication token for the NetBackup vSphere plug-ins
- Setting global limits on the use of VMware resources
- Validating VMware virtualization server certificates in NetBackup

Adding the VMware backup host to NetBackup

Use this procedure to enable a NetBackup client as the backup host.

Note: This procedure is not needed for the media servers that operate as backup hosts with the policy **Backup Media Server** option. With that option, NetBackup automatically enables media servers as backup hosts.

In the NetBackup Administration Console, do the following.

To add the VMware backup host

1. Click **Host Properties > Primary Servers**, double click the NetBackup primary server, and click **VMware Access Hosts**.
2. Click **Add**.
3. Enter the fully qualified domain name of the VMware backup host, and click **Add**.
4. When you are finished adding hosts, click **Close**.
5. Click **Apply** and then **OK**.
6. If the NetBackup primary server is clustered in a failover environment: repeat this procedure to add the backup host to each primary server node in the cluster.

Adding NetBackup credentials for VMware

To back up or restore virtual machines, NetBackup requires logon credentials to the VMware ESX servers, the VMware vCenter servers, or the VMware vCloud servers. In the NetBackup Administration Console, do the following.

To add NetBackup credentials

1. Click **Media and Device Management > Credentials > Virtual Machine Servers**.
2. Click **Actions > New > New Virtual Machine Server**.
3. On the **New Virtual Machine Server** dialog, enter the name of a virtual machine server (ESX server, vCenter server, or vCloud server).

Note: Enter the server name in the same format in which it is registered in DNS and in the VMware server (whether short or fully-qualified).

See "Using the VMware Managed Object Browser to verify the server name" on page 49.

Note: The vCenter name that you enter here must match the name that is set on the vCenter for `VimApiUrl` name and `Runtime` name. For assistance in setting those names on the vCenter, and for additional vCenter naming requirements relating to the NetBackup plug-ins for vSphere: See the topic on consistent vCenter naming in the *NetBackup Plug-in for VMware vSphere Web Client Guide*:

http://www.veritas.com/docs/000003214

Note: It is recommended the use of fully qualified names. The entire name must be properly formed without empty or null elements. For example, a fully-qualified name must include the domain name and not end in a period (.).

Note: The ESX server name is case-sensitive. Enter the ESX server name exactly as it is in the VMware environment. If the case is wrong, the credential validation fails and states "...expecting <correct_name_of_server>."

NetBackup needs access to this server for either of the following reasons:

- To browse the server's virtual machines and back them up.
- To use the server as a target for restoring virtual machines.
  Use the next dialog to identify the type of this server (vCenter, ESX, or ESX for restore only).

4 In the **Credentials** pane of the **New Virtual Machine Server** dialog, enter the following:

Virtual machine server type

Select the type of VMware server that NetBackup needs to access:

- **VMware Virtual Center server**
  Designates a vCenter (or VirtualCenter) server that manages ESX servers. When you create a policy to back up this server's virtual machines, NetBackup can browse this server and list its virtual machines. If the credentials provide full access privileges to the vCenter server, you can restore virtual machines to this server.

  Note: Do not enter logon credentials for the individual ESX servers that this vCenter server manages. NetBackup needs credentials for the vCenter only. If you enter credentials for both an ESXi server and a vCenter that manages it, problems such as the following may occur:

  - A VMware Intelligent Policy (VIP) may fail due to discovery of duplicate VMs.
  - For manual selection of VMs (not VIP): Tags and custom attributes (which require a vCenter) may cause intermittent problems if NetBackup attempts to back up the VM using the ESXi server.

- **VMware ESX Server**
  Designates a standalone ESX server that a vCenter server does not manage. NetBackup can browse the ESX server to present a list of its virtual machines for backup. You can also restore virtual machines to this ESX

server. To use the server as a target for restores, enter the credentials that provide full access privileges to the ESX server.

- **VMware Restore ESX Server**
  Designates an ESX server to which NetBackup can restore virtual machines. You must enter the credentials that provide full access privileges to the server.

  Note: NetBackup accesses this type of server for restores only, not for backups.

  The restore ESX server type has the following advantages:

  - For large environments with hundreds of hosts, NetBackup may not need full access to the vCenter server. With the restore ESX server type, you can give NetBackup full access to a single ESX server that is dedicated to restore.
  - SAN-based restores that go directly to a restore ESX server are faster than restores that go through the vCenter server.
  - Allows restoring to an ESX 5.x or later server that a vCenter 5.x or later server manages. NetBackup uses vCenter to create the virtual machine. NetBackup then writes the .vmdk files directly to the ESX server using the Restore ESX Server credentials to that server.

  Note: VMware does not support the restore of virtual machines directly to an ESX 5.x or later server that vCenter manages. To restore the virtual machine, select the vCenter server as the destination. As an alternative, you can set up an independent ESX server to be used for restores. You must add NetBackup restore credentials for that ESX server by means of the **VMware Restore ESX Server** type.

  For further information on the restore ESX server, refer to the following Veritas tech note:
  http://www.veritas.com/docs/000007351

- **VMware vCloud Director**
  Designates a vCloud Director server. NetBackup can browse the vCloud environment on this server to present a list of its virtual machines for backup. You can also restore virtual machines to this server.

  Note: The credentials must be for a system administrator account.

Note: For backup and restore to vCloud Director, both vCloud and vCenter credentials are required (**VMware Virtual Center server**).

Note: If the vCloud environment uses a load-balancer to manage multiple cells (nodes), add credentials for the load balancer, not for the cells. If vCloud Director has multiple cells but no load balancer, add credentials for only one of the cells, not for all of them. Note also: If the Domain Name System (DNS) cannot resolve the name of the load balancer or cell, do the following: Include a line in the hosts file on the VMware backup host that specifies the IP address of the load balancer or cell.

User name

Enter the user name for the virtual machine server. Note that spaces in user names are not allowed.

To enter a domain name with a user name, separate them with a backslash as follows:

```
domain\username
```

Password

Enter the password for the virtual machine server.

For backup host

You can select a particular backup host for which to validate the credentials. Note that the hosts that appear in the pull-down list can be the following: media servers, or NetBackup clients that have been added under **Host Properties, VMware Access Hosts**.

For a list of supported backup host platforms, see the NetBackup Software Compatibility List available from the following location:

NetBackup Primary Compatibility List

See “Adding the VMware backup host to NetBackup” on page 44.

If **For backup host** is set to <Any> (the default), NetBackup attempts to validate the credentials using each backup host in turn. NetBackup continues checking only until validation succeeds for a particular backup host or the list of backup hosts is exhausted.

During validation: An invalid user name or password is deleted if you have entered it for the first time and you do not select a backup host. If validation fails for any reason, the entry is removed.

Connect using port number

If the default port number has not been changed on the VMware server, no port specification is required. In that case, make sure that the **Connect using port number** box is not checked.

If the VMware server has been configured to use a different port, click the **Connect using port number** box and specify that port number.

5 Click **OK**.

6 If your site has multiple standalone ESX servers, use the **Virtual Machine Server** dialog to enter credentials for each ESX server.

7 If the NetBackup primary server is clustered, do the following on the other primary server nodes to verify the credentials for each backup host.

- Fail over to the next primary server node, to make it the active node.
- On the active node, click on **Media and Device Management > Credentials > Virtual Machine Servers** and double-click on the virtual machine server credential.
- In the **For backup host** field, select a particular backup host (do not select **Any**).
  If the backup host does not appear in the list, you must add the correct credentials for the backup host. (Click **Actions > New > New Virtual Machine Server**.)
- Click **OK**.
  NetBackup validates the credentials.
- Double-click the same virtual machine server credential and validate the credentials for another backup host (if any).
- For other primary server nodes, repeat step 7.

See “Setting global limits on the use of VMware resources” on page 51.

Using the VMware Managed Object Browser to verify the server name

When adding NetBackup credentials for a VMware server, enter the server name exactly as configured in the VMware server (whether short or fully-qualified). If the name you enter for the credentials does not match the name as defined on the VMware server, the credential validation fails.

You can use the vSphere Managed Object Browser to verify the server's name.

To verify the server's name

1. In a web browser, open the Managed Object Browser (MOB) by entering the fully-qualified domain name of the VMware server and `/mob`.

   For example: `https://vcenter1.acmecorp.com/mob`

2. Navigate to the **ManagedObjectReference:HostSystem** and find the name value for the server.

   The object structure is site-dependent.

3. When you create NetBackup credentials for the server, enter the name value exactly as it appears in the MOB.

   See "Adding NetBackup credentials for VMware" on page 45.

   For more information on the MOB, see your vSphere documentation.

Changing the host name of a VMware server in NetBackup

Use the following procedure if you need to change a VMware server's host name as it is stored in NetBackup.

Example reasons for changing the VMware server name are the following:

- You used a short host name for the server for its NetBackup credentials, and need to replace that name with the fully qualified host name.
- Two hosts currently resolve to the same IP address, and one of them must be renamed and assigned a new IP address.

To change the host name of a VMware host in NetBackup

1. Remove the current credentials that were entered for the VMware host.

   Do the following:

   - In the NetBackup Administration Console, click on **Media and Device Management > Credentials > Virtual Machine Servers**.
   - Right-click on the credentials definition for the VMware server and select **Delete** (or press the Delete key).

2. In the NetBackup Administration Console, re-enter NetBackup's credentials for the VMware server.

   See "Adding NetBackup credentials for VMware" on page 45.

   Make sure to enter the correct host name for the VMware server.

See "Setting global limits on the use of VMware resources" on page 51.

Setting privileges for posting events to vCenter

With the **Post vCenter events** option, NetBackup can send backup related events to the vCenter server, to view in vSphere Web Client. The NetBackup plug-in for vSphere Web Client or vSphere Client (HTML5) is not required.

Note the following requirements:

- You must enter the credentials that give NetBackup access to the vCenter server.
  See "Adding NetBackup credentials for VMware" on page 45.
- Make sure that the **Post vCenter events** option is enabled in the policy.
  See "VMware - Advanced Attributes dialog" on page 81.
- You must set the correct vCenter role privileges. Use the vSphere Web Client to make sure that the following **Global** privileges are set in vCenter: **Manage custom attributes** and **Set custom attribute**.
  For assistance setting privileges, refer to the appropriate VMware vSphere Documentation Center.

Authentication token for the NetBackup vSphere plug-ins

With the NetBackup vSphere Web Client plug-in and the vSphere Client (HTML5) plug-in, the VMware administrator can use the vSphere interface to recover virtual machines. To allow the plug-in to communicate with the NetBackup primary server, you must provide an authentication token to the VMware administrator.

To create an authentication token, see the *Veritas NetBackup Plug-in for VMware vSphere Web Client Guide* or the *Veritas NetBackup Plug-in for VMware vSphere Client (HTML5) Guide*:

http://www.veritas.com/docs/DOC5332

Setting global limits on the use of VMware resources

You can use the NetBackup Resource Limit dialog to control the number of simultaneous backups that can be performed on a VMware resource type. The settings apply to all NetBackup policies for the currently selected primary server.

For example, to avoid overloading the ESX server, you can place a limit on the number of concurrent backup jobs per ESX server. To control I/O overhead on the datastore's array, you can limit the number of concurrent backups per datastore.

The following limitations apply to setting global limits on the use of VMware resources:

- In NetBackup 9.1, you can set global limits for VMware resources only through the NetBackup Administration Console or the NetBackup Configuration API. You cannot set VMware resource limits with the NetBackup web UI. For more information about the Configuration API, see the NetBackup API Reference on SORT.
- New and changed resource limits may not take effect immediately. It can take a couple of jobs before the resource limit updates are in effect.
- The Resource Limit screen applies only to policies that use automatic selection of virtual machines (Query Builder). If virtual machines are selected manually on the Browse for Virtual Machines screen, the Resource Limit settings have no effect.
- To limit the number of simultaneous jobs per policy, use the **Limit jobs per policy** setting on the policy **Attributes** tab. The effect of this option depends on how the policy selects virtual machines.

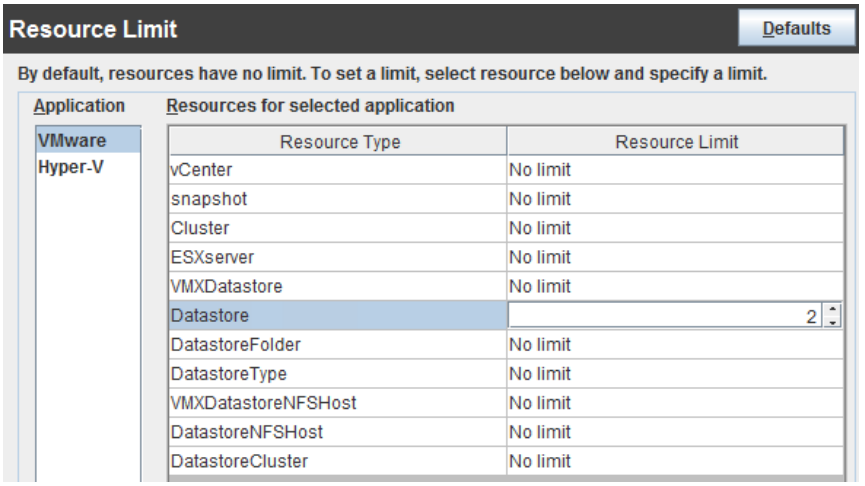
See “Limit jobs per policy on the Attributes tab (for VMware)” on page 72.

To set limits on the use of VMware resources

1. In the NetBackup Administration Console, click **Host Properties > Primary Servers** and double-click the NetBackup primary server.
2. In the **Properties** screen, scroll down in the left pane and click **Resource Limit**.

3 Under **Application**, click **VMware**.

4 Click in the **Resource Limit** column to set the maximum NetBackup usage for a particular resource type. The settings apply to all policies.



For each resource type, the default is 0, (No Limit). A resource limit of 4 for Datastore means that NetBackup policies can perform no more than four simultaneous backups on any particular datastore.

Table 4-1 describes the limits:

Table 4-1 Resource types and limits

Resource type	Resource limit
vCenter	The maximum number of simultaneous backups per vCenter server.
snapshot	The maximum number of simultaneous snapshot operations (create or delete) per vCenter.
Cluster	The maximum number of simultaneous backups per VMware cluster.
ESXserver	The maximum number of simultaneous backups per ESX server.

Table 4-1 Resource types and limits *(continued)*

Resource type	Resource limit
VMXDatastore	Controls the maximum number of simultaneous backups per Datastore. The Datastore is defined as the location of the VMX file that is associated with each VM. This resource type is useful for VMs that have VMDK files distributed across multiple Datastores. This setting is enforced globally within a NetBackup domain. See "NetBackup for VMware terminology" on page 20.
Datastore	The maximum number of simultaneous backups per datastore.
DatastoreFolder	The maximum number of simultaneous backups per datastore folder.
DatastoreType	The maximum number of simultaneous backups per datastore type.
VMXDatastoreNFSHost	Controls the maximum number of simultaneous backups per Datastore at the NFS host level where the Datastore type is NFS. The VMXDatastoreNFSHost is an NFS server that sources one or more NFS Datastores. For this resource type the Datastore is defined as the location of the VMX file that is associated with each VM. This resource type is useful for VMs that have VMDK files that are distributed across multiple Datastores. This setting is enforced globally within a NetBackup domain.
DatastoreNFSHost	The maximum number of simultaneous backups per NFS host of the datastore.
DatastoreCluster	The maximum number of simultaneous backups per datastore cluster.

Other resource-related considerations may be of interest.

See "NetBackup for VMware best practices" on page 281.

Validating VMware virtualization server certificates in NetBackup

NetBackup can now validate VMware virtualization server certificates using their root or intermediate certificate authority (CA) certificates.

The following procedure is applicable for the NetBackup primary server and all VMware access hosts.

To configure secure communication between VMware virtualization server and VMware access host

1. Configure an external CA trust store on the VMware access host.
2. Add CA certificates of the required VMware servers (VCenter, ESX, or ESXi server) in the trust store on the access host.

   In case of Windows certificate store, you need to add the CA certificate to the Windows Trusted Root Certification Authorities.

   Use the following command:

   ```
   certutil.exe -addstore -f "Root" certificate filename
   ```

3 Use the `nbsetconfig` command to configure the following NetBackup configuration options on the access host:

`ECA_TRUST_STORE_PATH`	Specifies the file path to the certificate bundle file that contains all trusted root CA certificates. This option is specific to file-based certificates. You should not configure this option if Windows certificate store is used. If you have already configured this external CA option, append the VMware CA certificates to the existing external certificate trust store. If you have not configured the option, add all the required virtualization server CA certificates to the trust store and set the option. See "ECA_TRUST_STORE_PATH for NetBackup servers and clients" on page 58.
`ECA_CRL_PATH`	Specifies the path to the directory where the certificate revocation lists (CRL) of the external CA are located. If the configuration option is already configured, append the virtualization server CRLs to the CRL cache. If the option is not configured, add all the required CRLs to the CRL cache and then set the option. See "ECA_CRL_PATH for NetBackup servers and clients" on page 59.
`VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED`	Lets you enable the validation of a virtualization server's certificate. See "VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED for servers and clients" on page 63.
`VIRTUALIZATION_CRL_CHECK`	Lets you validate the revocation status of the virtualization server certificate against the CRLs. By default, the option is disabled. See "VIRTUALIZATION_CRL_CHECK for NetBackup servers and clients" on page 64.

VIRTUALIZATION_HOSTS_CONNECT_TIMEOUT	Lets you specify the duration (in seconds) after which the connection between NetBackup and vCloud Director server ends. See "VIRTUALIZATION_HOSTS_CONNECT_TIMEOUT for servers and clients" on page 62.
VMWARE_TLS_MINIMUM_V1_2	Lets you specify the Transport Layer Security (TLS) version to be used for communication between NetBackup and VMware servers. See "VMWARE_TLS_MINIMUM_V1_2 for NetBackup servers and clients" on page 65.

For more information on external CA support in NetBackup, refer to the NetBackup Security and Encryption Guide.

ECA_TRUST_STORE_PATH for NetBackup servers and clients

The ECA_TRUST_STORE_PATH option specifies the file path to the certificate bundle file that contains all trusted root CA certificates.

This certificate file should have one or more certificates in PEM format.

Do not specify the ECA_TRUST_STORE_PATH option if you use the Windows certificate store.

The trust store supports certificates in the following formats:

- PKCS #7 or P7B file having certificates of the trusted root certificate authorities that are bundled together. This file may either be PEM or DER encoded.
- A file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.

This option is mandatory for file-based certificates.

Table 4-2 ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, RHV servers, or Nutanix AHV, this option must be set on the NetBackup primary server and respective access hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).

Table 4-2 ECA_TRUST_STORE_PATH information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_TRUST_STORE_PATH = Path to the external CA certificate` For example: `c:\rootCA.pem`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_PATH for NetBackup servers and clients

The `ECA_CRL_PATH` option specifies the path to the directory where the Certificate Revocation Lists (CRL) of the external certificate authority (CA) are located.

These CRLs are copied to NetBackup CRL cache. Revocation status of the external certificate is validated against the CRLs from the CRL cache.

CRLs in the CRL cache are periodically updated with the CRLs in the directory that is specified for `ECA_CRL_PATH` based on the `ECA_CRL_PATH_SYNC_HOURS` option.

See "ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients" on page 60.

If the `ECA_CRL_CHECK` or `HADOOP_CRL_CHECK` option is not set to `DISABLE` (or 0) and the `ECA_CRL_PATH` option is not specified, NetBackup downloads the CRLs from the URLs that are specified in the CRL distribution point (CDP) and uses them to verify revocation status of the peer host's certificate.

See "ECA_CRL_CHECK for NetBackup servers and clients" on page 61.

Note: For validating the revocation status of a virtualization server certificate, the `VIRTUALIZATION_CRL_CHECK` option is used.

See "VIRTUALIZATION_CRL_CHECK for NetBackup servers and clients" on page 64.

For validating the revocation status of a Hadoop server certificate, the `HADOOP_CRL_CHECK` option is used.

Table 4-3 ECA_CRL_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, RHV servers, Nutanix AHV, or Hadoop, this option must be set on the NetBackup primary server and respective access or backup hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format to specify a path to the CRL directory: `ECA_CRL_PATH = Path to the CRL directory`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients

The `ECA_CRL_PATH_SYNC_HOURS` option specifies the time interval in hours to update the Certificate revocation lists (CRL) in the NetBackup CRL cache with the CRLs in the directory specified for the `ECA_CRL_PATH` configuration option.

See "ECA_CRL_PATH for NetBackup servers and clients" on page 59.

The `ECA_CRL_PATH_SYNC_HOURS` option is not applicable if CDP is used for CRLs.

By default, CRLs in the cache are updated every one hour.

During host communication, revocation status of the external certificate is validated against the CRLs from the CRL cache.

Table 4-4 ECA_CRL_PATH_SYNC_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-4 ECA_CRL_PATH_SYNC_HOURS information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_CRL_PATH_SYNC_HOURS = Number of hours` Minimum number of hours that you can specify - 1 hour Maximum number of hours that you can specify - 720 hour The default value is one hour.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_CHECK for NetBackup servers and clients

The `ECA_CRL_CHECK` option lets you specify the revocation check level for external certificates of the host. It also lets you disable the revocation check for the external certificates. Based on the check, revocation status of the certificate is validated against the Certificate Revocation List (CRL) during host communication.

You can choose to use the CRLs from the directory that is specified for the `ECA_CRL_PATH` configuration option in the configuration file (`bp.conf` on UNIX or Windows registry) or the CRL Distribution Point (CDP).

See "ECA_CRL_PATH for NetBackup servers and clients" on page 59.

Table 4-5 ECA_CRL_CHECK information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-5 ECA_CRL_CHECK information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_CRL_CHECK = CRL check` You can specify one of the following: ■ DISABLE (or 0) - Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication. ■ LEAF (or 1) - Revocation status of the leaf certificate is validated against the CRL. This is the default value. ■ CHAIN (or 2) - Revocation status of all certificates from the certificate chain are validated against the CRL.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

VIRTUALIZATION_HOSTS_CONNECT_TIMEOUT for servers and clients

The `VIRTUALIZATION_HOSTS_CONNECT_TIMEOUT` option lets you specify the duration (in seconds) after which the connection between NetBackup and vCloud Director server ends.

Table 4-6

Usage	Description
Where to use	On NetBackup primary server or all access hosts.

Table 4-6 *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. By default, the `VIRTUALIZATION_HOSTS_CONNECT_TIMEOUT` option is set to 60 seconds. Use the following format to specify the time-out value: `VIRTUALIZATION_HOSTS_CONNECT_TIMEOUT = Time-out value in seconds`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties

VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED for servers and clients

The `VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED` option enables the validation of virtualization server certificates using its root or intermediate certificate authority (CA) certificates.

Before you enable the option, review the steps from the 'Validating VMware virtualization server certificates in NetBackup ' section in the NetBackup for VMware Administrator's Guide.

By default, the `VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED` option is set to `UNDEFINED`.

The security certificate validation is enabled for RHV and Nutanix AHV servers, but is disabled for VMware servers.

Note: In a scenario where an external CA can be configured for one virtualization server, but not for the other, two separate backup hosts must be used. The VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED option must be set to YES for the backup host where the external CA can be configured. The option must be set to NO for the other backup host.

Table 4-7 VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED information

Usage	Description
Where to use	On NetBackup primary server or all access hosts.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format to enable certificate validation for the RHV, VMware, or Nutanix AHV servers: VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED = YES
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

VIRTUALIZATION_CRL_CHECK for NetBackup servers and clients

The VIRTUALIZATION_CRL_CHECK option lets you specify the revocation check level for external certificates of the virtualization server. Based on the check, revocation status of the virtualization server certificate is validated against the certificate revocation list (CRL) during host communication.

By default, the VIRTUALIZATION_CRL_CHECK option is disabled. If you want to validate the revocation status of the virtualization server certificate against certificate revocation list (CRL), set the option to a different value.

You can choose to use the CRLs from the directory that is specified for the ECA_CRL_PATH configuration option or the CRL distribution point (CDP).

See "ECA_CRL_PATH for NetBackup servers and clients" on page 59.

Table 4-8 VIRTUALIZATION_CRL_CHECK information

Usage	Description
Where to use	On NetBackup primary server or all access hosts.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `VIRTUALIZATION_CRL_CHECK = CRL check` You can specify one of the following: ■ DISABLE (or 0) - Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication. This is the default value. ■ LEAF (or 1) - Revocation status of the leaf certificate is validated against the CRL. ■ CHAIN (or 2) - Revocation status of all certificates from the certificate chain are validated against the CRL.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

VMWARE_TLS_MINIMUM_V1_2 for NetBackup servers and clients

The `VMWARE_TLS_MINIMUM_V1_2` option lets you specify the Transport Layer Security (TLS) version to be used for communication between NetBackup and VMware servers.

Table 4-9

Usage	Description
Where to use	On NetBackup primary server or all access hosts.

Table 4-9 *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `VMWARE_TLS_MINIMUM_V1_2 = YES | NO` By default, the `VMWARE_TLS_MINIMUM_V1_2` option is set to `YES`. If the option is set to `YES`, TLS 1.2 version and the following cipher suites are used for communication with VMware servers: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_DSS_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256 If the option is set to `NO`, the TLS 1.2 or earlier version with the default cipher suite is used for communication between NetBackup and VMware server. The cipher suite is used based on the TLS and cipher suite configuration that are set on the respective VMware server.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

Chapter 5

Configure NetBackup policies for VMware

This chapter includes the following topics:

- Configuring a VMware policy from the Policy Wizard
- Configuring a VMware policy from the Policies utility
- Limit jobs per policy on the Attributes tab (for VMware)
- Backup options on the VMware tab
- Exclude Disks tab
- Browse for VMware virtual machines
- Limiting the VMware servers that NetBackup searches when browsing for virtual machines
- Virtual machine host names and display names should be unique if VMs are selected manually in the policy
- Primary VM identifier option and manual selection of virtual machines
- About incremental backups of virtual machines
- Configuring incremental backups
- Storage Foundation Volume Manager volumes in the virtual machine

Configuring a VMware policy from the Policy Wizard

Use the following procedure.

To create a backup policy by means of the Policy Configuration Wizard

1. In the NetBackup Administration Console (on the NetBackup primary server), click on the name of the primary server.
2. Click **Create a Policy**.
3. Under **Create a backup policy for,** click **VMware and Hyper-V**, and click **Next**.
4. Enter a name for the policy.
5. Click **VMware** as the virtual machine type.
6. Click **Next**, and follow the remaining panels in the wizard.

   The wizard creates the policy according to your selections.

Configuring a VMware policy from the Policies utility

Note: VMware policies can also be configured from the NetBackup web UI. To do so, on the left navigation pane, click **Protection > Policies**, and then select a listed VMware policy to change it. Or click **+Add**, enter a **Policy name**, and select **VMware** from the **Policy type** drop-down list.

You can create a NetBackup policy (full or incremental) to back up the virtual machine in either of two ways:

- Use the **Policies** utility of the NetBackup Administration Console (described in this topic).
- Use the Policy Configuration Wizard.
  See “Configuring a VMware policy from the Policy Wizard ” on page 68.

Note: To configure a policy for Replication Director, see the *NetBackup Replication Director Solutions Guide*.

To configure a policy to back up the virtual machine

1. In the NetBackup Administration Console, click **Policies** and select **Actions > New > Policy**.
2. Enter a name for the policy.
3. For **Policy type**, select **VMware**.

   VMware backup options are available on the **VMware** tab (described later in this procedure).
4. Select a policy storage unit or storage unit group.

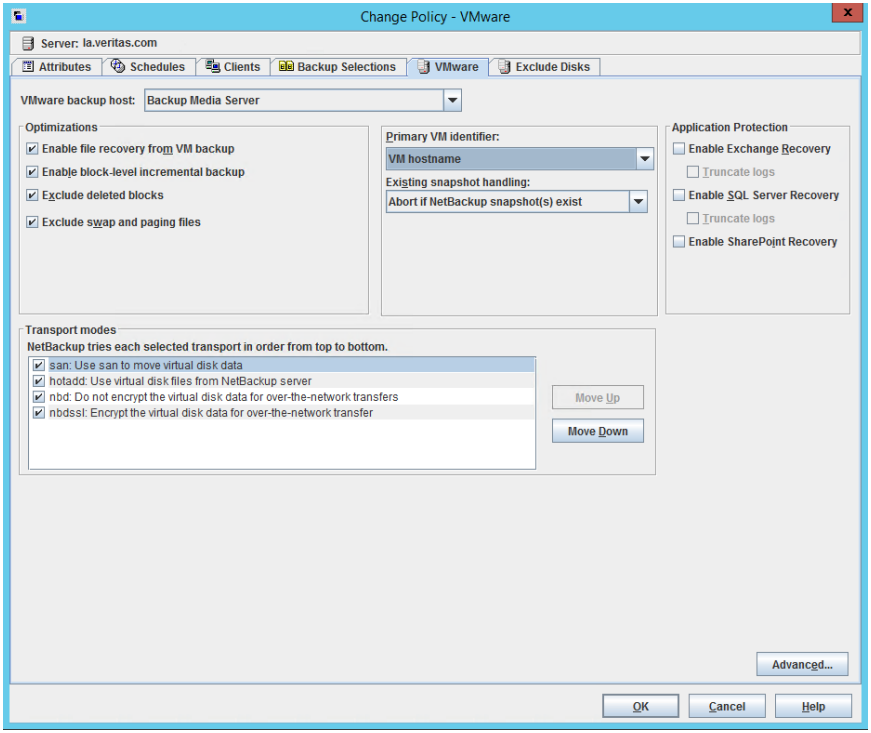
   Storage unit groups are described in the *NetBackup Administrator's Guide, Volume I*.
5. In most cases, you can leave the **Disable client-side deduplication** option at the default (unchecked).

   The **Disable client-side deduplication** option is described in the *NetBackup Administrator's Guide, Volume I*.
6. To enable the Accelerator, click **Use Accelerator**.

   When you click **Use Accelerator**, the **Enable block-level incremental backup** option on the **VMware** tab is selected and grayed out.

   See "About the NetBackup Accelerator for virtual machines" on page 161.

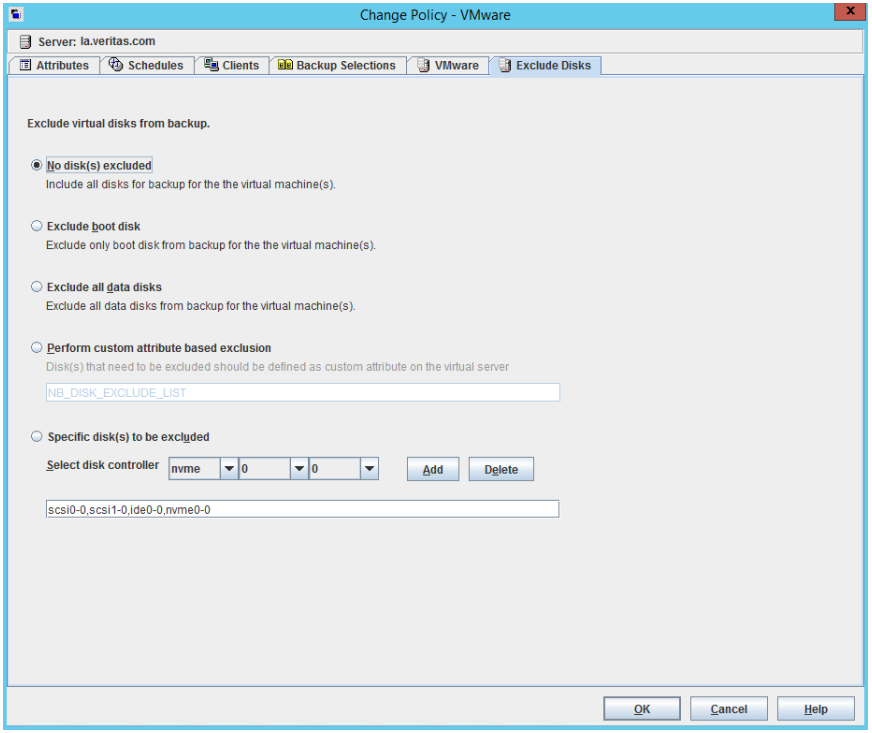
7 Click the **VMware** tab.



Use this dialog to set VMware-related options.

See “Backup options on the VMware tab” on page 73.

8 Click the **Exclude Disks** tab.



Use this tab to exclude disks from the backups.

See "Exclude Disks tab" on page 86.

9 To define a schedule, click the **Schedules** tab and click **New**.

For assistance with the **Accelerator forced rescan** option:

See "Accelerator forced rescan for virtual machines (schedule attribute)" on page 165.

On the **Schedules Attributes** tab, you can select **Full backup**, **Differential Incremental Backup**, or **Cumulative Incremental Backup**.

Note that incremental backups require one of the following selections on the policy **VMware** tab:

- **Enable file recovery from VM backup**, or
- **Enable block-level incremental backup**.
  Enable block-level incremental backup requires an ESX server 4.0 and a virtual machine at vmx-07 or later.

The following topic contains additional information.

See "About incremental backups of virtual machines" on page 99.

10 Click the **Clients** tab to select the virtual machines to back up.

The options for selecting virtual machines are as follows:

Select manually, and click **New**.	The Browse for VMware Virtual Machines screen appears. You can type the host name in the **Enter the VMware hostname** field, or click **Browse and select virtual machine**. **Note:** The **Backup Selections** tab is set to ALL_LOCAL_DRIVES. Individual drives cannot be specified. See "Browse for VMware virtual machines" on page 91.
Select automatically through VMware Intelligent Policy query	With this option, NetBackup can automatically select virtual machines for backup based on the filtering criteria that you enter. The following topics explain how to specify the criteria: See "About automatic virtual machine selection for NetBackup for VMware" on page 102. See "Configuring automatic virtual machine selection" on page 111. **Note:** The **Backup Selections** tab is filled in with the filtering rules from the query. NetBackup uses the `ALL_LOCAL_DRIVES` directive to back up the virtual machines.
Enable vCloud Director integration	Enables backup of the virtual machines that reside in a vCloud environment. Requires the automatic selection of virtual machines. With this option, the policy selects for backup only the virtual machines that vCloud manages: it skips the virtual machines that are not in vCloud. See "About NetBackup for vCloud Director" on page 262.
NetBackup host to perform automatic virtual machine selection	This option appears when you click **Select automatically through VMware Intelligent Policy query**. This host discovers virtual machines and automatically selects them for backup based on the query rules. See "About automatic virtual machine selection for NetBackup for VMware" on page 102.

11 When you click **OK**, a validation process checks the policy and reports any errors. If you click **Cancel**, no validation is performed.

Limit jobs per policy on the Attributes tab (for VMware)

The **Limit jobs per policy** option operates as follows, depending on how the policy selects virtual machines.

For the policies that select virtual machines automatically (Query Builder)

The **Limit jobs per policy** option controls the number of parent (discovery) jobs that run simultaneously for the policy. This option does not limit the number of snapshot jobs and backup (bpbkar) jobs that the parent job launches. For example, if this option is set to 1 and you begin a backup of a policy that discovers 100 virtual machines: all the snapshot jobs and backup jobs for each of the 100 virtual machines are allowed to execute simultaneously. Only the initial discovery job counts against **Limit jobs per policy**. If you begin a second backup of the policy, its discovery job cannot start until all the child jobs from the first backup are complete.

For the policies that use manual selection of virtual machines

Limit jobs per policy controls the number of virtual machines that the policy can back up simultaneously. Because no discovery job is needed, each virtual machine backup begins with a snapshot job. Each snapshot counts against the **Limit jobs per policy** setting. If this option is set to 1: the backup of the next virtual machine that is specified in the policy cannot begin until the first snapshot job and its backup are complete.

See "Setting global limits on the use of VMware resources" on page 51.

Backup options on the VMware tab

In the Administration Console, the VMware tab appears when you select VMware as the policy type.

Note: VMware policies can also be configured from the NetBackup web UI. To do so, on the left navigation pane, click **Protection > Policies**, and then select a listed VMware policy to change it. Or click **+Add**, enter a **Policy name**, and select **VMware** from the **Policy type** drop-down list.

The following topics describe the VMware backup options.

VMware backup host

The VMware backup host is a NetBackup client that performs backups on behalf of the virtual machines.

Table 5-1 VMware backup host selection

Option	Description
Backup Media Server	This option allows a media server that is selected in the policy to operate as the backup host. (The storage unit determines the selection of the media server.) To operate as the backup host, the media server must contain NetBackup client software. **Note:** The storage unit that is specified in the policy must be unique to the media servers that NetBackup supports as VMware backup hosts. If the storage unit is available on a media server that is not a supported VMware backup host, the snapshot may not succeed (status 20). For a list of supported platforms for the VMware backup host, see the NetBackup Software Compatibility List (SCL) available from the following location: NetBackup Primary Compatibility List **Note:** When the **Backup Media Server** option is selected, NetBackup cannot determine a host to perform policy validation. To validate the policy, temporarily select one of the possible media servers as the backup host (do not select **Backup Media Server**). When the policy validates successfully, reset the backup host to **Backup Media Server**. See "Media servers as backup or discovery hosts" on page 18.
backup_host_name	Select a backup host to perform the backup. The pull-down list contains any media servers that are supported as backup host. It also contains any NetBackup clients that have been added in the Administration Console under **Host Properties, VMware Access Hosts**. For a list of supported platforms for the backup host, see the *NetBackup Software Compatibility List* available from the following location: NetBackup Primary Compatibility List See "Adding the VMware backup host to NetBackup" on page 44.

Optimizations options (VMware)

The following options set the type and scope of the VMware virtual machine backup.

Table 5-2 Optimizations

Option	Description
Enable file recovery from VM backup	This option allows restore of individual files from the backup. With or without this option, you can restore the entire virtual machine. You can also use this option for incremental backups: in the policy schedule, select differential incremental backup or cumulative incremental backup. To perform a VMware backup to a deduplication storage unit, select this option. This option provides the best deduplication rates. To back up a virtual machine that contains Veritas Storage Foundation Volume Manager volumes, disable this option. Also make sure that the **Exclude deleted blocks** option is disabled. **Note:** For a Linux virtual machine, the name of an LVM volume can include any of the following special characters: . (period), _ (underscore), - (hyphen). No other special characters are supported. If other special characters are in the volume name, the **Enable file recovery from VM backup** option does not work. As a result, you cannot restore individual files from that volume. **Note:** During an incremental backup, any files that had been moved or renamed are not backed up. Those files are not available when you browse to restore individual files from the incremental backup. However, when you restore the entire VM from a block-level incremental backup, note: the file metadata is updated and the moved or renamed files in the restored VM reflect the updated metadata.
Enable block-level incremental backup	For block-level backups of the virtual machine. This option reduces the size of the backup image. For the Exchange, SQL, and SharePoint Agents, this option is selected and grayed out if you enable **Use Accelerator**. On the **Attributes** tab, **Perform block level incremental backups** is automatically selected and grayed out. See "Block-level backup (BLIB): full vs incremental" on page 151.
Exclude deleted blocks	Reduces the size of the backup image by excluding any unused or deleted blocks within the file system on the virtual machine. This option supports the following file systems: Windows NTFS, and Linux ext2, ext3, and ext4. This option uses proprietary mapping technology to identify vacant sectors (allocated but empty) within the file system. See "About reducing the size of VMware backups" on page 150. To back up a virtual machine that contains Veritas Storage Foundation Volume Manager volumes, disable this option. Also make sure that the **Enable file recovery from VM backup** option is disabled.

Table 5-2 Optimizations *(continued)*

Option	Description
Exclude swap and paging files	Reduces the size of the backup image by excluding the data in the guest OS system paging file (Windows) or the swap file (Linux). **Note:** This option does not exclude the swapping and paging files from the backup: it only excludes the data in those files. If the files are restored, they are restored as empty files. **Note:** For a Linux virtual machine, this option disables the swap file when you restore the virtual machine. You must reconfigure the swap file after the virtual machine is restored. To allow the virtual machine to be restored with its swap file enabled, do not select **Exclude swap and paging files**.

Primary VM identifier options (VMware)

This setting specifies the type of name by which NetBackup recognizes virtual machines when it selects them for backup.

The name you use for the **Primary VM identifier** may have restrictions.

See "NetBackup character restrictions for the Primary VM identifier" on page 37.

Table 5-3 Primary VM identifier

Option	Description
VM hostname	The network host name for the virtual machine. (This option is the default.) NetBackup obtains the host name by means of a reverse lookup on the virtual machine's IP address. **Note:** For NetBackup to look up the IP address, the virtual machine must already be turned on. If no host name can be found, the IPv4 address is used as the host name. In case of an IPv6 address, the field remains blank. See "Preventing browsing delays caused by DNS problems" on page 295.

Table 5-3 Primary VM identifier *(continued)*

Option	Description
VM display name	The name of the virtual machine as displayed in the VMware interface. A display name is assigned to the virtual machine when the virtual machine is created. When virtual machines are included in a NetBackup policy, restrictions apply to the characters that are allowed in the virtual machine display name. See "NetBackup character restrictions for the Primary VM identifier" on page 37. **Note:** The restrictions also apply to other vSphere objects, such as floppy image name, parallel port or serial port file name, and CD-ROM ISO name. Each display name must be unique in your VMware environment. See "NetBackup for VMware: notes and restrictions" on page 27. See "Restoring individual files" on page 224.
VM BIOS UUID	The ID assigned to the virtual machine when the virtual machine is created. This ID may or may not be unique, depending on whether the virtual machine has been duplicated. This option is included for compatibility with the policies that use the older VM UUID identifier.
VM DNS Name	The VMware DNS Name of the virtual machine. In vSphere Client, this name appears on the virtual machine's Summary tab. **Note:** This name may or may not be associated with the virtual machine's IP address. VMware Tools obtains this name from the host name that is configured in the virtual machine. For further information on this name, refer to the documentation for the guest operating system.
VM instance UUID	The globally unique ID assigned to the virtual machine when the virtual machine is created. This ID uniquely identifies the virtual machine within a vCenter server. Even if the virtual machine has been duplicated (such as within a vCloud), only the original virtual machine retains this instance ID. (The virtual machine duplicates are assigned different instance UUIDs.) This option is recommended instead of the **VM BIOS UUID** option.

Existing snapshot handling options (VMware)

This option specifies the action that NetBackup takes when a snapshot is discovered before NetBackup creates a new snapshot for the virtual machine backup. After it creates a snapshot, NetBackup usually deletes the snapshot when the backup completes. If snapshots are not automatically deleted (whether created by NetBackup or not), the performance of the virtual machine may eventually decline.

Undeleted snapshots can cause restore failures due to lack of disk space. If the virtual machine was configured on multiple datastores and a leftover snapshot existed on the virtual machine when it was backed up, note: NetBackup tries to restore all .vmdk files to the snapshot datastore. As a result, the datastore may not have enough space for the .vmdk files, and the restore fails. (For a successful restore, you can restore the virtual machine to an alternate location. Use the Storage Destination dialog in the **Virtual Machine Recovery** dialogs to select a datastore for the .vmdk files.)

Table 5-4 Existing snapshot handling: Options

Option	Description
Continue backup	NetBackup ignores any existing virtual machine snapshots (including snapshots previously created by NetBackup) and proceeds with snapshot creation and the backup.
Abort if any snapshot(s) exist	If any snapshot exists on the virtual machine, NetBackup aborts the job for that virtual machine only.
Remove NetBackup snapshot(s) and continue backup	If a virtual machine snapshot exists that a NetBackup backup previously created: NetBackup removes the old snapshot, creates an updated snapshot, and proceeds with the virtual machine backup.
Abort if NetBackup snapshot(s) exist	If a virtual machine snapshot exists that a NetBackup backup previously created, NetBackup aborts the job for that virtual machine only. (This option is the default.)

Transport modes options (VMware)

The transport modes determine how the snapshot data travels from the VMware datastore to the VMware backup host. The appropriate mode depends in part on the type of network that connects the VMware datastore to the VMware backup host.

By default, all modes are selected. NetBackup tries each transport mode in order, from top to bottom. It uses the first mode that succeeds for all disks in the virtual machine.

Table 5-5 Transport Modes

Mode	Description
san	For unencrypted transfer over Fibre Channel (SAN) or iSCSI. **Note:** This mode is not supported for the virtual machines that use VMware Virtual Volumes (VVols). See "Notes on VMware Virtual Volumes (VVols)" on page 33.
hotadd	Lets you run the VMware backup host in a virtual machine. See "Notes on the hotadd transport mode" on page 40. **Note:** For the virtual machines that use VVols, the virtual machine and the backup host (hotadd) virtual machine must reside on same VVol datastore. For instructions on this transport mode and on installing the backup host in a VMware virtual machine, refer to your VMware documentation.
nbd	For unencrypted transfer over a local network that uses the Network Block Device (NBD) driver protocol. This mode of transfer is usually slower than Fibre Channel.
nbdssl	For encrypted transfer (SSL) over a local network that uses the Network Block Device (NBD) driver protocol. This mode of transfer is usually slower than Fibre Channel.
Move Up, Move Down	Use these options to change the order in which NetBackup tries each selected mode. Highlight a mode and click **Move Up** or **Move Down**. For example: assume that all four transport modes are selected, and the order is SAN, hotadd, nbd, and nbdssl. If one of the virtual disks cannot be accessed using SAN, the SAN transport mode is not used for any of the virtual machine's disks. NetBackup then tries to use the hotadd mode for all the disks. NetBackup continues to try each mode until it finds one that succeeds for all the disks.

Application protection options (VMware)

To enable file-level recovery of database data that resides in the virtual machine, select from the following options. These options apply to full backups of the virtual machine; they do not apply to incremental backups.

Table 5-6 Application Protection options

Database option	Description
Enable Exchange Recovery	This option enables recovery of the Exchange databases or mailbox messages from the virtual machine backups. If this option is disabled, you can recover the entire virtual machine from the backup, but you cannot recover the databases or mailbox messages individually. To use the **Enable Exchange Recovery** option, you must enable the **Enable file recovery from VM backup** option. If you choose to exclude disks on the **Exclude disks** tab, ensure that the disks do not contain Exchange Server data. For more information, refer to the *NetBackup for Exchange Server Administrator's Guide*.
Truncate logs	For Exchange, this option truncates the transaction logs when the snapshot of the virtual machine is complete. Truncating the logs frees up disk space in the virtual machine. **Note:** To use this option, install the Veritas VSS Provider on the virtual machine. For instructions on how to install this provider, refer to the *NetBackup for Exchange Server Administrator's Guide*. If you do not select **Truncate logs**, the logs are not truncated.
Enable SQL Server Recovery	This option enables recovery of individual files from SQL Server data in the virtual machine backup. If this option is disabled, you can recover the entire virtual machine from the backup, but you cannot recover the SQL Server files individually. To use the **Enable SQL Server Recovery** option, you must enable the **Enable file recovery from VM backup** option. If you choose to exclude disks on the **Exclude disks** tab, ensure that the disks do not contain SQL Server data. For more information, refer to the *NetBackup for SQL Server Administrator's Guide*.
Truncate logs	For SQL Server, this option truncates the transaction logs when the backup occurs. Truncating the logs frees up disk space in the virtual machine. **Note:** To use this option, install the Veritas VSS Provider on the virtual machine. For instructions on how to install this provider, refer to the *NetBackup for SQL Server Administrator's Guide*. If you do not select **Truncate logs**, the logs are not truncated.
Enable SharePoint Recovery	This option enables recovery of SharePoint objects from the virtual machine backup. If this option is disabled, you can recover the entire virtual machine from the backup, but you cannot recover the SharePoint objects individually. To use the **Enable SharePoint Recovery** option, you must enable the **Enable file recovery from VM backup** option. If you choose to exclude disks on the **Exclude disks** tab, ensure that the disks do not contain SharePoint Server data. For more information, refer to the *NetBackup for SharePoint Server Administrator's Guide*.

VMware - Advanced Attributes dialog

This dialog appears when you click **Advanced...** on the **VMware policy** tab.

You can use the VMware Advanced Attributes dialog to set the following additional parameters for VMware backup. In most situations, the best settings are the defaults.

Table 5-7 VMware Advanced Attributes

Configuration parameter	Description
Virtual machine quiesce	This option is enabled by default. In the great majority of cases, you should accept the default. I/O on the virtual machine is quiesced before NetBackup creates the snapshot. Without quiescing file activity, data consistency in the snapshot cannot be guaranteed. If not consistent, the backed-up data may be of little or no value. If this option is disabled, the snapshot is created without quiescing I/O on the virtual machine. In this case, you must perform your own analysis for data consistency in the backup data. Caution: Veritas does not recommend that you disable quiesce. In most cases, this option should be enabled. **Note:** To use this option, VMware Tools must be installed on the virtual machine. **Note:** To use this option with Linux virtual machines, snapshot quiesce must be enabled in the Linux guest OS.
Ignore diskless VMs	If this option is enabled: NetBackup does not back up a replicated (passive) VM in a vCenter Site Recovery Manager (SRM) environment if that VM has no vmdk files. NetBackup skips that VM and backs up the corresponding active VM, which has vmdk files. Note that virtual machines without vmdk files can occur in a vCenter SRM environment. If a replicated virtual machine has never been active, it is in passive mode and may have no vmdk file(s). **Note:** If this option is enabled and NetBackup does not have access to the vCenter where the active virtual machine runs: the Query Builder policies run without error; no attempt is made to back up the virtual machine. For the policies that use manual selection of virtual machines, backups fail with status 156, because the virtual machine cannot be located. If this option is disabled: NetBackup attempts to back up a virtual machine regardless of whether it has vmdk files. If the virtual machine has no vmdk files, the backup fails with status 156.

Table 5-7 VMware Advanced Attributes *(continued)*

Configuration parameter	Description
Post vCenter events	Enables NetBackup to send backup related events to the vCenter server. The events appear in vSphere Client under **Home > Inventory > Hosts and Clusters, Tasks & Events** tab. See "Viewing NetBackup activity in vSphere Web Client or vSphere Client (HTML5)" on page 158. The following options are available: ■ **All Events**: NetBackup posts an event to the vCenter server on each backup success or failure. This setting is the default. ■ **No Events**: Disables the **Post vCenter events** option. NetBackup does not post any events to the vCenter server. ■ **Error Events**: NetBackup posts an event to the vCenter server only for backup failures. Further information on **Post vCenter events** is available: See "About the Post vCenter events option (VMware Advanced Attributes)" on page 85.
Multiple organizations per policy	This option is disabled by default. If it is enabled, the query rules can select virtual machines from different vCloud Director organizations and back them up to the same storage unit. If you do not want backups of virtual machines from different organizations to be stored on the same drive, leave this option disabled.
Ignore Instant Recovery VMs	If this option is enabled (the default): NetBackup skips any virtual machine that was restored with Instant Recovery for VMware if the virtual machine is running from a NetBackup NFS datastore. When the virtual machine data files have been migrated to the production datastore, the virtual machine can be backed up. NetBackup identifies Instant Recovery virtual machines according to the following criteria: ■ The virtual machine has a snapshot that is named `NBU_IR_SNAPSHOT`, ■ And the virtual machine is running from a datastore and the name of the datastore begins with `NBU_IR_`. If the virtual machine meets all these criteria, it is not backed up if this option is enabled. If this option is disabled: NetBackup backs up the virtual machine even if it is running from the NetBackup NFS datastore.
Snapshot retry count	Sets the number of times the snapshot is retried. The default is 10. The range is 0 to 100. This option and the snapshot time-out and snapshot creation interval provide flexibility in the creation of snapshots. For most environments, the default values are usually best. In special circumstances, it may be helpful to adjust these settings. Example considerations are the size of the virtual machine and the processing load on the VMware server.

Table 5-7 VMware Advanced Attributes *(continued)*

Configuration parameter	Description
Snapshot timeout (minutes)	Sets a time-out period (in minutes) for completion of the snapshot. The default is 0, which means no time-out. If snapshots do not complete, set this option to a specific period to force a time-out. Consider using the snapshot creation interval to retry the snapshot at a later time.
Snapshot creation interval (seconds)	Determines the wait time (in seconds) before the snapshot is retried. The default is 10 seconds. The range is 0 to 3600.
VMware server list	Specifies a colon-delimited list of virtual machine servers that NetBackup communicates with for this policy. In large virtual environments, you can use this list to improve backup performance: NetBackup communicates only with the servers that are in this list. For example, exclude from the list any vCenter or vCloud servers that do not contain virtual machines to be backed up by this policy. Also, if a duplicate of the virtual machine exists on a different server: the duplicate is not backed up if it resides on a server that is not included in this list. **Important:** IPv6 addresses are not supported in the **VMware server list** field. Use fully qualified domain names or host names. **Note:** Each host name must match exactly the name as configured in the NetBackup credentials. **Note:** Separate the names with a colon (:) not a comma (,). This option does not affect either of the following: the list of all possible values in the Query Builder for automatic selection of virtual machines, or browsing of virtual machines for manual selection. If the list is blank (the default), NetBackup communicates with any servers in the virtual environment.

Table 5-7 VMware Advanced Attributes *(continued)*

Configuration parameter	Description
Treat Tags as unset if unable to evaluate	Tags were introduced with VMware vCenter Version 5.1. The APIs to interface with the tagging service were not released until VMware vCenter Version 6.0. NetBackup for VMware supports the tags that are assigned to virtual machine objects starting with VMware vCenter Version 6.0. If you have a mixed vCenter environment, such as 5.1, 5.5, and 6.0: you can use this configuration parameter to modify how NetBackup treats tags for vCenter Version 5.1/5.5. This configuration parameter also applies to all versions of ESXi hosts whose credentials were added to the **Virtual Machine Servers** list. This option is disabled by default. If you use the tag field in the VMware Intelligent Policy query and your policy searches for virtual machines across a mixed vCenter environment, note: NetBackup reports the virtual machines that are discovered from vCenter Server 5.1/5.5 and ESXi hosts as failed if it needs to evaluate the tag portion of the query to make an include or exclude decision. When you enable this option NetBackup treats tags as **unset**. If you use the tag field in the VMware Intelligent Policy query and your policy searches for virtual machines across a mixed vCenter environment, note: NetBackup evaluates the tag part of the query as if no tags were set on the virtual machines that are discovered from vCenter Server 5.1, 5.5, and ESXi.
Continue VIP discovery if one vSphere login fails	**Note:** This option applies to VMware Intelligent Policies (VIP) only. When this option is set to Yes: For a VIP policy's discovery job, NetBackup ignores a failed logon to a vCenter and attempts to log on and discover VMs on other vCenters. On any vCenter that NetBackup can log on to, the VMs that match the VIP policy's query are backed up. When this option is set to No (the default): If the attempt to log on to a vCenter fails, the discovery job fails and no VMs are backed up for any vCenters. More information is available on the types of NetBackup jobs for VMware: See "Using the Activity Monitor to monitor virtual machine backups" on page 156.
Perform snapshot without quiescing if quiesced snapshots fail	This option is disabled by default. If it is enabled and a quiesced snapshot cannot be created, the snapshot is created without quiescing I/O on the virtual machine. The resulting snapshot is referred to as crash consistent. In this case, you must perform your own analysis for data consistency in the backed-up data. **Warning:** In most cases, Veritas does not recommend enabling this option. NetBackup cannot guarantee that all required data has been flushed to disk when the snapshot occurs. The data that is captured in the snapshot may be incomplete. If this option is disabled, the backup fails if a quiesced snapshot cannot be created.

Table 5-7 VMware Advanced Attributes *(continued)*

Configuration parameter	Description
VMDK Compression	Used to specify the VMDK compression method. When this option is set to `none` (default) compression is not used during the backup job. NetBackup uses the preferred VMDK compression method when it opens VMDKs. Backup jobs automatically set the compression method to `none` if NetBackup is unable to read the VMDK with the preferred method.

About the Post vCenter events option (VMware Advanced Attributes)

The **Post vCenter events** option is available on the **VMware - Advanced Attributes** dialog of a NetBackup policy. (On the **VMware** tab of the policy, click **Advanced...**.)

Post vCenter events enables NetBackup to send backup related events to the vCenter server.

Note: To post events to vCenter, NetBackup must perform the backup through a vCenter server. If NetBackup accesses the ESX server directly, the backup information cannot be displayed in vSphere Client.

Note: You must set the required permissions in vCenter:

See "Setting privileges for posting events to vCenter" on page 51.

Note: If a vSphere administrator created an attribute named NB_LAST_BACKUP of type Global, NetBackup cannot post backup events to that attribute. You must remove the NB_LAST_BACKUP attribute from vSphere. Make sure that **Post vCenter events** is set to All Events or Error Events. At the next backup, NetBackup creates a NB_LAST_BACKUP attribute of type Virtual Machine and posts events to that attribute.

Post vCenter events also records the date and time of the last successful backup of the virtual machine:

- The date and time appear in vSphere Client on the **Summary** tab as a custom attribute under **Annotations**. The attribute is labeled NB_LAST_BACKUP.
- The date and time appear in vSphere Web Client on the **Virtual Machines** display.

The events can also be viewed with the NetBackup vSphere Web Client plug-in and the NetBackup vSphere Client (HTML5) plug-in:

See "Viewing NetBackup activity in vSphere Web Client or vSphere Client (HTML5)" on page 158.

For instructions on installing and using the NetBackup plug-in, see the following guides:

NetBackup Plug-in for VMware vSphere Web Client Guide

NetBackup Plug-in for VMware vSphere Client (HTML5) Guide

http://www.veritas.com/docs/DOC5332

Exclude Disks tab

In the **Change Policy** dialog box, the **Exclude Disks** tab appears for policies of the **VMware** policy type. These options determine the kind of disks on the virtual machine that are excluded from the backup. These options can reduce the size of the backup, but should be used with care. These options are intended only for the virtual machines that have multiple virtual disks.

The following options appear on the **Exclude Disks** tab.

Table 5-8 Options on the **Exclude Disks** tab of the policy

Option	Description
No disks excluded	Backs up all virtual disks that are configured for the virtual machine.
Exclude boot disk	The virtual machine's boot disk (for example the C drive) is not included in the backup. Any other disks (such as D) are backed up. Consider this option if you have another means of recreating the boot disk, such as a virtual machine template for boot drives. See "About the exclude disk options for virtual disk selection" on page 88. **Note:** A virtual machine that is restored from this backup cannot start. Data files are available in the restored data disks.

Table 5-8 Options on the **Exclude Disks** tab of the policy *(continued)*

Option	Description
Exclude all data disks	The virtual machine's data disks (for example the D drive) are not included in the backup for this policy. Only the boot disk is backed up. Consider this option only if you have a different policy that backs up the data disks. See "About the exclude disk options for virtual disk selection" on page 88. **Note:** When the virtual machine is restored from the backup, the virtual machine data for the data disk may be missing or incomplete.
Perform custom attribute based exclusion	Exclude disks by a VMware Custom Attribute that is applied to a virtual machine. The VMware Custom Attribute identifies the disks that you want to exclude from backups. If you select this option, also enter the name of the Custom Attribute. NetBackup then excludes the disks that are defined in that attribute. The attribute must have comma separated values of device controllers for the disks to be excluded. For example: `scsi0-0,ide0-0,sata0-0,nvme0-0` The default value is `NB_DISK_EXCLUDE_LIST`. You can use this value as the custom attribute or choose your own value. **Note:** Custom Attribute based disk exclusion requires that you enter in NetBackup the credentials for the vCenter server or servers that host the VMs. ESXi server credentials are not sufficient. See "Adding NetBackup credentials for VMware" on page 45. Your VMware administrator must use a VMware interface to apply the custom attribute to the disks that you want to exclude from the virtual server. The **Virtual Disk Exclusion** wizard of the NetBackup plug-ins for vSphere provides a method to add a Custom Attribute to a virtual machine or virtual machines.
Specific disks to be excluded	Exclude a specific disk by selecting the disk controller type and device numbers that represent the virtual device node of the disk. Then click **Add**. NetBackup adds the controller ID to the list of nodes to be excluded. Repeat for each disk that you want to exclude. To delete a disk from the list of disks to exclude, select the disk controller type and device numbers, and then click **Delete**. The list is a comma-separated collection of controller IDs. Alternatively, you can add or delete specific disks by editing the contents of the text box in which the excluded disks appear. Wildcard characters are not supported.

Note: NetBackup does not support the exclude disks options for Replication Director backups.

See "Exclude disks from backups: an example to avoid" on page 90.

See "Restoring data from the backups that excluded the boot disk or data disks" on page 91.

For more information about VMware, see the NetBackup for VMware Guide.

About the exclude disk options for virtual disk selection

The backup policy **Exclude Disks** tab has options to exclude virtual disks from a backup. By default, no disks are excluded. You should use this setting in most cases.

If you want to exclude disks from a backup, the other options are **Exclude boot disk** and **Exclude all data disks**. These options are intended for the virtual machines that have multiple virtual disks. You should use these options with care.

To exclude a boot disk or data disk, note the following requirements:

- The virtual machine must have more than one disk.
- NetBackup must be able to identify the boot disk.
- The boot disk must not be part of a managed volume (Windows LDM or Linux LVM). The boot disk must be fully contained on a single disk.

The boot disk must include the following:

- The boot partition.
- The system directory (Windows system directory or Linux boot directory).

Important! The exclude disk options are meant only for the following cases:

- **Exclude boot disk**: Consider this option if you have another means of recreating the boot disk, such as a virtual machine template for boot drives. If **Exclude boot disk** is enabled, the policy does not back up the boot disk.

  Note: When the virtual machine is restored from the backup, the virtual machine data for the boot disk may be missing or incomplete.

  Note the following about **Exclude boot disk**:

  - If the virtual machine has a boot disk but has no other disks, the boot disk is backed up. It is not excluded.

- If the virtual machine's boot disk is an independent disk, but the virtual machine has no other disks, the boot drive is backed up. The restored boot drive however contains no data, because NetBackup cannot back up the data in an independent disk.
- If the virtual machine has a boot drive and an independent drive, the boot drive is not backed up. Only the independent drive is included in the backup. Since NetBackup cannot back up the data in an independent disk, the restored independent disk contains no data.
  Refer to the explanation on independent disks in the following topic:
  See "NetBackup for VMware terminology" on page 20.
- Adding a virtual disk and changing this option before the next backup can have unexpected results.
  See "Exclude disks from backups: an example to avoid" on page 90.

- **Exclude all data disks**: Consider this option if you have a different policy or other backup program that backs up the data disks. If **Exclude all data disks** is enabled in a policy, that policy does not back up the data disks.

  Note the following about excluding data disks:

  - If the virtual machine has only one disk (such as C:), that drive is backed up. It is not excluded.
  - If the virtual machine's boot disk is an independent disk, and the virtual machine has a separate data disk, the boot disk is backed up. The restored boot disk however contains no data, because NetBackup cannot back up the data in an independent disk.

  Note: When the virtual machine is restored from the backup, the virtual machine data for the data disk may be missing or incomplete.

- **Perform custom attribute based exclusion**: If this option is enabled, NetBackup excludes the disks that have a custom attribute from the backup. The default value for this attribute is `NB_DISK_EXCLUDE_DISK`. You can use this default attribute or change the attribute name on the **Exclude Disks** tab of the backup policy. Note that this option gives the VMware administrator control over which disks are excluded.

  Note: When a virtual machine is restored from the backup, the virtual machine data for the excluded disk may be missing or incomplete.

  - The attribute on the virtual machine must be populated with comma separated values of controller IDs for the disks to be excluded.

- If the custom attribute is not populated or does not exist on the virtual machine, none of the disks (except independent disks) is excluded.
- If you remove disks from the custom attribute value between the differential backups, only those files that changed since the last backup are available to restore individually. You can restore the entire virtual disk or the VM, in which case all files are restored including those you cannot restore individually. After the next full backup, you can restore any of the files individually.
- If you add disks to the custom attribute value between the differential backups, those disks are excluded from the next backup.

- **Specific disk(s) to be excluded**: If this option is enabled, NetBackup excludes the disks that you specify. Note that this option gives the NetBackup administrator control over which disks are excluded from backups.

  Note: When a virtual machine is restored from the backup, the virtual machine data for the excluded disk may be missing or incomplete.

  - You must include comma-separated values of controller IDs on the **Exclude Disks** tab of the backup policy.
  - If the disks do not exist on the specified controller and device IDs, none of the disks (except independent disks) is excluded.
  - If you remove controllers from the exclusion list between the differential backups, only those files that changed since the last backup are available to restore. All files are available to restore after the next full backup.
  - If you add controllers to the exclusion list between the differential backups, their disks are excluded from the next backup.

Caution: Use of the exclude disk options can have unintended consequences if these rules are not followed.

The following topics contain important guidance on the exclude disk options:

See "Restoring data from the backups that excluded the boot disk or data disks" on page 91.

Exclude disks from backups: an example to avoid

You should use the options on the **Exclude Disks** tab of the **Change Policy** dialog box with care. For example, if you add a disk to the virtual machine and change the settings that exclude disks, note: The next backup may not capture the virtual

machine in the state that you intended. You should back up the entire virtual machine (that is, do not exclude any disks) before you exclude a disk from future backups.

Restoring data from the backups that excluded the boot disk or data disks

If the policy's **Excludes Disks** option excluded the boot disk or data disks, you can restore the backed-up data as follows:

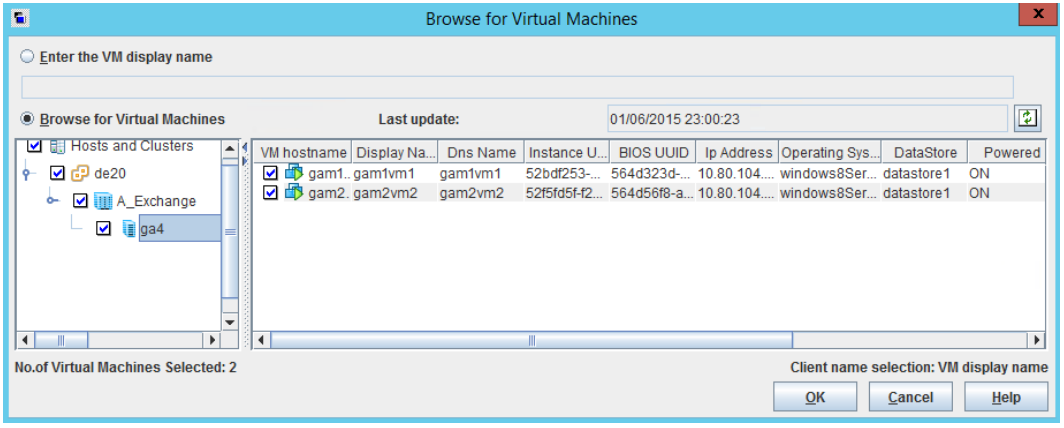
- If **Enable file recovery from VM backup** was enabled on the backup policy: You can restore individual files from those portions of the virtual machine that the Virtual disk selection option did not exclude.
  See "Restoring individual files" on page 224.
- If the **Excludes Disks** option was set to **Exclude boot disk**: You can restore the virtual machine and move the restored data disk(s) to another virtual machine.

Browse for VMware virtual machines

When you configure a NetBackup policy, you can use the Browse for Virtual Machines screen to select virtual machines for backup. You can enter the virtual machine's host name manually or browse and select it from a list.

As an alternative, NetBackup can automatically select virtual machines based on a range of criteria.

See "About automatic virtual machine selection for NetBackup for VMware" on page 102.



- **Enter the VM display name** (or **VM hostname, VM BIOS UUID, VM DNS Name, VM instance UUID**)
  Click this option if you want to manually enter the name or other identifier of a virtual machine. The format of the name depends on your system. It may be the fully qualified name or another name, depending on your network configuration and how the name is defined in the guest OS. If NetBackup cannot find the name you enter, policy validation fails.

  Note: The type of name to enter depends on the **Primary VM identifier** setting on the **VMware** tab of the policy.

  To enter a name, make sure that **Browse for Virtual Machines** is not selected.

- **Browse for Virtual Machines**
  Click this option to discover vCenter servers, clusters, data centers, vApps, and ESX servers (shown in the left pane). You can select virtual machines from a list (in the right pane).
  NetBackup uses the following icons for vSphere objects:

  vCenter server

  Datacenter

  Cluster

  vApp

  ESX server

  Virtual machine (powered off)

  Virtual machine (powered on)

  Virtual machine template

The virtual machines that are contained in a VMware vApp are displayed in the right pane along with other virtual machines.

The virtual machine names that are listed may be derived from a cache file. Use of the cache file is faster than rediscovering the virtual machines on the network if your site has a large number of virtual machines.

If NetBackup cannot obtain the IP address of the virtual machine, the host name and IP address are displayed as NONE.

Note that virtual machine host names or display names must be unique within a primary server's policies:

See "Virtual machine host names and display names should be unique if VMs are selected manually in the policy" on page 97.

- **Last Update**

  To update the cache file and re-display virtual machines, click the refresh icon to the right of the **Last Update** field. This field shows the date and time of the most recent cache file that contains the names of virtual machines.

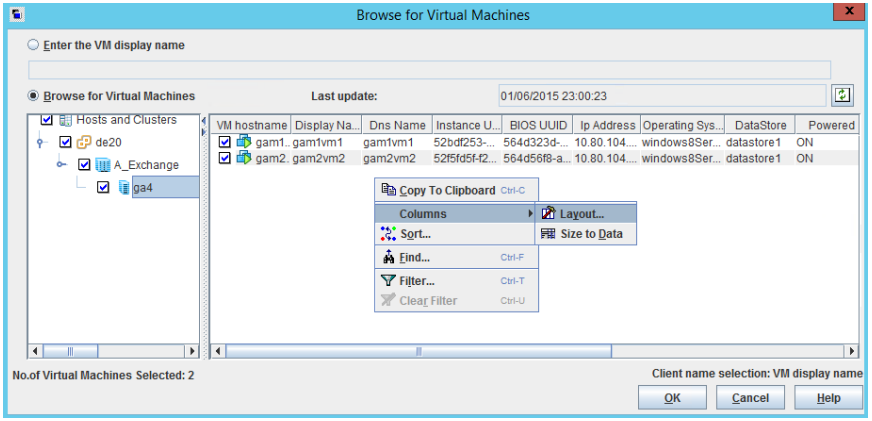
  For NetBackup to access the virtual machines, note the following:

  - The NetBackup primary server must have credentials for the VMware vCenter or ESX server(s).
    See "Adding NetBackup credentials for VMware" on page 45.
  - DNS problems may prevent or slow down discovery of the virtual machines.
    See "Preventing browsing delays caused by DNS problems" on page 295.
  - To limit the search to particular vCenter or ESX servers, you can create a `BACKUP` registry entry as an exclude list. Excluding unneeded servers can dramatically speed up the search for virtual machines.
    See "Limiting the VMware servers that NetBackup searches when browsing for virtual machines" on page 95.
  - The browsing time out value must not be set too low.
    See "Changing the browsing timeout for virtual machine discovery" on page 297.

- **VM hostname, Display Name, DNS Name, Instance UUID,** etc.

  When you select an ESX server in the left pane, information about its virtual machines appears in columns in the right pane.

  You can change the arrangement of these columns by right-clicking in the right pane:

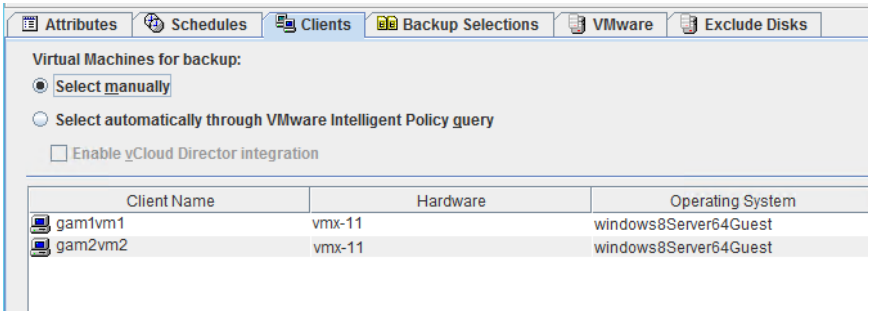


The columns are the following:

VM hostname	The host name of the virtual machine.
Display Name	The display name of the virtual machine.
Instance UUID	The UUID of the virtual machine.
BIOS UUID	The BIOS UUID of the virtual machine.
Dns Name	The VMware "DNS Name" of the virtual machine. In vSphere Client, this name appears on the virtual machine's Summary tab. See "Primary VM identifier options (VMware)" on page 76.
IP Address	The IP address of the virtual machine.
Operating System	The guest OS system as defined when the virtual machine was created.
DataStore	The datastore where the virtual machine configuration files are stored. If the datastore is in a datastore cluster, NetBackup displays the name of the datastore (not the name of the cluster).
Powered	The power on/off status of the virtual machine when it was last discovered.
RDM Status	Shows whether the virtual machine has a physical disk in raw device mapping mode (RDM) or has an independent drive.

Change Tracking Support	Shows whether the virtual machine supports the VMware **Changed Block Tracking** feature (for BLIB). Changed Block Tracking requires ESX server 4.0 and a virtual machine at vmx-07 or later.
Virtual Center Name	The vCenter server that manages the ESX server (also appears in the left pane).
Template	Shows whether the virtual machine is a template.

The virtual machines you selected are listed in the **Clients** tab.



Limiting the VMware servers that NetBackup searches when browsing for virtual machines

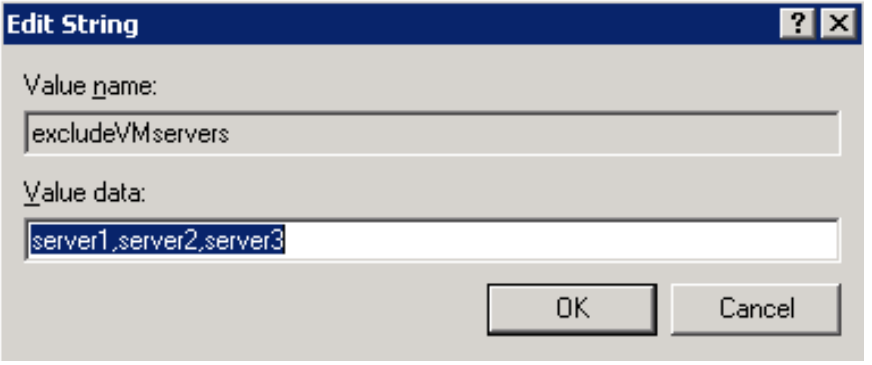
As part of creating a NetBackup policy, you must specify which virtual machines to back up. One approach is to let NetBackup search the network and list all available virtual machines. However, if your VMware environment contains many VMware servers and virtual machines, it may take too long to search and list all of them. For example, consider an environment with ten vCenter servers. To back up the virtual machines on one of the ten vCenter servers, browsing virtual machines on all ten servers is unnecessary.

To speed up browsing, you can exclude particular VMware servers from the search. When it probes the network for virtual machines, NetBackup queries only the VMware servers that are not named in the exclude list for the backup-host.

Use one of the following procedures, depending on the platform of the backup host (Windows or Linux).

To limit the VMware servers that NetBackup discovers, per Windows backup host

1. On the Windows desktop of the backup host, click **Start > Run** and enter `regedit`.
2. To be on the safe side, make a backup of the current registry (**File > Export**).
3. Go to **HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > Config** and create a key called `BACKUP`.
4. Right-click in the right pane and click **New > String Value**. Enter `excludeVMservers` as the name.
5. Right-click the `excludeVMservers` name and click **Modify**.
6. In the **Edit String** dialog, enter a comma-delimited list of the VMware servers that are NOT to be queried when NetBackup browses the network. Do not enter spaces. You can enter vCenter servers and individual ESX servers.



Note: The exclude list is used on the next backup. If any bpfis processes are running, the exclude list has no effect on them.

The exclude list applies only to this backup host. The servers are not queried when NetBackup browses for virtual machines to list on the policy's **Browse for Virtual Machines** dialog of the NetBackup Administration Console.

To limit the VMware servers that NetBackup discovers, per Linux backup host

1. On the Linux backup host, create (or open) the following file:

   `/usr/openv/netbackup/virtualization.conf`

2. Add the following to the file:

   ```
   [BACKUP]
   "excludeVMservers"="server1,server2,server3"
   ```

   where *server1,server2,server3* is a comma-delimited list of the VMware servers that are NOT to be queried when NetBackup browses the network. Do not enter spaces. You can enter vCenter servers and individual ESX servers.

   Note: If the file already contains a `[BACKUP]` line, do not add another `[BACKUP]` line. Any other lines that already exist under `[BACKUP]` should remain as they are.

3. Save the file.

   Note: The exclude list is used on the next backup. If any bpfis processes are running, the exclude list has no effect on them.

   The exclude list applies only to this backup host. The servers are not queried when NetBackup browses for virtual machines to list on the policy's **Browse for Virtual Machines** dialog of the NetBackup Administration Console.

As an alternative, NetBackup can automatically select virtual machines based on a range of criteria.

See "About automatic virtual machine selection for NetBackup for VMware" on page 102.

Virtual machine host names and display names should be unique if VMs are selected manually in the policy

Certain VMware environments do not require unique names for virtual machines. For instance, virtual machines within a vCenter server can have the same host or display names as virtual machines in another vCenter server. The same is true of datacenters, which are logical groupings of virtual resources within a vCenter server. Virtual machine host names or display names must be unique within a datacenter. They do not need to be unique between two datacenters on the same vCenter. A virtual machine named VM1 can exist in datacenter A. Another virtual machine (also named VM1) can exist in datacenter B, on the same vCenter server.

Identically named virtual machines can present a problem for any policies that are configured as follows:

- The primary server's policies use the **Select manually** option on the **Clients** tab to select the VMs for backup.
- The **Primary VM identifier** option on the **VMware** tab identifies VMs by their host names or display names.

These policies may back up a different but identically named VM, instead of the VM that you selected. In that case, the VM that you selected is not backed up. For these policies to work, the virtual machines' display names or host names must be unique.

Consider the following options:

- For manual policies that identify VMs by display name or host name, change the VM names so that each VM has a unique host name or display name.
- As an alternative, configure the policies' **Primary VM identifier** option to identify the VMs by their UUIDs instead of by host name or display name. Use the type of UUID that is appropriate for your virtual machine environment.
  See "Primary VM identifier options (VMware)" on page 76.
- Instead of policies with manual-selection, use VMware Intelligent policies to select the VMs through a query. Even if the **Primary VM identifier** option is set to host name or display name, NetBackup identifies each VM by its UUID.

Primary VM identifier option and manual selection of virtual machines

This topic applies to the manual selection of virtual machines on the NetBackup **Browse for Virtual Machines** screen.

A change to the policy's **Primary VM identifier** value can affect backups. If you change this option, you may have to delete the virtual machine selections on the **Clients** tab and re-enter them. Otherwise, NetBackup may no longer be able to identify the virtual machines to back up.

For example, the host names in the **Clients** tab cannot be used and the virtual machines are not backed up in the following case:

- If you change the **Primary VM identifier** from **VM hostname** to **VM display name**, and
- The display names of the virtual machines are different from the host names.

In this case, delete the host name entries on the **Clients** tab and browse the network to select the virtual machines by display name.

See "Browse for VMware virtual machines" on page 91.

Note: When creating virtual machines, use the same name for both host name and display name. If the **Primary VM identifier** is changed, the existing entries on the **Clients** tab still work.

If the policy selects virtual machines automatically, refer to the following topic:

See "Effect of Primary VM identifier parameter on Selection column in Test Query results" on page 144.

About incremental backups of virtual machines

NetBackup enables full virtual machine and file-level incrementals in the same backup (the **Enable file recovery from VM backup** option).

Better support for incremental backup is available when you use BLIB (**Enable block-level incremental backup**). BLIB requires ESX 4.x and virtual machines at vmx-07 or later.

Note: Individual file recovery is supported from full backups and from incremental backups, as long as the **Enable file recovery from VM backup** policy option is enabled.

Note: Make sure that the virtual machines to back up are time synchronized with the backup host. Otherwise, some changed data may not be included in the backup, depending on the clock differential between the backup host and the virtual machine.

Note: For incremental backups, you do not have to configure the client on the VMware backup host for timestamps. The VMware policies automatically default to the use of timestamps.

Configuring incremental backups

Use the following procedure for virtual machine backup.

Note: VMware policies can also be configured from the NetBackup web UI. To do so, on the left navigation pane, click **Protection > Policies**, and then select a listed VMware policy to change it. Or click **+Add**, enter a **Policy name**, and select **VMware** from the **Policy type** drop-down list.

To configure incremental backup of a virtual machine

1. In the NetBackup policy **Attributes** tab, select the **VMware** policy type.
2. On the **VMware** tab, select the VMware backup host.
3. Optional: for BLIB, select **Enable block-level incremental backup**.
4. Select **Enable file recovery from VM backup**.

   More information is available on the VMware options.

   See "Backup options on the VMware tab" on page 73.
5. Click **OK**.
6. On the **Schedules** tab, select **Differential Incremental Backup** or **Cumulative Incremental Backup**.
7. Fill in the **Clients** tab.

Storage Foundation Volume Manager volumes in the virtual machine

To back up a virtual machine that contains Veritas Storage Foundation Volume Manager volumes, make sure the following options on the policy's VMware tab are disabled:

Enable file recovery from VM backup

Exclude deleted blocks.

Note: Restore of selected files from a backup of the full virtual machine is not supported if the virtual machine contains Storage Foundation Volume Manager volumes.

See "NetBackup for VMware: notes and restrictions" on page 27.

Chapter 6

Configure a VMware Intelligent Policy

This chapter includes the following topics:

- About automatic virtual machine selection for NetBackup for VMware
- Support and use of VMware tag associations
- The basics of a NetBackup query rule
- Important notes on automatic virtual machine selection
- NetBackup requirements for automatic virtual machine selection
- Automatic virtual machine selection: Task overview
- Options for selecting VMware virtual machines
- Configuring automatic virtual machine selection
- Editing an existing query in Basic Mode
- Using the Query Builder in Advanced Mode
- AND vs. OR in queries
- Examples for the NetBackup Query Builder
- The IsSet operator in queries
- About selecting virtual machines by means of multiple policies
- Order of operations in queries (precedence rules)
- Parentheses in compound queries

- Query rules for resource pools
- Query rules for datacenter folders (host folder)
- Query rules for duplicate names
- Query rules for tags
- Query Builder field reference
- Test Query screen for VMware
- Test Query: Failed virtual machines
- Effect of Primary VM identifier parameter on Selection column in Test Query results
- Effect of Primary VM identifier parameter on VM Name column in Test query results
- Refreshing the display of virtual environment changes in the Query Builder
- Reducing the time required for VM discovery in a large VMware environment

About automatic virtual machine selection for NetBackup for VMware

Instead of manually selecting the virtual machines for backup, you can configure NetBackup to automatically select virtual machines based on a range of criteria. You specify the criteria (rules) in the **Query Builder** on the NetBackup policy **Clients** tab. NetBackup creates a list of the virtual machines that currently meet the rules and adds those virtual machines to the backup.

This feature is called the VMware Intelligent Policy.

Automatic selection of virtual machines has the following advantages:

- Simplifies the policy configuration for sites with large virtual environments. You do not need to manually select virtual machines from a long list of hosts: NetBackup selects all the virtual machines that meet the selection rules in the policy's Query Builder.
- Allows the backup list to stay up-to-date with changes in the virtual environment. Eliminates the need to revise the backup list whenever a virtual machine is added or removed.
- Virtual machine selection takes place dynamically at the time of the backup.

Examples of automatic virtual machine selection are the following:

Table 6-1 Examples for automatic virtual machine selection

Example	Description
Add new virtual machines	At the next backup, the policy can automatically discover the virtual machines that have recently been added to the environment. If the virtual machines match the query rules that you configure in the policy, they are automatically backed up.
Limit the backup list to the virtual machines that are currently turned on	If some of your virtual machines are occasionally turned off, NetBackup can be configured to automatically exclude those from the backup list. Among the virtual machines it discovers, NetBackup backs up only the virtual machines that are turned on.
Back up virtual machines based on physical boundaries	Examples of physical boundaries are vCenter servers, ESX servers, datastores, and clusters. For example, a query rule can select all the virtual machines in a particular ESX server, so the policy backs up only those virtual machines.
Back up virtual machines based on logical boundaries	Examples of logical boundaries are folders, vApps, templates, and resource pools. For example, a query rule can select all the virtual machines in a particular folder, so the policy backs up only those virtual machines.
Back up virtual machines based on VMware tags	NetBackup can include or exclude virtual machines based on the user assigned tags.

Support and use of VMware tag associations

NetBackup supports using VMware tags for virtual machine selection. You use this feature when you configure VMware Intelligent Policies to protect virtual machines. More information about this feature is available.

See “Notes and limitations for tag usage in VMware Intelligent Policy queries” on page 41.

See “Query rules for tags” on page 128.

NetBackup also supports the backup and restore of VMware tag associations with virtual machines when you use VMware Intelligent Policies. The tag association metadata for all tags that are associated with a virtual machine are backed up with that virtual machine. If those tags exist on the vCenter Server, they are recreated when the virtual machine is restored. More information about this feature is available.

See "Notes and limitations for the backup and restore of VMware tag associations" on page 42.

See "How NetBackup handles VMware tag associations at restore" on page 230.

The basics of a NetBackup query rule

For automatic virtual machine selection, NetBackup uses query rules to determine which VMware virtual machines to select for backup. You create the rules in the Query Builder, on the **Clients** tab of the policy.

Note: VMware policies can also be configured from the NetBackup web UI. To do so, on the left navigation pane, click **Protection > Policies**, and then select a listed VMware policy to change it. Or click **+Add**, enter a **Policy name**, and select **VMware** from the **Policy type** drop-down list.

In the NetBackup web UI, you must use OData keywords and OData operators in query rules:

See "Query Builder field reference" on page 129.

A query rule consists of the following:

- A keyword, such as **Displayname** or **Datacenter** (many keywords are available).
  For example: For automatic selection of the virtual machines with the display names that contain certain characters, you need the **Displayname** keyword in the rule.
- An operator, such as **Contains**, **StartsWith**, or **Equal**.
  The operator describes how NetBackup analyzes the keyword. For example: **Displayname StartsWith** tells NetBackup to look for the display names that start with particular characters.
- Values for the keyword.
  For the **Displayname** keyword, a value might be "prod". In that case, NetBackup looks for the virtual machines that have the display names that include the characters prod.
- An optional joining element (AND, AND NOT, OR, OR NOT) to refine or expand the query.

The policy uses these elements to discover and select virtual machines for backup.

Table 6-2 contains the examples of rules.

Table 6-2 Examples of rules

Rule	OData rule *	Description
`Displayname Contains "vm"`	`contains(displayName, 'vm')`	NetBackup selects the virtual machines that have the characters `vm` anywhere in their display names.
`Displayname EndsWith "vm"`	`endswith(displayName, 'vm')`	NetBackup selects the virtual machines that have the characters `vm` at the end of their display names.
`Datacenter AnyOf "datacenter1","datacenter2"`	`datacenter in ('datacenter1','datacenter2')`	NetBackup selects the virtual machines that use datacenter1 or datacenter2.
`Powerstate Equal poweredOn`	`powerState eq 'poweredOn'`	NetBackup selects only the virtual machines that are currently turned on.
`Powerstate Equal poweredOn AND Tag Equal "Production"`	`powerState eq 'poweredOn' and tagName eq 'Production'`	NetBackup selects only virtual machines that are currently powered on with the "Production" tag.

* Use OData keywords only when you build queries with the NetBackup web UI.

Important notes on automatic virtual machine selection

The Virtual Machine Intelligent Policy feature in NetBackup is a different approach to VMware virtual machine selection in the policy. It represents a paradigm shift in the way you select virtual machines for backup. As with all major changes, the effective use of this feature requires forethought, preparation, and care.

Table 6-3 Important notes on automatic virtual machine selection!

Note!	Explanation
Create rules carefully.... 	Instead of manually selecting virtual machines for backup, you create guidelines for automatic selection of virtual machines. The guidelines are called rules; you enter the rules in the policy's Query Builder. You make the rules, and NetBackup follows them. If the rules state: Back up all virtual machines with a host name that contains "prod", NetBackup does that. Any virtual machine that is added to the environment with a host name containing "prod" is automatically selected and backed up when the policy runs. Virtual machines with the names that do not contain "prod" are not backed up. To have other virtual machines automatically backed up, you must change the query rules (or create additional policies).

Table 6-3 Important notes on automatic virtual machine selection! *(continued)*

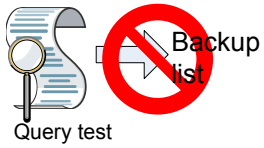
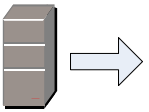
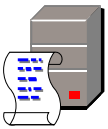
Note!	Explanation
Changes to the virtual environment can affect backup times. 	If many virtual machines are temporarily added to your environment and happen to fall within the scope of the query rules, they are backed up. The backups can therefore run much longer than expected.
Test the query rules. 	Test the query rules ahead of time. The policy includes a Test Query function for that purpose. It's important to verify that your query operates as expected. Otherwise, the query may inadvertently select too many or too few virtual machines. As an alternative, you can use the `nbdiscover` command to test a query. Refer to the *NetBackup Commands Reference Guide*. Note also: The policy's **Primary VM identifier** parameter can affect the automatic selection process. See "Effect of Primary VM identifier parameter on Selection column in Test Query results" on page 144.
A query test does not create the backup list. NetBackup creates the backup list when the backup runs.  Query test  Backup execution	The automatic selection process is dynamic. Changes in the virtual environment may affect which virtual machines the query rules choose when the backup runs. **Note:** If virtual machine changes occur, the virtual machines that are selected for backup may not be identical to those listed in your query test results.

Table 6-3 Important notes on automatic virtual machine selection! *(continued)*

Note!	Explanation
The policy does not display a list of the virtual machines that are to be backed up. Use the Activity Monitor or OpsCenter. 	If you select virtual machines manually (with the Browse for Virtual machines screen), the selected virtual machines are listed on the policy **Clients** tab. But when you use the Query Builder for automatic selection, the selected virtual machines are not listed on the **Clients** tab. For a list of the backed up virtual machines, use the NetBackup Activity Monitor or the OpsCenter web interface. See "Using the Activity Monitor to monitor virtual machine backups" on page 156. See "Using OpsCenter to report on virtual machine backups" on page 160.
When you save the policy, the query rules are not validated.  Policy	When you save a policy, policy validation does not consult the query rules and select virtual machines for backup. Because of the potential for changes in the virtual environment, virtual machine selection must wait until the backup runs. As a result, when you save the policy, NetBackup does not check the policy attributes against a backup list. If the query rules select the virtual machines that are incompatible with a policy attribute, policy validation cannot flag that fact. The incompatibility becomes apparent when NetBackup determines the backup list at the time of the backup. Take for example a policy that is configured for **Enable block-level incremental backup** (BLIB). BLIB works only with ESX 4.0 virtual machines at version vmx-07 or later. If the query rules select a virtual machine at a version earlier than vmx-07, the policy cannot back up that virtual machine. The mismatch between the policy and the virtual machine is revealed when the backup runs, not when the policy is validated. The Activity Monitor's job details log indicates which virtual machines can or cannot be backed up.

NetBackup requirements for automatic virtual machine selection

Note the following requirements for automatic selection of VMware virtual machines:

- The system where the NetBackup Administration Console runs must have access to the vCenter server.
- Automatic virtual machine selection requires no additional license beyond the NetBackup Enterprise Client license.
- Automatic virtual machine selection is required for backups in vCloud Director or for Replication Director for VMware.

Automatic virtual machine selection: Task overview

This topic is a high-level overview of how to set up a NetBackup policy for automatic selection of VMware virtual machines. Follow the links in the table for more details.

Table 6-4 Automatic selection of virtual machines: overview of the tasks

Steps to configure automatic selection	Description and notes
Configure a VMware policy	Use the policy Attributes tab. See "Configuring a VMware policy from the Policies utility" on page 68.
Set rules for virtual machine selection in the policy Query Builder	On the policy **Clients** tab, click **Select automatically through VMware Intelligent Policy query**. Choose a host for virtual machine selection (default is the VMware backup host). To add rules, use the Query Builder drop-down fields. See "Configuring automatic virtual machine selection" on page 111. See "Options for selecting VMware virtual machines" on page 109.
Test the rules	Click **Test Query** in the Query Builder on the **Clients** tab. Virtual machines are labeled as included or excluded, based on the rules. **Note:** The list of virtual machines is not saved in the **Clients** tab. **Note:** The query rules are also displayed in the **Backup Selections** tab. The backup selections are pre-set to All_LOCAL_DRIVES (not displayed). As an alternative, you can use the `nbdiscover` command to test a query. Refer to the *NetBackup Commands Reference Guide*.
Execute a backup	When the policy executes, NetBackup consults the rules in the Query Builder, creates a list of virtual machines, and backs them up.
Check the backup	To see which virtual machines were backed up, use the Activity Monitor, or run a **Virtual Client Summary** report in OpsCenter. See "Using the Activity Monitor to monitor virtual machine backups" on page 156. See "Using OpsCenter to report on virtual machine backups" on page 160.

Options for selecting VMware virtual machines

This topic describes the options on the policy **Clients** tab, or in the Backup Policy Wizard.

You can use these options to manually select virtual machines, or to configure NetBackup to select virtual machines automatically. For automatic selection, you specify the selection criteria (rules) in the policy's Query Builder. When the backup job runs, NetBackup discovers the virtual machines that currently meet the criteria and backs up those virtual machines.

A procedure is available.

See "Configuring automatic virtual machine selection" on page 111.

Table 6-5 Virtual machine selection

Option	Description
Select manually	Click this option and click **New** to manually enter virtual machines names, or to browse and select them from a list. See "Browse for VMware virtual machines" on page 91. **Note:** The rest of the fields and options are for automatic selection of virtual machines.
Select automatically through VMware Intelligent Policy query	Click this option to allow NetBackup to automatically select virtual machines for backup based on the rules that you enter in the Query Builder.
Enable vCloud Director integration	Enables backup of the virtual machines that reside in a vCloud environment. Requires the automatic selection of virtual machines. With this option, the policy selects for backup only the virtual machines that vCloud manages: it skips the virtual machines that are not in vCloud.
NetBackup host to perform automatic virtual machine selection	This host discovers virtual machines and automatically selects them for backup based on your query rules. The resulting list determines which virtual machines are backed up. To designate your media servers as discovery hosts, select **Backup Media Server** from the pull-down.

Table 6-6 Query Builder

Option	Description
Query Builder (Join, Field, Operator, Values)	Use these pull-down fields to define rules for automatic selection of virtual machines. From left to right, each pull-down further defines the rule. Click the plus sign to add the rule to the **Query** pane. Click the reset icon (curved arrow) to blank out the pull-down fields. See "Query Builder field reference" on page 129. See "Examples for the NetBackup Query Builder" on page 118.
Advanced Mode	Places the Query Builder in Advanced Mode for manual entry of rules. See "Using the Query Builder in Advanced Mode" on page 116. See "Query Builder field reference" on page 129. See "Examples for the NetBackup Query Builder" on page 118.
Basic Mode	Returns the Query Builder from Advanced Mode to Basic Mode. See "Query Builder field reference" on page 129.
Edit	Use this option to change an existing query rule when in Basic Mode, as follows: ■ Click the rule and then click **Edit**. ■ Make new selections in the Query Builder pull-down fields. ■ Click the save option (diskette icon).
Remove	Deletes a query rule when in Basic Mode. Click on the rule and then click **Remove**.
Test Query...	Click this option to test which virtual machines NetBackup selects based on the rules in the Query Builder. **Note:** This test option does not create the backup list for the policy. When the next backup runs from this policy, NetBackup re-discovers virtual machines and consults the query rules. At that time, NetBackup backs up the virtual machines that match the rules. See "Test Query screen for VMware" on page 141. As an alternative, you can use the `nbdiscover` command to test a query. Refer to the *NetBackup Commands Reference Guide*.

Table 6-6 Query Builder *(continued)*

Option	Description
Reuse VM selection query results for:	Sets the refresh rate of an internal cache of the query results. NetBackup uses the cache to determine which virtual machines to select at the time of the backup. The cache speeds up the selection of virtual machines without burdening the vCenter server at each scheduled backup. A faster cache refresh rate synchronizes the cache with the changes recorded in vCenter, such as the addition or removal of virtual machines. However, each cache refresh consumes vCenter resources. With a slower refresh rate, new virtual machines may not be included immediately in the next backup. New or changed virtual machines are included when the cache is refreshed. Note that fewer vCenter resources are consumed with a slower refresh rate. The default is 8 hours. For 8 hours, NetBackup uses the cache and does not attempt to rediscover virtual machines. Changes to the virtual environment do not affect the cache during that period. After 8 hours, the next execution of the policy causes NetBackup to rediscover virtual machines. If any changes match a rule in the query, the list of selected virtual machines is modified accordingly. **Note:** The cache is refreshed before the next scheduled backup whenever the policy is changed and saved. More information is available on the **Reuse VM selection query results for:** option: See "About the Reuse VM selection query results option" on page 366.

Configuring automatic virtual machine selection

NetBackup can automatically select VMware virtual machines for backup based on the criteria that you enter. You specify the criteria (rules) in the Query Builder on the NetBackup policy **Clients** tab. You can set up rules to include certain virtual machines for backup, or to exclude virtual machines.

Note: VMware policies can also be configured from the NetBackup web UI. To do so, on the left navigation pane, click **Protection > Policies**, and then select a listed VMware policy to change it. Or click **+Add**, enter a **Policy name**, and select **VMware** from the **Policy type** drop-down list.

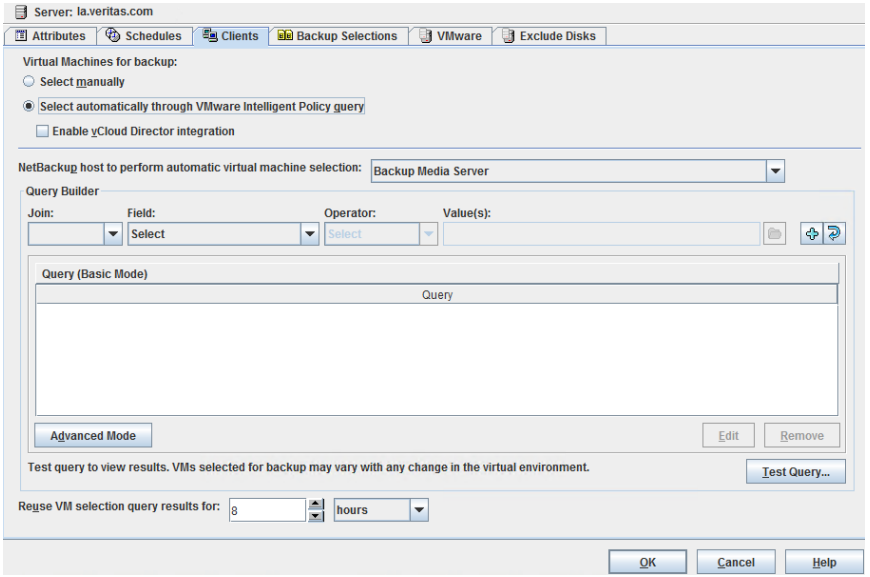
In the NetBackup web UI, you must use OData keywords and OData operators in query rules:

See "Query Builder field reference" on page 129.

When the backup job runs, NetBackup creates a list of the virtual machines that currently meet the query rules and backs them up.

The following is the policy Clients tab with **Select automatically through VMware Intelligent Policy query** selected.

Figure 6-1 Policy Clients tab for automatic selection of virtual machines



The Query Builder can operate in Basic Mode or in Advanced Mode.

To configure automatic virtual machine selection in Basic Mode

1. On the policy **Attributes** tab, select **VMware** for the policy type.
2. On the policy **VMware** tab, select a VMware backup host.

   Review the other options on the **VMware** tab.

   See "Backup options on the VMware tab" on page 73.
3. Make other policy selections as needed (for example, create a Schedule).
4. Click the **Clients** tab, and click **Select automatically through VMware Intelligent Policy query**.

   If you selected virtual machines manually in the **Browse for Virtual Machines** dialog, those virtual machines are removed from the policy.

5 To back up virtual machines in vCloud Director, click **Enable vCloud Director integration**.

More information is available on backups and restores into vCloud.

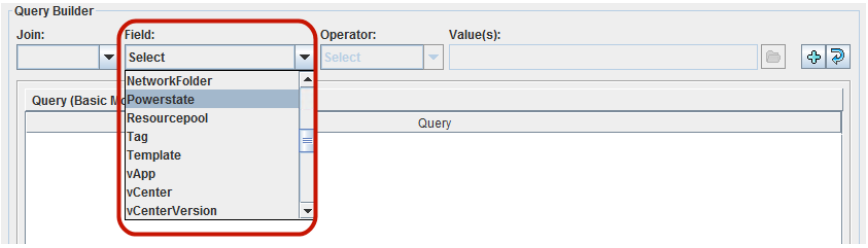
See "About NetBackup for vCloud Director" on page 262.

Note: Enable vCloud Director integration makes several vCloud Director keywords available in the policy Query Builder Field, for rule-based selection of virtual machines. If this option is not selected, NetBackup cannot use the vCloud keywords to locate virtual machines in vCloud Director, and the backup fails.

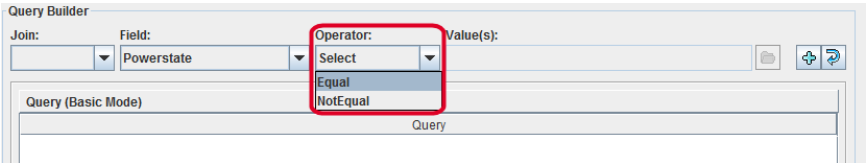
---

6 To create a rule, make selections from the pull-down menus.

For the first rule, you can start with the **Field** pull-down, depending on the type of rule. (For the first rule, the only selections available for the **Join** field are blank (none), or NOT.)

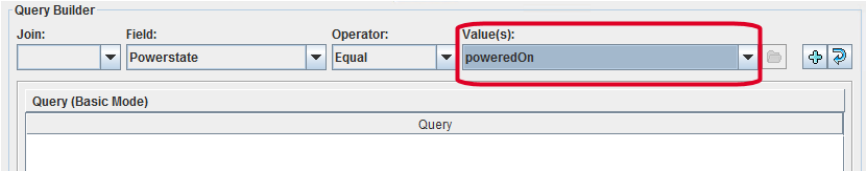


Then make a selection for **Operator**:

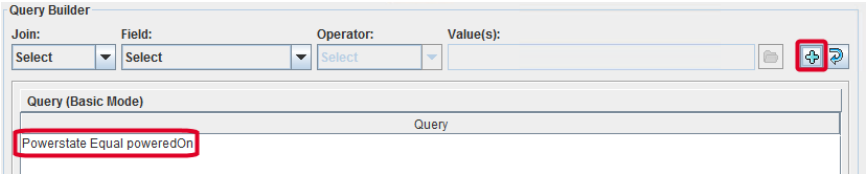


For the **Value(s)** field: Click the folder icon to browse for values, enter the value manually, or in some cases use the **Value(s)** drop-down (as in this example). The characters you enter manually in the **Values** field must be enclosed in single quotes or double quotes. Note that browsing for values may take some time in large virtual environments.

See “Query Builder field reference” on page 129.



7 Click the plus sign to add the rule to the **Query** pane.



8 Create more rules as needed.

See “Query Builder field reference” on page 129.

See “Examples for the NetBackup Query Builder” on page 118.

9 To see which virtual machines NetBackup currently selects based on your query, click **Test Query**.

On the Test Query screen, the Virtual machines in your current environment that match the rules for selection in the policy are labeled INCLUDED. Note however that the Test Query option does not create the backup list for the policy. When the next backup runs from this policy, NetBackup re-discovers virtual machines and consults the query rules. At that time, NetBackup backs up the virtual machines that match the query rules.

The list of virtual machines is saved but the virtual machines are not displayed in the policy's **Clients** tab.

See “Test Query screen for VMware” on page 141.

10 You can specify how long NetBackup uses the latest query results as the backup list for future executions of the policy. Set the time period in **Reuse VM selection query results for**.

The default is 8 hours.

More information is available on this setting:

See “About the Reuse VM selection query results option” on page 366.

11 To create queries manually instead of using the pull-down menus, click **Advanced Mode**.

See “Using the Query Builder in Advanced Mode” on page 116.

Editing an existing query in Basic Mode

You can use the Query Builder to enter rules for the automatic selection of VMware virtual machines for backup.

Note: VMware policies can also be configured from the NetBackup web UI. To do so, on the left navigation pane, click **Protection > Policies**, and then select a listed VMware policy to change it. Or click **+Add**, enter a **Policy name**, and select **VMware** from the **Policy type** drop-down list.

In the NetBackup web UI, you must use OData keywords and OData operators in query rules:

See “Query Builder field reference” on page 129.

To edit an existing query in Basic Mode

1. Click on the query rule you want to change and click **Edit**.
2. Make selections in the pull-down menus.
3. Click the save option (diskette icon).
4. To delete a rule, click on it and click **Remove**.

See "Using the Query Builder in Advanced Mode" on page 116.

Using the Query Builder in Advanced Mode

You can use the Query Builder to enter rules for the automatic selection of VMware virtual machines for backup.

The Query Builder's Advanced Mode provides more flexibility in crafting rules for virtual machine selection, including the use of parentheses for grouping.

Note: VMware policies can also be configured from the NetBackup web UI. To do so, on the left navigation pane, click **Protection > Policies**, and then select a listed VMware policy to change it. Or click **+Add**, enter a **Policy name**, and select **VMware** from the **Policy type** drop-down list.

In the NetBackup web UI, you must use OData keywords and OData operators in query rules:

See "Query Builder field reference" on page 129.

To use the Query Builder in Advanced Mode

1. Set up a VMware policy and specify a VMware backup host or backup media server.

   For assistance, you can refer to the first few steps of the following procedure:

   See "Configuring automatic virtual machine selection" on page 111.
2. Click the **Clients** tab.
3. Click **Select automatically through VMware Intelligent Policy query**.
4. Beneath the Query Builder pane, click **Advanced Mode**.

5 You can use the Query Builder drop-down menus to add query rules. You can also type in rules manually.

Here are a few example queries:

```
VMFolder Contains "mango"

Datastore StartsWith "Acc" OR Datastore StartsWith "Prod"

vCenter Contains "ROS" AND ESXserver Equal "VM_test1" AND
Powerstate Equal poweredOn
```

6 To insert a rule between existing rules, place the cursor where you want the new rule to start and type it in.

When you create a rule with the drown-down menus, it appears at the end of the query. You can cut and paste it into the proper location.

7 To establish the proper order of evaluation in compound queries, use parentheses to group rules as needed. Compound queries contain two or more rules, joined by AND, AND NOT, OR, or OR NOT.

See "AND vs. OR in queries" on page 117.

See "Order of operations in queries (precedence rules)" on page 123.

See "Parentheses in compound queries" on page 124.

AND vs. OR in queries

The **Join** field in the Query Builder provides connectors for joining rules (AND, AND NOT, OR, OR NOT). The effect of AND versus OR in the Query Builder may not be obvious at first glance.

In essence, AND and OR work in this way:

- AND limits or restricts the scope of the query.
- OR opens up the query to an additional possibility, expanding the scope of the query.

Note: Do not use AND to join the rules that are intended to include additional virtual machines in the backup list. For instance, AND cannot be used to mean "include virtual machine X AND virtual machine Y."

For example: To include the virtual machines that have either "vm1" or "vm2" in their names, use OR to join the rules:

```
Displayname Contains "vm1"
OR Displayname Contains "vm2"
```

If you use AND to join these rules:

```
Displayname Contains "vm1"
AND Displayname Contains "vm2"
```

the result is different: the backup list includes only the virtual machines that have both vm1 and vm2 in their names (such as "acmevm1vm2"). A virtual machine with the name "acmevm1" is not included in the backup.

Table 6-7 provides the examples with AND and OR.

Table 6-7 Queries with AND, OR

Query	Description
Displayname Contains "vm1" OR Displayname Contains "vm2"	This query selects any virtual machine that has either vm1 or vm2 in its display name. For example, this query selects both "seabizvm1" and "seabizvm2" for backup.
vCenter Equal "vCenterServer_1" AND Datacenter Equal "dc_A" AND ESXserver Equal "prod" AND VMHostName Contains "manu"	This query is very specific. Virtual machines with the host names that contain "manu" are included in the backup only if: they reside in vCenter server "vCenterServer_1", datacenter "dc_A", and ESX server "prod". The virtual machines that do not reside in that hierarchy are not included. For example: if a virtual machine resides in "vCenterServer_1" and datacenter "dc_A", but not in ESX server "prod", that virtual machine is not included.
vCenter Equal "vCenterServer_1" OR Datacenter Equal "dc_A" OR ESXserver Equal "prod" OR VMHostName Contains "manu"	This query uses the same keywords and values, but combines them with OR. The result may be a much larger list of virtual machines. A virtual machine that meets any of these rules is included: ■ Any virtual machines in vCenter "vCenterServer_1". Their host names, datacenter, or ESX server do not matter. ■ Any virtual machines in datacenter "dc_A". Their host names or server do not matter. ■ Any virtual machines in ESXserver "prod". Their host names, datacenter, or vCenter server do not matter. ■ Any virtual machines with a host name that contains "manu". Their server or datacenter do not matter.

Examples for the NetBackup Query Builder

The following table provides example query rules.

To use the Query Builder, you must click **Select automatically through VMware Intelligent Policy query** on the **Clients** tab.

Click **Advanced** to see the query rule in Advanced Mode. Only Advanced Mode supports the use of parentheses for grouping sets of rules.

See "Using the Query Builder in Advanced Mode" on page 116.

Note: In the NetBackup web UI, you must use OData keywords and OData operators in query rules:

See "Query Builder field reference" on page 129.

Another topic is available on the difference between AND and OR in a query.

See "AND vs. OR in queries" on page 117.

Table 6-8 Query Builder examples

VIP Example query	OData example query *	Query result when backup job executes
No query rules specified (Query pane is empty)	No query rules specified (Query pane is empty)	All virtual machines are added to the backup list. Exceptions are those that do not have a host name, or that have invalid characters in the display name. See "Effect of Primary VM identifier parameter on Selection column in Test Query results" on page 144.
Displayname Contains "prod"	contains(displayName, 'prod')	All virtual machines with the display names that contain the string "prod" are added to the backup list. See "Effect of Primary VM identifier parameter on Selection column in Test Query results" on page 144.
powerstate Equal "poweredOn"	powerState eq 'poweredOn'	Any virtual machine that is turned on is added to the backup list.
VMGuestOS Equal "windows7Guest"	vmGuestOs eq 'windows7Guest'	All virtual machines with a guest OS of Windows 7 are added to the backup list.
DisplayName AnyOf "grayfox7","grayfox9"	displayName in ('grayfox7', 'grayfox9')	The virtual machines named "grayfox7"and "grayfox9" are added to the backup list. (Note that each value must be enclosed in its own quotes, with a comma in between.)
powerstate Equal "poweredOn" AND Datastore Equal "Storage_1" AND VMGuestOS Equal "rhel4Guest"	powerState eq 'poweredOn' and datastoreName eq 'Storage_1' and vmGuestOs eq 'rhel4Guest'	In datastore Storage_1: any virtual machine that is turned on and has a guest OS of Red Hat Linux 4 is added to the backup list.

Table 6-8 Query Builder examples *(continued)*

VIP Example query	OData example query *	Query result when backup job executes
vCenter Equal "vCenterServer_1" AND ESXserver Contains "prod"	vCenter eq 'vCenterServer_1' and contains(host, 'prod')	In the vCenter server vCenterServer_1, virtual machines that are in ESX servers with names containing "prod" are added to the backup list.
Cluster Equal "VMcluster_1" AND ESXserver AnyOf "ESX_1","ESX_2","ESX_3" AND VMHostName Contains "Finance"	cluster eq 'VMcluster_1' and host in ('ESX_1', 'ESX_2', 'ESX_3') and contains(hostName, 'Finance')	In cluster VMcluster_1, all virtual machines with the host names that contain "Finance", in ESX servers ESX_1, ESX_2, ESX_3, are added to the backup list.
VMFolder StartsWith "Prod" OR VMFolder NotEqual "VM_test"	startswith(vmFolder, 'Prod') or vmFolder ne 'VM_test'	For any folder whose name starts with "Prod" or whose name is not "VM_test", add its virtual machines to the backup list.
Examples with IsSet		See "The IsSet operator in queries" on page 120.
Datacenter Contains "prod" AND Tag Equal "Finance"	contains(datacenter, 'prod') and tagName eq 'Finance'	This query selects any virtual machine where the Datacenter contains "prod" and the user-specified tag is "Finance".
Datacenter Equal "prod" AND NOT Tag Equal "Test"	datacenter eq 'prod' and not (tagName eq 'test')	Selects virtual machines where Datacenter is "prod" but excludes any virtual machines that have the user-specified tag "Test".

* Use OData keywords only when you build queries with the NetBackup web UI.

The IsSet operator in queries

In a query, you can use the IsSet operator to ensure that certain virtual machines are included or excluded from the backup.

For example: if the **Primary VM identifier** parameter is set to VM hostname, NetBackup is unable to identify virtual machines for backup that do not have a host name. You can use IsSet to exclude such virtual machines from the backup list.

Table 6-9 Examples of queries with the IsSet operator

Query rules with IsSet operator	OData query rules with IsSet operator *	Effect of the query on virtual machine selection
Cluster Contains "dev" AND VMDNSName IsSet	contains(cluster, 'dev') and dnsName ne null	INCLUDED: Any virtual machine in a cluster that has a name that contains the string "dev" if the virtual machine also has a VMware DNS name. EXCLUDED: Any virtual machines that do not have a VMware DNS Name. Without VMDNSName IsSet in this query, virtual machines without a DNS name cannot be excluded. They would be listed as FAILED.
Displayname Contains "prod" AND VMHostName IsSet	contains(displayName, 'prod') and hostName ne null	INCLUDED: Any virtual machine with a display name that contains the string "prod" if the virtual machine also has a host name. EXCLUDED: Any virtual machines that do not have host names. Without VMHostName IsSet in this query, virtual machines without a host name cannot be excluded. They would be listed as FAILED.

* Use OData operators only when you build queries with the NetBackup web UI.

The policy's **Primary VM identifier** parameter has an important effect on which virtual machines NetBackup can back up. This parameter affects the test query results.

See "Effect of Primary VM identifier parameter on Selection column in Test Query results" on page 144.

About selecting virtual machines by means of multiple policies

If your virtual environment has many virtual machines with inconsistent naming conventions, you may need multiple policies working in tandem. It may be difficult to create a single policy that automatically selects all the virtual machines that you want to back up.

For this situation, configure several policies such that each policy backs up a portion of the environment. One policy backs up a particular set or group of virtual machines, such as those that have host names. A second policy backs up a different group of virtual machines that were not backed up by the first policy, and so forth. When all the policies have run, all the virtual machines are backed up.

The following table describes the policies that are designed to back up the virtual environment in three phases. Note that each policy relies on a different setting for the **Primary VM identifier** parameter.

Table 6-10 Three policies that back up virtual machines in phases

Policy	Query Builder rules	OData Query Builder rules *	Backup result
First policy **Primary VM identifier** parameter: VM hostname	VMHostName IsSet	hostName ne null	This policy backs up all virtual machines that have a host name. Any virtual machines that do not have a host name are excluded from the backup.
Second policy **Primary VM identifier** parameter: VM display name	NOT VMHostName IsSet AND VMHasVDSName Equal 'TRUE'	not (hostName ne null) and vmHasVdsName eq 'TRUE'	This policy backs up all virtual machines that do not have a host name but that do have a valid display name. Any virtual machines that do not have a host name or a valid display name are excluded from the backup. See "NetBackup character restrictions for the Primary VM identifier" on page 37.
Third policy **Primary VM identifier** parameter: VM UUID	NOT VMHostName IsSet AND NOT VMHasVDSName Equal 'TRUE'	not (hostName ne null) and not(vmHasVdsName eq 'TRUE')	This policy backs up the virtual machines that were not backed up by the first two policies. This policy selects the virtual machines that do not have a host name or a valid display name, but that do have a UUID.

* Use OData operators only when you build queries with the NetBackup web UI.

More information is available on the **Primary VM identifier** parameter and its effect on virtual machine selection.

See "Effect of Primary VM identifier parameter on Selection column in Test Query results" on page 144.

Order of operations in queries (precedence rules)

The information in this topic is for advanced users who understand precedence in programming languages. In the Query Builder, the order in which operations occur can determine which virtual machines are selected and backed up.

The following table lists the order of operations, or precedence, from highest to lowest (7 is the highest). For example, an operation with a precedence of 6 (such as Contains) is evaluated before an operation with a precedence of 5 (such as Greater).

Table 6-11 Order of operations

Operation	Description	Precedence
!x	Produces the value 0 if x is true (nonzero) and the value 1 if x is false (0).	7
x Contains y	Does y exist somewhere in x	6
x StartsWith y	Does x start with y	6
x EndsWith y	Does x end with y	6
x AnyOf list	Does x appear in list	6
x Greater y	Is x greater than y	5
x GreaterEqual y	Is x greater than or equal to y	5
x Less y	Is x less than y	5
x LessEqual y	Is x less than or equal to y	5
x Equal y	Is x equal to y	4
x NotEqual y	Is x not equal to y	4
Not x	operator produces the value 0 if x is true (nonzero) and the value 1 if x is false (0).	3
x And y	True if both x and y are true	2
x OR y	True if either x or y are true	1

Note the following:

- AND has a higher precedence than OR.
  In the Query Builder's Advanced Mode, you can use parentheses to change the order of evaluation in the rules that use AND or OR.

See “Parentheses in compound queries” on page 124.

- In the Query Builder's Advanced Mode, you can combine two or more operations in a single rule without AND or OR to join them. Precedence determines the order in which the operations are evaluated within the rule.
  Example of a rule that includes three operations:

  ```
  Displayname StartsWith “L” NotEqual Displayname contains “x”
  ```

  This rule selects the following virtual machines:
  Virtual machines with the names that start with L but do not contain x.
  Virtual machines with the names that do not start with L but that do contain x.
  Explanation: The StartsWith and Contains operations have a precedence of 6, whereas NotEqual has a lower precedence of 3. Starting on the left, the StartsWith operation is evaluated first and the Contains operation is evaluated next. The last operation to be evaluated is Not Equal.

See “Using the Query Builder in Advanced Mode” on page 116.

Parentheses in compound queries

You can use the Query Builder to make precise queries containing as many rules as necessary to identify the appropriate virtual machines. In a query such as powerstate Equal "poweredOn", the result of the query is easy to predict: only the virtual machines that are turned on are included in the backup. But if several rules are combined with AND and OR, the result may not be obvious. This kind of query is called a compound query. Compound queries contain two or more rules, joined by AND, AND NOT, OR, or OR NOT.

The order in which the Query Builder evaluates compound rules affects the outcome of the query. Grouping the rules with parentheses can change the order of evaluation and thus the outcome of the query.

The examples in the following table demonstrate how the Query Builder evaluates compound queries with and without parentheses.

Note: Only the Query Builder's Advanced Mode supports the use of parentheses.

Table 6-12 Examples of compound queries with and without parentheses

Example query	The following virtual machines are selected
ESXServer Equal "ESX001" OR Folder Equal "FolderEngA" AND powerstate Equal ON	All virtual machines under ESX001 (regardless of power state), and virtual machines under FolderEngA that are turned on To select only the virtual machines that are turned on in the ESX server and in the folder, use parentheses (see next example).
(ESXServer Equal "ESX001" OR Folder Equal "FolderEngA") AND powerstate Equal ON	All the virtual machines that are turned on in ESX001 and in FolderEngA.

Query rules for resource pools

If the resource pool that you query is nested, the choice of Operator determines which virtual machines in the resource pool hierarchy are discovered.

For example, assume the following hierarchy of resource pools that contain virtual machines:

```
Res/ResourcePool_1
                VM1
                VM2
                /ResourcePool_2
                            VM3
                            VM4
                            /ResourcePool_3
                                        VM5
                                        VM6
```

where ResourcePool_1 contains virtual machines VM1 and VM2, and so forth.

The following table shows the query results with the Contains, Equal, StartsWith, and EndsWith operators. (Other operators can be used.)

Note: If you want the query to include all virtual machines in a hierarchy of nested resource pools, do not use Equal as the Operator.

Table 6-13 Example rules for nested resource pools

Query rule	Included virtual machines
Resourcepool Contains "Res/ResourcePool_1"	Includes all the virtual machines in the three resource pools (VM1 through VM6).

Table 6-13 Example rules for nested resource pools *(continued)*

Query rule	Included virtual machines
Resourcepool Equal "Res/ResourcePool_1"	Includes only the virtual machines that are in ResourcePool_1 (VM1, VM2). Virtual machines in the sub-pools are not included (VM3 through VM6).
Resourcepool Equal "Res/ResourcePool_1/ResourcePool_2"	Includes only the virtual machines that are in ResourcePool_2 (VM3, VM4).
Resourcepool StartsWith "Res/ResourcePool"	Includes all the virtual machines in the three resource pools (VM1 through VM6).
Resourcepool StartsWith "Res/ResourcePool_1/ResourcePool_2"	Includes only the virtual machines that are in ResourcePool_2 and 3. Virtual machines in ResourcePool_1 are not included.
Resourcepool EndsWith "ResourcePool_2"	Includes the virtual machines in ResourcePool_2 (VM3, VM4) but not in ResourcePool_1 or 3.

These examples also apply to host folders.

See “Query rules for datacenter folders (host folder)” on page 126.

Query rules for datacenter folders (host folder)

In NetBackup terminology, a host folder is a folder that has been defined within a VMware datacenter. A host folder can contain ESX servers or clusters, as well as other folders. For example:

```
Folder_1
       ESX1
       ESX2
       subfolder_A
                 ESX3
                 ESX4
       subfolder_B
                 ESX_5
                 ESX_6
```

If you want NetBackup to select all the virtual machines within the top-level folder and any subfolders, use the Contains or StartsWith operator. For example:

HostFolder Contains "Folder_1"

Note: If you want the query to include all virtual machines in the hierarchy of folders, do not use Equal as the Operator.

If you want NetBackup to select the virtual machines within a subfolder only (such as subfolder_A), use the Contains or Equal operator. For example:

HostFolder Equal "Folder_1/subfolder_A"

In this case, NetBackup includes only the virtual machines that reside on servers ESX3 and ESX4.

For host folders, these operators work the same as they do for resource pools. For further query builder examples, refer to the following topic (substitute host folder for resource pool in the examples):

See "Query rules for resource pools" on page 125.

Note: If an ESX cluster is not contained within a folder and you click the browse for values button: The ESX cluster name appears in the **Select From List** dialog.

Query rules for duplicate names

If you have clusters, datastores, or virtual machine display names that have duplicates elsewhere in your virtual environment, note: The query rules must specify the parent datacenter or host folder to avoid conflicts during discovery. (A host folder is one that has been defined within a datacenter.)

Take the following example of duplicate virtual machine names:

```
Folder_1
       ESXi_prod
              VM_1
Folder_2
       ESXi_mrkt
               VM_1
```

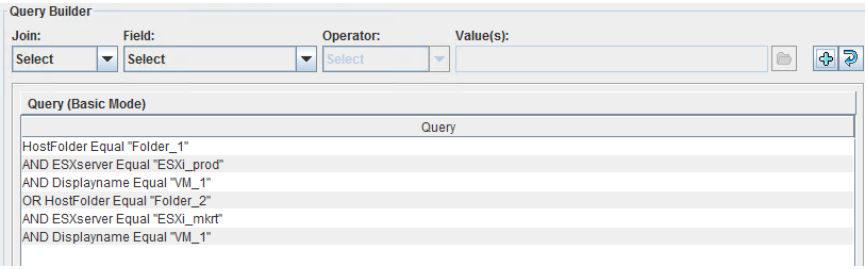
To back up `ESXi_prod/VM_1` but not `ESXi_mrkt/VM_1`, use the following query:

```
HostFolder Equal "Folder_1"
AND ESXserver Equal "ESXi_prod"
AND Displayname Equal "VM_1"
```

To back up only `ESXi_mrkt/VM_1`, use the following query:

```
HostFolder Equal "Folder_2"
AND ESXserver Equal "ESXi_mrkt"
AND Displayname Equal "VM_1"
```

Note: To back up both of these virtual machines from the same policy, include both of these rules in the policy, as follows:



Instead of `Equal`, you can use other field values, such as `Contains`.

See "Query rules for datacenter folders (host folder)" on page 126.

Query rules for tags

Be aware of the following rules when you use **tags** in your queries:

- If you use VMware tags, you can base your backup selections on these tags. Be aware these tags are case-sensitive, so `UNIX` is different from `unix`.
- When NetBackup uses tags to select virtual machines, the selection is based only on tag names. The selection is independent of the category.
  Example:
  - `Virtual_machine_1` has a user-specified tag `HR` from the category `production`.
  - `Virtual_machine_2` has a user-specified tag `HR` from the category `test`.

  Queries that select virtual machines with the tag `HR` select both virtual machines.
- NetBackup uses a different VMware interface to access tag information from vCenter Servers than is used for other query fields. Therefore, tag related calls to the vCenter Server execute only if they are required. Calls are skipped if the query is satisfied without the tag information. NetBackup only collects this information once per vCenter Server. NetBackup collects tag metadata as part of virtual machine backup, but it collects tag metadata only from those vCenter Servers for which a virtual machine is selected. If no virtual machine is selected from a vCenter Server and tags are not used in the query then tag metadata is not collected from that vCenter Server.

- Example 1: `Tag Equal "Production" OR Powerstate Equal poweredOn`
- Example 2: `Powerstate Equal poweredOn OR Tag Equal "Production"`

In Example 1, NetBackup retrieves virtual machine data as well as tag data from each virtual server for which it has credentials.

In Example 2, NetBackup retrieves virtual machine data for each virtual server for which it has credentials. But NetBackup only needs to retrieve tag data for virtual machines where the `Powerstate` is not equal to `poweredOn`.

Query Builder field reference

You can use the Query Builder to enter rules for the automatic selection of VMware virtual machines for backup.

Note: You can configure and manage VMware policies with the NetBackup web UI. In the web UI, the Query Builder uses OData keywords and operators. Otherwise, the Query Builder functions the same way as in the NetBackup Administration Console.

Table 6-14 describes the drop-down fields and options for creating rules in the Query Builder.

Table 6-14 Query Builder drop-down options: Join, Field, Operator, Value(s)

Query Builder drop-down fields	Description
Join	Selects a connector to join rules. For the first rule, choices are blank (none) or NOT. After you add a rule, the available connectors are AND, AND NOT, OR, OR NOT.
Field	Selects a parameter on which to build the rule. Select one from the list (scroll down for additional parameters). You can type the first character to speed up selection. For example, on entering “d”, the list moves to first entry starting with "d". Another entry of "d" moves through the list to the next entry starting with "d". The selected entry is automatically filled in. See Table 6-15 on page 130.
Operator	Selects an operator. The available operators depend on the parameter that is selected for **Field**. See Table 6-16 on page 139.

Table 6-14 Query Builder drop-down options: Join, Field, Operator, Value(s) *(continued)*

Query Builder drop-down fields	Description
Value(s)	Specifies a value for the **Field** parameter. The **Value** field allows manual entry. It may also be a drop-down, depending on the selections that are made in the other fields. For manual entry, you can specify multiple comma-separated values. See Table 6-17 on page 141.
	Allows browsing for specific values, depending on the selections that are made in the other drop-down fields.
	Adds the current drop-down selections to the **Query** pane as a new rule.
	Blanks out the drop-down fields.

Field (keywords)

Table 6-15 describes the keywords available in the **Field** drop-down. The table also indicates whether the values for each keyword (in the **Values** field) are case-sensitive.

Note that the inclusion or exclusion of virtual machines is not determined by the **Field** keyword alone, but depends on the rule you construct: the combination of Join, Field, Operator, and Values.

Table 6-15 Keywords in the **Field** drop-down

Field keyword	OData field keyword *	Data type	Description
Annotation	annotation	Alphanumeric string	The text that is added to virtual machine annotations in vSphere Client. Values are case-sensitive.
AssetGroup	assetGroup		NEW

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description
Cluster	cluster	Alphanumeric string	The name of the cluster (a group of ESX servers) that the virtual machine is configured in. Values are not case-sensitive. **Note:** A virtual machine may be assigned to an ESX server that is not in a cluster. Note also that in VMware, a cluster name need only be unique within a datacenter path.
Datacenter	datacenter	Alphanumeric string	The name of the VMware datacenter. Values are not case-sensitive.
DatacenterPath	datacenterPath	Alphanumeric string	The folder structure that defines the path to a datacenter. Use this option if the datacenter name that you want to filter on is not unique in your environment. Values are case-sensitive.
Datastore	datastoreName	Alphanumeric string	The name of the datastore. Values are case-sensitive. **Note:** Multiple ESX servers can share access to the same datastore. Also, a datastore name can be duplicated between multiple ESX servers. Use DatacenterPath or ESXserver to uniquely identify the datacenter.
DatastoreCluster	datastoreCluster	Alphanumeric string	The name of the datastore cluster that contains the datastores. Values are not case-sensitive.
DatastoreFolder	datastoreFolder	Alphanumeric string	The name of the folder that contains the datastores. Values are not case-sensitive.
DatastoreNFSHost	datastoreNfsHost	Alphanumeric string	The name of the datastore's NFS host. Values are not case-sensitive.

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description
DatastoreNFSPath	datastoreNfsPath	Alphanumeric string	The folder structure that defines the path to an NFS datastore. Use this option if the NFS host name of the datastore that you want to filter on is not unique in your environment. Values are not case-sensitive.
DatastoreType	datastoreType	Alphanumeric string	The type of the datastore. Values are NFS, NFS41, VMFS, vsan, and VVOL. Values are not case-sensitive.
Displayname	displayName	Alphanumeric string	The virtual machine's display name. Values are case-sensitive.
ESXserver	host	Alphanumeric string	The name of the ESX server. Values are not case-sensitive. The ESX host name must match the name as defined in the vCenter server.
HostFolder	hostFolder	Alphanumeric string	The folder path between the datacenter level and a cluster, ESX hosts, or a subfolder. If an ESX cluster is not contained within a folder and you click the browse for values button, note: The ESX cluster name appears in the **Select From List** dialog. Values are not case-sensitive. See "Query rules for datacenter folders (host folder)" on page 126.
InstanceUUID	instanceUuid	Alphanumeric string	The virtual machine's instance UUID. Example query: `InstanceUUID Equal "501b13c3-52de-9a06-cd9a-ecb25aa975d1"` Values are not case-sensitive.
Network	network	Alphanumeric string	The name of the network switch (on an ESX server) or distributed switch. Values are not case-sensitive.

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description
NetworkFolder	networkFolder	Alphanumeric string	The name of the folder that contains the network. Values are not case-sensitive.
Powerstate	powerState	Alphabetic	The power state of the virtual machine. Values are poweredOff, poweredOn, suspended.
Resourcepool	resourcePool	Alphanumeric string	The name of the resource pool. (A resource pool is similar to a vApp.) Values are case-sensitive. If a resource pool contains other resource pools (sub-pools), the choice of Operator determines whether virtual machines in the sub-pools are included. See "Query rules for resource pools" on page 125.
Tag	tagName	Alphanumeric string	The name of the tag. Values are case-sensitive. When NetBackup uses tags to select virtual machines, the selection is based only on tag names. The selection is independent of the category. See "Query rules for tags" on page 128.
Template	template	Boolean	TRUE if the virtual machine is a virtual machine template.

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description
vApp	vApp	Alphanumeric string	The name of the vApp. Values are case-sensitive. A vApp is a collection of virtual machines. vApps can also contain resource pools and other vApps. vApps are components of standalone ESX servers or of clusters. Like vSphere Client, NetBackup refers only to the top level of a vApp that contains sub vApps. For the following rule: `vApp Equal "vapp1"` if vapp1 has a sub vApp named "vapp2", any virtual machines in vapp1 or vapp2 are included. You cannot make a rule that refers specifically to vapp2.
vCDCatalog	vcdCatalog	Alphanumeric string	The name of the vCloud Director catalog. Values are not case-sensitive.
vCDIsExpired	vcdIsExpired	Alphabetic	Expired if the vCloud Director vApp or vApp template is expired. Possible values are Expired, Not Expired, and Unknown. Unknown indicates that an error occurred between vCloud Director and the vSphere environment. Examples are errors in provisioning or in a deletion operation.
vCDIsvAppTemplate	vcdIsvAppTemplate	Boolean	TRUE if the vCloud Director vApp is a template.
vCDOrg	vcdOrg	Alphanumeric string	The name of the vCloud Director organization. Values are not case-sensitive.
vCDOrgvDC	vcdOrgvDC	Alphanumeric string	The name of the organization virtual datacenter in vCloud Director. Values are not case-sensitive.

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description
vCDServer	vcdServer	Alphanumeric string	The name of the vCloud Director server. Values are not case-sensitive.
vCDvApp	vcdVapp	Alphanumeric string	The name of the vCloud Director vApp. Values are not case-sensitive.
vCenter	vCenter	Alphanumeric string	The name of the vCenter server. Values are not case-sensitive. The vCenter name that is specified in the Query Builder must match the name as entered in the Administration Console for NetBackup credentials. (**Media and Device Management > Credentials > Virtual Machine Servers**.) Note that a fully qualified domain name is recommended.
vCenterVersion	vCenterVersion	Alphanumeric string	The version of the vCenter Server. For example: 5.1.0, 5.5.0, 6.0.0 The possible values of this field are automatically updated and populated based on the environment. Only the versions of the vCenter servers that are registered with NetBackup are shown.
VMDNSName	dnsName	Alphanumeric string	The virtual machine DNS name in vSphere Client. Values are not case-sensitive.

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description

VMFolder	vmFolder	Alphanumeric string	The name of the VM folder (within a datacenter), including the path to the folder that contains the VMs.
			Values are not case-sensitive.
			For example, assume the following VM folders containing a total of 65 VMs:
			`vm\VM_backup_prod1 (contains 5 VMs)`
			`vm\VM_backup_prod1\cluster1 (contains 10`
			`vm\VM_backup_prod2 (contains 50 VMs)`
			To include the VMs in `vm\VM_backup_prod1` but not the VMs in `cluster1` or in any other folder:
			`VMFolder Equal "vm\VM_backup_prod1"`
			To include the VMs in `vm\VM_backup_prod1` and in its subfolder `cluster1`:
			`VMFolder Equal "vm\VM_backup_prod1" OR VMFolder StartsWith "vm\VM_backup_prod1`
			Note: The first backslash is an escape character that causes the following backslash to be interpreted as a literal character.
			To include all 65 VMs:
			`VMFolder StartsWith "vm\VM_backup_prod"`
			Note: Any VM that is in a path that begins with `vm\VM_backup_prod` is included.

VMGuestOS	vmGuestOs	Alphanumeric string	The virtual machine guest OS type that is recorded in vSphere Client. Values are case-sensitive.
VMHasIDE	vmHasIde	Boolean	TRUE if the virtual machine has IDE drives.
VMhasIndD	vmHasIndD		NEW

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description
VMHasMDS	vmHasMds	Boolean	TRUE if the virtual machine has multiple datastores. You can use this keyword to select any virtual machine that is configured to use more than one datastore.
VMHasNVME	vmHasNvme	Boolean	TRUE if the virtual machine has NVMe drives.
VMHasRDM	vmHasRdm	Boolean	TRUE if the virtual machine uses Raw Device Mapping (RDM).
VMHasRDMO	vmHasRdmo		NEW
VMHasSATA	vmHasSata	Boolean	TRUE if the virtual machine has SATA drives.
VMHasSnap	VMHasSnap	Boolean	TRUE if a VMware snapshot of the virtual machine is currently active.
VMHasVDSName	vmHasVdsName	Boolean	TRUE if the virtual machine has a display name that is valid for use as the host name.
VMHostName	hostName	Alphanumeric string	The virtual machine name that is derived from a reverse lookup of its IP address. Values are not case-sensitive.
VMIsConn	vmIsConn	Boolean	TRUE if the virtual machine is connected and available. For example: If a virtual machine's ESX server is down, that virtual machine is not connected.
VMVersion	vmVersion	Alphanumeric string	The VMware version of the virtual machine. Values are case-sensitive. For example: vmx-04, vmx-07, vmx-08.

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description
VMXDatastore	vmxDatastore	Alphanumeric string	The name of the vmx datastore (sometimes called the vmx directory or configuration datastore). Values are case-sensitive. More information on the vmx datastore is available. See "NetBackup for VMware terminology" on page 20.
VMXDatastoreFolder	vmxDatastoreFolder	Alphanumeric string	The name of the folder that contains the vmx datastores. Values are not case-sensitive.
VMXDatastoreNFSHost	vmxDatastoreNfsHost	Alphanumeric string	The name of the vmx datastore's NFS host. Values are not case-sensitive.
VMXDatastoreNFSPath	vmxDatastoreNfsPath	Alphanumeric string	The folder structure that defines the path to a vmx NFS datastore. Use this option if the NFS host name of the datastore that you want to filter on is not unique in your environment. Values are not case-sensitive.
VMXDatastoreType	vmxDatastoreType	Alphanumeric string	The type of the vmx datastore. Values are NFS or VMFS. Values are not case-sensitive.

Table 6-15 Keywords in the **Field** drop-down *(continued)*

Field keyword	OData field keyword *	Data type	Description
[vSphere custom attributes]	[vSphere custom attributes]	Alphanumeric string	The value of a custom attribute that is set in vSphere Client for one or more virtual machines. Note: in vSphere Client, the attribute must have a value for at least one virtual machine. The attribute type must be Virtual Machine. The values are case-sensitive. Custom Attribute based disk exclusion requires that you enter in NetBackup the credentials for the vCenter server or servers that host the VMs. ESXi server credentials are not sufficient. See "Adding NetBackup credentials for VMware" on page 45.

* Use OData keywords only when you build queries with the NetBackup web UI.

Operators

Table 6-16 describes the operators available in the **Operator** drop-down.

Table 6-16 Operators in the **Operator** drop-down

Operator	OData operator *	Description
AnyOf	in	Matches any of the specified values in the Value(s) field. For example: If the ESX servers in the Value(s) field are "ESX01","ESX02,"ESX03", AnyOf matches any ESX server that has one of those names. If the names of your servers are not identical to any of the specified values, no match occurs. A server named ESX01A is not a match.
Contains	contains	Matches the value in the Value(s) field wherever that value occurs in the string. For example: If the Value(s) entry is "dev", Contains matches strings such as "01dev", "01dev99", "devOP", and "Development_machine".
EndsWith	endswith	Matches the value in the Value(s) field when it occurs at the end of a string. For example: If the Value(s) entry is "dev", EndsWith matches the string "01dev" but not "01dev99", "devOP", or "Development_machine".

Table 6-16 Operators in the **Operator** drop-down *(continued)*

Operator	OData operator *	Description
Equal	eq	Matches only the value that is specified in the Value(s) field. For example: If the display name to search for is "VMtest27", Equal matches virtual machine names such as VMTest27 or vmtest27 or vmTEST27, and so forth. The name VMtest28 is not matched.
Greater	gt	Matches any value that is greater than the specified Value(s), according to the UTF-8 collating sequence.
GreaterEqual	ge	Matches any value that is greater than or equal to the specified Value(s), according to the UTF-8 collating sequence.
IsSet	ne null	Determines whether a value is returned for the **Field** keyword. Use IsSet with another rule as a condition, to ensure that the query selects the appropriate virtual machines. Note that you do not make an entry under Value(s) for a rule that uses IsSet. See "The IsSet operator in queries" on page 120. See "Effect of Primary VM identifier parameter on Selection column in Test Query results" on page 144. See "Test Query: Failed virtual machines" on page 143.
Less	lt	Matches any value that is less than the specified Value(s), according to the UTF-8 collating sequence.
LessEqual	le	Matches any value that is less than or equal to the specified Value(s), according to the UTF-8 collating sequence.
NotEqual	ne	Matches any value that is not equal to the value in the Value(s) field.
StartsWith	startswith	Matches the value in the Value(s) field when it occurs at the start of a string. For example: If the Value(s) entry is "box", StartsWith matches the string "box_car" but not "flatbox".

* Use OData operators only when you build queries with the NetBackup web UI.

Value(s)

Table 6-17 describes the characters that can be entered in the **Value(s)** field. The **Field** keyword determines case sensitivity.

Note: The character string you enter in the **Value(s)** field must be enclosed in single quotes or double quotes.

Table 6-17 Characters you can enter for Value(s)

Character types	String characters allowed
Alphanumerics	A to Z, a to z, 0 to 9, - (minus sign), and special characters. **Note:** Decimal numbers only.
Wildcards	* (asterisk) matches everything. For example: "*prod*" matches the string "prod" preceded or followed by any characters. ? (question mark) matches any single character. For example: "prod??" matches the string "prod" followed by any two characters.
Escape character	\ (backslash) escapes the wildcard or meta-character that follows it. For example: To search for a string that contains an asterisk (such as test*), enter "test*"
Quotation marks	Note: The characters you enter in Value(s) must be enclosed in single or double quotes. To search for a string that contains quotation marks, either escape each quote (\") or enclose the entire string in the opposite type of quotes. For example: To search for a string that includes double quotes (such as "name"), enter '"name"' (enclosing it in single quotes) or "\"name\""

Test Query screen for VMware

This screen lists the virtual machines that NetBackup discovered in your virtual environment when you clicked **Test Query**. Later changes in the virtual environment may affect which virtual machines match the query rules. For example: if virtual machines are added, the test results may not be identical to the virtual machines that are selected for backup when the backup runs.

When the next backup runs from this policy, the following occur: NetBackup re-discovers virtual machines, consults the query rules, and backs up the virtual machines that match the rules.

The list of backed up virtual machines is saved but the virtual machines are not displayed in the policy's **Clients** tab. You can use the Activity Monitor to view the virtual machine jobs, or you can run a **Virtual Client Summary** report in OpsCenter.

Note: An alternative to the Test Query screen is the `nbdiscover` command. For more information, see the *NetBackup Commands Reference Guide*.

See "Using the Activity Monitor to monitor virtual machine backups" on page 156.

See "Using OpsCenter to report on virtual machine backups" on page 160.

The **Test Query** function runs in the background. You can continue to configure the policy while the test runs. Any changes you make in the Query Builder however are not included in the currently running test. You must re-initiate the test to see the results of your Query Builder changes.

Table 6-18

Field	Description
Test query for policy	Lists the rules in the Query Builder that were used in this test. The rules are specified in the Query Builder on the policy **Clients** tab.
Test Query Results	**VM Name**: Shows the display name of all discovered virtual machines. **Selection**: Lists the virtual machines that were discovered, as follows: ■ **INCLUDED**: The virtual machine matches the rules in the query. ■ **EXCLUDED**: The virtual machine does not match the rules in the query. ■ **FAILED**: The virtual machine cannot be selected for backup because of a host name problem or other error. Also, the query cannot exclude the virtual machine. An explanation appears at the bottom of the **Test Query** screen. For example: `VM does not have a host name to use as a client name, display name =` See "Test Query: Failed virtual machines" on page 143. The operator IsSet can be used to filter out such virtual machines. More information is available on IsSet. See Table 6-16 on page 139. See "The IsSet operator in queries" on page 120.
Included: **Excluded:** **Failed:**	Gives a tally of how many virtual machines were included, excluded, or failed in the test.

See "Using the Activity Monitor to monitor virtual machine backups" on page 156.

See "About automatic virtual machine selection for NetBackup for VMware" on page 102.

See "Configuring automatic virtual machine selection" on page 111.

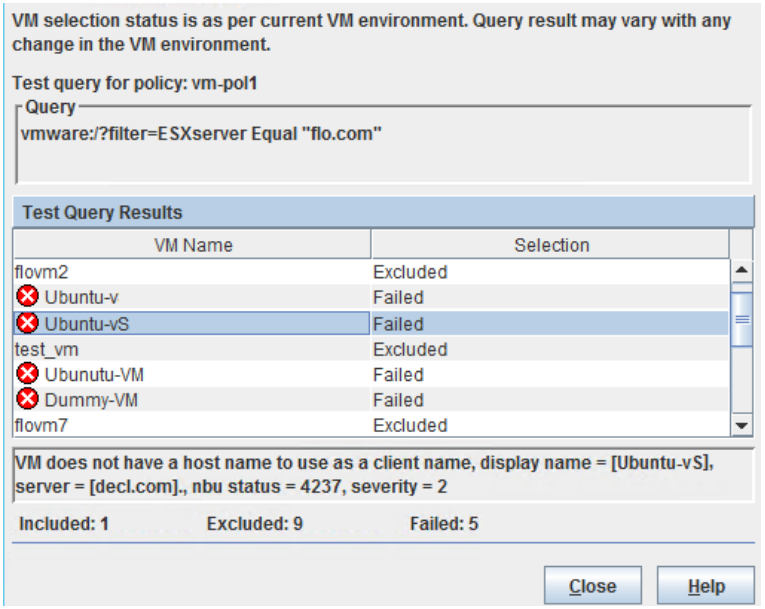
Test Query: Failed virtual machines

If the query rules cannot exclude a virtual machine, and that virtual machine cannot be selected for backup, it is marked as FAILED. The virtual machine is listed as not run in the job details log.

For example: the virtual machine does not have the type of name specified by the **Primary VM identifier** parameter (such as host name or display name). Or the virtual machine name contains invalid characters. In any case, a virtual machine that is listed as FAILED should be investigated: it may be one that you want to back up.

To see the reason for the failure, click on the virtual machine in the Test Query Results. An explanation appears at the bottom of the screen.

For example:



Explanation: The virtual machine that is listed as **Ubuntu-vS** in the example does not have a VMware host name. In the NetBackup policy, on the **VMware** tab, the **Primary VM identifier** parameter may be set to **VM hostname**. In that case, NetBackup cannot refer to the virtual machine by its host name and thus cannot back it up.

You can fix this problem in a couple of ways:

- Use vSphere Client to configure a host name for the virtual machine.

- To exclude the virtual machines that have no host name, construct a query with the IsSet operator.

See "The IsSet operator in queries" on page 120.

Effect of Primary VM identifier parameter on Selection column in Test Query results

The NetBackup policy's **Primary VM identifier** parameter tells NetBackup how to identify virtual machines. For example, if the parameter is set to **VM hostname**, NetBackup identifies virtual machines by their host names. If they do not have a host name, the policy cannot back them up.

The **Primary VM identifier** parameter has a direct effect on the query test results. Note that for each virtual machine, the query test result is one of three possibilities: INCLUDED, EXCLUDED, or FAILED.

If NetBackup cannot identify a virtual machine according to the **Primary VM identifier** parameter, one of two test results can occur:

- If the virtual machine is filtered out by the query rules, it is listed as EXCLUDED.
- If the virtual machine is not filtered out by the query rules, it is listed as FAILED. The following table gives the test query results from example combinations of the **Primary VM identifier** parameter and a query rule.

Table 6-19 Effect of Primary VM identifier parameter and query rules on test query results

Primary VM identifier setting on VMware policy tab	Query rule in Query Builder	OData query rule in Query Builder *	Test query result
VM hostname	VMHostName Contains "VM"	contains(displayName, 'VM')	INCLUDED: Any virtual machines with a host name that contains "VM". Since the Primary VM identifier parameter tells NetBackup to select the virtual machine by host name, it can back up the virtual machines. EXCLUDED: All other virtual machines.

Table 6-19 Effect of Primary VM identifier parameter and query rules on test query results *(continued)*

Primary VM identifier setting on VMware policy tab	Query rule in Query Builder	OData query rule in Query Builder *	Test query result
VM hostname	Displayname Contains "VM"	contains(displayName, 'VM') and hostName ne null	INCLUDED: Any virtual machines that have a host name and that have a display name that contains "VM". EXCLUDED: Any virtual machines that have a host name, but that do not have a display name containing "VM". FAILED: Any virtual machines that do not have a host name. Since the **Primary VM identifier** parameter is set to VM hostname, NetBackup cannot select the virtual machine for backup.
VM hostname	Displayname Contains "VM" AND VMHostName IsSet	contains(displayName, 'VM') and hostName ne null	INCLUDED: Any virtual machines that have a host name and that have a display name that contains "VM". EXCLUDED: All other virtual machines. The IsSet rule means that if a virtual machine does not have a host name, it is excluded.
VM hostname	Displayname Contains "VM" AND VMHostName IsSet OR Annotation Contains "test" AND NOT VMHostName IsSet	contains(displayName, 'VM') and hostName ne null or contains(annotation, 'test') and not (hostName ne null)	INCLUDED: ■ Any virtual machines that have a host name and that have a display name that contains "VM". ■ Any virtual machines without a host name that have an annotation that contains "test". EXCLUDED: All other virtual machines.

Table 6-19 Effect of Primary VM identifier parameter and query rules on test query results *(continued)*

Primary VM identifier setting on VMware policy tab	Query rule in Query Builder	OData query rule in Query Builder *	Test query result
VM display name	Displayname Contains "VM"	contains(displayName, 'VM')	INCLUDED: Any virtual machines with the display names that contain "VM". Since the Primary VM identifier parameter tells NetBackup to select the virtual machine by display name, it can back up the virtual machines. EXCLUDED: All other virtual machines.
VM display name	VMHostName Contains "VM"	contains(hostName, 'VM')	INCLUDED: Any virtual machines that have a display name and that have a host name that contains "VM". EXCLUDED: Any virtual machines that have a display name, but that do not have a host name containing "VM". FAILED: Any virtual machines that do not have a display name. Since the **Primary VM identifier** parameter is set to VM display name, NetBackup cannot select those virtual machines for backup.

* Use OData keywords only when you build queries with the NetBackup web UI.

Effect of Primary VM identifier parameter on VM Name column in Test query results

The policy's **Primary VM identifier** parameter affects the type of virtual machine name that appears in the **VM Name** column of the Test Query screen, as follows:

- If a virtual machine is EXCLUDED or FAILED, it is listed according to its virtual machine display name. The **Primary VM identifier** parameter does not matter.

- But if a virtual machine is listed as INCLUDED, note: The name that appears under **VM Name** is the type of name that is specified on the **Primary VM identifier** parameter.

  For example: If the **Primary VM identifier** parameter is VM hostname, the included virtual machine is listed according to its host name. Even if the query rule specified Display name (such as `Displayname Equal "vm1"`), the virtual machine appears on the Test Query screen by its host name.

See "Primary VM identifier options (VMware)" on page 76.

Refreshing the display of virtual environment changes in the Query Builder

By default, NetBackup waits one hour before the policy Query Builder detects changes in the virtual environment. Until one hour has passed, the Query Builder does not detect the changes when you click the "Load values" folder icon next to the **Value(s)** field. To make the changes immediately available to the **Value(s)** field, use the following procedure to refresh the display.

Note: The Query Builder's **Reuse VM selection query results for** option does not affect the display of virtual environment changes in the Query Builder. The reuse option determines how long NetBackup reuses the current backup list for future executions of the policy.

To refresh the Query Builder's view of the virtual environment (Windows):

1. On the Windows desktop of the local host, click **Start > Run** and enter `regedit`.
2. To be on the safe side, make a backup of the current registry (**File > Export**).
3. Go to **HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > Config** and create a key that is called `BACKUP`.
4. Under `BACKUP`, create a new DWORD that is called `xmlCacheLimit`.
5. Set this DWORD to the number of seconds for the refresh.

   A value of 15 allows the Query Builder to be refreshed after 15 seconds.
6. If the policy editor is open in the **NetBackup Administration Console**, close it and reopen it.

To refresh the Query Builder's view of the virtual environment (Linux):

1. On the Linux desktop of the local host, create (or open) the following file:

   `/usr/openv/netbackup/virtualization.conf`

2. Enter a new `dword` line under `[BACKUP]` to set the number of seconds for the refresh. For example:

   ```
   [BACKUP]
   "xmlCacheLimit"=dword:15
   ```

   This example allows the Query Builder to be refreshed after 15 seconds.

   Note: If the file already contains a `[BACKUP]` line, do not add another `[BACKUP]` line. Any other lines that already exist under `[BACKUP]` should remain as they are.

3. Save the file.
4. If the policy editor is open in the NetBackup Administration Console, close it and reopen it.

Reducing the time required for VM discovery in a large VMware environment

NetBackup VMware Intelligent Policies use query rules to automatically search and filter the vSphere environment. By default, the query rules search all the VMware servers in your environment. If the environment contains many VMware servers with many virtual machines, VM discovery may take a long time. You can speed up VM discovery by limiting the search to specific VMware servers or virtual machines.

The following is an example of a policy Query Builder rule that searches all VMware servers and all virtual machines:

```
vmware:/?filter=Displayname Contains "vm1"
```

To limit the search to particular servers or virtual machines, insert an additional expression in the Query Builder rule as explained in the following procedure.

To use the Administration Console to reduce the time required for VM discovery in a VMware environment

1. In the NetBackup Administration Console, open the VMware Intelligent Policy.
2. On the **Clients** tab of the policy, make sure **Select automatically through VMware Intelligent Policy query** is selected.
3. In the **Query Builder**, click **Advanced**.
4. Under **Query (Advanced Mode)**, create one or more rules to search for VMs in specific VMware servers or for specific virtual machines.

Be aware that to create two or more rules, you must be in **Advanced Mode** not **Basic Mode**. Additionally, each query rule must begin on its own line.

You can use the types of rules shown:

- To search for VMs in a particular VMware server
  `vmware://VMware_server?filter=filter`
- To search for a specific virtual machine on a particular VMware server
  `vmware://VMware_server/vm/virtual_machine_instance_uuid`

Chapter 7

Reduce the size of backups

This chapter includes the following topics:

- About reducing the size of VMware backups
- Block-level backup (BLIB): full vs incremental
- Deleting a vSphere Client snapshot

About reducing the size of VMware backups

NetBackup provides the following options for reducing the backup size for a VMware virtual machine:

Table 7-1 Options for reducing the virtual machine backup size

Option	Description
Block level incremental backup (BLIB)	BLIB reduces the size of backups (full and incremental) by tracking block-level changes. Only the blocks that have changed since the last full or incremental are included in the backup. For incremental backups, this option applies to cumulative and to differential backups. BLIB works with VMware's Changed Block Tracking in vSphere to track block-level changes in the virtual machine. The **Enable block-level incremental backup** option is enabled by default on the NetBackup policy **VMware** tab. NetBackup uses BLIB for storage optimization when the backup runs. **Note:** The first backup you run with BLIB must be a full backup. See "Block-level backup (BLIB): full vs incremental" on page 151. **Note:** BLIB works only with ESX 4.0 or later virtual machines at version vmx-07 or later. **Note:** If you used vSphere Client to manually create a VM snapshot and that snapshot is currently active, you may have to delete the snapshot. See "Deleting a vSphere Client snapshot" on page 152.
Exclusion of deleted blocks.	Reduces the size of virtual machine backups by excluding any deleted sectors in the file system on the virtual machine. To enable this option, click **Exclude deleted blocks** on the policy **VMware** tab. Refer to **Exclude deleted blocks** in the following topic: See "Optimizations options (VMware)" on page 74.

Block-level backup (BLIB): full vs incremental

When you use the **Enable block-level incremental backup** option in the policy, NetBackup uses VMware's Changed Block Tracking feature (CBT) to reduce the backup size.

This option reduces the size of full backups as well as the size of incremental backups, as follows.

Table 7-2 Block-level backup of the virtual machine: full vs incremental schedule

Type of backup	Optimization that is used in backup
Backup of entire virtual machine, with full schedule	Backs up only the blocks that have changed since the .vmdk was created. Note that the blocks that are not initialized are excluded from the backup.

Table 7-2 Block-level backup of the virtual machine: full vs incremental schedule *(continued)*

Type of backup	Optimization that is used in backup
Backup of entire virtual machine, with incremental schedule	Backs up only the blocks that have changed since the last backup, as follows: ■ For cumulative incrementals, BLIB backs up only the blocks that changed since the last full backup. ■ For differential incrementals, BLIB backs up only the blocks that changed since the previous backup of any kind. **Note:** On incremental backups, the **Enable block-level incremental backup** option backs up the changed files as well as their metadata. **Note:** VMware CBT may occasionally reset tracking of file changes in the virtual machine, such as after a power failure or hard shutdown. For the next backup, NetBackup reads all the data from the vmdk files and the backup takes longer than expected. If deduplication is enabled, the deduplication rate is lower than expected. The following VMware article contains more information on CBT: Changed Block Tracking (CBT) on virtual machines (1020128)

Deleting a vSphere Client snapshot

To use BLIB with NetBackup for VMware, you must delete an existing vSphere Client snapshot if both of the following are true:

- You used the vSphere Client interface to manually create a snapshot of the virtual machine and that snapshot is currently active.
- A NetBackup policy with the **Enable block-level incremental backup** feature had never been used to back up the virtual machine before you started the vSphere Client snapshot.

In this case, NetBackup cannot enable BLIB for the virtual machine. You must delete the vSphere Client snapshot. Then, when the NetBackup policy runs, BLIB is enabled.

More information is available on NetBackup block-level backups:

To delete a vSphere Client snapshot

1. In the vSphere Client interface, right-click on the virtual machine and select **Snapshot > Snapshot Manager**.
2. Select the snapshot and click **Delete**.
3. To back up the virtual machine with BLIB, you can now run a NetBackup policy that uses **Enable block-level incremental backup**.

   NetBackup backups from this policy continue to use storage optimization, even if you manually create a snapshot of the virtual machine using vSphere Client.

Chapter 8

Back up virtual machines

This chapter includes the following topics:

- Backing up virtual machines
- Using the Activity Monitor to monitor virtual machine backups
- Restarting jobs individually in the Activity Monitor
- Viewing NetBackup activity in vSphere Web Client or vSphere Client (HTML5)
- Using OpsCenter to report on virtual machine backups

Backing up virtual machines

Virtual machine backups initiate from a NetBackup policy. You can start the backup manually from a policy, or have it run automatically according to a schedule that is defined in the policy.

To create the policy, you can use the **Policies** utility in the NetBackup Administration Console, or the Policy Configuration Wizard.

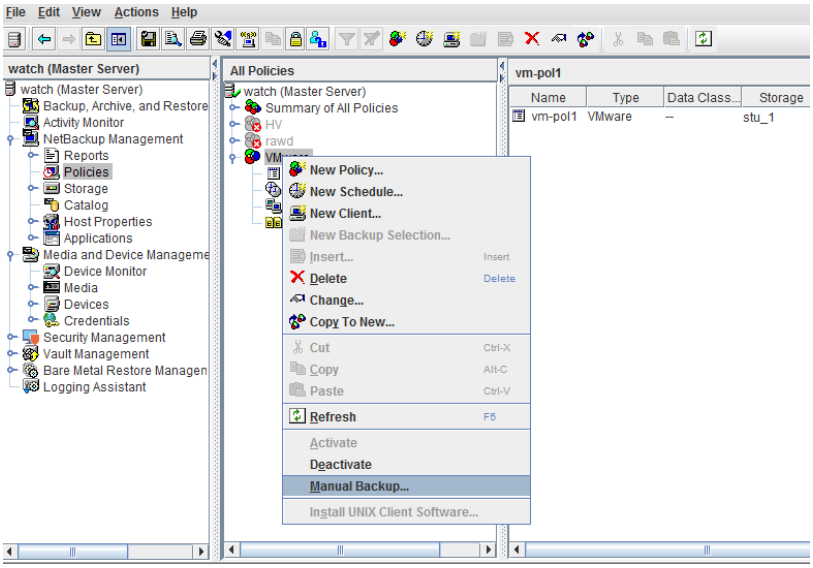
See “Configuring a VMware policy from the Policies utility” on page 68.

See “Configuring a VMware policy from the Policy Wizard ” on page 68.

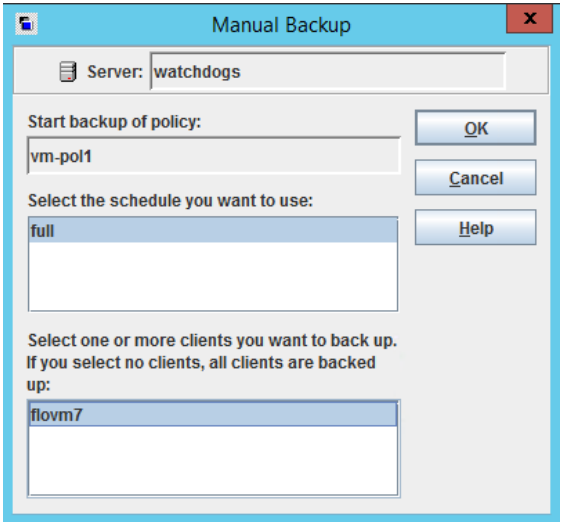
For further information on policies and backup schedules, see the "Creating backup policies" chapter of the *NetBackup Administrator's Guide, Volume I*.

To back up a virtual machine manually from an existing policy

1 Click on **Policies** in the NetBackup Administration Console, right-click on the policy, and click **Manual Backup...**.



The Manual Backup dialog appears.



2 Select the type of schedule for the backup.

3 Select the clients (virtual machines) to back up.

If the policy was configured for automatic selection of virtual machines, the Clients pane shows the VMware backup host rather than the virtual machines.

4 Click **OK** to start the backup.

5 To see the job progress, click **Activity Monitor** in the NetBackup Administration Console.

It may take a few moments for the job to appear in the Activity Monitor. Do not start another backup if a job does not immediately appear. If the job does not show up after a few moments, close and restart the NetBackup Administration Console.

Note that your VMware backup request launches more than one job. The first job automatically creates and deletes snapshots. This job has a dash (-) in the Schedule column. The second job backs up the virtual machine files from the snapshot.

Using the Activity Monitor to monitor virtual machine backups

You can use the NetBackup Activity Monitor to keep track of the VMware virtual machines that a policy backs up.

To monitor virtual machine backups

1 Click **Activity Monitor** in the left pane of the Administration Console.

2 Note each job as it appears by row.

If the policy selects virtual machines automatically (based on a query), the backup consists of three generations of jobs:

- The first job discovers the virtual machines. This job is labeled **Backup**. (This job is unique to policies that use a query to select virtual machines.)
- The discovery (**Backup**) job starts a child job to take a VMware snapshot of the virtual machine. A snapshot job is started for each virtual machine. Each of these jobs is labeled **Snapshot**.
- Each snapshot job starts a child job to back up the virtual machine. A backup job is started for each virtual machine. Each of these jobs is labeled **Backup**. The job flow is as follows:

```
discovery job --> snapshot job --> backup job
```

3 To trace the discovery job to the virtual machine backup jobs, note the **Job ID** and the **Parent Job ID** columns.

Job Id	Parent Job ID	Type	State	State Details	Status	Job Policy	Job Sched...	Client	Start Time
121	120	Backup	Active			vm-pol1	full	floblcl...	01/14/2016 15:35:34
120	119	Snapshot	Active			vm-pol1	-	floblcl...	01/14/2016 15:34:06
119	119	Backup	Active			vm-pol1	-	watch...	01/14/2016 15:33:53

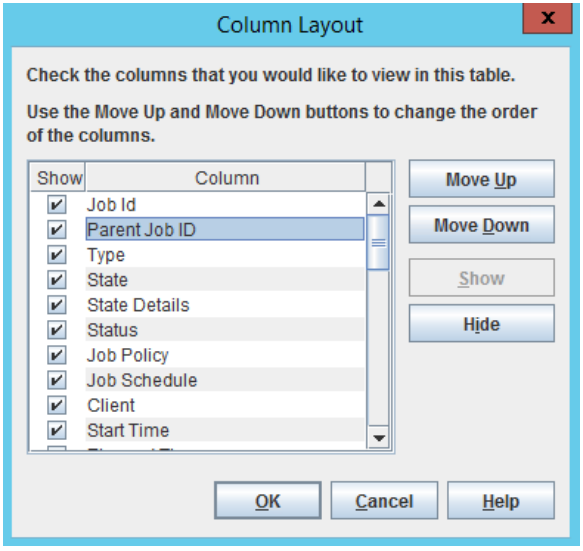
In this example, the discovery job is 119. Job 119 started job 120 (Snapshot). Job 120 started job 121 (Backup).

4 Right-click on the job row and click **Details**.

On the **Job Details** screen, click the **Detailed Status** tab for more information on the job.

5 If a column is not displayed in the Activity Monitor, or to re-arrange the columns, do the following:

- Right-click anywhere in the **Jobs** pane and click **Columns > Layout**.
- Click the row for the heading that you want to display, hide, or re-arrange (such as **Parent Job ID**).



- Use **Move Up**, **Move Down**, **Show**, and **Hide** as needed.
- Click **OK**. The columns should now be visible in the Activity Monitor.

See “Limit jobs per policy on the Attributes tab (for VMware)” on page 72.

Restarting jobs individually in the Activity Monitor

If the policy automatically selects virtual machines for backup, you can restart the virtual machine jobs individually. This feature is handy if the policy backs up a large number of virtual machines: you can restart one or more of the jobs individually rather than re-running the entire policy.

To restart jobs individually in the Activity Monitor

- In the Activity Monitor, right-click on the job and select **Restart Job**.

  In some cases, to restart a child job you may have to restart its parent job.

Viewing NetBackup activity in vSphere Web Client or vSphere Client (HTML5)

In VMware vCenter, NetBackup can record the backup activity for virtual machines. You can view the events in vSphere Web Client or vSphere Client (HTML5) at the level of any parent object (such as folder, datacenter, cluster, or host). You can also view the events for the virtual machine.

Note: The NetBackup plug-in is not required.

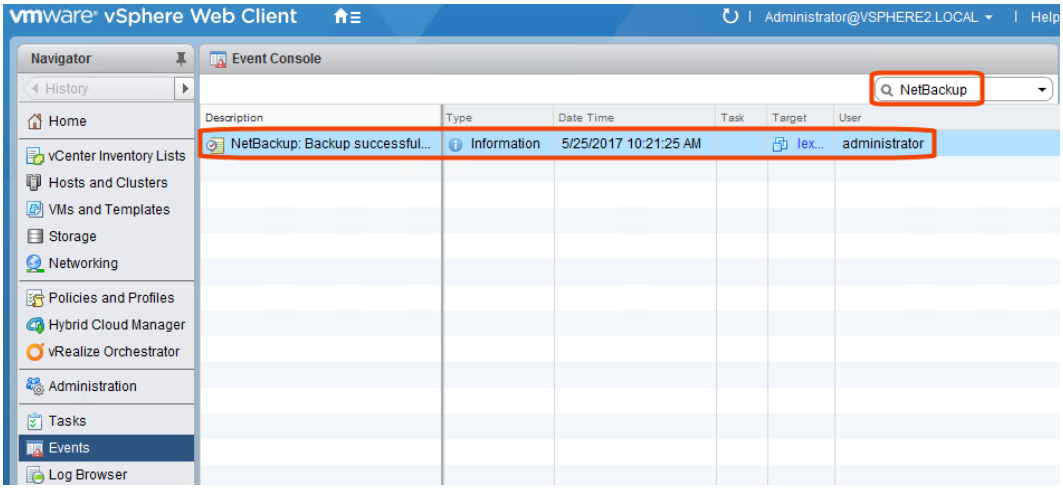
Make sure that the policy's **Post vCenter events** option is enabled:

See “VMware - Advanced Attributes dialog” on page 81.

To view backup events and the last backup time in vSphere Web Client

1. Open vSphere Web Client or vSphere Client (HTML5).
2. Go to **Home > Events**.

3 In the **Event Console**, enter `NetBackup` in the search field.



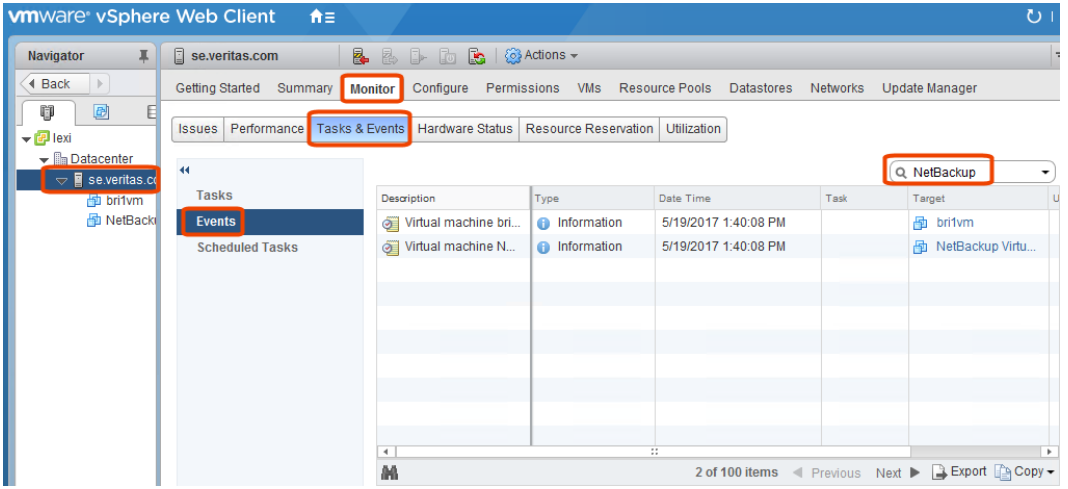
Each NetBackup event includes the following details:

Description	Shows the NetBackup operation that succeeded or failed, and includes policy details and duration. When you click on the row of the event, the **Event Details** pane shows the same information.
Type	The types are **Information** for a successful operation, and **Error** for a failed operation.
Date Time	The date and time of the event.
Task	Not used.
Target	The virtual machine that was backed up. Click on the virtual machine link to see the **Summary** tab. **Note:** On the **Summary** tab in vSphere 6.5, under **Custom Attributes**, the timestamp of the virtual machine's last backup is listed on the `NB_LAST_BACKUP` attribute.
User	The user that ran the backup.

4 To view backup events for a particular object (such as ESX host or VM), select the object and do the following:

- Click the **Monitor** tab.

- Click **Task & Events**.
- Click the **Events** view.
- Enter `NetBackup` in the search field.



Using OpsCenter to report on virtual machine backups

To use OpsCenter to obtain a backup report on VMware virtual machines

1. Start the OpsCenter console in a web browser.

   On a system that has a network connection to the OpsCenter server, enter the following in a browser:

   ```
   http://host.domain/opscenter
   ```

   where `host.domain` is the fully qualified domain name or IP address of the OpsCenter server.

2. Click the **Reports** tab.
3. Click **Client Reports > Virtual Client Summary**.

   The **Virtual Client Summary** report is described in the *OpsCenter Reporting Guide*.

Chapter 9

Use Accelerator to back up virtual machines

This chapter includes the following topics:

- About the NetBackup Accelerator for virtual machines
- Accelerator: full vs. incremental schedules
- How the NetBackup Accelerator works with virtual machines
- Accelerator notes and requirements for virtual machines
- Accelerator forced rescan for virtual machines (schedule attribute)
- Accelerator requires the OptimizedImage attribute
- Accelerator backups and the NetBackup catalog
- Accelerator messages in the backup job details log
- NetBackup logs for Accelerator with virtual machines
- About reporting the amount of Accelerator backup data that was transferred over the network
- Replacing the Accelerator image size with the network-transferred data in NetBackup command output

About the NetBackup Accelerator for virtual machines

NetBackup Accelerator reduces the backup time for VMware backups. NetBackup uses VMware Changed Block Tracking (CBT) to identify the changes that were

made within a virtual machine. Only the changed data blocks are sent to the NetBackup media server, to significantly reduce the I/O and backup time. The media server combines the new data with previous backup data and produces a traditional full NetBackup image that includes the complete virtual machine files.

Note: Accelerator is most appropriate for virtual machine data that does not experience a high rate of change.

Accelerator has the following benefits:

- Performs the full backups faster than traditional backup. Creates a compact backup stream that uses less network bandwidth between the backup host and the server.
  Accelerator sends only changed data blocks for the backup. NetBackup then creates a full traditional NetBackup image that includes the changed block data.
- Accelerator backups support Granular Recovery Technology (GRT) for restoring Exchange, SQL, and SharePoint applications (using a full schedule only).
- Accelerator backups (full and incremental) support instant recovery of virtual machines.
- If the **Enable file recovery from VM backup** option on the policy **VMware** tab is enabled, you can restore individual files from the backup (full or incremental).
- Reduces the I/O on the backup host.
- Reduces the CPU load on the backup host.

Accelerator: full vs. incremental schedules

NetBackup Accelerator supports full and incremental backups.

Note: After an initial full backup, Accelerator backups with a full schedule have about the same effect on I/O and performance as traditional incremental backups. The NetBackup catalog however includes all catalog references that would be made if the backup was a traditional (non-Accelerator) full.

For virtual machine restore, note the following about full vs. incremental backups with Accelerator:

- For applications (Exchange, SQL, and SharePoint), NetBackup Accelerator supports Granular Recovery Technology (GRT) restores from full backups only.
- For any other kind of virtual machine restore, the Accelerator supports full backups and incremental backups.

How the NetBackup Accelerator works with virtual machines

To enable acceleration of virtual machine backups, click **Use Accelerator** on the policy **Attributes** tab.

See "Configuring a VMware policy from the Policies utility" on page 68.

The NetBackup Accelerator creates the backup stream and backup image for each virtual machine as follows:

- If the virtual machine has no previous backup, NetBackup performs a full backup and uses VMware Changed Block Tracking to track the data in use for each VMDK.
- At the next backup, NetBackup identifies data that has changed since the previous backup. Only changed blocks and the header information are included in the backup, to create a full virtual disk backup.
- The backup host sends to the media server a tar backup stream that consists of the following: The virtual machine's changed blocks, and the previous backup ID and data extents (block offset and size) of the unchanged blocks.
- The media server reads the virtual machine's changed blocks, the backup ID, and information about the data extents of the unchanged blocks. From the backup ID and data extents, the media server locates the rest of the virtual machine's data in existing backups.
- The media server directs the storage server to create a new full image that consists of the following: The newly changed blocks, and the existing unchanged blocks that reside on the storage server. The storage server may not write the existing blocks but rather link them to the image.

Accelerator notes and requirements for virtual machines

Note the following about Accelerator for virtual machines:

- Accelerator for virtual machines uses VMware Changed Block Tracking (CBT) to identify the changes that were made within a virtual machine.
  VMware CBT may occasionally reset tracking of file changes, such as after a power failure or hard shutdown. In that case, for the next backup NetBackup reads all the data from the vmdk files and the backup takes longer than expected. If deduplication is enabled, the deduplication rate is lower than expected.
  For more information on CBT, see the following VMware article:
  Changed Block Tracking (CBT) on virtual machines (1020128)

- Supports the disk storage units that have the following storage destinations:
  - Cloud storage. Storage that a supported cloud storage vendor provides.
  - NetBackup Media Server Deduplication Pool. In addition to NetBackup media servers, NetBackup 5200 series appliances support Media Server Deduplication Pool storage.
  - Qualified third-party OpenStorage devices.

  To verify that your storage unit supports Accelerator, refer to the NetBackup hardware compatibility list for the currently supported OST vendors:
  NetBackup Master Compatibility List
- It is recommended that you not enable **Expire after copy** retention for any storage units that are used with storage lifecycle policies (SLP) in combination with Accelerator. The **Expire after copy** retention can cause images to expire while the backup runs. To synthesize a new full backup, the SLP backup needs the previous backup image. If the previous image expires during the backup, the backup fails.
- Update the NetBackup device mapping files if needed.
  The NetBackup device mapping files contain all storage device types that NetBackup can use. To add support for the new devices or upgraded devices that support Accelerator, download the current device mapping files from the Veritas Technical Support website.
  See the *NetBackup Administrator's Guide Volume I* for information on the device mapping files and how to download them.
- Storage unit groups are supported only if the storage unit selection in the group is Failover.
- Supports the full backups and incremental backups. Every Accelerator backup (from a full schedule or incremental schedule) results in a complete image of the virtual machine.
- You can use incremental backups (cumulative or differential) as follows: To reduce the file-mapping overhead and to reduce the number of files that are recorded in the NetBackup catalog. Cumulative backups may involve more file-mapping because they do not use the random indexing method to determine which files have changed. In some cases, differential backups may be faster than cumulative backups.
- If a backup of the virtual machine does not exist, NetBackup performs a full backup. On the backup host it also accesses the VMware CBT information. This initial backup occurs at the speed of a normal (non-accelerated) full backup. Subsequent Accelerator backups of the virtual machine use VMware Changed Block Tracking to accelerate the backup.

Note: When you first enable a VMware policy to use Accelerator, the next backup (whether full or incremental) is in effect a full backup: It backs up all the virtual machine files that are selected in the policy. If that backup is an incremental, it may not complete within the backup window.

- If the storage unit that is associated with the policy cannot be validated when you create the policy, note: The storage unit is validated later when the backup job begins. If Accelerator does not support the storage unit, the backup fails. In the `bpbrm` log, a message appears that is similar to one of the following:

  ```
  Storage server %s, type %s, doesn't support image include.

  Storage server type %s, doesn't support accelerator backup.
  ```

- Accelerator requires the storage to have the `OptimizedImage` attribute enabled. See "Accelerator requires the `OptimizedImage` attribute" on page 166.
- Because of a VMware restriction, BLIB is not supported for VMware templates. As a result, NetBackup Accelerator cannot be used to back up VMware virtual machine templates.

Accelerator forced rescan for virtual machines (schedule attribute)

Accelerator for virtual machines uses Changed Block Tracking (CBT) technology from VMware to identify changed blocks. NetBackup requires the changed blocks when it creates a full virtual machine (synthesized) image. NetBackup is therefore dependent on VMware CBT for correctly identifying changed blocks. To protect against any potential omissions by underlying VMware CBT using timestamps, the **Accelerator forced rescan** option conducts the backup by collecting all in-use blocks as reported by VMware CBT.

When **Accelerator forced rescan** is used, all the data on the virtual machine is backed up. This backup is similar to the first Accelerator backup for a policy. For the forced rescan job, the optimization percentage for Accelerator is 0. The duration of the backup is similar to a non-Accelerator full backup.

Note: Under normal operations, an Accelerator forced rescan schedule is not necessary for VMware backups. It can be used to enforce a new baseline backup in case VMware CBT issues are discovered. Engaging with Veritas support is recommended in such situations.

Accelerator forced rescan is unavailable if the **Use Accelerator** option on the **Attributes** tab is not selected.

Accelerator requires the `OptimizedImage` attribute

Accelerator requires that the storage has the `OptimizedImage` attribute enabled.

To ensure that your storage is configured properly, see the documentation for your storage option:

- NetBackup Media Server Deduplication Pool.
  The `OptimizedImage` attribute is enabled by default. If you created the storage servers and pools in an earlier release, you must configure them for `OptimizedImage`.
  See the *NetBackup Deduplication Guide*.
- Backups to a third-party disk appliance.
  The storage device must support the `OptimizedImage` attribute.
  See the *NetBackup OpenStorage Solutions Guide for Disk*.
- Cloud storage that NetBackup supports.
  See the *NetBackup Cloud Administrator's Guide*.

Accelerator backups and the NetBackup catalog

Use of Accelerator does not affect the size of the NetBackup catalog. A full backup with Accelerator generates the same catalog size as a full backup of the same data without Accelerator. The same is true of incremental backups: use of Accelerator does not require more catalog space than the same backup without Accelerator.

A potential catalog effect does exist, depending on how often you use Accelerator with full backups. A full backup with Accelerator completes faster than a normal full. It may therefore be tempting to replace your incremental backups with Accelerator full backups. Note: Since a full backup requires more catalog space than an incremental, replacing incrementals with fulls increases the catalog size. When changing your incrementals to fulls, you must weigh the advantage of Accelerator fulls against the greater catalog space that fulls require compared to incrementals.

Accelerator messages in the backup job details log

When a virtual machine is first backed up, Accelerator is not used for that backup. The following messages appear in the job details log:

```
7/25/2012 4:45:35 PM - Info bpbrm(pid=6192) There is no complete
 backup image match with track journal, a regular full backup will
 be performed

...

7/25/2012 4:53:22 PM - Info bpbkar32(pid=5624) accelerator sent
5844728320 bytes out of 5844726784 bytes to server, optimization 0.0%
```

When subsequent backups of the virtual machine use Accelerator, the following messages appear in the job details log:

```
7/27/2012 4:40:01 AM - Info bpbrm(pid=412) accelerator enabled

...

7/27/2012 4:43:07 AM - Info bpbkar32(pid=4636) accelerator sent
74764288 bytes out of 5953504256 bytes to server, optimization 98.7%
```

This message is a key trace for Accelerator. In this example Accelerator was successful at reducing the backup data by 98.7%.

NetBackup logs for Accelerator with virtual machines

Accelerator does not require its own log directory. For log messages about Accelerator, see the following standard NetBackup log directories.

Table 9-1 NetBackup logs that may contain Accelerator information

Log directory	Resides on
UNIX: `/usr/openv/netbackup/logs/bpbrm` Windows: *`install_path`*`\NetBackup\logs\bpbrm`	NetBackup master or media server
UNIX: `/usr/openv/netbackup/logs/bptm` Windows: *`install_path`*`\NetBackup\logs\bptm`	NetBackup media server

Table 9-1 NetBackup logs that may contain Accelerator information *(continued)*

Log directory	Resides on
`/usr/openv/netbackup/logs/bpbkar` Windows: *`install_path`*`\NetBackup\logs\bpbkar`	Backup host
`/usr/openv/netbackup/logs/bpfis` Windows: *`install_path`*`\NetBackup\logs\bpfis`	Backup host
VxMS logs	See "NetBackup logging for VMware" on page 288.

To create the log directories, run the following command on the NetBackup servers and backup host:

On Windows:

`install_path``\NetBackup\logs\mklogdir.bat`

On UNIX/Linux:

`/usr/openv/netbackup/logs/mklogdir`

About reporting the amount of Accelerator backup data that was transferred over the network

For Accelerator backup reporting, several NetBackup commands can report the amount of data that is transferred over the network for each Accelerator backup. The amount of transferred data is often much less than the size of the Accelerator backup image.

For each Accelerator backup, NetBackup combines the client's (or VM's) changed blocks with the unchanged data from previous backups to synthesize a backup image. However, NetBackup sends only the changed data over the network when the backup occurs. The resulting backup image may be much larger than the amount of backup data that travels the network. For backup reporting, it may be important to distinguish between the backup image size and the amount of data that was transferred over the network.

For Accelerator backups, the network-transferred data can appear in the output of the following NetBackup commands: `bpdbjobs`, `bpimagelist`, and `bpclimagelist`.

Table 9-2 lists the default location of these commands.

Table 9-2 Default location of `bpdbjobs`, `bpimagelist`, and `bpclimagelist`

Command	Default location
`bpdbjobs`, `bpimagelist`	Windows: *install_path*\NetBackup\bin\admincmd\ UNIX, Linux /usr/openv/netbackup/bin/admincmd/
`bpclimagelist`	Windows: *install_path*\NetBackup\bin\ UNIX, Linux /usr/openv/netbackup/bin/

The following example uses the `bpimagelist` command to show the results of a backup of `acmevm2`:

```
bpimagelist -backupid acmevm2
```

Example output:

```
IMAGE acmevm2 0 0 12 acmevm2 accl_vmware 40 *NULL* root f 0 9 14344
79628 558 2147483647 0 0 7799632 28196 1 2 0 accl_vmware_1434479628_FULL.f *NULL
* *NULL* 0 1 0 0 0 *NULL* 0 0 1 0 0 1434479628 1434479628 *NULL* 0 0 0 *NULL* 9
0 0 3398732 0 0 *NULL* *NULL* 0 1434479620 0 0 *NULL* *NULL* 0 0 0 225792
HISTO 0 0 0 0 0 0 0 0 0 0
FRAG 1 -1 3319 76 0 0 0 @aaaab acmevm6.acme.com 262144 0 0 -1 102
4 1;PureDisk; acmevm6.acme.com;msdp_dp;PureDiskVolume;0 2147483647
0 65545 0 0 0 6 0 1434480186 1 1 *NULL* *NULL* 0 0
FRAG 1 1 7796313 0 0 0 0 @aaaab acmevm6.acme.com 262144 0 0 -1 10
28 1;PureDisk; acmevm6.acme.com;msdp_dp;PureDiskVolume;0 214748364
7 0 65545 0 0 0 6 0 1434480186 1 1 *NULL* *NULL* 0 0
```

In this example, the backup image size in kilobytes is 7799632, and the amount of data that was transferred over the network is 225792.

You can use the following commands to show the amount of data that was transferred over the network for an Accelerator backup.

bpimagelist

```
bpimagelist -backupid backup_id [-l | -L | -json | -json_compact]
```

Brackets [ ] indicate optional elements, and the vertical bars | indicate that you can choose only one of the options within the brackets.

Table 9-3 describes how the network-transferred data field appears in the `bpimagelist` output.

Table 9-3 The **bpimagelist** options that show the amount of network-transferred data for Accelerator backups

bpimagelist option	How the network-transferred data field appears
No option	The field is unlabeled. For example: `225792` See the `bpimagelist` example output earlier in this topic.
`-l`	The field is unlabeled (same as no option). For example: `225792`
`-L`	The field is labeled. For example: `Kilobytes Data Transferred: 225792`
`-json`	The field is labeled. For example: `"kilobytes_data_transferred": 225792,`
`-json_compact`	The field is labeled. For example: `"kilobytes_data_transferred":225792,`

bpdbjobs

```
bpdbjobs -jobid job_id -report -most_columns
```

or

```
bpdbjobs -jobid job_id -report -all_columns
```

The network-transferred data field appears at the end of the output.

bpclimagelist

```
bpclimagelist -client client_name
```

This command can only show the network-transferred data in the field that normally shows the Accelerator backup image size. To show the network-transferred data with this command, you must configure a NetBackup setting:

See "Replacing the Accelerator image size with the network-transferred data in NetBackup command output" on page 171.

Additional details on these commands are available in the *NetBackup Commands Reference Guide* or in the NetBackup man pages.

Replacing the Accelerator image size with the network-transferred data in NetBackup command output

You can configure the output of `bpimagelist`, `bpdbjobs`, and `bpclimagelist` to show the amount of Accelerator backup data that was transferred over the network instead of the backup image size.

The following is the default `bpimagelist` output that shows the Accelerator image size (see the circled value 7799632). The amount of network-transferred data appears farther down in the output (225792):

```
IMAGE acmevm2 0 0 12 acmevm2 accl_vmware 40 *NULL* root f 0 9 14344
79628 558 2147483647 0 0 7799632 28196 1 2 0 accl_vmware_1434479628_FULL.f *NULL
* *NULL* 0 1 0 0 0 *NULL* 0 0 1 0 0 1434479628 1434479628 *NULL* 0 0 0 *NULL* 9
0 0 3398732 0 0 *NULL* *NULL* 0 1434479620 0 0 *NULL* *NULL* 0 0 0 225792
HISTO 0 0 0 0 0 0 0 0 0 0
FRAG 1 -1 3319 76 0 0 0 @aaaab acmevm6.acme.com 262144 0 0 -1 102
4 1;PureDisk; acmevm6.acme.com;msdp_dp;PureDiskVolume;0 2147483647
0 65545 0 0 0 6 0 1434480186 1 1 *NULL* *NULL* 0 0
FRAG 1 1 7796313 0 0 0 0 @aaaab acmevm6.acme.com 262144 0 0 -1 10
28 1;PureDisk; acmevm6.acme.com;msdp_dp;PureDiskVolume;0 214748364
7 0 65545 0 0 0 6 0 1434480186 1 1 *NULL* *NULL* 0 0
```

You can configure NetBackup command output to show the network-transferred data in the image size field. In the output, the image size value is replaced with the network-transferred data value (see the following example). A script that reads the image size from the command output now reads the amount of network-transferred data.

In the following `bpimagelist` output, the image size field shows the network-transferred data (225792):

```
IMAGE acmevm2 0 0 12 acmevm2 accl_vmware 40 *NULL* root f 0 9 14344
79628 558 2147483647 0 0 225792 28196 1 2 0 accl_vmware_1434479628_FULL.f *NULL
* *NULL* 0 1 0 0 0 *NULL* 0 0 1 0 0 1434479628 1434479628 *NULL* 0 0 0 *NULL* 9
0 0 3398732 0 0 *NULL* *NULL* 0 1434479620 0 0 *NULL* *NULL* 0 0 0 225792
HISTO 0 0 0 0 0 0 0 0 0 0
FRAG 1 -1 3319 76 0 0 0 @aaaab acmevm6.acme.com 262144 0 0 -1 102
4 1;PureDisk; acmevm6.acme.com;msdp_dp;PureDiskVolume;0 2147483647
0 65545 0 0 0 6 0 1434480186 1 1 *NULL* *NULL* 0 0
FRAG 1 1 7796313 0 0 0 0 @aaaab acmevm6.acme.com 262144 0 0 -1 10
28 1;PureDisk; acmevm6.acme.com;msdp_dp;PureDiskVolume;0 214748364
7 0 65545 0 0 0 6 0 1434480186 1 1 *NULL* *NULL* 0 0
```

Note: The same change occurs in the labeled output of the commands (such as with the `-L` option of `bpimagelist`). For example, the `Kilobytes` field shows the transferred data value (225792 in the example) rather than the Accelerator backup image size.

To enable the reporting of network-transferred data in the Accelerator image size field of bpimagelist, bpdbjobs, and bpclimagelist

- Use the `bpsetconfig` command to enable the output change.

  To enable this change for the `bpclimagelist` command, enter the `bpsetconfig` command on the master server. To enable this change for `bpimagelist` or `bpdbjobs`, enter the `bpsetconfig` command on the server where you intend to run `bpimagelist` or `bpdbjobs`.

  Refer to Table 9-4 for the `bpsetconfig` command to use based on the type of Accelerator backup that you want to report on.

Table 9-4 To enable the reporting of network-transferred data in the Accelerator image size field of **bpimagelist**, **bpclimagelist**, or **bpdbjobs** output

Type of backup to report on	Enter this command

Incremental VMware Accelerator backups	Windows
	`echo REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_ FOR_ACCL_INC_VMWARE | install_path\NetBackup\bin\admincmd\bpsetconfig`
	UNIX, Linux
	`echo "REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_ FOR_ACCL_INC_VMWARE" | /usr/openv/netbackup/bin/admincmd/bpsetconfig`

All VMware Accelerator backups (full and incremental)	Windows
	`echo REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_ FOR_ACCL_ALL_VMWARE | install_path\NetBackup\bin\admincmd\bpsetconfig`
	UNIX, Linux
	`echo "REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_ FOR_ACCL_ALL_VMWARE" | /usr/openv/netbackup/bin/admincmd/bpsetconfig`

Incremental Accelerator virtual machine backups (VMware and Hyper-V)	Windows
	`echo REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_ FOR_ACCL_INC_VIRTUAL | install_path\NetBackup\bin\admincmd\bpsetconfig`
	UNIX, Linux
	`echo "REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_ FOR_ACCL_INC_VIRTUAL" | /usr/openv/netbackup/bin/admincmd/bpsetconfig`

All Accelerator virtual machine backups (VMware and Hyper-V, full and incremental)	Windows
	`echo REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_ FOR_ACCL_ALL_VIRTUAL | install_path\NetBackup\bin\admincmd\bpsetconfig`
	UNIX, Linux
	`echo "REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_ FOR_ACCL_ALL_VIRTUAL" | /usr/openv/netbackup/bin/admincmd/bpsetconfig`

Table 9-4 To enable the reporting of network-transferred data in the Accelerator image size field of **bpimagelist**, **bpclimagelist**, or **bpdbjobs** output *(continued)*

Type of backup to report on	Enter this command

All incremental Accelerator backups (physical clients and virtual machines)	Windows
	`echo REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_FOR_ACCL_INC_ALL | install_path\NetBackup\bin\admincmd\bpsetconfig`
	UNIX, Linux
	`echo "REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_FOR_ACCL_INC_ALL" | /usr/openv/netbackup/bin/admincmd/bpsetconfig`

All Accelerator backups (full and incremental, physical clients and virtual machines)	Windows
	`echo REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_FOR_ACCL_ALL_ALL | install_path\NetBackup\bin\admincmd\bpsetconfig`
	UNIX, Linux
	`echo "REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED = REPLACE_IMAGE_SIZE_FOR_ACCL_ALL_ALL" | /usr/openv/netbackup/bin/admincmd/bpsetconfig`

To reset the command output to the default setting

- To disable the reporting of network-transferred data in the Accelerator image size field (return to default), enter the following:

  Windows

  ```
  echo REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED =
  REPLACE_IMAGE_SIZE_DISABLED |
  install_path\NetBackup\bin\admincmd\bpsetconfig
  ```

  UNIX, Linux

  ```
  echo "REPLACE_IMAGE_SIZE_WITH_DATA_TRANSFERRED =
  REPLACE_IMAGE_SIZE_DISABLED" |
  /usr/openv/netbackup/bin/admincmd/bpsetconfig
  ```

Chapter 10

Restore virtual machines

This chapter includes the following topics:

- Restore notes and restrictions
- Restore notes and restrictions on Linux
- Restoring the full VMware virtual machine
- About VMware virtual machine disk restore
- Restoring VMware virtual machine disks by using Backup, Archive, and Restore
- Restoring VMware virtual machine disks by using NetBackup commands
- About restore of individual files
- Restoring individual files
- How NetBackup handles VMware tag associations at restore
- Browse and search virtual machines for restore
- If the recovery host is not at the same NetBackup release level as the backup host

Restore notes and restrictions

Before you begin the restore, note the following:

- Cross-platform restore of individual files is not supported. You can restore Windows files to Windows guest operating systems but not to Linux. You can restore Linux files to supported Linux guest operating systems but not to Windows. In other words, the restore host must be the same platform as the files that you want to restore.
  See “About restore of individual files” on page 223.

- Unless a NetBackup client is installed on the virtual machine, you must do the restore from the NetBackup primary server.
- To restore files to the original virtual machine location, the destination must be specified as the virtual machine's host name (not display name or UUID).
- To restore directly to an ESX server, the name that is specified for the restore must match the ESX server's official host name. The name must be in the same format in which it is registered in DNS and in the VMware server (whether short or fully-qualified).
  See "Adding NetBackup credentials for VMware" on page 45.
- If the VM's display name was changed after the VM was backed up, the pre-recovery check may fail when you click **Start Recovery**:

  ```
  VM exists overwrite -Failed. Vmxdir for VM exists
  ```

  You can ignore the error and click **Start Recovery**, but note: The restore may succeed but the folder that contains the vmx file for the newly restored VM has a different name than the vmx folder of the existing VM. VMware does not rename this folder when the VM is renamed, but continues to use the existing folder.
  As an alternative, restore the VM to a different location.
- A virtual machine template cannot be restored to a standalone ESX server. Because templates are a feature of vCenter servers, you must restore the template through vCenter. If you restore a template to a standalone ESX server, the template is converted to a normal virtual machine and is no longer a template.
- NetBackup supports backup and recovery of VMware NVRAM files and the vTPM devices that are associated with virtual machines.
  - A NetBackup 8.3 or later backup or recovery host is required for NVRAM and vTPM protection. Supported recovery methods include Full VM recovery and VMware Instant Recovery.
  - NetBackup does not support the backup or restore of NVRAM and vTPM for the virtual machines whose display names begin with a period ('.'). An existing VMware limitation prevents downloading or uploading data store files beginning with a period ('.') to a virtual machine's working directory as these appear as hidden files.
- If the virtual machine was backed up by its display name or UUID, and the display name differs from the host name, note: You must specify the correct destination client for the restore. Use the **Specify NetBackup Machines and Policy Type** dialog in the NetBackup Backup, Archive, and Restore interface.
  See "Invalid client error when you restore files using NetBackup BAR interface installed on the virtual machine" on page 308.

- Restore of individual files from a backup of the full virtual machine is not supported if the virtual machine contains Storage Foundation Volume Manager volumes.
- To restore Windows NTFS-encrypted files individually, you must install a NetBackup client on the virtual machine.
  See "NetBackup for VMware best practices" on page 281.
- If the attempt to restore a full virtual machine fails while using the SAN transport type, try the NBD transport type instead.
- Restoring a virtual machine with a transport mode of NBD or NBDSSL may be slow in the following cases:
  - The virtual machine had many small data extents due to heavy fragmentation. (A file system extent is a contiguous storage area defined by block offset and size.)
  - The restore is from a block-level incremental backup and the changed blocks on the disk were heavily fragmented when the incremental backup occurred.

  For faster restores in either of these cases, use the hotadd transport mode instead of NBD or NBDSSL.
- VMware does not support the restore of virtual machines directly to an ESX 5.x server that vCenter manages. To restore the virtual machine, select the vCenter server as the destination.
  As an alternative, you can set up an independent ESX server to be used for restores. You must add NetBackup restore credentials for that ESX server by means of the **VMware restore ESX server** server type.
  See "Adding NetBackup credentials for VMware" on page 45.
- For the SAN transport mode, the job may be slow when you restore to a vCenter Server. For greater speed, designate a VMware restore ESX server as the destination for the restore.
  See "Adding NetBackup credentials for VMware" on page 45.
- For the SAN transport mode and a restore host on Windows, the restore fails if the datastore's LUN is offline. The detailed status log contains messages similar to the following:

  ```
  5/22/2013 4:10:12 AM - Info tar32(pid=5832) done. status: 24:
  socket write failed
  5/22/2013 4:10:12 AM - Error bpbrm(pid=5792) client restore EXIT
  STATUS 24: socket write failed
  ```

  - Make sure the status of the SAN disk on the restore host is online (not offline). Disk status can be checked or changed using the Windows diskpart.exe

utility or the Disk Management utility (diskmgmt.msc). When the disk status reads online, retry the restore.

- If multipathing is enabled, make sure all the paths are online.

- A restore by means of the SAN transport mode may be slow in other circumstances. The following Veritas article provides details:
  VMware Transport Modes: Best practices and troubleshooting

- The APIs in VMware's Virtual Disk Development Kit (VDDK) contain the following limitation: The maximum write speed during virtual machine restore is roughly one third of the hardware's maximum speed. The following Veritas tech note contains further information:
  Two causes of slow NetBackup for VMware restore performance
  http://www.veritas.com/docs/TECH169860

- If a virtual machine had vmdk files in different directories in the same datastore, note: When the virtual machine is restored to the original location its vmdk files are restored to a single directory, not to the original directories. (This behavior follows current VMware design.)
  As a workaround, do the following: Remove the vmdk files from the restored virtual machine, move the files to their respective directories, then re-attach the moved files to the virtual machine.

- If the original VM contains encrypted vmdk files, after restoring the full VMware virtual machine to the original location or after an in-place disk restore, the restored disks may not be compliant to the VM encryption policy. Therefore, the restored VM must be reconfigured manually to comply with the policy. Otherwise, the virtual disks of the restored VM might be left in an unencrypted state.

- When restoring large files, make sure that no snapshots are active on the destination virtual machine. Otherwise, the files are restored to the VMware configuration datastore, which may be too small to contain the files you want to restore. In that case, the restore fails.
  The configuration datastore (sometimes called the vmx directory) contains the configuration files that describe the virtual machine, such as `*.vmx` files. Note that active snapshots of vmdk files are also stored on the configuration datastore.

- If you cancel the virtual machine restore before it completes, the not-fully-restored virtual machine remains at the target location. NetBackup does not delete the incomplete virtual machine when the restore job is canceled. You must manually remove the incomplete virtual machine.

- If the virtual machine display name contains unsupported characters, the backup may succeed but the restore fail. To restore the virtual machine, you must change the display name to contain supported characters only and retry the restore.
  See "NetBackup character restrictions for the Primary VM identifier" on page 37.

- NetBackup for VMware does not support individual file restore by means of client-direct restore.
- On a restore, NetBackup recreates the linking between a hard link and its original file only in this case: The link file and its target file are restored in the same job. If each file is restored individually in separate restore jobs, they are restored as separate files and the link is not re-established.
- If you restore a VM in vCloud to an expired vApp, the vApp is automatically renewed and added back into the vCloud organization. If the expired vApp contained other VMs, all those VMs are also removed from the expired list and added to the organization.
  Note that in vCloud Director, an expired vApp must be renewed before you can import a VM into that vApp.
- With a remote connection from a Windows Java GUI that uses the English locale, the restore of files that have non-ASCII characters may fail.
  See the following tech note for further information on how to restore the files:
  http://www.veritas.com/docs/TECH75745
- In VMware vSphere 6.0 U1b and later, a full restore of a virtual machine may trigger an alarm if the original VM was not deleted. The alarm is a VM MAC address conflict alarm. This VMware alarm behavior is by design. If there is a MAC address conflict, VMware eventually changes the MAC address of the new VM. If you do not want to receive alarms, disable the VM MAC address conflict alarms in vCenter.
- See “NetBackup for VMware: notes and restrictions” on page 27.

Restore notes and restrictions on Linux

Before you begin the restore, note the following:

- Cross-platform restore of individual files is not supported. You can restore Linux files to supported Linux guest operating systems but not to Windows.
- To migrate an ext2 or ext3 file system to ext4, note: Make sure to follow the instructions under "Converting an ext3 file system to ext4" on the following page of the Ext4 wiki:
  https://ext4.wiki.kernel.org/index.php/UpgradeToExt4
  If you do not follow these instructions, data in a newly created ext4 file is not promptly flushed from memory to disk. As a result, NetBackup cannot back up the data of recently created files in the ext4 file system. (The NetBackup snapshot captures the file as zero length.)

  As a workaround for the file systems that were not correctly migrated, do one of the following:

- Run the Linux sync command on the ext4 file system before starting each backup.
- Make sure that snapshot quiesce is enabled in the Linux guest OS. Contact your operating system vendor and VMware for additional information.

- For Linux virtual machines, NetBackup cannot restore individual files from software RAID volumes. The files are restored when you restore the entire virtual machine.
- The Linux ext4 file system includes a persistent pre-allocation feature, to guarantee disk space for files without padding the allocated space with zeros. When NetBackup restores a pre-allocated file (to any supported ext file system), the file loses its preallocation and is restored as a sparse file. The restored sparse file is only as large as the last byte that was written to the original file. Note also that subsequent writes to the sparse file may be non-contiguous.
- NetBackup supports backup and restore of Linux LVM2 volumes, including individual file restore from an LVM2 volume. Note however that NetBackup does not support individual file restore from a snapshot that was created by means of the snapshot feature in LVM2. If an LVM2 snapshot exists at the time of the backup, the data in the snapshot is captured in the backup. The data can be restored along with the rest of the virtual machine data when you recover the entire virtual machine.
- NetBackup supports backup of Linux FIFO files and socket files. NetBackup does not support restoring FIFO files and socket files individually. FIFO files and socket files can be restored along with the rest of the virtual machine data when you recover the entire virtual machine.
- For Linux virtual machines, the ext2, ext3, and ext4 file systems are supported for individual file restore. If a partition uses some other file system, the backup succeeds but files in that partition cannot be individually restored. To allow NetBackup to present mount points for restore in the Backup, Archive, and Restore interface, note: The "/" (root) partition must be formatted with ext2, ext3, or ext4.
  See "Mount points not available when restoring files from a Linux virtual machine" on page 308.
- When you restore Linux files individually to an NFS-shared device on a Linux virtual machine, NetBackup can only restore the file data and attributes. The extended attributes cannot be restored to NFS-shared devices.
- For a virtual machine that is running a Linux guest operating system: When you restore a virtual machine, the ESX server may assign the virtual machine a new (virtual) MAC address. After you restart the virtual machine, you may have to configure its MAC address. For instance, the original MAC address of the virtual machine may be in a configuration file that has to be updated.

Refer to your VMware documentation for more details.

- For Linux, additional notes apply.
  See "NetBackup for VMware: notes on Linux virtual machines" on page 34.

Restoring the full VMware virtual machine

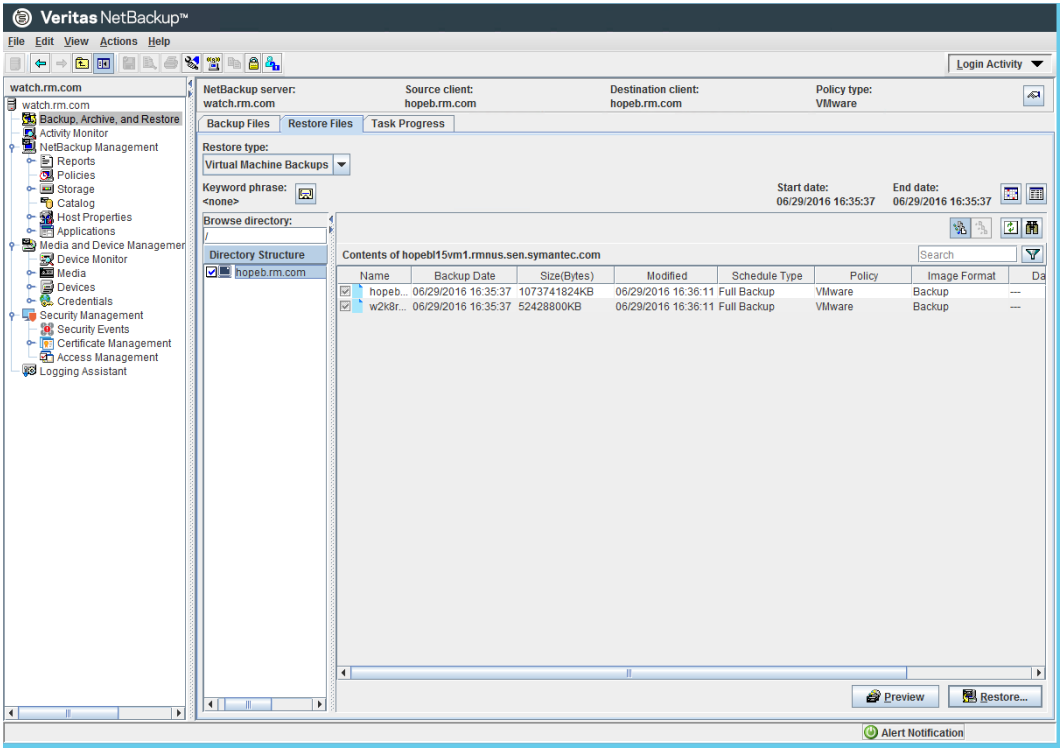
To restore the full virtual machine

1. In the NetBackup Administration Console, click **Backup, Archive, and Restore**.
2. Click **Actions > Specify NetBackup Machines and Policy Type**.
3. Specify the following:

Server to use for backup and restores	The NetBackup primary server that directed the backup
Source client for restores	The VMware virtual machine that was backed up. Click **Search VM Clients** to search or browse for a virtual machine. Use this option to locate a virtual machine in a large, multi-layered virtual environment. See "Browse and search virtual machines for restore" on page 232. Or enter the type of name that was selected for the **Primary VM identifier** option on the policy **VMware** tab. For example, if the **Primary VM identifier** option is set to VM host name, enter the virtual machine's host name.
Destination client for restores	This field is ignored. The destination for the restore is specified in a different screen as explained in a later procedure.
Policy type for restores	The type of policy that made the backup (VMware).

4. Click **OK**.
5. For the **Restore type,** select **Virtual Machine Backups**.
6. You can use the **Start date** and **End date** icons to select the date range within which the backup occurred.

7 Under **Directory Structure**, click on the backup you want to restore.



8 Click **Restore**.

The type of dialog that appears depends on whether or not the backup was enabled for vCloud.

vSphere (not vCloud) See "Virtual Machine Recovery dialog boxes (restore to original location)" on page 182.

See "Virtual Machine Recovery dialogs boxes (restore to alternate location)" on page 188.

vCloud See "Virtual machine recovery dialog boxes for vCloud Director" on page 275.

Virtual Machine Recovery dialog boxes (restore to original location)

The following topics describe the Backup, Archive, and Restore screens for restoring a virtual machine to the original location. These screens do not apply to vCloud Director.

See "Virtual machine recovery dialog boxes for vCloud Director" on page 275.

Recovery Destination dialog box

You can select the type of destination for the virtual machine recovery: the original location or alternate location.

This dialog includes the following:

- **Original settings of the virtual machine at the backup**
  Shows the configuration of the virtual machine at the time of the backup.
  When you restore the virtual machine to its original location, these configuration settings are used and cannot be changed.
  When you restore to an alternate location (not to the original location), you can change these settings after you click **Next**.
- **Recover virtual machine to**
  Select **Original Location** or **Alternate Location**.

Recovery Options dialog box

Select the recovery host and transport mode, as follows:

- **Destination settings**
  Shows the configuration of the virtual machine at the time of backup. These settings are applied to the virtual machine when it is restored.

  Note: This information is included for recovery to vSphere only (not for vCloud).

- **NetBackup Recovery Host**
  The host that performs the recovery. The default is the host that performed the backup (the backup host).
  In most cases, you can use the host that performed the backup. Selecting a different host as the recovery host can result in a slow restore or a failed restore, depending on the transport mode.

  For example, the restore fails if you select the SAN transport mode in the following case:

  - The host that performed the backup used a SAN connection to access the datastore.
  - The host you select as recovery host does not have SAN access to the datastore.
- **Media Server**
  You can use this option to select a media server that has access to the storage unit that contains the backup image. An example of such an environment is a Media Server Deduplication Pool (MSDP) with multiple media servers.

Note: If the storage unit that contains the backup image is not shared with multiple media servers, this option is grayed out.

- **Transport modes**
  Determines how the restore data is sent from the recovery host to the VMware datastore. The appropriate option depends in part on the type of network that connects the VMware datastore to the recovery host.
  The default is the type that the backup used.

san	For unencrypted transfer over Fibre Channel (SAN) or iSCSI.
nbd	For unencrypted transfer over a local network that uses the Network Block Device (NBD) driver protocol. This mode of transfer is usually slower than Fibre Channel.
nbdssl	For encrypted transfer (SSL) over a local network that uses the Network Block Device (NBD) driver protocol. This mode of transfer is usually slower than Fibre Channel.
hotadd	Requires the recovery host in a virtual machine. For instructions on this transport mode and on installing the recovery host in a VMware virtual machine, refer to your VMware documentation.
Move Up, Move Down	Use these options to change the order in which NetBackup tries each selected mode. Highlight a mode and click **Move Up** or **Move Down**. For example: Assume that all four transport modes are selected, and the order is SAN, hotadd, nbd, and nbdssl. If one of the virtual disks cannot be accessed using SAN, the SAN transport mode is not used for any of the virtual machine's disks. NetBackup then tries to use the hotadd mode for all the disks. NetBackup continues to try each mode until it finds one that succeeds for all the disks.

Virtual Machine Options dialog box

Virtual Machine Options:

- **Restore BIOS UUID xxx instead of creating a new UUID**

Retains the UUID of the original virtual machine (note that the UUID is a globally unique identifier). The virtual machine is restored with the same UUID that it had before the restore.

Note the following:

- If a virtual machine with the same display name but with a different UUID exists at the target restore location, the restore fails. You must either delete the existing virtual machine and run the restore, or keep the existing virtual machine and abandon the restore.
- If you do not want to keep the existing virtual machine, you can do one of the following: Remove the existing virtual machine, or log into the ESX server and remove the directory where the virtual machine resides.

- **Restore Instance UUID xxx instead of creating a new UUID**
  Retains the Instance UUID of the original virtual machine (note that the Instance UUID is a vCenter specific unique identifier of a virtual machine). The virtual machine is restored with the same Instance UUID that it had when it was backed up.
  If the restore of the virtual machine is to a standalone ESXi host, this option is disabled.
  If a virtual machine with the same Instance UUID exists at the target restore location, a message appears that the UUID is used already. In this case, the original instance UUID is not restored and a new UUID is assigned for the virtual machine.
- **Overwrite the existing virtual machine**
  If a virtual machine with the same display name exists at the destination, that virtual machine must be deleted before the restore begins. Otherwise, the restore fails. Select this option to have the virtual machine deleted.
- **Remove backing information for devices like DVD/CD-ROM drives, serial or parallel ports**
  If a virtual machine had an ISO file that was mounted on a CD when the virtual machine was backed up, note: The ISO file must be available on the target ESX server when you restore the virtual machine. If the ISO file is not available on the ESX server, the restore fails.
  This option restores the virtual machine without restoring an ISO file that was mounted when the virtual machine was backed up.
- **Remove network interfaces**
  Removes any network interfaces from the restored virtual machine.

  Select this option if:

  - The network connections on the destination virtual machine have changed since the backup was made.

  - Or if the original virtual machine still exists and a duplicate may cause conflicts.

- **Remove tag associations**
  When this option is selected, NetBackup does not attempt to restore tag associations when it restores the virtual machine. If the box is not checked, NetBackup attempts to restore all tag associations from the backup. If NetBackup cannot restore one or more of the tag associations, the restore exits with a NetBackup Status Code 1.
- **Power on virtual machine after recovery**
  Select this option to have the recovered virtual machine automatically turned on when the recovery is complete.
- **Override default job priority**
  Place a check mark in this box to override the default priority.
- **Job Priority**
  Use this field to set a higher priority.
- **Retain original hardware version**
  This option restores the virtual machine with its original hardware version (such as 4). It retains the original version even if the target ESX server by default uses a different hardware version (such as 7 or 8). If the target ESX server does not support the virtual machine's hardware version, the restore may fail.
  If this option is disabled, the restored virtual machine is converted to the default hardware version that the ESX server uses.

Format of restored virtual disks:

- **Original provisioning**
  Restores the virtual machine's virtual disks with their original provisioning.

  Note: Regarding restore into vCloud Director: For **Original provisioning**, NetBackup restores the virtual machine's virtual disks with the format they had when the virtual machine was backed up. That format may be different from either of the following: The default format of the vCloud organization when the virtual machine was originally created, or the format for the destination organization.

- **Thick provisioning Lazy Zeroed**
  Configures the restored virtual disks in the thick format. The virtual disk space is allocated when the disk is created. This option restores the populated blocks, but initializes vacant blocks with zeros later, on demand.
- **Thick provisioning Eager Zeroed**

Configures the restored virtual disks in the thick format. Restores the populated blocks and immediately initializes vacant blocks with zeros (eager zeroed). Creation of the virtual disks may take more time with this option. However, if the restore occurs over a SAN, the eager zeroed feature may speed up the restore by reducing network communication with the vCenter server.

- **Thin provisioning**
  Configures the restored virtual disks in the thin format. Restores the populated blocks but does not initialize vacant blocks or commit them.
  Thin provisioning saves disk space through dynamic growth of the vmdk file. The vmdk files are no larger than the space that the data on the virtual machine requires. The virtual disks automatically increase in size as needed.

  Note: If the vmdk is completely written, VMware automatically converts a thin disk to **Thick provisioning Eager Zeroed**.

  For more information on virtual disk provisioning, refer to VMware's documentation.

Perform Recovery dialog box

Review the settings to be applied to the restored virtual machine.

- **Recovery settings**
  Lists the settings that are used for the recovery.
- **Run Pre-Recovery Check**
  Click this option to verify the following: The credentials, the available space on the datastore, and other important requirements. For a description of the checks, see Table 10-1.
- **Start Recovery**
  Starts the recovery of the virtual machine.

Table 10-1 Pre-recovery checks

Type of check	Description
Verify vSphere server credential	Verifies that NetBackup has the correct credentials to access the vSphere server for the restore.
Verify datacenter path	Verifies that NetBackup can access the datacenter that is designated for the restore.
Verify folder path	Verifies that NetBackup can access the VM folder that is designated for the restore.
Unsupported non-ASCII characters	Checks for unsupported characters in the VM display name, datastore name, or network name.

Table 10-1 Pre-recovery checks *(continued)*

Type of check	Description
VM exists overwrite	If the original VM exists at the restore destination, verifies that the **Overwrite the existing virtual machine** option is selected. If the VM exists and the overwrite option is selected, the VM is overwritten with the restored VM. If the original VM does not exist at the restore destination, verifies that the original VM's vmx configuration file directory does not exist. If the original VM does not exist but the vmx directory exists, specify a different display name for the restored the VM.
Adequate space on datastore (or datastore cluster) for configuration file	Verifies that the datastore (or datastore cluster) for the restore has enough space for the restored VM's vmx configuration file.
VMware connectivity test	Verifies that the NetBackup restore host can communicate with the vCenter server.
Datastore/Datastore Cluster space available	Verifies that the datastore (or datastore cluster) for the restore has enough space for the restored VM files.
SAN datastore compatibility	Verifies that the selected datastore has a compatible block size. For example, this check fails if it detects the following problem: The VM's vmdk files are not a multiple of the VMFS block size. In that case, the last partial-block write may fail during the restore, and the restore job fails with status 2820. The NetBackup job details log contains messages similar to the following: `12/12/2011 3:12:28 AM - Critical bpbrm(pid=3560) from client io.acme.com: FTL - Virtual machine restore: file write failed` In this case, use the NBD or the NBDSSL transport mode when you restore the VM.
Verify unique BIOS UUID	If only the SAN transport mode is selected for the restore, determines if a VM with the same BIOS UUID exists on the specified vCenter.

Virtual Machine Recovery dialogs boxes (restore to alternate location)

The following topics describe the Backup, Archive, and Restore screens for restoring a virtual machine to an alternate location. These screens do not apply to vCloud Director.

See "Virtual machine recovery dialog boxes for vCloud Director" on page 275.

Recovery Destination dialog box (restore to alternate location)

- **Original settings of the virtual machine when it was backed up**

Shows the configuration of the virtual machine at the time of the backup. When restoring to an alternate location (not to the original location), you can change these settings after you click **Next**.

- **Recover virtual machine to**
  Select **Alternate location**.

Recovery Options dialog box (restore to alternate location)

The Recovery Options dialog initially displays the original virtual machine settings that were recorded in the NetBackup catalog when the virtual machine was backed up. Before accepting any default values, you may have to verify that the original hosts or servers are still available.

The dialog contains the following fields:

- **NetBackup Recovery Host**
  The recovery host transfers the virtual machine files to the VMware destination that is specified in other fields on this dialog. The default for the recovery host is the backup host that backed up the virtual machine.

  Consider the following when selecting a recovery host:

  - To use the original VMware backup host for the recovery, verify that the backup host still exists. The original backup host may have been removed or reconfigured after the backup occurred.
  - The current processing load on the host that you want to use may be a factor. The recovery host undergoes significant I/O activity when it restores a virtual machine.
  - The network connection between the recovery host and the destination datastore may limit the type and speed of data transmission. For example, to use the SAN transport mode, the recovery host must have access to the appropriate LUNs in the datastore.

- **Media Server**
  You can use this option to select a media server that has access to the storage unit that contains the backup image. An example of such an environment is a Media Server Deduplication Pool (MSDP) with multiple media servers.

  Note: If the storage unit that contains the backup image is not shared with multiple media servers, this option is grayed out.

- **Transport modes**

Determines how the data is sent from the recovery host to the VMware datastore. The appropriate mode depends on the type of connection between the NetBackup recovery host and the VMware datastore.

More information is available about these options.

See "Recovery Options dialog box" on page 183.

- **vCenter Server**

  Specifies the vCenter server for the restored virtual machine. To use the original vCenter Server (the default), verify that the original vCenter server still exists.

  To use a different vCenter Server, consider whether it is compatible with the virtual machine you want to restore. If you attempt to restore to an earlier vSphere server that does not support the virtual machine's hardware version, note: The VMware Tools component converts the virtual machine to an earlier hardware version. But the restore may fail if the virtual machine uses devices that only the later hardware version supports.

  In other cases, you can use the **Retain original hardware version** option on the **Virtual Machine Options** dialog.

  The restore may finish faster if you use the SAN transport mode with a restore ESX server (bypassing any vCenter servers).

  When choosing a target host for the restore, note the following:

  - If NetBackup has credentials to a vCenter server but does not have credentials to a restore ESX server, you can perform the restore. NetBackup uses the vCenter credentials to access the ESX server but does not send the virtual machine data through the vCenter.

    Note: If you use the SAN transport mode for the restore, the restore job may take longer than expected.

    The credentials must give NetBackup full access privileges to the vCenter server.

    See "Adding NetBackup credentials for VMware" on page 45.

  - If NetBackup has credentials to a vCenter server as well as to a VMware restore ESX server, the restore may complete faster. In this case, by default NetBackup communicates with the restore ESX server during data transfer. You can select a vCenter folder in which to place the restored virtual machine. The credentials must give NetBackup full access privileges to the restore ESXi server.

    Select the vCenter Server, and click **Change** to select the VMware restore ESXi server.

Note: NetBackup uses the selected vCenter to create the virtual machine. NetBackup then writes the .vmdk files directly to the ESX server using the Restore ESX Server credentials to that server.

- If NetBackup has credentials to an ESX server, you can designate that server as the target for the restore. The credentials must give NetBackup full access privileges to the ESX server.
  Select **None** for the vCenter Server, and click **Change** to select the ESX server.

  Note: To restore to an ESX server, the ESX must be standalone, not managed by vCenter. To restore to an ESX under vCenter, NetBackup must have VMware restore ESX server credentials for the ESX. Select the vCenter, and click **Change** to select the VMware restore ESX server.

- **ESX Server/Cluster**
  Specifies the ESX server or cluster on which the restored virtual machine is to reside. To use the original ESX server or cluster (the default), verify that the original ESX server or cluster still exists.
  Click **Change** to browse for a different ESX server or cluster.
  See "Select ESX server dialog box (restore to alternate location)" on page 192.
- **Datacenter**
  Shows the VMware data center containing the selected ESX server.
- **Folder**
  A folder is a logical entity within the vCenter that contains VMware objects, such as datastores, networks, and virtual machines.
  By default, this field shows the VMware folder that contained the virtual machine when the virtual machine was backed up. If you select a different ESX server to which to restore the virtual machine, this field changes to None. You must then click **Change** to select a folder within the data center for the restored virtual machine.
  See "Select Folder dialog box (restore to alternate location)" on page 193.
- **Display Name**
  Specifies the VMware display name for the restored virtual machine. The default is the display name that the virtual machine had when it was backed up.
  The display name must be unique for the vCenter Server where the virtual machine is restored.

Note: If a virtual machine with this display name already exists at this location (or at the original location), you are prompted to click **Overwrite the existing virtual machine**. You cannot restore the virtual machine if the result is two virtual machines with the same display name on the same vCenter server.

- **Resource Pool/vApp**
  Use this option to have the restored virtual machine assigned to either a VMware resource pool or to a vApp. Resource pools manage the host's CPU and memory. vApps are logical containers for virtual machines, and also share some functionality with virtual machines.
- **Datastore/Datastore Cluster**
  Specifies the VMware datastore or datastore cluster that contains the virtual machine configuration files. Click **Change** to make a selection.
  This datastore (sometimes called the vmx directory) contains the configuration files that describe the virtual machine, such as `*.vmx` files. Active snapshots of vmdk files are also stored on this datastore.

Note: The Datastore field shows the name of the datastore that contained the virtual machine data when the virtual machine was backed up. Even if the datastore was in a datastore cluster, the field shows the name of the datastore, not the datastore cluster. When the virtual machine is restored, NetBackup determines how the datastore is currently configured (in a cluster or not) and configures the virtual machine accordingly.

- **Use the same datastore/datastore cluster for all VMDKs**
  This option assigns all the restored virtual machines to the datastore or datastore cluster that is selected in the **Datastore/Datastore Cluster** field.
  If this option is not selected, you assign the VMDKs to specific datastores or datastore clusters in a later dialog (the Storage Destination dialog).

Select ESX server dialog box (restore to alternate location)

Use this dialog to enter the name of the ESX server or cluster, or drill down in the list to select the server or cluster.

- **Specify ESX server**
  Enter the name of the ESX server or cluster in this field. As you type a name, the list of available servers or clusters automatically expands and the nearest match is highlighted.
- **Search**

If necessary, click **Search** to locate the server name or cluster name that you typed.

Note: Some older ESX servers may not support the version of the virtual machine that you want to restore. Verify that the ESX server is compatible with the virtual machine.

Select Folder dialog box (restore to alternate location)

The Select Folder dialog shows the vCenter folders that exist on the datacenter that is shown in the **Datacenter** field.

Pick a folder from the list of available folders. The restored virtual machine is placed in this folder.

If two datacenters of the same name exist in the vCenter server, all folders for the identically named datacenters are displayed. After you select a folder and click OK, verify that the folder on the **Recovery Options** dialog contains the destination ESX server. If the selected folder is on the wrong datacenter, the restore fails.

Select Datastore or Datastore Cluster dialog box (restore to alternate location)

Use this screen to select a datastore or datastore cluster for the restored virtual machine. You can use the search field, or drill down manually into the list.

Note: Only datastores and clusters visible to the ESX server are displayed.

Specify Datastore

Type a name and click **Search**. The list of available datastores and datastore clusters automatically expands and the nearest match is highlighted.

Virtual Machine Options dialog box (restore to alternate location)

This dialog is described in a previous topic:

See “Virtual Machine Options dialog box” on page 184.

Storage Destination dialog box (restore to alternate location)

Select the datastores where the .vmdk files are to be restored.

- **Source VMDK File Name**
  Shows the names of the .vmdk files that were backed up.
- **Datastore/Datastore Cluster**
  Shows the VMware datastore or datastore cluster where the .vmdk files are to be restored. Click in this field to select another datastore.
  See "Select Datastore or Datastore Cluster dialog box (restore to alternate location)" on page 193.
  If the datastore is in a datastore cluster, NetBackup displays the name of the datastore (not the name of the cluster).
- **Datastore/Datastore Cluster Status**
  Indicates whether the datastore or datastore cluster has enough space to contain the selected .vmdk file.

OK	The datastore or datastore cluster has enough space to contain the selected .vmdk file.
Insufficient space	The datastore or datastore cluster does not have enough space to contain the selected .vmdk file.

Network Connections and Other Recovery Options dialog box (restore to alternate location)

For restore into vSphere, this dialog displays all of the networks that the restored virtual machine can connect to.

For restore into vCloud Director, this dialog displays the networks that the virtual machine was connected to (if any) at the time of the backup.

For vCloud Director: If the virtual machine was not connected to any networks during backup, or if none of those networks are currently available, the dialog states: "No networks available for selected virtual machine." In that case, if a network connection is required, create it after the restore completes.

- **Retain original network configuration**
  If possible, this option retains the original MAC address and other configuration settings of the virtual machine. Note that vCenter assigns a new MAC address if the original exists. This option configures the virtual machine with its original network labels, even if those networks are not available at the restore location. When you select this option, any network names that are shown in this dialog are ignored.
  If this option is unselected, the virtual machine's original network settings are discarded. You can select available networks under **Network Names**.

- **Network Names**
  The available virtual networks are displayed in addition to physical networks. Select the networks that you want the restored virtual machine to be connected to. This option creates new network adaptors for the selected networks.

  Note: On the restored virtual machine, the network adapters are not configured.

  Note: Click the **Network Names** check box to select or unselect all the networks in the list.

  Use **Move Up** and **Move Down** to reorder the networks. The order in the list determines the order of the corresponding virtual network adapters (NIC cards) for the virtual machine.
  When the virtual machine is backed up, its network connections (physical or virtual) are recorded in the NetBackup catalog.

  For vSphere, NetBackup determines what networks currently exist at the restore location and lists the network names as follows:

  - If a network that was recorded in the backup catalog for the virtual machine still exists, it is listed on this screen and automatically selected.
  - If a network is available that was not listed in the NetBackup catalog, it is listed on this screen but not selected.
  - If a network was recorded in the backup catalog but is not currently available, it is not listed.

Perform Recovery dialog box (restore to alternate location)

- **Recovery settings**
  Lists the settings that are used for the recovery.
- **Run Pre-Recovery Check**
  Verifies the credentials and appropriate paths and connectivity, determines whether the datastore or datastore cluster has available space, and reviews other requirements. You must run this check at least once. You can proceed with the restore even if the check fails. More details are available on the **Pre-Recovery Check**.
  See “Perform Recovery dialog box” on page 187.
- **Start Recovery**
  Starts the recovery of the virtual machine.

About VMware virtual machine disk restore

NetBackup supports the restore of individual VMware virtual machine disks to the following destinations:

To the original VM	You can restore the disks to the same VM from which the disks were backed up. You can either overwrite the original disks or attach the virtual disks without overwriting the original disks. NetBackup creates a temporary VM to which it restores the virtual disks. Then, NetBackup attaches the virtual disks to the existing, target VM. Finally, NetBackup deletes the temporary VM after the disk or disks are attached successfully. A special case, called in-place disk restore, replaces all disks of an existing VM with the data in its backup. Raw devices (RDMs) and independent disks are not replaced or deleted. For In-place Disk Restore, the disks are restored to the same disk controller configuration acquired at the time of backup.
To a different VM	You can restore the disks to a different VM. NetBackup creates a temporary VM to which it restores the virtual disks. Then, NetBackup attaches the virtual disks to the existing, target VM. Finally, NetBackup deletes the temporary VM after the disk or disks are attached successfully. You can also perform an in-place disk restore to a different VM.
To a new VM	NetBackup creates a new virtual machine and restores the specified disks to the new VM. The new VM is intended to be a container for the restored disks. It does not have enough resources to run most operating systems. After the restore, you should attach the restored virtual disks to a VM that can support them and then delete the restore VM.

The following are the general support requirements for virtual disk restore.

- Sufficient storage must exist for the restore.
- NetBackup does not support the following virtual machine disk restores:
  - From NetBackup Replication Director for VMware backups.
  - To templates. However, virtual disks from a backup of a VM template can be restored to a virtual machine.

Restoring VMware virtual machine disks by using Backup, Archive, and Restore

This restore method uses the Backup, Archive, and Restore interface to select the parameters for the restore and to restore the disks. NetBackup 8.1 or later is required.

To restore virtual machine disks

1. In the NetBackup Administration Console, select **Backup, Archive, and Restore**.

   Note: The NetBackup Administration Console does not support the in-place disk restore option.

2. Select the **Restore Files** tab.
3. Click **Actions > Specify NetBackup Machines and Policy Type**.

4 Specify the following:

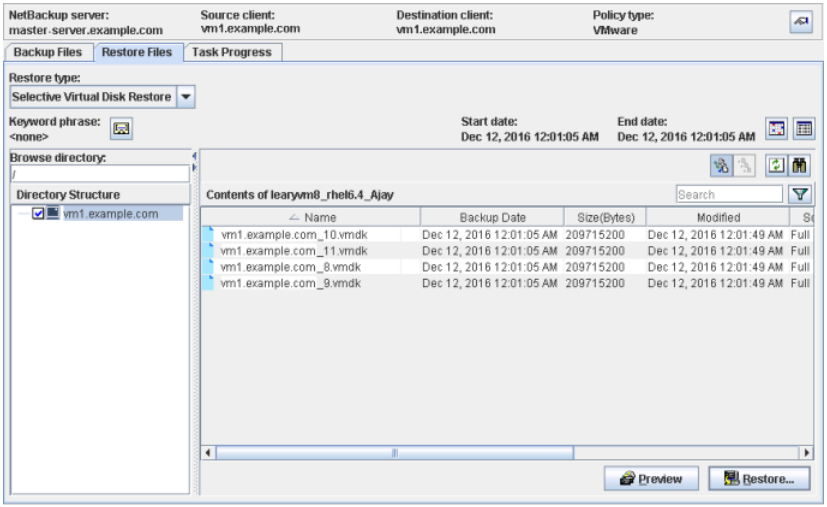
Server to use for backup and restores	The NetBackup primary server that directed the backup
Source client for restores	The VMware virtual machine that was backed up. Click **Search VM Clients** to search or browse for a virtual machine. Use this option to locate a virtual machine in a large, multi-layered virtual environment. See "Browse and search virtual machines for restore" on page 232. Or enter the type of name that was selected for the **Primary VM identifier** option on the policy **VMware** tab. For example, if the **Primary VM identifier** option is set to VM host name, enter the virtual machine's host name.
Destination client for restores	This field defaults to the same client selected in the **Source client for restores** field. You select the destination client in the wizard, so you do not have to change this field.
Policy type for restores	Select **VMware**.

If any backups for the client are within the specified date range, NetBackup populates the **Directory Structure** pane and the **Contents of...** pane with the information about the most recent backup.

5 In the **Restore type** drop-down menu on the **Restore Files** tab, select **Virtual Disk Restore**.

The **Directory Structure** pane changes to show the client name.

6 In the **Directory Structure** pane, select the client.



7 To restore disks from a backup other than the most recent:

a. On the **Actions** menu, select **Set Date Range > Backup History**.

b. In the **Backup History** dialog box, select the wanted backup and click **OK**.

8 Click **Restore**.

The **Select Virtual Disks** panel of the **Restore Virtual Machine Disks** wizard appears.

9 Complete the wizard panels to restore the virtual disks.

See “Select Virtual Disks panel” on page 199.

See “Recovery Destination panel” on page 200.

See “Virtual Disk Destination panel” on page 201.

See “Storage Destination panel” on page 203.

See “Recovery Summary panel” on page 203.

Select Virtual Disks panel

The **Select Virtual Disks** wizard panel shows all of the virtual disks that were in the VM at back-up time, even those that were excluded from the backup. By default, the wizard displays the virtual disks. To select file systems, click **File Systems**.

- **Virtual Disks**
  Select the disks that you want to restore.
  If you use the check box in the column header to select all, the wizard selects only those disks that were included in the backup.
- **File Systems**
  Select the wanted file systems. When you select a file system, the wizard selects the virtual disks on which the file system resides.
  If you use the check box in the column header to select all, the wizard selects only those file systems that were included in the backup.

Recovery Destination panel

On the **Recovery Destination** panel, you can configure the transport mode and the recovery destination parameters.

- **NetBackup Recovery Host**
  The host that performs the restore. If not specified, NetBackup uses the backup host value from the backup image.
- **Media Server**
  You can use this option to select a media server that has access to the storage unit that contains the backup image. An example of such an environment is a Media Server Deduplication Pool (MSDP) with multiple media servers. Note: If the storage unit that contains the backup image is not shared with multiple media servers, this option is grayed out.
- **Transport modes**
  The transport modes to use for the restore. Select the wanted transport modes and move them so they are in the wanted order. If all methods fail, the restore fails.
  By default, the wizard displays the transport mode combination and the order that were used for the backup.
- **Recover virtual disks to**

  The destination VM for the restore, as follows:

  - **Original Virtual Machine**. NetBackup restores the selected disks to the VM from which they were backed up.
    You can select whether to overwrite the existing virtual disks on the **Storage Destination** panel.
    See “Storage Destination panel” on page 203.
  - **Alternate Virtual Machine**. NetBackup restores the selected disks to a different VM than the original.

- **New (Temporary) Virtual Machine**. NetBackup creates a new virtual machine and restores the selected disks to the new VM. The new VM is intended to be a container for the restored disks. It does not have enough resources to run most operating systems. After the restore, you should attach the restored virtual disks to a VM that can support them and then delete the temporary VM.

- **Advanced Restore Options**

  The following items describe the advanced restore options:

  - **Delete restored staging VM on error**. Whether to delete the temporary VM if the disk attach operation fails. If you select **No** and the disks are not successfully attached to the target VM, you can access the data on the temporary VM.
  - **Wait time in seconds for VM shutdown**. The restore process shuts down the target virtual machine before it attaches the disk or disks. The duration of the shutdown operation depends on the VMware workload. Use this parameter to specify how long the restore process should wait for shutdown before giving up on restore.

Virtual Disk Destination panel

The contents of the **Virtual Disk Destination** wizard panel depend on the recovery destination, as follows:

- **Original Virtual Machine**
  The panel displays **Destination details** of the original VM.
  You can select the power state of the VM after the restore. You also can refresh **Virtual Machine Server** details.
  See **Power on virtual machine after restore** and **Last update** in Table 10-2.

- **Alternate Virtual Machine**
  The panel displays **Destination details** of the original VM.
  To select a destination VM:

  a. Optionally, select a different **Virtual Machine Server**.

  b. Optionally, enter a term in the Search box to find a VM on the **Virtual Machine Server** and click **Search**.

  c. Select the destination VM for the restored virtual disks.

  When you select a VM, the wizard populates the **Destination details** with the details of that VM.

You can select the power state of the VM after the restore. You also can refresh **Virtual Machine Server** details.

See **Power on virtual machine after restore** and **Last update** in Table 10-2.

- **New (Temporary) Virtual Machine**

  You must select the destination details.

  See the field descriptions in Table 10-2.

Table 10-2 Virtual disk destination field descriptions

Field	Description
Virtual Machine Server	The name of the VMware host on which the destination VM resides or should be created.
ESX Server	Restore to a new VM only. The name of the ESX host to which NetBackup should restore the virtual machine disks. By default, NetBackup uses the value from the backup. To use a different host, click **Browse** to select or search for a host.
Data Center	Restore to a new VM only. The data center to which to restore the virtual disks.
Folder	Restore to a new VM only. The pathname of the VM folder to which NetBackup should restore the virtual machine disks. By default, NetBackup uses the value from the backup. Click **Browse** to select a different folder.
Virtual Machine	Restore to a new VM only. The display name of the temporary virtual machine for the restored disk or disks. The wizard populates this field with the name of the original VM client and appends a timestamp to it. The timestamp is the decimal number of seconds since January 1, 1970. The name must be unique.
Resource Pool/vApp	Restore to a new VM only. The resource pool or vApp to which NetBackup should restore the virtual machine disks. By default, NetBackup uses the value from the backup.

Table 10-2 Virtual disk destination field descriptions *(continued)*

Field	Description
Power on virtual machine after restore	Restore to the original or to an alternate VM only. Select to start the virtual machine after the restore completes successfully.
Last update	Restore to the original or to an alternate VM only. The date and time on which the **Virtual Machine Server** provided the information for this wizard panel. Click the refresh option to update the **Virtual Machine Server** details.

Storage Destination panel

The **Storage Destination** wizard panel shows the virtual disks to restore. They are either the disks you selected or the disks on which the file systems you selected for restore reside.

Settings for all virtual disks region

To change the values that apply to all of the virtual disks, use the fields in the **Settings for all virtual disks** region of the wizard panel, as follows:

- **Restored virtual disks provisioning**
  The default disk provisioning for all of the disks to be restored: **Thin**, **Thick Lazy Zeroed**, or **Thick Eager Zeroed**.
- **Datastore**
  The name of the **Datastore** or the datastore cluster that is the destination for the restore.
  Click **Browse** to select a different datastore or datastore cluster.
- **Overwrite all virtual disks**
  Whether to overwrite the existing virtual disk or disks on the target VM. If **Yes**, overwrite the original virtual disk and retain the disk UUID. If **No**, restore the virtual disk to the target VM as a new disk; VMware assigns a new UUID to the disk.

Original Virtual Disk list

To override the global settings, change the values for individual virtual disks in the **Original Virtual Disk** list.

Recovery Summary panel

The **Recovery Summary** wizard panel displays the parameters of the recovery.

Verify the settings for the recovery. If they are correct, click **Start Recovery**. Otherwise, click **Back** to return and change the settings.

Restoring VMware virtual machine disks by using NetBackup commands

This restore method requires that you describe in a text file the parameters of the restore and then use a NetBackup command to restore the disks. The file in which you describe the restore includes the following information:

- The backup image from which you want to restore.
- The target VM if restoring to an existing VM.
- The virtual machine disks to restore.
- Other parameters that control aspects of the restore.

The NetBackup `nbrestorevm` command includes an option that you can use to create the required *restore parameters* file from a backup image. The NetBackup `nbrestorevm` command then reads that file to accomplish the restore.

The restore parameters file uses the JavaScript Object Notation (JSON) format to describe the restore parameters.

The following table identifies the tasks in the process to restore an individual VMware virtual machine disk or disks. It also includes links to the individual task topics.

Table 10-3 Restore VMware virtual machine disk process

Step	Description	Link
Step 1	Optionally, determine the ID of the backup image from which to create the restore parameters file. If you want to use a date range to specify the backup image, you do not have to perform this task.	See "Determining the backup image ID from which to restore a VMware virtual machine disk" on page 205.
Step 2	Create the file that describes the parameters of the restore. You use the file as input for the command that restores the virtual disks.	See "Creating the VMware virtual machine disk restore file" on page 206.
Step 3	Modify the parameters of the virtual machine disk restore file. You must modify the file to describe your specific restore instance.	See "Modifying the virtual machine disk restore file" on page 208.

Table 10-3 Restore VMware virtual machine disk process *(continued)*

Step	Description	Link
Step 4	Validate the virtual machine disk restore file to ensure that the restore occurs correctly.	See "Validating the virtual machine disk restore file" on page 212.
Step 5	Restore the disk or disks.	See "Restoring the virtual machine disk or disks by using the `nbrestorevm` command" on page 213.

See "Troubleshooting vmdk restore to existing VM" on page 318.

Determining the backup image ID from which to restore a VMware virtual machine disk

This topic describes how to determine the ID of the backup image from which to restore a VMware virtual machine disk. You then use the backup image ID to specify the backup from which to create the restore parameters file. Two methods exist to determine the backup ID, as follows:

NetBackup Administration Console	See To determine the backup image ID by using NetBackup Administration Console.
`bpclimagelist` command	See To determine the backup image ID by using the `bpclimagelist` command.

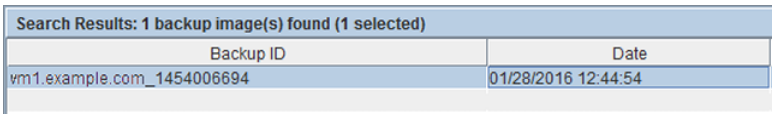
Note: If you want to use a date range to specify the backup from which to create the restore parameters file, you can skip this task.

This task is part of a larger process that describes how to restore an individual VMware virtual machine disk or disks.

See "Restoring VMware virtual machine disks by using NetBackup commands" on page 204.

To determine the backup image ID by using NetBackup Administration Console

1 Use the **NetBackup Administration Console Catalog** utility to search for the backup image of the client from which to restore. The **Search Results** pane of the **Catalog** utility shows the backup ID:



2 Continue to the next task in the individual virtual machine disk restore process.

See "Creating the VMware virtual machine disk restore file" on page 206.

To determine the backup image ID by using the `bpclimagelist` command

1 Invoke the NetBackup `bpclimagelist` command to display the backups for the client, as follows:

On UNIX: `/usr/openv/netbackup/bin/bpclimagelist -client client_name -Likelydate -policy policy_name`

On Windows: `install_path\NetBackup\bin\bpclimagelist -client client_name -Likelydate -policy policy_name`

2 Construct the backup ID by combining the client name, an underscore character (_), and the backup time notation (the decimal number of seconds since January 1, 1970). For the following example output, `vm1.example.com_1454006694` is the backup ID:

```
bpclimagelist -client vm1.example.com -Likelydate -policy backups
Client:            vm1.example.com
Policy:            backups
Keyword:           NONE
Backup Time:       Thu Jan 28 12:44:54 2016 (1454006694)
Schedule Type:     FULL
```

3 Continue to the next task in the individual virtual machine disk restore process.

See "Creating the VMware virtual machine disk restore file" on page 206.

Creating the VMware virtual machine disk restore file

This topic describes how to use the NetBackup `nbrestorevm` command to create the text file that describes the virtual machine disk restore parameters. The file uses the JavaScript Object Notation (JSON) format to describe the restore parameters.

Two methods exist to specify the backup that is used to create the restore parameters file, as follows:

Specify a backup image ID	See To create the VMware virtual machine disk restore file by specifying a backup ID . A separate procedure describes how to determine the backup ID. See "Determining the backup image ID from which to restore a VMware virtual machine disk" on page 205.
Specify a date range	If you specify a date range, NetBackup uses the most recent backup in that date range. See To create the VMware virtual machine disk restore file by specifying a date range.

This task is part of a larger process that describes how to restore an individual VMware virtual machine disk or disks.

See "Restoring VMware virtual machine disks by using NetBackup commands" on page 204.

To create the VMware virtual machine disk restore file by specifying a backup ID

1. Create the file that describes the virtual machine disk or disks that you want to restore by specifying a backup ID, as follows:

   On Windows: `install_path\NetBackup\bin\nbrestorevm -vmw -C vm_client -S primary_server -backupid value -restorespecout filename`

   On UNIX: `/usr/openv/netbackup/bin/brestorevm -vmw -C vm_client -S primary_server -backupid value -restorespecout filename`

   - The `-backupid value` option and argument specifies the backup image from which to create the file.
   - The `-restorespecout filename` option and argument specifies the name of the file.
     By default, `nbrestorevm` creates the file in the current working directory. To create the file in a different directory, specify a pathname for the *filename*.

2. Continue to the next task in the individual virtual machine disk restore process.

   See "Modifying the virtual machine disk restore file" on page 208.

To create the VMware virtual machine disk restore file by specifying a date range

1. Create the file that describes the virtual machine disk or disks that you want to restore by specifying a date range, as follows:

   On Windows: *install_path*\NetBackup\bin\nbrestorevm -vmw -C *vm_client* -S *primary_server* -s *mm/dd/yyyy hh:mm:ss* -e *mm/dd/yyyy hh:mm:ss* -restorespecout ***filename***

   On UNIX: /usr/openv/netbackup/bin/nbrestorevm -vmw -C *vm_client* -S *primary_server* -s *mm/dd/yyyy hh:mm:ss* -e *mm/dd/yyyy hh:mm:ss* -restorespecout ***filename***

   - The *hh:mm:ss* for the start date and the end date are optional.
   - The -restorespecout ***filename*** option and argument specifies the name of the file.
     By default, nbrestorevm creates the file in the current working directory. To create the file in a different directory, specify a pathname for the ***filename***.

2. Continue to the next task in the individual virtual machine disk restore process.

   See "Modifying the virtual machine disk restore file" on page 208.

Modifying the virtual machine disk restore file

This topic describes how to modify the file that describes the virtual machine disk restore parameters. You must modify the file to describe your specific restore instance.

Two methods exist to modify the restore file, as follows:

A text editor	With a text editor, you can modify any or all of the fields. See To modify a VMware virtual machine disk restore file by using a text editor.

A Veritas provided Perl script

With the `restore_spec_utility.pl` Perl script, you can perform the following operations:

- `-modify`, to change the value of a field, one field at a time. Use this option to modify the fields that do *not* describe `VMWareVirtualDiskDestination` parameters.
- `-keep_disks`, to specify the disks to retain in the restore parameters file. Any other disks are removed from the file.
- `-delete_disks`, to specify the disks to delete from the restore parameters file. The disks that remain are restored.

Examine the script for a description of the options and example usage statements.

Perl must be installed on the host on which you modify the restore parameters file. Examine the script to determine which modules are required; some may require separate installation.

See To modify a VMware virtual machine disk restore file by using the `restore_spec_utility.pl` script.

The following table describes some restore scenarios and the values of the fields that are required to accommodate those scenarios.

Table 10-4 Restore parameters file items to edit

Item	Description
Disks	Edit the `VMwareVirtualDiskDestination` section of the file so that it contains only the virtual machine disk or disks that you want to restore. To ensure data integrity, be aware of the following: ■ If a file system volume spans multiple virtual machine disks, restore all of the virtual disks for that volume. ■ If a volume manager manages the volumes, restore all of the virtual disks in that volume set.
Restore to a datastore cluster	For a restore of virtual disks to a datastore cluster, specify the name of the datastore cluster in the `Datastore` field of the `VMwareVirtualDiskDestination` section. Do *not* specify the cluster in the `Path` field. **Note:** If the restore is to an existing VM, the VMDKs are not located in the existing datastore path for the VM. They reside in a datastore path based on the name of the temporary VM used in the restore. The name of the temporary VM is available in the details for the restore job in NetBackup.

Table 10-4 Restore parameters file items to edit *(continued)*

Item	Description

Restore to an existing VM	By default, the restore parameters file that the `nbrestorevm -restorespecout` command creates is configured to restore to a new VM. To restore the virtual disks to an existing VM, do the following:
	■ Specify the name of the VM in the `VMName` field. The VM must exist in the target vCenter or ESXi serve; if it does not exist, the restore fails with status code 2820.
	■ Change the value of the `AttachDisksToExistingVM` field from `No` to `Yes` or, in the case of in-place disk restores, `DeleteAllDisksAndReplace`.
	■ If a virtual disk to restore exists on the target VM already, configure the `OverwriteExistingDisk` field, as follows:
	  ■ To overwrite the original virtual disk and retain the disk UUID, specify `Yes`.
	  ■ To restore the virtual disk to the target VM as a new disk, specify `No`. VMware assigns a new UUID to the disk. The default is `No`.
	  Disk UUIDs are always preserved with in-place disk restores.
	■ The restore process shuts down the target virtual machine before it attaches the disk or disks. By default, NetBackup does not turn on the target VM. To turn on the target VM, specify `Yes` for the `PowerOn` option.
	The `VMwareAdvancedRestoreOptions` section of the restore parameters file includes other parameters that are related to restoring to an existing VM.
	The restore job details show the datastore path of the virtual disk when it was backed up and after it is restored.

Standalone ESXi hypervisor	To restore to a standalone ESXi hypervisor when the backup was through a vCenter, edit the following fields so that their values are `None`, as follows: ■ `"vCenterServer": "None"` ■ `"Folder": "None"` ■ `"Datacenter" : "None"`
The VM name	The `nbrestorevm -restorespecout` command adds a timestamp to the name of the original VM client when it populates the `VMName` field in the restore parameters file. The timestamp is the decimal number of seconds since January 1, 1970. Depending on the requirements of the restore instance, you may need to edit the `VMName` field.

Table 10-4 Restore parameters file items to edit *(continued)*

Item	Description
Other fields	Edit any of the other fields so that the values that describe the restore meet your needs. See "VMware virtual machine disk restore file" on page 214.

This task is part of a larger process that describes how to restore an individual VMware virtual machine disk or disks.

See "Restoring VMware virtual machine disks by using NetBackup commands" on page 204.

To modify a VMware virtual machine disk restore file by using a text editor

1. Open the restore file in a text editor.
2. Modify the parameters as necessary, save the file, and then close the editor.

   See "VMware virtual machine disk restore file" on page 214.
3. Continue to the next task in the individual virtual machine disk restore process.

   See "Validating the virtual machine disk restore file" on page 212.

To modify a VMware virtual machine disk restore file by using the `restore_spec_utility.pl` script

1. Invoke the Perl script to modify the restore parameters file as necessary, one field at a time. Examples of three supported `-req_type` operations follow:

   - The following is an example of a `modify` operation to change the `VMName` field:

     Windows: `perl.exe C:\Progra~1\Veritas\NetBackup\bin\goodies\restore_spec_utility.pl -req_type modify -file_path` **`restore_filename`** `-field VMName -value` **`new_vm_name`**

     UNIX: `perl /usr/openv/netbackup/bin/goodies/restore_spec_utility.pl -req_type modify -file_path` **`restore_filename`** `-field VMName -value` **`new_vm_name`**

   - The following is an example of a `keep_disks` operation to retain a subset of the disks that are described in a restore parameters file. It retains the `scsi0-1` and `scsi0-2` virtual disks and deletes all of the other defined disks from the file:

     Windows: `perl.exe C:\Progra~1\Veritas\NetBackup\bin\goodies\restore_spec_utility.pl`

```
-req_type keep_disks -file_path restore_filename -controller
scsi0-1,scsi0-2
```

UNIX:

```
perl
/usr/openv/netbackup/bin/goodies/restore_spec_utility.pl
-req_type keep_disks -file_path restore_filename -controller
scsi0-1,scsi0-2
```

- The following is an example of a `delete_disks` operation to delete a subset of the disks that are described in a restore parameters file. It deletes the `scsi0-1` and `scsi0-2` virtual disks and retains the other defined disks in the file:

  Windows:

  ```
  perl.exe
  C:\Progra~1\Veritas\NetBackup\bin\goodies\restore_spec_utility.pl
  -req_type delete_disks -file_path restore_filename -controller
  scsi0-0,scsi0-1
  ```

  UNIX:

  ```
  perl
  /usr/openv/netbackup/bin/goodies/restore_spec_utility.pl
  -req_type delete_disks -file_path restore_filename -controller
  scsi0-0,scsi0-1
  ```

- The following is an example of modifying a restore specification for In-place disk restore:

  Windows:

  ```
  perl.exe
  C:\Progra~1\Veritas\NetBackup\bin\goodies\restore_spec_utility.pl
  -req_type modify -file_path restore_filename -field
  AttachDisksToExistingVM -value DeleteAllDisksAndReplace
  ```

  UNIX:

  ```
  perl
  /usr/openv/netbackup/bin/goodies/restore_spec_utility.pl
  -req_type modify -file_path restore_filename -field
  AttachDisksToExistingVM -value DeleteAllDisksAndReplace
  ```

2. Repeat step 1 until you have finished modifying the file.
3. Continue to the next task in the individual virtual machine disk restore process.

   See "Validating the virtual machine disk restore file" on page 212.

Validating the virtual machine disk restore file

This topic describes how to use the NetBackup `nbrestorevm` command to validate the file that describes the virtual machine disk restore parameters.

This task is part of a larger process that describes how to restore an individual VMware virtual machine disk or disks.

See "Restoring VMware virtual machine disks by using NetBackup commands" on page 204.

To validate the virtual machine disk restore file

1. Invoke the following NetBackup command:

   On Windows: *install_path*\NetBackup\bin\nbrestorevm -validate -restorespec ***filename***

   On UNIX: /usr/openv/netbackup/bin/nbrestorevm -validate -restorespec ***filename***

2. Examine the command output. If the output indicates problems, edit the file to fix the problems.
3. Repeat steps 1 and 2 until the file is valid.
4. Continue to the next task in the individual virtual machine disk restore process.

   See "Restoring the virtual machine disk or disks by using the nbrestorevm command" on page 213.

Restoring the virtual machine disk or disks by using the nbrestorevm command

This topic describes how to use the NetBackup nbrestorevm command to restore one or more virtual machine disks to a new VMware virtual machine.

This task is part of a larger process that describes how to restore an individual VMware virtual machine disk or disks.

See "Restoring VMware virtual machine disks by using NetBackup commands" on page 204.

To restore a VMware virtual machine disk

1. If the file is valid, restore the virtual machine by invoking the following NetBackup command:

   On Windows: *install_path*\NetBackup\bin\nbrestorevm -restorespec ***filename*** [-L *progress_log*] [-w [*hh:mm:ss*]]

   On UNIX: /usr/openv/netbackup/bin/nbrestorevm -restorespec ***filename*** [-L *progress_log*] [-w [*hh:mm:ss*]]

   - The -restorespec ***filename*** option specifies the name of the file that contains the parameters of the restore.

- The `-L progress_log` option specifies the name of an existing file in which to write progress information. Only default paths are allowed for this option; the following are the default paths:
  UNIX systems: `/usr/openv/netbackup/logs/user_ops/proglog`
  Windows systems: *install_path*`\NetBackup\logs\user_ops\proglog`
- The `-w [hh:mm:ss]` option causes NetBackup to wait for a completion status from the server before it returns you to the system prompt.
  The required date and time values format in NetBackup commands varies according to your locale. The `/usr/openv/msg/.conf` file (UNIX) and the *install_path*`\VERITAS\msg\LC.CONF` file (Windows) contain information such as the date-time format for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.
  You can optionally specify a wait time in hours, minutes, and seconds. The maximum wait time you can specify is `23:59:59`. If the wait time expires before the restore is complete, the command exits with a time-out status. The restore, however, still completes on the server.
  If you specify 0 or do not specify a time, the wait time is indefinite for the completion status.

2. Monitor the restore in the **NetBackup Administration Console Activity Monitor**.

   See "Troubleshooting vmdk restore to existing VM" on page 318.

3. After the restore completes, do the following as necessary:
   - For the virtual disks that are restored to a new VM, add the disks to a VM that can support them after the restore succeeds. Optionally, delete the VM that NetBackup created for the restore.
   - For the virtual disks that are restored to an existing VM, assign a drive letter (Windows) or mount the disk (Linux) so you can access the data.

   How to add disks, delete virtual machines, and mount drives is beyond the scope of the NetBackup documentation. See your VMware documentation.

VMware virtual machine disk restore file

This topic describes the parameters that NetBackup uses to restore a virtual machine disk or disks. NetBackup requires that the parameters be described in a text file that uses the JavaScript Object Notation (JSON) format. The NetBackup `nbrestorevm` command reads the file to obtain the necessary information about the virtual machine disks. NetBackup has no requirements for the file name other than those imposed by the operating system.

You can use the `nbrestorevm` command to generate the file from an existing backup. How to do so is described in a different topic.

See "Creating the VMware virtual machine disk restore file" on page 206.

The following is an example template of the required file:

```
{
  "ClientType": "VMware",
  "ClientName": "VM-client-name",
  "RestoreType": "SelectiveDiskRestore",
  "BackupImageSelection": {
    "PrimaryServer": "Primary-server-name",
    "StartDate": "mm/dd/yy hh:mm:ss",
    "EndDate": "mm/dd/yy hh:mm:ss",
    "BackupId": "clientname_timestamp"
  },
  "VMwareRestoreParameters": {
    "vCenterServer": "vCenter-name-for-restore",
    "VMwareRecoveryHost": "Recovery-host-name",
    "DefaultDiskProvisioning": "thin",
    "TransportMode": "san:hotadd:nbd",
    "vmdk_compression": "none",
    "VMwareVirtualMachineDestination": {
      "VMName": "Restore-vm-name",
      "AttachDisksToExistingVM": "No",
      "PowerOn": "No",
      "Datacenter": "Path-of-Datacenter-for-destination-vm",
      "ESX": "Hostname-of-the-ESX-host",
      "Folder": "Path-to-destination-VM-folder",
      "ResourcePool/Vapp": "Path-of-vApp-or-resource-pool-destination",
      "VmxDatastore": ""
    },
    "VMwareVirtualDiskDestination": [
      {
         "VirtualDisk" : "/DS1/BackedupVM/BackedupVM.vmdk",
         "OverwriteExistingDisk": "No",
         "Datastore": "[Datastore-name]",
         "Path": "",
         "Provisioning": "thin"
         "Controller": "scsi0-0"
      },
      {
         "VirtualDisk": "/DS2/BackedupVM/BackedupVM_1.vmdk",
```

```
        "OverwriteExistingDisk": "No",
        "Datastore": "",
        "Path": "[datastore_name] MyVm/MyVM_1.vmdk”,
        "Provisioning": "eagerzeroed"
        "Controller": "scsi0-1"
      }
    ]
    "VMwareAdvancedRestoreOptions": {
      "DeleteRestoredVMOnError": "No",
      "VMShutdownWaitSeconds": 900
    }
  }
}
```

The following is an example of the required file for In-place disk restore:

```
{
  "BackupImageSelection": {
    "StartDate": "mm/dd/yy hh:mm:ss",
    "BackupId": "clientname_timestamp"
    "EndDate": "mm/dd/yy hh:mm:ss",
    "PrimaryServer": "Primary-server-name",
  },
  "ClientName": "VM-client-name",
  "VMwareRestoreParameters": {
    "vmdk_compression": "none",
    "VMwareAdvancedRestoreOptions": {
      "VMShutdownWaitSeconds": 900,
      "DeleteRestoredVMOnError": "No"
    },
    "VMwareRecoveryHost": "VM-recovery-host-name",
    "VMwareVirtualMachineDestination": {
      "ResourcePool/Vapp": "Path-of-vApp-or-resource-pool-destination",
      "VmxDatastore": "Vmx-datastore-name",
      "Datacenter": "Path-of-Datacenter-for-destination-vm",
      "AttachDisksToExistingVM": "DeleteAllDisksAndReplace",
      "ESX": "Hostname-of-the-ESX-host",
      "VMName": "Restore-vm-name",
      "Folder": "Path-to-destination-VM-folder",
      "PowerOn": "Yes"
    },
    "DefaultDiskProvisioning": "unknown",
    "TransportMode": "nbdssl",
    "VMwareVirtualDiskDestination": [],
```

```
    "vCenterServer": "vCenter-name-for-restore"
  },
  "ClientType": "VMware",
  "RestoreType": "SelectiveDiskRestore"
}
```

The following subsections describe the parameters in the file. The optional sections or optional fields that you do not want to use must be omitted from the file.

See "About VMware virtual machine disk restore" on page 196.

Global fields

The first section of the file specifies the required information about the client that contains the disks that you want to restore. The following table describes the fields in the first, global section:

Table 10-5 Global fields (required)

Field name	Description	Required?
`ClientType`	The client type as configured in the backup policy. For Vmware virtual machine disk restore, use `VMware`.	Required.
`ClientName`	The client name as configured in the backup policy.	Required.
`RestoreType`	The type of restore. For Vmware virtual machine disk restore, use `SelectiveDiskRestore`.	Required.

BackupImageSelection

The `BackupImageSelection` section of the file specifies the information that NetBackup requires to identify the backup image to restore. If this section is not specified, NetBackup restores the most recent backup. The following table describes the fields in the `BackupImageSelection` section:

Table 10-6 The `BackupImageSelection` section (optional)

Field name	Description	Required?
`PrimaryServer`	The fully-qualified domain name of the NetBackup primary server to use to query the VM details. If not specified, NetBackup uses the primary server that backs up the VM.	Optional.
`StartDate`	The start date to look for backup images, in *mm/dd/yy hh:mm:ss* format. If more than one backup image exits in the date range, NetBackup selects the most recent backup. If not specified, the start date is 6 months earlier than the current date.	Optional.

Table 10-6 The `BackupImageSelection` section (optional) *(continued)*

Field name	Description	Required?
`EndDate`	The end date to look for backup images, in *mm/dd/yy hh:mm:ss* format. If more than one backup image exits in the date range, NetBackup selects the most recent backup. If not specified, NetBackup uses the current date.	Optional.
`BackupId`	The ID of the backup image to use for the restore, in *`clientname_backuptime`* format. The *`backuptime`* is the decimal number of seconds since January 1, 1970. If not specified, NetBackup uses the most recent backup image. If you specify a `StartDate`, `EndDate`, and a valid `BackupId`, NetBackup restores from the `BackupId` image.	Optional.

VMwareRestoreParameters

The `VMwareRestoreParameters` section of the file contains the following:

- The restore parameters of the VM. All of the fields in this section are optional; however, the section is required because it also contains two required subsections. See Table 10-7.
- A `VMwareVirtualMachineDestination` subsection, which specifies the destination parameters for the restore.
  See the section called “VMwareVirtualMachineDestination” on page 219.
- A `VMwareVirtualDiskDestination` subsection, which specifies the disks to restore and the restore parameters for those disks.
  See the section called “VMwareVirtualDiskDestination” on page 221.
- A `VMwareAdvancedRestoreOptions` subsection, which specifies parameters to restore to an existing VM.
  See the section called “VMwareAdvancedRestoreOptions” on page 223.

Table 10-7 The `VMwareRestoreParameters` section (required)

Field name	Description	Required?
`vCenterServer`	The host name of the destination vCenter for the restore, in the same format as specified in the **NetBackup Virtual Server** credentials. To restore to a standalone ESXi hypervisor when the backup was through a vCenter, the value of this field must be `None`.	Optional.

Table 10-7 The `VMwareRestoreParameters` section (required) *(continued)*

Field name	Description	Required?
`VMwareRecoveryHost`	The host that performs the restore. If not specified, NetBackup uses the backup host value from the backup image.	Optional.
`DefaultDiskProvisioning`	The default disk provisioning for all of the disks to be restored: `thin`, `thick`, `eagerzeroed`, or `unknown`. For each disk, you can override this default by specifying a different `Provisioning` value in the `VMwareVirtualDiskDestination` section of the file. If neither `DefaultDiskProvisioning` or `Provisioning` are specified, NetBackup uses the provisioning specified in the backup.	Optional.
`TransportMode`	The transport mode combination to use for the restore as specified in lowercase, colon separated values: `hotadd:nbd:nbdssl:san`. The order of the specification is significant; NetBackup attempts each method in turn until the restore succeeds. If all methods fail, the restore fails. If not specified, NetBackup uses the transport mode combination that was used for the backup.	Optional.
`vmdk_compression`	The vmdk compression type to use for full and selective vmdk restores. Vmdk compression types are: `zlib`, `skipz`, and `fastlz`. If not specified, NetBackup uses `none` as the value.	Optional.

VMwareVirtualMachineDestination

The `VMwareVirtualMachineDestination` section of the file specifies the destination parameters for the restore. The following table describes the fields in the `VMwareVirtualMachineDestination` section. This section is subordinate to the `VMwareRestoreParameters` section.

Table 10-8 The `VMwareVirtualMachineDestination` section (required)

Field name	Description	Required?
`VMName`	The unique display name of the new virtual machine for the restored disk or disks. The `nbrestorevm` command adds a timestamp to the name of the original VM client when it populates this field. The timestamp is the decimal number of seconds since January 1, 1970. NetBackup restores the virtual machine disks to a new VM. Therefore, if this name conflicts with an existing display name, the restore fails.	Required.
`AttachDisksToExistingVM`	Whether to restore the selected VMDKs to an existing VM or to a new VM, as follows: ■ If the value is `Yes`, the VM specified in the `VMName` field must exist in the target vCenter or ESX server. If it does not exist, the restore fails with status code 2820. ■ If the value is `No`, the VM specified in the `VMName` field must not exit in the target vCenter or ESX server. If it exists, the restore fails with status code 2820. ■ If the value is `DeleteAllDisksAndReplace`, the VM specified in the `VMName` field must exist in the target vCenter or ESX server. If it does not exist, the restore fails with status code 2820. The default value is `No`.	Required.
`PowerOn`	Whether to turn on the target VM after the restore, as follows: ■ If the value is `Yes`, the target VM is powered ON at the end of a successful restore. ■ If the value is `No`, the target VM is not turned on after the restore. If the restore is to an existing VM, the VM is turned off before the virtual disks are attached to it during the restore. The default value is `No`.	Required.
`Datacenter`	The name of the VMware **Datacenter** for the virtual disk, in pathname format. To restore to a standalone ESXi hypervisor when the backup was through a vCenter, the value of this field must be `None`. If not specified, NetBackup uses the value from the backup.	Optional.

Table 10-8 The `VMwareVirtualMachineDestination` section (required) *(continued)*

Field name	Description	Required?
`ESX`	The name of the ESX host to which NetBackup should restore the virtual machine disks. If not specified, NetBackup uses the value from the backup.	Optional.
`Folder`	The pathname of the VM folder to which NetBackup should restore the virtual machine disks. To restore to a standalone ESXi hypervisor when the backup was through a vCenter, the value of this field must be `None`. If not specified, NetBackup uses the value from the backup.	Optional.
`ResourcePool/Vapp`	The pathname of the resource pool to which NetBackup should restore the virtual machine disks. If the restore is to a vApp, specify the path of the vApp. If not specified, NetBackup uses the value from the backup.	Optional.
`VmxDatastore`	The name of the `Datastore` to which NetBackup should restore the `.vmx` configuration file and other VM configuration files. You may enclose the name in square brackets but do not have to. If not specified, NetBackup uses the value from the backup.	Optional.
`DefaultDiskDatastore`	The name of the `Datastore` to which NetBackup should restore all the virtual disks for in-place disk restore. If not specified, NetBackup uses the value from the backup. This option is only used for In-place disk restore and is ignored otherwise.	Optional.

VMwareVirtualDiskDestination

The `VMwareVirtualDiskDestination` section of the file is a JSON array that specifies the disks to restore and the restore parameters for those disks. It can contain one or more sets of the fields that are described in the following table, one set per virtual machine disk. A comma must separate fields in a set, and a comma must separate sets. This section is subordinate to the `VMwareRestoreParameters` section.

Note: This section is not applicable for in-place disk restores.

Table 10-9 The `VMwareVirtualDiskDestination` section (required)

Field name	Description	Required?
`VirtualDisk`	The full pathname of the virtual disk to restore. This path must match exactly the path of the `.vmdk` file when it was backed up.	Required.
`OverwriteExistingDisk`	Whether to overwrite the existing virtual disk or disks on the target VM, as follows: ■ If the value is `Yes`, overwrite the original virtual disk and retain the disk UUID. ■ If the value is `No`, restore the virtual disk to the target VM as a new disk. VMware assigns a new UUID to the disk. The default value is `No`.	Required.
`Datastore`	The name of the `Datastore` that is the destination for the restore. You may enclose the name in square brackets but do not have to. (VMware generates the `Datastore` pathname using the naming conventions for the VM.) For a restore of virtual disks to a datastore cluster, specify the name of the datastore cluster in this field. If not specified, NetBackup uses the value that is specified in the `Path` field. If neither `Datastore` or `Path` are specified, NetBackup uses the `Datastore` from the backup image.	Optional.
`Path`	The full pathname to the restore destination for the virtual disk, in the following format: `[`*`datastore_name`*`] MyVM/MyVM.vmdk` The `nbrestorevm -restorespecout` option does not populate the `Path` field. If you specify a `Path` and it is not available or a disk already exists at that path, the restore fails. If neither `Datastore` or `Path` are specified, NetBackup uses the `Datastore` from the backup image. If a specific vmdk name is not required, Veritas recommends that you leave this field empty.	Optional.
`Provisioning`	The disk provisioning for this specific disk: `thin`, `thick`, `eagerzeroed`, or `unknown`. If not specified, the NetBackup uses the `DefaultDiskProvisioning` value.	Optional.

Table 10-9 The `VMwareVirtualDiskDestination` section (required) *(continued)*

Field name	Description	Required?
`Controller`	The virtual disk controller to which the disk is attached in the original VM. This field is informational only to help you determine which virtual disk or disks to restore. The value is not used during a restore.	Optional

VMwareAdvancedRestoreOptions

The `VMwareAdvancedRestoreOptions` section of the file specifies parameters to restore to an existing VM. This section is subordinate to the `VMwareRestoreParameters` section.

Table 10-10 The `VMwareAdvancedRestoreOptions` section (optional)

Field name	Description	Required?
`DeleteRestoredVMOnError`	NetBackup creates a temporary VM during the restore process and then attaches the virtual disks to the target VM. The value of this parameter determines whether NetBackup deletes the temporary VM if the disk attach operation fails, as follows: ■ If the value is `Yes`, delete the temporary VM. ■ If the value is `No`, do not delete the temporary VM. If the disks are not successfully attached to the target VM, you can access the data on the temporary VM. The default value is `No`.	Optional.
`VMShutdownWaitSeconds`	For restores to an existing VM, the restore process shuts down the target virtual machine before it attaches the disk or disks. The duration of the shutdown operation depends on the VMware workload. Use this parameter to specify how long the restore process should wait for shutdown before giving up on restore. The default value is `900` seconds (15 minutes).	Optional.

About restore of individual files

You can use either of the following procedures to restore files individually.

One-stage process	Restore individual files directly to a virtual machine in one of the following ways: ■ Restore the files to a virtual machine on which NetBackup client software is installed. ■ Windows only: Restore the files to virtual machine drives that have been mapped to a host on which NetBackup client software is installed. See "Setting up NetBackup Client Service for restore to a Windows shared virtual machine drive" on page 227.
Two-stage process	Restore individual files to a host on which the NetBackup client software is installed (not to the virtual machine). See the *NetBackup Backup, Archive, and Restore Getting Started Guide* on how to restore to different locations. Then manually copy the restored files to the virtual machine. (NetBackup does not perform this step.)

Note: Individual file recovery is supported from full backups and from incremental backups, as long as the **Enable file recovery from VM backup** policy option is enabled.

Restoring individual files

If the VMware backup was made with the **Enable file recovery from VM backup** option, you can restore individual files.

See "Optimizations options (VMware)" on page 74.

To restore individual files

1. In the NetBackup Administration Console, click **Backup, Archive, and Restore**
2. Click **Actions > Specify NetBackup Machines and Policy Type...**.
3. Enter the following:

Server to use for backup and restores	The NetBackup primary server that directed the backup.

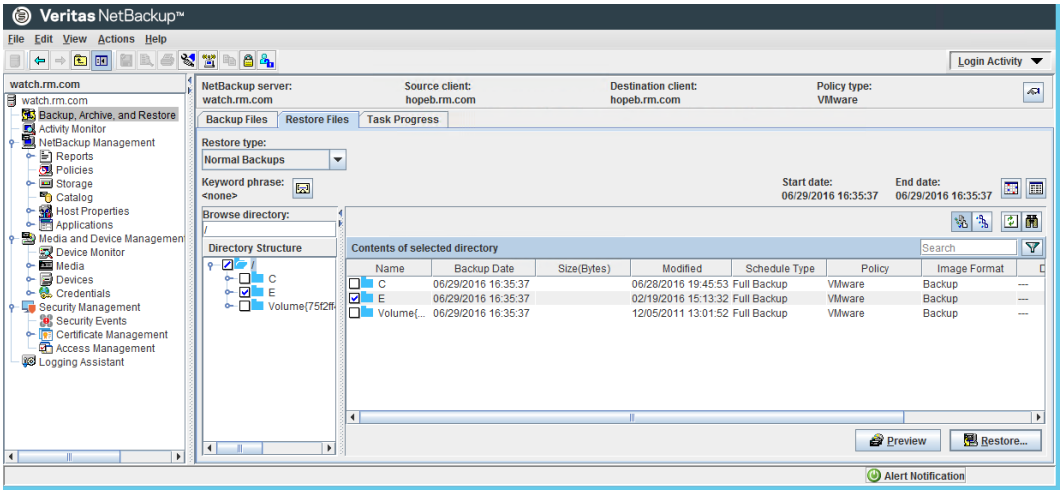
Source client for restores	The VMware virtual machine that was backed up. Click **Search VM Clients** to search or browse for a virtual machine. This option helps to locate a virtual machine in a large, multi-layered virtual environment. See "Browse and search virtual machines for restore" on page 232. Or, enter the type of name that was selected for the **Primary VM identifier** option on the policy **VMware** tab. For example, if the **Primary VM identifier** option is set to VM host name, enter the virtual machine's host name.
Destination client for restores	Enter one of the following: ■ The host name of the VMware virtual machine that was backed up, if NetBackup client software has been installed on the virtual machine. Enter the host name even if the policy identified the virtual machine by its VM display name, UUID, or DNS name. Do not enter the VM display name, UUID, or DNS name. ■ Any NetBackup client that has the same operating system and file system of the VM that was backed up. **Note:** The NetBackup Client Service must be logged on as Administrator. See "Setting up NetBackup Client Service for restore to a Windows shared virtual machine drive" on page 227.
Policy type for restores	The type of policy that made the backup (VMware).
Date / time range	The time period within which to search for backups.

4 Click **OK**.

5 For the **Restore type,** select **Normal Backups**.

6 You can use the **Start date** and **End date** icons to select the date range within which the backup occurred.

7 Under **Directory Structure**, drill into the folders and click the folders and files you want to restore.



8 Click **Restore**.

9 On the **Restore Marked Files** dialog: If NetBackup client software is not installed on the destination virtual machine, select one of the following:

- **Restore everything to its original location**
- **Restore everything to a different location (maintaining existing structure)**
- **Restore individual directories and files to different locations**
  Destinations must be entered as UNC path names that refer to shared drives on the virtual machine. For example, to restore the file `E:\folder1\file1` on virtual machine `vm1`, enter the following destination:

  ```
  \\vm1\e$\folder1\file1
  ```

  The NetBackup Client Service must be logged on under an account that has Administrator privileges.

See “Setting up NetBackup Client Service for restore to a Windows shared virtual machine drive” on page 227.

See “About restore of individual files” on page 223.

Setting up NetBackup Client Service for restore to a Windows shared virtual machine drive

To restore individual files to a Windows virtual machine that has a shared drive, note: the NetBackup Client Service must be logged on under an account that has Administrator privileges (not as the Local System account). An account with Administrator privileges lets NetBackup write to the directories on the virtual machine to which the data is restored.

If you try to restore files while the NetBackup Client Service is logged on as the Local System account, the restore fails.

To log on the NetBackup Client Service as Administrator

1. In Windows Services on the VMware recovery host, double-click the NetBackup Client Service.
2. Check the **Log On** tab: if the service is not logged on under an account that has Administrator privileges, stop the service.
3. Change the logon to the Administrator account, or to an account that has Administrator privileges.

   The account must have Administrator privileges in the domain in which both the virtual machine and the VMware backup host reside.
4. Restart the service.
5. Retry the restore.

Restore Marked Files dialog for restore of VMware files

This topic describes the **Restore Marked Files** dialog for restoring individual folders and files from a VMware virtual machine backup.

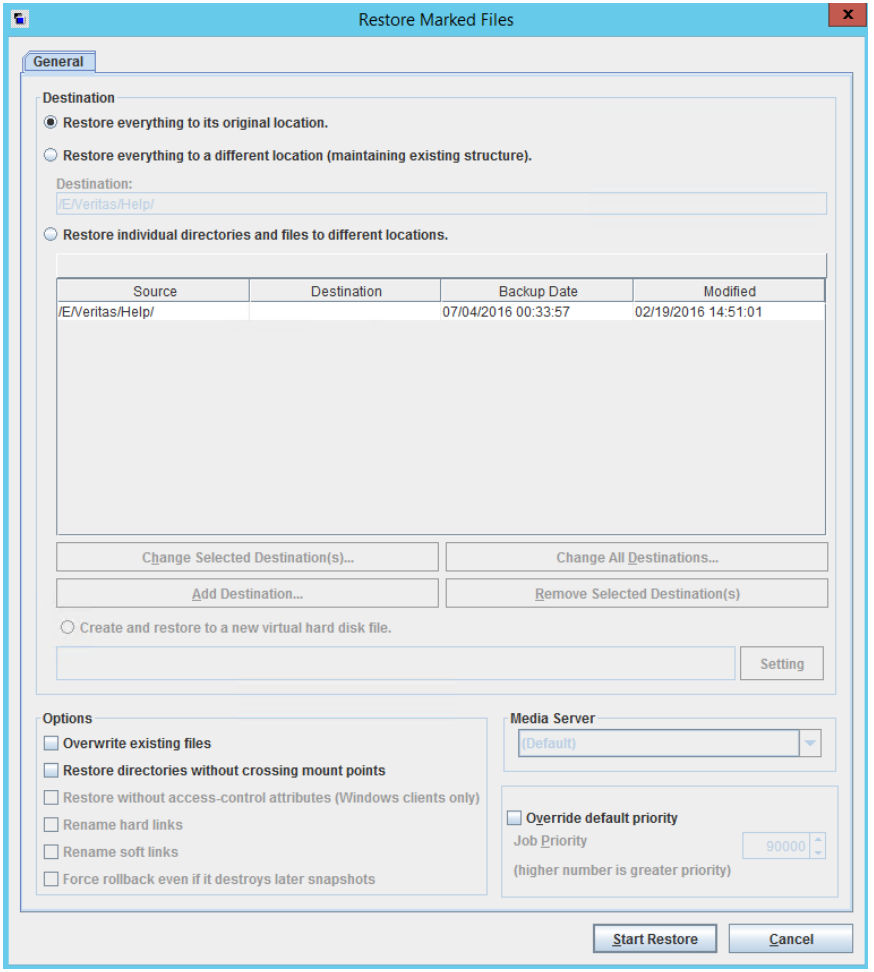


Table 10-11 Options for individual file restore on the **Restore Marked Files** dialog box

Option	Description
Destination	Select from the following options.
Restore everything to its original location	Restores the folders and files to the location where they resided when the backup occurred.

Table 10-11 Options for individual file restore on the **Restore Marked Files** dialog box *(continued)*

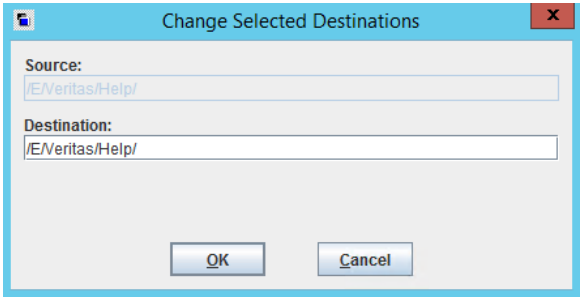
Option	Description
Restore everything to a different location (maintaining existing structure)	Restores the folders and files with their original hierarchy, but to a different location. Use the **Destination** field to enter the restore location. Click **Browse** to browse to the restore location.
Restore individual directories and files to different locations	Restores the folders and files to individually designated locations. To designate a restore destination for each source folder, double click on its row. Use the following dialog to enter or browse for the destination:  To restore to a Windows mounted drive: Destinations must be entered as UNC path names that refer to shared drives on the virtual machine. For example, to restore the file `E:\folder1\file1` on virtual machine `vm1`, enter the following destination: `\\vm1\e$\folder1\file1` See "Setting up NetBackup Client Service for restore to a Windows shared virtual machine drive" on page 227.
Create and restore to a new virtual hard disk file	This option is not implemented.
Options	For a description of the restore options, see the NetBackup help for the Backup, Archive, and Restore interface.

Table 10-11 Options for individual file restore on the **Restore Marked Files** dialog box *(continued)*

Option	Description
Media Server	You can use this option to select a media server that has access to the storage unit that contains the backup image. An example of such an environment is a Media Server Deduplication Pool (MSDP) with multiple media servers. **Note:** If the storage unit that contains the backup image is not shared with multiple media servers, this option is grayed out.
Override default priority	Determines the restore job's priority for restore resources. A higher priority means that NetBackup assigns the first available drive to the first restore job with the highest priority. Enter a number (maximum 99999). The default for all restore jobs is 0, the lowest priority possible. Any restore job with a priority greater than zero has priority over the default setting.

How NetBackup handles VMware tag associations at restore

To better understand the NetBackup restore behavior, it's important to understand some of the internal mechanics of how VMware handles tag associations. For each tag that is created in VMware, there is a corresponding internal identifier you cannot see or edit. This feature allows VMware to function correctly without the need to account for variation in naming conventions. Tags are replicated throughout the environment through the Platform Services Controller (PSC).

NetBackup recognizes and uses tag names when they are part of the VIP query. Backups of the virtual machine store the tag name and VMware internal identifier for all tags that are associated with that virtual machine. During the restore, however, NetBackup only creates the tag associations based on the VMware internal identifiers that are defined on the target vCenter server.

Figure 10-1 Sample VMware environment

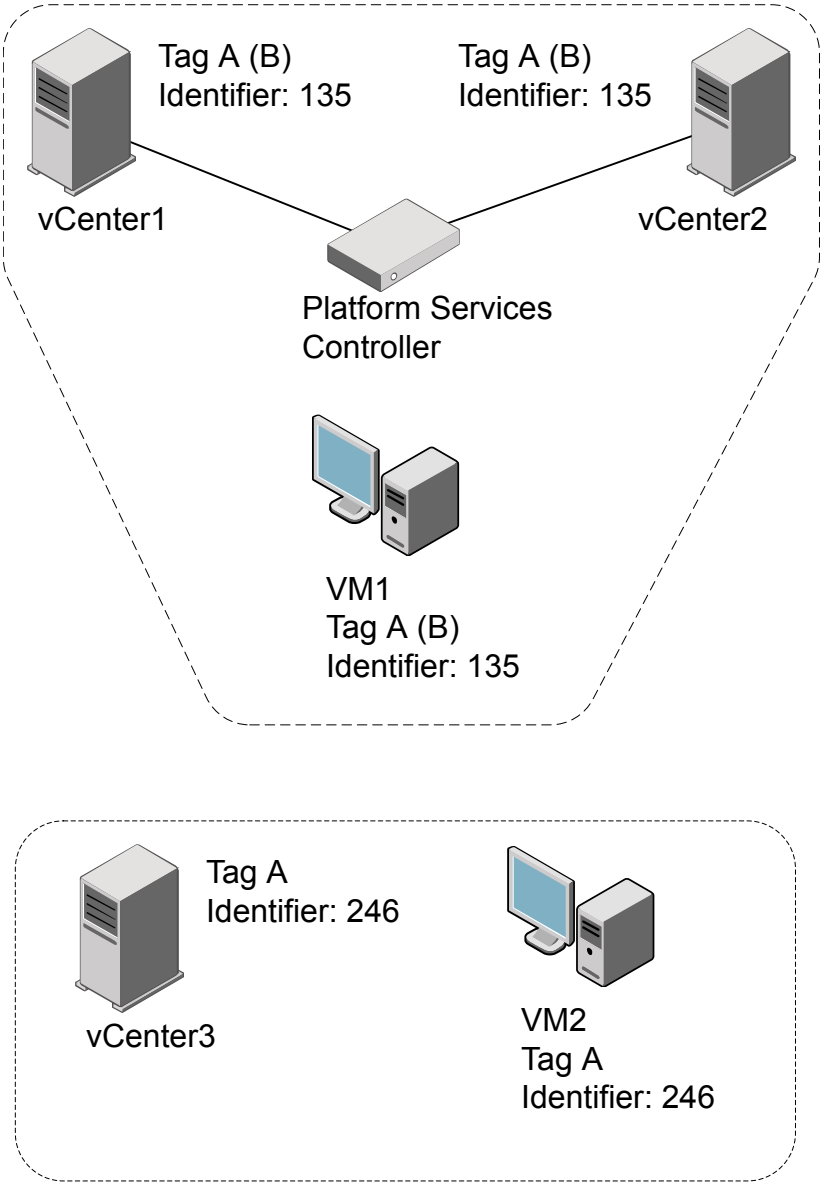


Figure 10-1 shows a sample VMware environment with multiple vCenter servers, virtual machines, and tags. Assume that a backup of all virtual machines completes successfully with a NetBackup status code 0.

- If you restore VM1 to either vCenter1 or vCenter2, it is restored with tag **A** and the restore exits with a NetBackup status code 0. This behavior is true both for a restore to the same name as well as an alternate client restore. This behavior is the result of VMware replicating tags across all vCenter servers that are attached to a single PSC.
- If you restore VM1 to vCenter3, it is restored without any tags. The restore exits with a NetBackup status code 1. This behavior is because VMware uses the internal identifier. While there is a tag name **A** in vCenter3, the internal identifier for tag **A** does not match the internal identifier that is restored. This behavior is true both for a restore to the same name as well as an alternate client restore.
- After the NetBackup backup, if tag **A** is renamed to **B**, when VM1 is restored to either vCenter1 or vCenter2 it is restored with tag **B**. The restore exits with a NetBackup status code 0. This behavior is because VMware uses the internal identifier, and now associates this identifier with the tag name **B**.
- After the NetBackup backup, if tag **A** is deleted, when VM1 is restored to either vCenter1 or vCenter2 it is restored without any tag associations. The restore exits with a NetBackup status code 1.

If for any reason the backup of the virtual machines in Figure 10-1 did not successfully capture the tag associations, the backup exits with NetBackup status code 0. The reasons for failing to capture tag associations appear in the Activity Monitor. Any restores based on this backup exit with NetBackup status code 0, but no tag information is restored. Depending on the backup error, more information regarding tag associations may appear in the Activity Monitor.

Browse and search virtual machines for restore

To browse and search virtual machines for restore

1. In the **Backup, Archive, and Restore** interface, click **Actions > Specify NetBackup Machines and Policy Type....**
2. Under **Policy type for restores**, select **VMware**.
3. Click **Search VM Clients**.

   The **Browse and Search Virtual Machines for Restore** dialog appears. Use this dialog to find a virtual machine.

Note: This dialog finds the virtual machines that were backed up with the VMware policy type. It does not search for other types of backups.

Note: If the backup was made before NetBackup 7.6, the backup image must be imported and verified before it can be browsed or searched.

Table 10-12 Browse and Search Virtual Machines for Restore dialog box

Dialog box item	Description
Search virtual machines	Search for virtual machines by name, IP address, UUID, or by other criteria. See "Search Virtual Machines for Restore dialog" on page 233.
Browse virtual machines	Browse for virtual machines by drilling down through the virtual objects. Select the type of view for browsing: ■ **vCloud view** Shows the virtual objects as they appear in vCloud Director. ■ **vSphere view** Shows the virtual objects as they appear in vSphere Client. See "Browse the vCloud or vSphere view for virtual machine clients" on page 235.

Note: Although VMware allows up to 128 characters for an object name, the NetBackup database restricts searches to the first 126 characters only.

Search Virtual Machines for Restore dialog

Use this screen to search for virtual machines by name or other identifier, or to use other filter criteria.

Enter Display Name, Host Name, IP Address, UUID, DNS Name or vApp to search for:

Enter the name or number of the virtual machine to search for and click **Next**. Any matching virtual machines appear in the **Search results** dialog.

See "Search results dialog" on page 236.

Advanced Search:

Click to create a rule-based search query. See Table 10-13.

Table 10-13 Advanced Search: filter parameters

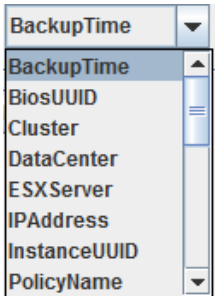
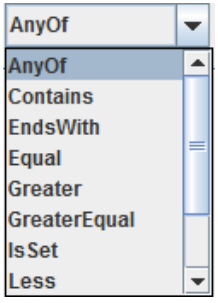
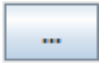
Search item	Description
	Available when you click the plus sign to add a rule to the search. AND: Limits or restricts the scope of the search. OR: Opens the search to an additional possibility, expanding the scope of the search.
	Select a parameter on which to search. You can type the first character of the parameter to select it.
	Select an operator. You can type the first character of the operator to select it. The available operators depend on the parameter that was selected.
	Enter a value for the parameter. The search looks for the virtual machines that match the value.
	Choose a date and time.
	Refine or expand the search (add another rule).

Table 10-13 Advanced Search: filter parameters *(continued)*

Search item	Description
	Remove the rule from the search.
Basic Search	Search by display name, host name, IP address, UUID, DNS name, or vApp.
Next	Run the search. The matching virtual machines appear in the **Search results** dialog. See "Search results dialog" on page 236.

Note the following about the search behavior:

- Although VMware allows up to 128 characters for an object name, the NetBackup database restricts searches to the first 126 characters only.
- To search for a vSphere vApp by name without specifying its path: Use the search operator **Contains** or **EndsWith** (do not use **Equal**). To use **Equal**, you must specify the entire path of the vApp.
- To search by IP address: If the virtual machine has two or more IP addresses (such as virtual addresses), use **Contains** as the search operator instead of **Equal**.
- You must include a leading forward slash (/) when searching for a data center, VM folder, or resource pool. If you use the **Contains** operator, a leading slash is not required.
- Regarding wildcards: * and ? are not supported for **Greater**, **GreaterEqual**, **Less**, and **LessEqual** operators. The * and ? characters are treated as literals, not wildcards.
  For the rest of the operators, * matches everything, and ? matches any single character.
  Note: SQL has a limitation that wildcards * and ? (SQL equivalents are % and _) do not match null values. If a virtual machine does not have an IP address, the query "**IPAddress Equal ***" does not find the virtual machine.

Browse the vCloud or vSphere view for virtual machine clients

The **Browse virtual machines using the vCloud (or vSphere) view** dialog shows your virtual environment starting with the vCenter server. The objects appear according to the view you chose (vCloud or vSphere).

To select a virtual machine, click on an ESX server or vApp. Highlight the virtual machine you want and then click **Select**.

To switch the view to vCloud or vSphere, click on the link in the upper right.

Note: Although VMware allows up to 128 characters for an object name, the NetBackup database restricts searches to the first 126 characters only.

See "Browse and search virtual machines for restore" on page 232.

Search results dialog

The virtual machines that match an advanced search (from the **Search Virtual Machines for Restore** dialog) are listed in the **Search results** dialog. The search criteria are listed at the top.

Click on the virtual machine that you want to restore and click **Select**. Click **Refresh** on the **Specify NetBackup Machines and Policy Type** screen.

If no virtual machines appear, click **Back** to revise your search criteria.

See "Browse and search virtual machines for restore" on page 232.

If the recovery host is not at the same NetBackup release level as the backup host

Note the following about mixed-level backups and restores:

- To restore from a NetBackup 8.x backup
  To restore a virtual machine from a backup that a NetBackup 7.x backup host performed, a NetBackup 8.x recovery host is required. You cannot use a NetBackup 7.7.x recovery host to restore a virtual machine that was backed up by a NetBackup 8.x backup host.

Chapter 11

Restore virtual machines with Instant Recovery

This chapter includes the following topics:

- About Instant Recovery for VMware
- Task overview for Instant Recovery for VMware
- Performance recommendations for Instant Recovery for VMware
- Requirements for Instant Recovery for VMware
- Notes on Instant Recovery for VMware
- Restarting the Client for NFS service on a Windows restore host
- Instant Recovery options on the nbrestorevm command
- Restoring a virtual machine with Instant Recovery for VMware
- Restoring a virtual machine to a different location with Instant Recovery for VMware
- Restoring individual files with Instant Recovery for VMware while the current virtual machine is running
- Job types for Instant Recovery for VMware
- Reactivating a restored virtual machine with Instant Recovery for VMware

About Instant Recovery for VMware

NetBackup can recover a virtual machine almost instantly, without waiting to transfer the virtual machine's data from the backup. NetBackup starts the virtual machine

directly from the backup image and makes it accessible to users on the target ESX host immediately. You can copy files (including vmdk files) without restoring the entire virtual machine. To restore the virtual machine, use VMware Storage vMotion to migrate the virtual machine data files from the backup image to the ESX host.

Some example uses for instant recovery:

- Access and restore individual files and folders from any type of OS and then delete the virtual machine. (Note for Windows or Linux: Instead of instant recovery, you can use the policy **Enable file recovery from VM backup** option and restore individual files with the Backup, Archive, and Restore interface.)
- Test a patch on a restored virtual machine before you apply the patch to production systems.
- Troubleshoot a virtual machine or host, such as when the production ESX host is down. You can start the virtual machine from its backup and use it until the production system is back online.
- Permanently recover the virtual machine by means of Storage vMotion.
- Verify the backup image.
- Copy a vmdk file and then delete the virtual machine.
- Verify an application.

In any case, the virtual machine is started directly from the backup image and is available in seconds or minutes. The startup time depends on the network speed and storage speed, not on the size of the virtual machine.

Table 11-1 describes the steps in a virtual machine instant recovery.

Table 11-1 How Instant Recovery for VMware works

Sequence	Actions
Step 1	Run the nbrestorevm command* to access the virtual machine from its backup image. The NetBackup File System Service (NBFSD) on the media server accesses the backup image file system and mounts the image as an NFS datastore. The datastore becomes accessible to the ESX host where the virtual machine is to be restored. On the same command, select a temporary datastore that is accessible to the ESX host.
Step 2	NetBackup creates a virtual machine on the ESX host and configures the virtual machine with write access to a temporary (local) datastore.
Step 3	NetBackup creates a snapshot of the virtual machine. Any new write requests in the virtual machine use the temporary datastore. The virtual machine uses the NFS datastore as read-only.

Table 11-1 How Instant Recovery for VMware works *(continued)*

Sequence	Actions
Step 4	NetBackup starts up the virtual machine on the ESX host.
Step 5	To keep the restored VM: Use Storage vMotion to copy the virtual machine data from the NFS datastore to the temporary datastore.
Step 6	When vMotion is complete, use nbrestorevm to unmount the NFS datastore.

*NetBackup provides a command-line interface for instant recovery of virtual machines (nbrestorevm). A graphical user interface (the Instant Recovery Wizard) is available in the NetBackup vSphere Web Client plug-in and the NetBackup vSphere Client (HTML5) plug-in. For details, see the *NetBackup Plug-in for VMware vSphere Web Client Guide* and the *NetBackup Plug-in for VMware vSphere Client (HTML5) Guide*, available from this location:

http://www.veritas.com/docs/000003214

Task overview for Instant Recovery for VMware

Table 11-2 describes the tasks for Instant Recovery for VMware.

Table 11-2 Instant Recovery tasks

Step	Description	Reference topic
Step 1	Review the performance recommendations	See "Performance recommendations for Instant Recovery for VMware" on page 240.
Step 2	Review the notes and requirements	See "Requirements for Instant Recovery for VMware" on page 241. See "Notes on Instant Recovery for VMware" on page 242.
Step 3	Restart the Client for NFS service on the restore host	See "Restarting the Client for NFS service on a Windows restore host" on page 243.
Step 4	Review the Instant Recovery options on the nbrestorevm command	See "Instant Recovery options on the nbrestorevm command" on page 244.

Table 11-2 Instant Recovery tasks *(continued)*

Step	Description	Reference topic
Step 5	Use the nbrestorevm command to perform Instant Recovery	See "Restoring a virtual machine with Instant Recovery for VMware" on page 249. See "Restoring individual files with Instant Recovery for VMware while the current virtual machine is running" on page 256.

Performance recommendations for Instant Recovery for VMware

After Instant Recovery, the virtual machine is on an NFS-attached datastore that is presented by the NetBackup media server. The performance of the virtual machine and of Storage vMotion depends on the following: the network speed and latency between the ESXi host and the media server, and the speed of NetBackup storage that the backup is recovered from.

It is recommended the following:

- A SAN connection from the NetBackup media server to its disk storage unit.
- For Fibre Channel SAN, a minimum speed of 4 gigabits per second.
- For iSCSI SAN, a minimum speed of 1 gigabit per second.
- When you use Storage vMotion to migrate a restored virtual machine, migrate one virtual machine at a time per media server. The migration may be slow if you simultaneously migrate multiple virtual machines per media server.
- For disaster recovery testing, it is recommended that you restore no more than three or four virtual machines per media server. The number to restore depends on the I/O load on the media server. It is recommended restoring each VM one-by-one, not simultaneously.

Note: For large-scale recovery of multiple virtual machines, use the virtual machine restore feature in the Backup, Archive, and Restore interface. Do not use Instant Recovery for VMware.

Requirements for Instant Recovery for VMware

For virtual machine instant recovery, your environment must meet the following requirements:

- The virtual machine to restore must have been backed up from a VMware policy.
- The target ESX server for the restore must be at vSphere 5.0 or later.
- The restore host can be on Windows or Linux.

  Note: For the VMware virtual machines that have non-ASCII characters in their paths, NetBackup does not support Instant Recovery using Windows restore hosts and media servers. You must use a Linux restore host and media server for Instant Recovery of such virtual machines.

  The requirements and limitations for non-ASCII character support are described in a different topic.

  See "NetBackup for VMware: notes and restrictions" on page 27.

- For a restore host that is separate from the NetBackup primary server or media server: You must add the restore host to the list of servers that can access the primary server.
  In the NetBackup Administration Console, click **Host Properties > Primary Servers**, double-click the NetBackup primary server, and click **Servers**. On the **Additional Servers** tab, click **Add** to add the restore host.
  See "Allowing other servers or clients to restore virtual machines" on page 350.
- The NFS Client service must be enabled on the ESXi host.
- The Network File System (NFS) must be installed on the Linux media server and restore host and the `portmap` service must be active.
  For information about how to install NFS, see the media server host operating system documentation.
- The Services for Network File System (NFS) must be installed on the Windows media server and restore host.
  See "About configuring services for NFS on Windows 2012 or 2016 (NetBackup for VMware)" on page 353.
  The NetBackup media server platform must support Granular Recovery Technology. See the *NetBackup Enterprise Server and Server OS Software Compatibility List*:
  NetBackup Primary Compatibility List

- The Client for NFS service may have to be restarted on a NetBackup Windows restore host.
  See "Restarting the Client for NFS service on a Windows restore host" on page 243.
- The media server must use IPv4 or have a dual stack configuration if the vCenter server has a dual stack configuration.
- NetBackup requires logon credentials for the vCenter server and the restore host.
  See "Adding NetBackup credentials for VMware" on page 45.

Notes on Instant Recovery for VMware

Note the following about instant recovery of VMware virtual machines:

- Supports the following storage unit types (disk only): BasicDisk, AdvancedDisk, Media Server Deduplication Pool (MSDP), and qualified third-party OpenStorage devices.
  Note: Snapshot-only backups are not supported.
- Does not support a virtual machine that had the disks that were excluded from the backup. The policy **Virtual disk selection** option must have been set to include all disks.
- Does not support a virtual machine that has a disk in raw device mapping mode (RDM) or that has a disk in Persistent mode.
- Supports the following policy schedule types: Full backups, and the incremental backups that include the **Use Accelerator** option with a disk-based storage unit. Incrementals without the **Use Accelerator** policy option are not supported.
- Does not support virtual machine templates.
- If the virtual machine contains an IDE drive, the restored virtual machine may not start. This issue is not unique to instant recovery.
  See "VMware virtual machine does not restart after restore" on page 309.
- To avoid host name or IP address conflicts between the current virtual machine and the virtual machine version you want to restore: Shut down the virtual machine in your production environment before you start the recovery. Then change the display name of the current virtual machine, or use the `-R` option on nbrestorevm to rename the restored virtual machine.
- For a virtual machine that is running under a high load, migration of the virtual machine may take longer than expected. For this reason, NetBackup changes the virtual machine's `fsr.maxSwitchoverSeconds` property to 900.

For example, this increase may be necessary when the virtual machine is restored from a deduplication storage unit.
The following VMware Knowledge Base article contains more information on the `fsr.maxSwitchoverSeconds` property:
Using Storage vMotion to migrate a virtual machine with many disks timeout

- Note the following about the virtual machine's datastore name:
  - If the name of the datastore includes spaces, the name should be enclosed in double quotes ("").
  - A virtual machine restore may fail if the name of the datastore (that was used at the time of the backup) ended with a period.
    The following tech note contains additional information.
    http://www.veritas.com/docs/TECH199771
- Instant recovery cannot restore a vCloud virtual machine into vCloud. The virtual machine is restored into vSphere. You can copy or import the restored virtual machine into vCloud by means of the **Copy** option in vCloud.
  Note that the vCloud **Move** option does not work with a virtual machine that runs from a NetBackup datastore.
- Storage lifecycle policies (SLPs) can use Auto Image Replication to replicate a virtual machine backup image to another NetBackup domain. To restore the virtual machine from the replicated image, you must include the -vmproxy option on the nbrestorevm command. Use the -vmproxy option to specify the backup host (access host) that is in the domain where the virtual machine was replicated. Without the -vmproxy option, nbrestorevm defaults to the backup host in the original domain and the restore fails.
- Supports recovery of virtual machines containing independent disks. The independent disks that are associated with the virtual machine are recovered to the virtual machine working directory on the temporary datastore. This functionality requires a NetBackup 8.3 or later recovery host.

Restarting the Client for NFS service on a Windows restore host

It may be necessary to stop and restart the NFS Client service. If you use the Microsoft services snap-in (`Services.msc`) to restart it, the service does not start until you restart the server.

To restart the Client for NFS service without a server restart

- From the Windows command prompt, run the following commands:

```
net stop nfsclnt
net stop nfsrdr
net start nfsrdr
net start nfsclnt
```

The Client for NFS service should restart without a restart of the server.

Instant Recovery options on the nbrestorevm command

NetBackup provides a command-line interface for instant recovery of virtual machines: the nbrestorevm command.

The following is a list of the available nbrestorevm options for performing Instant Recovery of a VMware virtual machine. The options are listed in man page format.

Note: Although the nbrestorevm command has additional options, only the options that are described in this topic apply to Instant Recovery.

To initiate Instant Recovery (activate the virtual machine)

Options without brackets are required.

```
nbrestorevm -vmw -ir_activate -C vm_client
      -temp_location temp_location_for_writes
      [-S primary_server] [-vmpo] [-vmInstanceId] [-vmsn] [-vmst]
      [-vmserver vm_server] [-vmproxy vm_proxy] [-vmkeephv] [-vmid]
      [-vmnewdiskuuid] [-s mm/dd/yyyy [HH:MM:SS]]
      [-e mm/dd/yyyy [HH:MM:SS]]
      [-R absolute_path_to_rename_file]
      [-disk_media_server media_server]
```

Note: Only `-vmw`, `-ir_activate`, `-C`, and `-temp_location` are required. If the other options are not specified, NetBackup automatically supplies values for those options from the backup. In most cases, if you do not restore the virtual machine to a different location, you can omit the bracketed options.

To list details about the activated virtual machine

```
nbrestorevm -ir_listvm
```

To deactivate or delete the virtual machine

```
nbrestorevm -ir_deactivate instant_recovery_identifier [-force]
```

To complete the VM instant recovery job after the data is migrated

```
nbrestorevm -ir_done instant_recovery_identifier
```

To reactivate a virtual machine that was interrupted during recovery

```
nbrestorevm  -ir_reactivate instant_recovery_identifier [-force]
nbrestorevm -ir_reactivate_all -vmhost vm_host -media_server
      media_server_activate_vm [-force]
```

Table 11-3 describes the nbrestorevm options for Instant Recovery of virtual machines. These options are also described in the NetBackup Commands Reference Guide, and in the man page for nbrestorevm.

Table 11-3 Options on the nbrestorevm command for Instant Recovery

Option	Description
-vmw	Indicates the type of virtual machine to restore (VMware).
-C *virtual_machine*	The name of the virtual machine as identified in the backup. For example, if the policy backed up the virtual machine by its host name, specify that host name. **Note:** If a virtual machine with the same name already exists on the target ESX host, the command fails. You can change the display name of the virtual machine in vCenter. As an alternative, use the `-R` option on nbrestorevm to change the display name or location of the restored virtual machine.
-ir_activate	Starts the restore by mounting the backup image of the virtual machine as an NFS datastore. The datastore becomes accessible to the ESX host where the virtual machine is to be restored. The following procedure has further details: See "To restore a virtual machine with instant recovery" on page 250.

Table 11-3 Options on the nbrestorevm command for Instant Recovery *(continued)*

Option	Description
-temp_location *temporary_datastore*	A temporary datastore on the ESX server where all writes occur until the virtual machine is restored. All writes occur on this datastore until Storage vMotion is complete or until you are finished with the virtual machine (such as for troubleshooting). **Note:** This datastore must exist before you run nbrestorevm.
-S *primary_server*	Specifies a different primary server, to restore a virtual machine from a backup that was made by that primary.

-R *rename_file_path*	The absolute path to a file that contains directives for restore to a different location.
	The following are the entries that you can use in the file (each entry begins with `change`):
	`change esxhost to new_ESX_host`
	`change resourcepool to new_resource_pool`
	`change vmname to new_virtual_machine_name`
	`change network to new_network`
	Note: The `change` line should be entered exactly as it appears in this list, except for the variable at the end (such as *new_virtual_machine_name*). Replace that variable with the new name.
	For example:
	`change esxhost to esx01.prod4.com`
	`change resourcepool to /Tech1/esx01.prod4.com/Res`
	`change vmname to T1vm5`
	Each `change` line must end with a carriage return.
	Note: If the file contains only one `change` line, (such as `change vmname to T1vm5`), that line must end with a carriage return.
	If you restore to a different ESX server, you may have to specify a different resource pool. (The original resource pool cannot be used to create a VM on a different ESX server.) You must specify a resource pool by including the following line in the rename file:
	`change resourcepool to path_to_new_resource_pool`

-vmst	Removes the virtual machine's tags.
-vmserver *vCenter_server*	The name of the vCenter server that manages the target ESX host for the restore. To restore to the same vCenter where the virtual machine originally resided, omit this option.
-vmproxy *restore_host*	The host to perform the restore (a NetBackup client). The default is the host that performed the backup.

Table 11-3 Options on the nbrestorevm command for Instant Recovery *(continued)*

Option	Description
-disk_media_server *media_server*	Specifies which media server performs the Instant Recovery. This option is useful if NetBackup storage is configured over several media servers, such as for load balancing. Without the -disk_media_server option, the Instant Recovery job may select any of the available media servers to do the restore. If only one of the media servers is configured for Instant Recovery, specify that server with the -disk_media_server option. See "Notes on Instant Recovery for VMware" on page 242.
-vmpo	Turns on the virtual machine after the restore.
-vmInstanceId	Retains the Instance UUID of the original virtual machine (note that the Instance UUID is a vCenter specific unique identifier of a virtual machine). The virtual machine is restored with the same Instance UUID that it had when it was backed up. If the restore of the virtual machine is to a standalone ESXi host, this option is disabled. If a virtual machine with the same Instance UUID exists at the target restore location, a message appears that the UUID is used already. In this case, the original instance UUID is not restored and a new UUID is assigned for the virtual machine.
-vmsn	Removes the virtual machine's network interface. See "Restoring individual files with Instant Recovery for VMware while the current virtual machine is running" on page 256.
-vmkeephv	Retains the virtual machine's hardware version: the virtual machine is restored with the same hardware version that it had when it was backed up. Without this option, the virtual machine is restored with the default hardware version of the target ESX server or vCenter. The default is typically the latest supported hardware version.
-vmid	Retains the BIOS UUID of the original virtual machine.
-vmnewdiskuuid	Generate new virtual machine disk UUIDs during an instant recovery. Use this option with the `-ir_activate` option. The VMs that activate with this option do not retain the new vmdk UUID during a subsequent `-ir_reactivate` operation. In such a scenario, the VMDKs revert to their UUIDs at the time of the backup.

Table 11-3 Options on the nbrestorevm command for Instant Recovery *(continued)*

Option	Description
-ir_deactivate *instant recovery ID*	Removes the virtual machine from the ESX host. If no other virtual machine uses the NetBackup NFS datastore, this option removes that datastore and releases its resources on the NetBackup media server. This option is for removing the virtual machine when you are finished copying its files and do not intend to keep it. **Note:** If the virtual machine has been migrated to a production datastore by means of vMotion, -ir_deactivate is the same as ir_done. **Note:** If vMotion is still in progress for this virtual machine, you should cancel the vMotion job before you use `-ir_deactivate`. See "To restore a virtual machine with instant recovery" on page 250.
-ir_done *instant recovery ID*	When vMotion migration of the virtual machine is finished, this option completes the virtual machine instant recovery job. It also removes the NetBackup NFS datastore if no other virtual machine uses it. When the datastore is removed, its resources are released on the media server. See "To restore a virtual machine with instant recovery" on page 250.
-ir_reactivate *instant_recovery_identifier* -ir_reactivate_all	Reactivates a restored virtual machine: remounts the NetBackup NFS datastore, and from the temporary datastore on the ESX host it registers the restored virtual machines on the ESX host. *instant recovery ID* is the virtual machine's numeric identifier from the -ir_listvm output. If more than one virtual machine needs reactivation: -ir_reactivate_all remounts the NetBackup NFS datastores on the media server and reactivates the virtual machines. For example: If VM1, VM5, and VM6 were mounted on the specified ESX server (-vmhost), and their datastores were mounted on the specified media server (-media_server), those three VMs are reactivated.
-vmhost *vm_host*	When you reactivate virtual machines, this option specifies the ESX host on which the virtual machines were mounted.
-media_server *media_server_activate_vm*	When you reactivate virtual machines, this option specifies the media server on which the NFS datastores that contain the backup images were mounted.
-force	For the -ir_deactivate, –ir_reactivate, or –ir_reactivate_all option, -force suppresses confirmation prompts.

Table 11-3 Options on the nbrestorevm command for Instant Recovery *(continued)*

Option	Description
-s *start_time* -e *end_time*	By default NetBackup selects the latest full backup plus Accelerator-enabled incremental backups (if any). This option limits the selectable backup images to those with the timestamps that fall within the specified period. NetBackup selects the latest suitable backup image within the range.

Restoring a virtual machine with Instant Recovery for VMware

You can use this procedure to do either of the following:

- Copy files from a virtual machine backup.
- Restore the full virtual machine.

In either case, you can restore the virtual machine to its original location or to an alternate location.

Note: To avoid host name or IP address conflicts, shut down the current virtual machine in your production environment before you start instant recovery.

To copy files while the current virtual machine is running, use a different procedure:

See "Restoring individual files with Instant Recovery for VMware while the current virtual machine is running" on page 256.

Table 11-4 Basic steps for VMware instant recovery

Type of recovery	Steps
Copy files or troubleshoot an issue, then delete the restored virtual machine	Basic steps are these: ■ Restore the VM: Use nbrestorevm with the -ir_activate option. ■ Copy files from the VM; or use the VM as a stand-in until the production host is back online. ■ Delete the VM and release the media server resources: Use nbrestorevm with the -ir_deactivate option. See the following procedure for command details.

Table 11-4 Basic steps for VMware instant recovery *(continued)*

Type of recovery	Steps
Restore and keep the virtual machine	Basics steps are these: ■ Restore the VM: Use nbrestorevm with the ir_activate option. ■ Transfer the virtual machine files to an ESX host: Use the **Migrate** option in vSphere Client. ■ Release the media server resources: Use nbrestorevm with the ir_done option. See the following procedure for command details.

See "Requirements for Instant Recovery for VMware" on page 241.

The detailed procedure follows.

To restore a virtual machine with instant recovery

1 On the primary server, media server, or restore host, enter the nbrestorevm command.

This command is in the following location:

UNIX, Linux: /usr/openv/netbackup/bin/

Windows: *install_path*\NetBackup\bin\

Enter the command as follows.

To restore the VM to its original location:

```
nbrestorevm -vmw -ir_activate -C virtual_machine -temp_location
temporary_datastore [-vmproxy VMware_access_host] -vmpo
```

To restore the VM to a different location:

```
nbrestorevm -vmw -ir_activate -C virtual_machine -temp_location
temporary_datastore [-vmserver vCenter_server] -R rename_file_path
[-vmproxy VMware_access_host] -vmpo
```

`-C virtual_machine` identifies the virtual machine by the name or ID that was set in the policy's **Primary VM identifier** attribute for the backup. On the `-C` option, specify the same type of identifier that was used in the policy: VM host name, VM display name, VM BIOS UUID, VM DNS name, or VM instance UUID.

The `-R` option provides the path to a file that contains directives for restore to a different location.

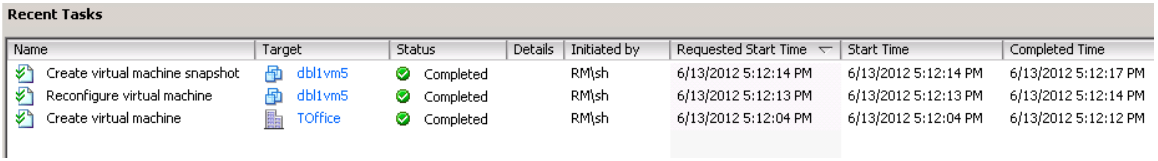
See "Restoring a virtual machine to a different location with Instant Recovery for VMware" on page 253.

See "Instant Recovery options on the nbrestorevm command" on page 244.

The nbrestorevm command mounts the virtual machine's backup image as an NFS datastore and makes the datastore accessible to the ESX host. It also creates the VM on the ESX host. It then creates a snapshot of the virtual machine.

Note: Storage lifecycle policies (SLPs) can use Auto Image Replication to replicate a virtual machine backup image to another NetBackup domain. To restore the virtual machine from the replicated image, you must include the -vmproxy option on the command. Use the -vmproxy option to specify the backup host (access host) that is in the domain where the virtual machine was replicated. Without the -vmproxy option, nbrestorevm defaults to the backup host in the original domain and the restore fails.

The following tasks appear in the vSphere Client interface. In this example, dbl1vm5 is the virtual machine to be restored.



Recent Tasks

Name	Target	Status	Details	Initiated by	Requested Start Time	Start Time	Completed Time
Create virtual machine snapshot	dbl1vm5	Completed		RM\sh	6/13/2012 5:12:14 PM	6/13/2012 5:12:14 PM	6/13/2012 5:12:17 PM
Reconfigure virtual machine	dbl1vm5	Completed		RM\sh	6/13/2012 5:12:13 PM	6/13/2012 5:12:13 PM	6/13/2012 5:12:14 PM
Create virtual machine	TOffice	Completed		RM\sh	6/13/2012 5:12:04 PM	6/13/2012 5:12:04 PM	6/13/2012 5:12:12 PM

Note the following:

- The nbrestorevm command creates a NetBackup job of type "VM Instant Recovery."
  See "Job types for Instant Recovery for VMware" on page 259.
- If you cancel the instant recovery job or stop all NetBackup services, the NetBackup NFS datastore is unmounted and its media server resources are released.

  Caution: The virtual machine is deleted from the ESX host.

  ---

2 In vSphere Client, turn on the virtual machine.

  If you included the -vmpo option on the nbrestorevm command, the virtual machine is already turned on.

3 Browse and copy the virtual machine files as needed.

To copy files while the current virtual machine is running, use a different procedure.

See "Restoring individual files with Instant Recovery for VMware while the current virtual machine is running" on page 256.

4 If you do not want to keep the restored virtual machine, enter the following:

```
nbrestorevm -ir_listvm
```

In the output, find the VM Instant Recovery ID for the restored VM.

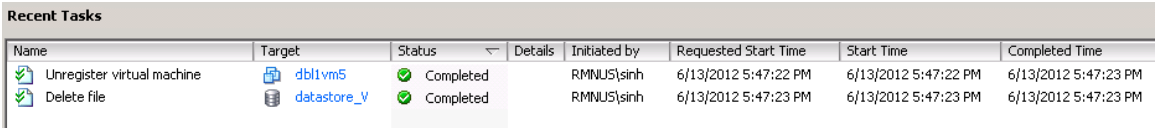
To remove the VM from the ESX host:

```
nbrestorevm -ir_deactivate instant recovery ID [-force]
```

where *instant recovery ID* is the virtual machine's numeric identifier from the -ir_listvm output. -force is optional, to suppress confirmation prompts.

The VM is removed from the ESX host. If no other VM uses the NetBackup NFS datastore, NetBackup removes that datastore and releases its resources on the media server.

The following tasks appear in the vSphere Client interface. In this example, dbl1vm5 is the virtual machine to be removed and datastore_V is the temporary datastore that it used.



This step completes the VM Instant Recovery job. Skip the rest of this procedure.

Step 5 uses Storage vMotion to move the virtual machine to a production datastore. If vMotion is already in progress for this virtual machine, you should cancel the vMotion job before you enter `-ir_deactivate`. Otherwise, vMotion moves the virtual machine to a production datastore where `-ir_deactivate` cannot remove it.

5 To keep the restored virtual machine:

In vSphere Client, right-click on the restored virtual machine and select **Migrate**. Select the migration type and the destination.

Note: For the destination, select a permanent (production) location for the virtual machine. Do not select the temporary datastore that was used for the instant restore.

Storage vMotion transfers the virtual machine data files from the NetBackup NFS datastore to the datastore that you selected.

Note: You should migrate no more than one restored virtual machine at a time per media server.

6 After the migration is complete, use vSphere Client to merge or consolidate the virtual machine's redo log (or snapshot) files manually. See your VMware documentation for details.

When the migration to the production datastore is complete, use the following steps to unmount the NFS datastore and release its resources.

7 Enter the following:

```
nbrestorevm -ir_listvm
```

In the -ir_listvm output, find the VM Instant Recovery ID for the restored VM.

8 When the data migration is complete, enter the following:

```
nbrestorevm -ir_done instant recovery ID
```

where *instant recovery ID* is the virtual machine's numeric identifier from the -ir_listvm output.

The -ir_done option completes the VM Instant Recovery job. It also removes the NetBackup NFS datastore if no other VM uses it. When the datastore is removed, its resources are released on the media server.

Restoring a virtual machine to a different location with Instant Recovery for VMware

This topic explains how to use the nbrestorevm command to restore a VM to a different location.

The overall instant recovery procedure is available in another topic:

See “Restoring a virtual machine with Instant Recovery for VMware” on page 249.

To restore a VM to a different location

1 Find the path to a resource pool at the restore destination. (If you already know the full path, you can skip this step.)

Note: To restore to a different location, it is usually necessary to designate a different resource pool. Here is an example of a resource pool path:

```
/TechOffice/host/F2/pl9.acme.com/Resources
```

To find the path, enter the following on the primary server, media server, or restore host:

UNIX, Linux:

```
/usr/openv/netbackup/bin/bpVMreq <restore_host> 11 0 <ESXi_server>
<VMserver_or_vCenter_server>
```

Windows:

```
<install_path>\NetBackup\bin\bpVMreq.exe <restore_host> 11 0
<ESXi_server> <VMserver_or_vCenter_server>
```

Note: The numeric value `11 0` is required and must be entered as shown.

For example:

```
bpVMreq battleship.acme.com 11 0 ESXi_pl9.acme.com
vC_p9vm3.acme.com
```

Where `battleship.acme.com` is the restore host, `ESXi_pl9.acme.com` is the destination ESXi server, and `vC_p9vm3.acme.com` is the destination vCenter server.

This command generates a path to an XML file in a temporary location. The XML file lists all the available resource pools.

Here is an example of an XML file that `bpVMreq` creates:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<ResourcePoolList><ResourcePool Name="Resources"
Path="/TechOffice/host/F2/pl9.acme.com/Resources"
Type="ResourcePool"><ResourcePoolList/>
</ResourcePool></ResourcePoolList>
```

In this example, the path to the resource pool is `/TechOffice/host/F2/pl9.acme.com/Resources`. Make a note of the path for use in the next step.

2 Create a text file with the following `change` entries.

Note: Each `change` entry helps to define the location for the restore. Each `change` line must end with a carriage return.

`change vmname to <new_virtual_machine_name>`	(The `change vmname` entry is optional)
`change esxhost to <new_ESXi_host>`	
`change resourcepool to <path_to_new_resouce_pool>`	
`change networkname to <new_network>`	(The `change networkname` entry is optional)

Enter each `change` line exactly as it appears in this list, except for the variable at the end (such as *new_virtual_machine_name*). Replace the variable with the new name. For example:

```
change esxhost to ESXi01.prod4.com
```

For the *new_resouce_pool*, use the path that was obtained in the first step of this procedure. For example:

```
change resourcepool to /TechOffice/host/F2/pl9.acme.com/Resources
```

This text file is called the `-R` rename file, and is used with the nbrestorevm command in the next step.

3 To restore the VM using the `-R` rename file, enter the `nbrestorevm` command with the `-R` option as follows.

Note: The `-R` option specifies the path to the text file (rename file).

- To restore to the same vCenter server but to a different ESXi host, enter the following:

  ```
  nbrestorevm -vmw -ir_activate -C <virtual_machine>
  -temp_location <temporary_datastore> -R <rename_file_path>
  ```

- To restore to a different vCenter server and a different ESXi host, enter the following:

  ```
  nbrestorevm -vmw -ir_activate -C <virtual_machine>
  -temp_location <temporary_datastore> -R <rename_file_path>
  -vmserver <vCenter_server>
  ```

To restore a VM after Auto Image Replication (AIR) to a disaster recovery (DR) site: you must also include the -vmproxy option on the nbrestorevm command to specify the restore host at the DR site.

Restoring individual files with Instant Recovery for VMware while the current virtual machine is running

You can use instant recovery to restore files individually from a virtual machine backup. You can restore the virtual machine from its backup image and mount it on a private network (such as a sandbox). This approach avoids the potential for network conflicts with the virtual machine in your production environment. Another virtual machine on a public network can be used as an intermediary, to copy the files from the virtual machine on the private network.

Note: This procedure lets you restore files into a running VM. You do not need to shut down the current virtual machine in your production environment before you start this procedure.

Before you start this procedure, you need an intermediary virtual machine that has a network connection to the public network or production network. In this procedure you connect the intermediary to the private network where the restored virtual machine is to be mounted.

At the end of the procedure, you can copy files from the restored virtual machine to the intermediary virtual machine. Then the virtual machines on the public network can access the files on the intermediary.

To restore individual files using instant recovery

1. Use vSphere Client to log on to the vCenter server.

   You must use a logon that allows access to the files that you want to recover.

2. Create a vSphere standard switch.

   This switch is for access to the ESX host from the sandbox or private network where the VM is to be activated from its backup.

   Note: The switch is for internal communication within the ESX host only.

   For example, in vSphere Client 5:

   - Select the ESX host for communication between the restored virtual machine and the intermediary virtual machine.
   - On the **Configuration** tab, in the **Hardware** pane, click **Networking**.
   - Click **Add Networking**.

- Select **Virtual Machine** as the connection type.
- Select **Create a vSphere standard switch**.
- For **Port Group Properties**, **Network Label**, enter a name for the internal switch (such as NB or NetBackup).
- Click **Finish**.

3 On the intermediary virtual machine, add a network card (NIC) to be connected to the vSphere standard switch.

Use this connection to retrieve files from the restored virtual machine that is to be mounted on the private network.

Note: This intermediary virtual machine must already have a network connection to the public network or production network.

For example, in vSphere Client 5:

- Select the intermediary virtual machine.
- On the **Summary** tab, click **Edit Settings**.
- Click **Add**.
- Select **Ethernet Adapter**.
- For the **Network label**, select the private network that is created in step 2.
- Click **Finish**.

4 If the intermediary's guest OS does not automatically assign an IP address for the private network after step 3, note: You must manually configure the IP address, default gateway, and subnet mask.

The intermediary should now be connected to both the public network and to the private network where the virtual machine is to be restored.

5 Use the nbrestorevm command to restore the virtual machine.

```
nbrestorevm -vmw -ir_activate -C virtual_machine -temp_location
temporary_datastore -R rename_file_path -vmsn
```

-vmsn specifies that no network is enabled for the virtual machine when it is activated from the backup image. Without the -vmsn option, network conflicts with the production virtual machine may occur.

The file that is designated by `-R rename_file_path` specifies a different display name or location for the restored virtual machine. You must change the virtual machine name or location to avoid conflicts with the current virtual machine in production. For example, to rename the virtual machine, the rename file can consist of the following entry (ending with a carriage return):

```
change vmname to acme_vm5
```

Note: The words `change vmname to` are literals, followed by the actual name to change to (such as `acme_vm5`).

See "Instant Recovery options on the nbrestorevm command" on page 244.

For other nbrestorevm options, see the man page or the *NetBackup Commands Reference Guide*.

6 Add a network card (NIC) to the restored virtual machine and connect the NIC to the vSphere standard switch from step 2.

7 Turn on the restored virtual machine.

8 If the guest OS does not automatically assign an IP address for the private network, configure the IP address, default gateway, and subnet mask.

9 Set up file sharing (such as through FTP, NFS, or CIFS) between the restored virtual machine and the intermediary virtual machine.

Then copy the files from the restored virtual machine to the intermediary virtual machine. The current virtual machine in production can access the files.

10 If you do not want to keep the restored virtual machine, enter the following:

```
nbrestorevm -ir_listvm
```

In the -ir_listvm output, find the VM Instant Recovery ID for the restored virtual machine.

To remove the restored virtual machine:

```
nbrestorevm -ir_deactivate instant recovery ID
```

where *instant recovery ID* is the virtual machine's numeric identifier from the -ir_listvm output.

Job types for Instant Recovery for VMware

Instant Recovery jobs appear as the following job types in the NetBackup Activity Monitor.

Table 11-5 VMware Instant Recovery job types in the Activity Monitor

Job type	Description

VM Instant Recovery	This job is the parent job for restoring a VM by means of Instant Recovery.
	To complete this job, you must enter one of the following:
	`nbrestorevm -ir_done instant recovery ID`
	`nbrestorevm -ir_deactivate instant recovery ID`
	For details on these commands:
	See "Restoring a virtual machine with Instant Recovery for VMware" on page 249.

Activate Instant Recovery	The parent VM Instant Recovery job starts an Activate Instant Recovery job to create the VM on the ESX host.
Stop Instant Recovery	This job runs when you use `nbrestorevm -ir_done` to remove the NetBackup NFS datastore and release its resources on the media server.
Deactivate Instant Recovery	This job runs when you use `nbrestorevm -ir_deactivate` to delete the restored VM from the ESX host.

Table 11-5 VMware Instant Recovery job types in the Activity Monitor *(continued)*

Job type	Description
Reactivate Instant Recovery	This job runs when you use `nbrestorevm` with the ir_reconfigure option to restart an interrupted virtual machine recovery.

Reactivating a restored virtual machine with Instant Recovery for VMware

If an interruption occurs during an instant recovery (such as a restart of the host or media server), the ESX connection to the media server may fail. In that case, it may be possible to re-establish the connection and return the virtual machine to the state it was in before the outage. Any transactions that occurred in the virtual machine before the outage are retained.

To reactivate a restored virtual machine

1. If only one VM had been restored to the ESX host, enter the following:

   ```
   nbrestorevm –ir_listvm
   ```

   Find the VM Instant Recovery ID for the restored VM in the -ir_listvm output. Then enter the following:

   ```
   nbrestorevm –ir_reactivate Instant Recovery ID [-force]
   ```

   where *instant recovery ID* is the virtual machine's numeric identifier from the -ir_listvm output. -force is an optional parameter to suppress confirmation prompts.

   The ir_reactivate option remounts the NetBackup NFS datastore. From the temporary datastore on the ESX host it registers the restored virtual machines on the ESX host.

2. If more than one VM had been restored to the ESX host:

   ```
   nbrestorevm –ir_reactivate_all -vmhost vm_host –media_server
   media_server [-force]
   ```

   Note: For multiple virtual machines, do not use the –ir_reactivate option. Use –ir_reactivate_all.

   The -vmhost option specifies the ESX host on which the virtual machines were mounted. The -media_server option specifies the media server on which the NFS datastores that contain the backup images were mounted. -force is an optional parameter to suppress confirmation prompts.

   The nbrestorevm -ir_reactivate_all command remounts the NetBackup NFS datastores on the media server and reactivates the virtual machines.

3. When the virtual machine is reactivated, you can copy its files or migrate its data to the ESX host.

   See “To restore a virtual machine with instant recovery” on page 250.

4. If Storage vMotion was migrating the virtual machine files when the outage occurred, restart the migration.

   In vSphere Client, right-click on the restored virtual machine and select **Migrate**.

Chapter 12

Use NetBackup for vCloud Director

This chapter includes the following topics:

- About NetBackup for vCloud Director
- Notes on creating a NetBackup policy for vCloud
- Notes on restoring virtual machines into vCloud Director
- Restoring virtual machines into vCloud Director
- Reducing the time required for VM discovery in a large vCloud environment
- Virtual machine recovery dialog boxes for vCloud Director

About NetBackup for vCloud Director

NetBackup can back up VMware vCloud Director environments and restore virtual machines into vCloud Director.

Table 12-1 describes the configuration requirements for backup of vCloud Director.

Table 12-1 Configuration for backup of vCloud Director virtual machines

Task	Description (NetBackup Administration Console)
Enter NetBackup credentials for the vCloud Director server and for its vCenter servers.	**Media and Device Management > Credentials > Virtual Machine Servers**. See "Adding NetBackup credentials for VMware" on page 45.

Table 12-1 Configuration for backup of vCloud Director virtual machines *(continued)*

Task	Description (NetBackup Administration Console)
Configure the policy **Clients** tab	Select the following: ■ **Select automatically through VMware Intelligent Policy query** ■ **Enable vCloud Director integration** With the Enable vCloud Director option, the policy selects only vCloud-managed virtual machines for backup: it skips the virtual machines that are not in vCloud. NetBackup collects information on the vCloud environment, such as its organizations, virtual datacenters, and vApps. NetBackup also retrieves information about a vApp for later restore of the vApp and its virtual machines. **Note:** **Enable vCloud Director integration** makes several vCloud keywords available in the policy Query Builder Field, for rule-based selection of virtual machines. If **Enable vCloud Director integration** is not selected, NetBackup cannot use the keywords to locate virtual machines in vCloud Director and the backup fails. **Note:** The browsing icon (next to the **Query Builder** drop-down fields) may list non-vCloud objects. If you select an object that is not in vCloud Director, it is excluded from the backup. See "Configuring a VMware policy from the Policies utility" on page 68. See "Notes on creating a NetBackup policy for vCloud" on page 263.

Note: The NetBackup for VMware restrictions also apply to vCloud Director objects. VMware restrictions also may apply; see your VMware documention.

See "NetBackup for VMware: notes and restrictions" on page 27.

Notes on creating a NetBackup policy for vCloud

When you create a backup policy for vCloud virtual machines, note the following:

- The configuration requirements are described in the following topic:
  See "About NetBackup for vCloud Director" on page 262.
- To back up all the existing vApp templates, use the **vCDIsvAppTemplate** keyword in the Query Builder (**vCDIsvAppTemplate Equal TRUE**).
- To back up specific vApp templates, use the **vCDvApp** keyword in the Query Builder with appropriate operator and values to select the particular templates.

- To allow a policy to back up virtual machines from multiple vCloud Director organizations: On the **VMware** tab of the policy, click **Advanced**, and enable **Multiple organizations per policy**.

Notes on restoring virtual machines into vCloud Director

To restore a virtual machine into vCloud Director, note the following:

- The Backup, Archive, and Restore interface allows the restore of one virtual machine at a time.
  You can use the `nbrestorevm` command to restore multiple virtual machines.
  See "Using the nbrestorevm command to restore virtual machines into vCloud Director" on page 338.
- When you back up a virtual machine in vCloud Director, it is recommended the **VMware display name** setting for **Primary VM identifier** on the **VMware** tab. Use of the **VM BIOS UUID** setting is not recommended.
- To restore a virtual machine into vCloud Director, the virtual machine must have been in vCloud Director when it was backed up.
  To restore a virtual machine into vCloud Director, the backup policy must have been configured as described in the following topic:
  See "About NetBackup for vCloud Director" on page 262.
- For vCloud Director restores, you can use the following configuration setting to have NetBackup automatically delete the VM left at the vCenter on import failure:
  ```
  DELETE_VM_ON_IMPORT_FAILURE = 1
  ```
  Enter this setting in `bp.conf` or the registry on the primary server.
- When a vApp is restored, vCloud Director resets the vApp's expiration date. For example: Assume the original vApp was created on the first day of the month and was set to expire in 30 days. If the vApp is restored 15 days before its expiration (on the 15th), vCloud resets the vApp to expire in 30 days from the 15th.
  The VM administrator can reset the expiration date to its original date.
- You cannot restore a virtual machine into an existing vApp template. VMware sets this restriction.
- After you restore a vApp template, the template cannot be changed and no further virtual machines can be added to it (a VMware restriction). To restore a vApp template that is to contain multiple VMs, you must restore all but one of the VMs separately into a non-template vApp. Then restore the last virtual machine by means of the **Capture vApp as a template in catalog** option.

See "Restoring a vApp template that has multiple virtual machines" on page 269.

- You can restore the vCloud Director virtual machine into vSphere instead of vCloud Director. On the **Recovery Destination** screen, select **Alternate location in vSphere.**
- vCloud organization networks are not displayed on the **Network Connections** screen for restore; only vSphere networks are displayed.
- For a restore of a vCloud Director virtual machine that resides in a vApp with special characters in its name, the VM may not show up when using the **Browse Virtual Machines** selection method. In that case, the VM can be found using the **Search Virtual Machines** selection method.
- To restore into an existing vCloud Director vApp with the **Capture vApp as a template in catalog** option, the vApp must be turned off.
- vCloud backup images cannot be restored by means of the NetBackup vSphere Web Client plug-in or the NetBackup vSphere Client (HTML5) plug-in. This type of restore can be performed by means of the Backup, Archive, and Restore interface.
- vSphere 5 provides storage profiles for managing the datastores on which virtual machines are created. When you restore into vCloud, the NetBackup restore interface lets you select a target datastore but not a storage profile. If the target datastore does not comply with the storage profile or if the datastore you select has been disabled, note: NetBackup automatically migrates the virtual machine to a compliant datastore if possible when you import to vCloud Director.

  Note: At the end of a successful restore, NetBackup verifies that the virtual machine is on compliant storage (on a datastore with the defined storage profile).

- To ensure that any VM guest customizations are restored into vCloud Director, you must set a NetBackup parameter. The parameter value specifies a wait period in seconds so that the guest customizations can be restored successfully. (The VMware API requires that the VMware Tools are installed and running, but the state of the VMware Tools cannot be identified after the restore. Therefore, we wait the specified amount of time so that the VMware Tools are running in the initial restore environment.)
  See "Ensuring that guest customizations can be restored in vCloud Director" on page 317.

Restoring virtual machines into vCloud Director

This topic includes two procedures:

- Restoring virtual machines into a vApp, or restoring a single virtual machine into a vApp template.
- Restoring a vApp template that has multiple virtual machines.

Note: You can also restore the virtual machine to an alternate location in vSphere.

See "Recovery Destination dialog box" on page 275.

Restoring a single virtual machine into a vApp or vApp template

1. Begin with the steps in the following procedure:

   See "Restoring the full VMware virtual machine" on page 181.

   When you start the Restore, the **Recovery Destination** screen appears.

2. Select the recovery destination:

Original location in vCloud Director	You can restore a virtual machine into an existing vApp or into a new vApp that replaces the existing one. You can also restore a virtual machine that is in a vApp template. **Note:** The restored vApp template can only contain one virtual machine; no further virtual machines can be added.
Alternate location in vCloud Director	You can restore a virtual machine into an existing vApp or into a new vApp or vApp template. To restore multiple virtual machines into a vApp template: See "Restoring a vApp template that has multiple virtual machines" on page 269.

3. On the **Recovery Options** screen, select the NetBackup recovery host and transport mode for the restore.

   See "Recovery Options dialog box" on page 183.

4 On the **Recovery vApp Options for vCloud Director** screen, set the vApp recovery options.

You can either restore the virtual machine into an existing vApp (if that vApp is not a template), or you can create a new vApp.

For restore to original location	Select **Restore into existing vApp**, or **Remove existing vApp and recreate the vApp**. Caution: If you remove the existing vApp, all virtual machines in the vApp are deleted. You must select the **Delete** option to acknowledge the deletion. See "Recovery vApp Options for vCloud Director dialog box (restore to original location)" on page 276. To restore a virtual machine in a vApp template, select **Remove existing vApp Template and recreate the vApp Template**. The restored vApp template can only contain one virtual machine; no further virtual machines can be added. To restore multiple virtual machines into a vApp template: See "Restoring a vApp template that has multiple virtual machines" on page 269.
For restore to alternate location	Select **Restore into existing vApp** or **Create new vApp**. You can enter details for the vApp to restore to. See "Recovery vApp Options for vCloud Director dialog box (restore to alternate location)" on page 278. **Note:** To restore the virtual machine into a vApp template that is to contain this virtual machine only, select **Create new vApp** and **Create vApp as a template in catalog**. To restore the virtual machine into a vApp template that is to contain multiple virtual machines: See "Restoring a vApp template that has multiple virtual machines" on page 269.

5 For restore to an alternate location: On the **Recovery Destination Options for vCloud Director** screen, select the ESX server, the virtual machine that you want to restore, and a datastore.

See "Recovery Destination Options for vCloud Director dialog box (restore to alternate location)" on page 279.

6 On the **Virtual Machine Options** screen, select the appropriate options for the virtual machine and its disk provisioning.

See “Virtual Machine Options dialog box” on page 184.

7 On the **Network Connections** screen, select the network for the restored virtual machine.

Note: If the virtual machine was not connected to any networks during backup, or if none of those networks are currently available, the dialog states: "No networks available for selected virtual machine." If a network connection is required, create it in vCloud Director after the restore completes.

Note: For restore to an alternate location (a different organization or vCloud server), no networks are displayed in the dialog. If a network connection is required, create it in vCloud Director after the restore completes.

See “Network Connections and Other Recovery Options dialog box (restore to alternate location)” on page 194.

8 On the **Perform Recovery** screen, run a pre-recovery check.

To begin the restore click **Start Recovery**.

9 To restore additional virtual machines into the same vApp (not a vApp template), repeat this procedure.

Note: On the **Recovery vApp Options for vCloud Director** screen, select **Restore into existing vApp**. Make sure to select the vApp into which you want to restore the additional virtual machines.

Restoring a vApp template that has multiple virtual machines

1. Use the Backup, Archive, and Restore interface to restore all but one of the virtual machines into a non-template vApp.

   You can restore one virtual machine at a time. After you have restored the first virtual machine, restore the second virtual machine with **Restore into existing vApp** on the **Recovery vApp Options for vCloud Director** screen. Select the same vApp into which you restored the first virtual machine. Step through the restore screens to restore each virtual machine in this way, except for the last virtual machine.

   Note: Use the following steps to restore the last virtual machine and to copy all the restored virtual machines into a vApp template.

2. On the **Recovery Destination** screen, select **Alternate location in vCloud Director**.
3. On the **Recovery vApp Options for vCloud Director** screen, do the following:
   - Select **Restore into existing vApp**.
   - Select the vCloud server and the organization that includes the vApp into which you have restored the other virtual machines.
   - If necessary, browse for the vApp into which you have restored the other virtual machines.
   - Select **Capture vApp as a template in catalog**.
   - Select the catalog to contain the template vApp.
     Note: The organization determines the available catalogs.
   - Enter a name for the vApp template.
   - **Remove vApp after capture**: Deletes the non-template vApp into which you restored the other virtual machines at the beginning of this procedure. Use this option to free up space on the datastore after the restore is complete.
     See "Recovery vApp Options for vCloud Director dialog box (restore to alternate location)" on page 278.
4. On the **Recovery Destination Options for vCloud Director** screen, select the last virtual machine that you want to restore into the template vApp.

   See "Recovery Destination Options for vCloud Director dialog box (restore to alternate location)" on page 279.

5 On the **Virtual Machine Options** screen, select the appropriate options for the virtual machine and its disk provisioning.

6 On the **Network Connections** screen, select the network for the restored virtual machine.

See "Network Connections and Other Recovery Options dialog box (restore to alternate location)" on page 194.

7 On the **Perform Recovery** screen, run a pre-recovery check.

To begin the restore click **Start Recovery**.

NetBackup copies the current virtual machine and the previously restored virtual machines into a new vApp template. When the restore is complete, no further virtual machines can be added to the template vApp.

Reducing the time required for VM discovery in a large vCloud environment

NetBackup backup policies for vCloud Director use query rules to automatically search and filter the vCloud environment. By default, the query rules search all the vCloud Director (vCD) servers in your environment. If the environment contains many vCloud servers with many vApps, VM discovery may take a long time. You can speed up VM discovery by limiting the search to specific vCloud servers or vApps.

The following is an example of a policy Query Builder rule that searches all vCloud servers and all vApps:

```
vmware:/?filter=vCDvApp Contains "vapp1"
```

With the Query Builder in the NetBackup web UI, the following is an example that uses OData keywords:

```
vmware:/?filter=Displayname contains(vcdvApp, 'vapp1')
```

To limit the search to particular servers or vApps, insert an additional vCloud expression in the Query Builder rule as explained in the following procedure.

To use the Administration Console to reduce the time required for VM discovery in a vCloud environment

1 In the NetBackup Administration Console, open the vCloud Director policy.

2 On the **Clients** tab of the policy, make sure **Select automatically through VMware Intelligent Policy query** and **Enable vCloud Director integration** are selected.

3 In the **Query Builder**, click **Advanced**.

4 Under **Query (Advanced Mode)**, create one or more rules to search for VMs in specific vCloud Director servers or vApps.

To create two or more rules, you must be in **Advanced Mode** (not **Basic Mode**).

Each query rule must begin on its own line.

You can use the following types of rules:

- To search for VMs in a particular vCloud server

  `vmware://<vCloud_server>?filter=<filter>`

- To search for VMs in a particular vApp or vApp template

  `vmware:/vApp/vapp-<vApp_id>?filter=<filter>`

  `vmware:/vAppTemplate/vappTemplate-<vAppTemplate_id>?filter=<filter>`

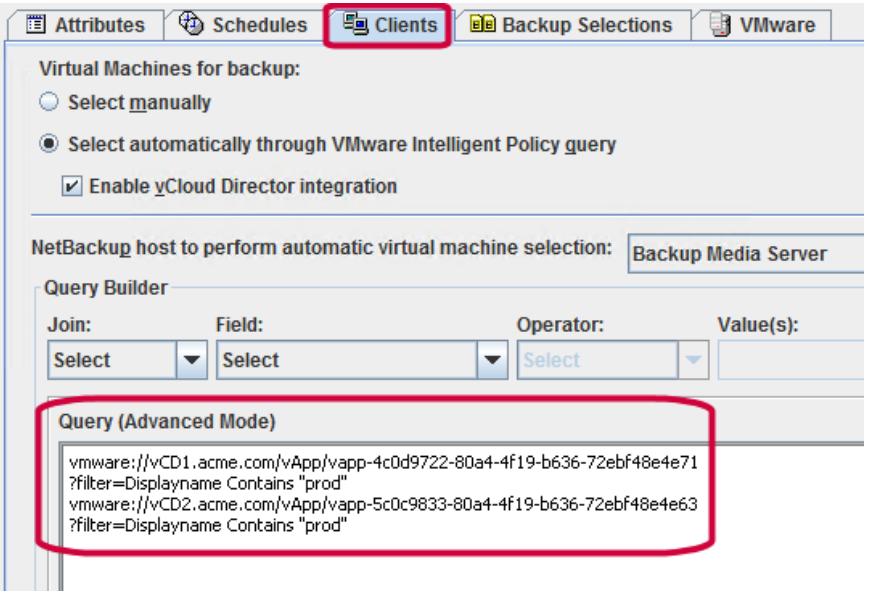
- To search for VMs in a particular vApp or vApp template on a particular vCloud server

  `vmware://<vCloud_server>/vApp/vapp-<vApp_id>?filter=<filter>`

  `vmware://<vCloud_server>/vAppTemplate/vappTemplate-<vAppTemplate_id>?filter=<filter>`

The following detail from a **Query Builder** screen **(Advanced Mode)** shows two rules for narrowing the search within a vCloud environment. The first rule searches a single vApp on vCloud server `vCD1.acme.com`. The second rule searches a different vApp on vCloud server `vCD2.acme.com`. For help in finding the vApp identifiers, see the following topic:

Example Query Builder rules for searching specific vCloud servers or vApps



5 For two or more search rules, you must enable multiple organizations for the policy.

- In the policy **VMware** tab, click **Advanced**.
- In the **VMware - Advanced Attributes** dialog, enable **Multiple organizations per policy**.
- To use the `nbdiscover` command instead of the policy **Query Builder**, see the following topic:
  Examples of the nbdiscover command for searching specific vCloud servers or vApps

Example Query Builder rules for searching specific vCloud servers or vApps

In the NetBackup policy Query Builder, you can speed up discovery of vCloud VMs by using the following types of query rules:

- To search for VMs in a particular vCloud server (note the double forward slash):
  `vmware://<vCloud_server>?filter=<filter>`
  Example rule:
  `vmware://vCD1.acme.com?filter=vCDvApp Contains "vapp1"`
  Example using OData keywords in the NetBackup web UI:
  `vmware://vCD1.acme.com?filter=contains(vcdvApp, 'vapp1')`

NetBackup searches for VMs only in the `vCD1.acme.com` server.

- To search for VMs in a particular vApp or vApp template (note the single forward slash):

  `vmware:/vApp/vapp-<vApp_id>?filter=<filter>`

  `vmware:/vAppTemplate/vappTemplate-<vAppTemplate_id>?filter=<filter>`

  The vApp_id or vAppTemplate_id is the identifier on the end of the vCloud vApp `href`. You can use a vCloud Director REST API query to find the identifier. For example, the following is a REST API query for a vApp that is named `acmvappvm7`:

  ```
  https://acmvm5.acme.com/api/query?type=adminVApp&filter=
  name==acmvappvm7
  ```

  The following example is an excerpt from the API query Response:

  ```
  href="https://acmvm5.acme.com/api/vApp/vapp-afaafb99
  -228c-4838-ad07-5bf3aa649d42"
  ```

  In this example, the vApp identifier for vApp `acmvappvm7` is `afaafb99-228c-4838-ad07-5bf3aa649d42`. You can use this identifier in a NetBackup Query Builder rule as follows:

  ```
  vmware:/vApp/vapp-afaafb99-228c-4838-ad07-5bf3aa649d42
  ?filter=Displayname Contains "prod"
  ```

  Where `Displayname Contains "prod"` is an example filter for the rule.

  Example using OData keywords in the NetBackup web UI:

  `vmware:/vApp/vapp-afaafb99-228c-4838-ad07-5bf3aa649d42?filter=contains(displayName, 'prod')`

- To search for VMs in a particular vApp on a particular vCloud Director server:

  `vmware://<vCloud_server>/vApp/vapp-<vApp_id>?filter=<filter>`

  Example rule:

  ```
  vmware://vCD1.acme.com/vApp/vapp-4c0d9722-80a4-4f19-b636-72ebf48e4e71
  ?filter=Displayname Contains "prod"
  ```

  Example using OData keywords in the NetBackup web UI:

  `vmware://vCD1.acme.com/vApp/vapp-4c0d9722-80a4-4f19-b636-72ebf48e4e71?filter=contains(displayName, 'prod')`

- To search additional vCloud Director servers or vApps from the same backup policy, include additional query rules in the Query Builder.

Note: To enter multiple rules in the **Query Builder**, you must be in **Advanced Mode**.

Note: Start each rule on its own line.

Example of two rules in the Query Builder:

```
vmware://vCD1.acme.com/vApp/vapp-4c0d9722-80a4-4f19-b636-72ebf48e4e71
?filter=Displayname Contains "prod"
vmware://vCD2.acme.com/vApp/vapp-5c0c9833-80a4-4f19-b636-72ebf48e4e63
?filter=Displayname Contains "prod"
```

Examples using OData keywords in the NetBackup web UI:

```
vmware://vCD1.acme.com/vApp/vapp-4c0d9722-80a4-4f19-b636-72ebf48e4e71
?filter=contains(displayName, 'prod')
vmware://vCD2.acme.com/vApp/vapp-5c0c9833-80a4-4f19-b636-72ebf48e4e63
?filter=contains(displayName, 'prod')
```

Examples of the nbdiscover command for searching specific vCloud servers or vApps

Use the following `nbdiscover` command format to search for VMs in specific vCloud servers or vCloud vApps:

```
nbdiscover "<vCloud_query>" -job_info "snaparg=enable_vCloud=1"
```

Example 1. Search for VMs in vCloud server `vCD1.acme.com` only:

```
nbdiscover -noxmloutput "vmware://vCD1.acme.com?filter=DisplayName
Contains 'prod1'" -job_info "snaparg=enable_vCloud=1"
```

The `-noxmloutput` option displays one VM per line.

Example 2. Search for VMs in a vCloud vApp that has the following vApp identifier:

```
4c0d9722-80a4-4f19-b636-72ebf48e4e71
```

```
nbdiscover -noxmloutput "vmware:/vApp/vapp-4c0d9722-80a4-4f19-b636
-72ebf48e4e71?filter=DisplayName Contains 'prod1'" -job_info
"snaparg=enable_vCloud=1"
```

The following topic provides assistance in finding the vApp identifier:

See the section called "Example Query Builder rules for searching specific vCloud servers or vApps" on page 272.

Example 3. Use two query rules to search for VMs prod1 and prod2 in a vCloud vApp:

```
nbdiscover -noxmloutput "vmware:/vApp/vapp-4c0d9722-80a4-4f19-b636
-72ebf48e4e71?filter=DisplayName Contains 'prod1'" "vmware:/vApp/
vapp-4c0d9722-80a4-4f19-b636-72ebf48e4e71?filter=DisplayName Contains
 'prod2'" -job_info "snaparg=enable_vCloud=1,multi_org=1"
```

Note the two rules, each enclosed with double quotes and separated by a space, and the `multi_org=1` option.

See "Notes on creating a VMware policy for vCloud Director" on page 327.

Virtual machine recovery dialog boxes for vCloud Director

The following topics describe the Backup, Archive, and Restore screens for restoring a virtual machine into vCloud Director.

You can restore a virtual machine into an existing vApp or into a new vApp.

Recovery Destination dialog box

You can select the type of destination for the virtual machine recovery: the original location in vCloud, an alternate location in vCloud, or an alternate location in vSphere.

- **Original settings of the virtual machine at backup**
  Shows the configuration of the virtual machine at the time of the backup.
  When you restore the virtual machine to its original location, these configuration settings are used and cannot be changed.
  When you restore to an alternate location, you can change these settings after you click **Next**.
- **vApp details**
  Shows the information about the virtual machine's vApp at the time of the backup.

vApp Name	The name of the vApp that contained the virtual machine when it was backed up.
vApp Status	The status of the vApp (active or expired) at the time of the backup. When the virtual machine is restored, its vApp becomes active even if the current vApp in the restore location is expired.

vCloud Catalog	The name of the catalog that contains the vApp template. "..." means that the vApp is not a template.
Other virtual machines in vApp	A link to the names of the other virtual machines in the vApp, if any.

- **Select Recovery Destination**
  You can restore to the original location in vCloud, to an alternate location in vCloud, or to an alternate location in vSphere (not in vCloud).

Recovery Options dialog box (vCloud Director)

Select the recovery host and transport mode. For a description of these options, refer to the following topic:

See "Recovery Options dialog box" on page 183.

Recovery vApp Options for vCloud Director dialog box (restore to original location)

You can choose whether to restore the virtual machine into an existing vApp or to remove the vApp and recreate it.

Restore into existing vApp	To restore the virtual machine into an existing vApp, select **Overwrite the existing virtual machine**. If the existing virtual machine is already turned on, this option fails. **Note:** If you restore a vApp template, this option is not available.
Remove existing vApp and recreate the vApp	For a vApp template, this option is labeled **Remove existing vApp Template and recreate the vApp Template** To remove the vApp (or vApp template) and recreate it, select **Delete all virtual machines to recreate this vApp**. **Note:** All virtual machines in the vApp are deleted. Click on the numeric link to see the names of the virtual machines that exist in the vApp.

Virtual Machine Options dialog box for vCloud Director

This dialog is described in a previous topic:

See "Virtual Machine Options dialog box" on page 184.

Perform Recovery dialog box for vCloud Director

Review the settings to be applied to the restored virtual machine.

- **Recovery settings**
  Lists your recovery selections, including the vCloud Director and vSphere settings.
- **Run Pre-Recovery Check**
  Verifies the credentials and appropriate paths and connectivity, determines whether the datastore or datastore cluster has available space, and reviews other important requirements. You must run this check at least once. You can proceed with the restore even if the check fails.
  Table 12-2 describes the pre-recovery checks that are unique to vCloud Director. The standard vSphere pre-recovery checks are described in another topic:
  See "Perform Recovery dialog box" on page 187.
- **Start Recovery**
  Starts the recovery of the virtual machine

Table 12-2 Pre-recovery checks for vCloud Director

Type of check	Description
vCloud server credential found	Validates the vCloud Director server credentials.
Verify login to vCloud Director server	Verifies that the NetBackup restore host can log on to the vCloud Director server.
Verify vCloud Organization	Validates the selected vCloud Director organization to restore to.
Verify vCloud ORGvDC	Validates the selected organization virtual datacenter to restore to in vCloud Director.
Verify template catalog	If the option to capture the vApp as a template is selected, validates the selected vCloud Director catalog to restore to.
Verify vApp powered off before capturing to template	If the options to restore into an existing vApp and the capture vApp as template are selected, verifies that the vApp is powered off.

Recovery Options dialog box for vCloud Director (restore to alternate location)

Select the recovery host and transport mode. For a description of these options, refer to the following topic:

See “Recovery Options dialog box” on page 183.

Recovery vApp Options for vCloud Director dialog box (restore to alternate location)

You can restore the virtual machine into an existing vApp (**Restore into existing vApp**) or into a new vApp (**Create a new vApp**).

Table 12-3 describes the fields for specifying the vApp to restore to.

Note: The defaults are the server name, organization, and other details that were recorded in the backup.

Table 12-3 Details for the vApp to be restored to

Field	Description
vCloud Server	Select the vCloud Director server for the restore. The servers in the list are the ones for which NetBackup has credentials of type **VMware vCloud Director**. See “Adding NetBackup credentials for VMware” on page 45.
Organization	Select the vCloud Director organization for the restore.
Org vDC	Select the organization virtual datacenter.
vApp name	Select or enter the name of the vApp for the restore. If you restore into an existing vApp, click **Browse** to search for a vApp. See “Select a vApp dialog box” on page 279. This option defaults to the original vApp that was recorded in the backup.
Capture vApp as a template in catalog	This option is available when you restore to an existing vApp. This option copies the vApp that is specified in the **vApp Name** field into a new vApp template. It also copies all of the vApp's virtual machines into the same vApp template. Note that this operation may take a lot of time. By default, the source vApp for the copy is retained after the copy; you can have the source vApp removed after the copy. See the **Remove vApp after capture** option.

Table 12-3 Details for the vApp to be restored to *(continued)*

Field	Description
Create vApp as a template in catalog	This option is available when you create a new vApp for the restore. This option restores the virtual machine into a new vApp template. The name of the new template is the same as the vApp that was specified in the vApp Name field.
Catalog	Select the catalog in which to place the vApp template. The organization determines the available catalogs.
vApp template name	When you restore into an existing vApp and capture the vApp as a template: Enter the name for the new vApp template.
Remove vApp after capture	When you restore into an existing vApp and capture the vApp as a template: Select this option to remove the source vApp after the vApp copy to the new vApp template completes. At the end of the copy, the new template and its virtual machines are retained. The vApp that was the source for the copy is deleted.

Select a vApp dialog box

Use this dialog to search the organization for a vApp.

Specify vApp name Enter the vApp name. As you type, the organization is expanded and the first name that contains the typed character(s) is highlighted.

Wildcards are not allowed.

Click **Search** to find further instances of the name.

vApps in Organization You can drill into the organization and highlight a vApp.

Click **OK** to select the highlighted vApp.

Recovery Destination Options for vCloud Director dialog box (restore to alternate location)

Specify details about the virtual machine to restore.

The vCloud options that you selected in the **Recovery vApp Options for vCloud Director** dialog determine the vCenter server, resource pool, and datacenter.

ESX server	Select the ESX server in which to restore the virtual machine.
Virtual machine name	Enter the name for the restored virtual machine.
Datastore/ Datastore cluster	**Specify manually**: Select a datastore from the pull-down. Or click **Pick the datastore with the largest space available**.

Virtual Machine Options (restore to alternate location)

This dialog is described in a previous topic:

See "Virtual Machine Options dialog box" on page 184.

Network connections (restore to alternate location)

The following topic describes the network information that appears on this dialog:

See "Network Connections and Other Recovery Options dialog box (restore to alternate location)" on page 194.

Perform Recovery dialog box for vCloud Director (restore to alternate location)

- **Recovery settings**
  Lists your recovery selections, including the vCloud Director and vSphere settings.
- **Run Pre-Recovery Check**
  Verifies the credentials and appropriate paths and connectivity, determines whether the datastore or datastore cluster has available space, and reviews other important requirements. You must run this check at least once. You can proceed with the restore even if the check fails. More details are available on the **Pre-Recovery Check**:
  See "Perform Recovery dialog box for vCloud Director" on page 277.
  See "Perform Recovery dialog box" on page 187.
- **Start Recovery**
  Starts the recovery of the virtual machine.

Chapter 13

Best practices and more information

This chapter includes the following topics:

- NetBackup for VMware best practices
- Best practices for VMware tag usage
- Further assistance with NetBackup for VMware

NetBackup for VMware best practices

The following are best practices for NetBackup for VMware:

- For a more efficient backup, the NetBackup media server and the VMware backup host should be installed on the same host.
- When creating virtual machines, use the same name for both host name and display name. If the policy's **Primary VM identifier** option is changed, the existing entries on the policy **Clients** tab still work.
- VMware recommends that you run no more than four simultaneous backups of virtual machines that reside on the same datastore.
- Successful VMware snapshots depend on the following:
  - The amount of I/O that occurs on the virtual machine datastore. Backups should be scheduled when relatively little I/O activity is expected. Reducing the number of simultaneous backups can also help.
    Limit access to the datastore per policy: Use the **Limit jobs per policy** attribute in the NetBackup policy.
    Limit access to the datastore globally (across all policies): Use the Host Properties **Resource Limit** screen.

See “Setting global limits on the use of VMware resources” on page 51.

- The design of the I/O substructure that is associated with each virtual machine datastore. For correct I/O design and implementation, consult your VMware documentation.

- Make sure that the VMware backup host has enough memory to handle the number of simultaneous backups that occur.
- Include in a single NetBackup policy those virtual machines that use the same datastore. This practice lets you control the amount of backup-related I/O that occurs per datastore, to limit the backup effect on the target virtual machines.
- NetBackup supports multiple backup hosts. When a single backup host is saturated with a backup process, another backup host can be added to increase backup throughput.
- If a VM's disks are accessible to multiple ESX hosts, the disks can be accessed for backup or restore through any of the ESX hosts. The ESX host may or may not be the ESX host where the virtual machine is running or registered. All of the following must be accessible to each other and should have DNS configured:
  - The vCenter server.
  - All ESX hosts under the vCenter that have access to the VM's vmdk files.
  - The backup host.
- Upgrade to the latest version of VMware vSphere or Virtual Infrastructure.

NetBackup for VMware with deduplication

For a VMware backup to a deduplication storage unit, select the **Enable file recovery from VM backup** option on the **VMware** policy tab. This option provides the best deduplication rates. Without the **Enable file recovery from VM backup** option, the result is a lower rate of deduplication.

More information is available on the VMware options.

See “Backup options on the VMware tab” on page 73.

Best practices for VMware tag usage

Use unique tag names whenever possible

The combination of **Category** and **Tag** uniquely identifies a tag association to a virtual machine. Veritas, however, does not support selection of virtual machines based on **Category**. As such, avoid the creation of tags with identical names in different **Categories**.

When you create a VMware Intelligent Policy and select virtual machines based on tags, identical tag names in different categories may have unintended consequences. All virtual machines with the tag name are selected independent of the **Category**. Be aware of this behavior as you create your VMware Intelligent Policies.

Use a primary server or a media server as a discovery host for VMware Intelligent Policies that use tags

Because tag queries require Java, the discovery host used for VMware Intelligent policies must have Java installed. NetBackup primary servers have Java installed by default. Java is an optional component for NetBackup media servers and for UNIX and Linux clients, and may or may not be installed in your environment. Windows clients that are used as a discovery host require a separate installation of the Remote Console.

Successful use of tags in a mixed vCenter Server environment

NetBackup support for VMware tags begins at vCenter 6.0. In a mixed vCenter Server environment (e.g. 5.x and 6.0), a VMware Intelligent Policy query that uses the **Tag** keyword can return some virtual machines as **Failed** if the configuration of the query requires tag evaluation on a 5.x vCenter. This behavior is observed when you select **Test Query** during policy configuration. This behavior is also observed when you run the policy. The parent (discovery) job exits with a non-zero status and its details enumerate the virtual machines that **Failed**. The virtual machines that the query has included are backed up normally.

You can use any of the options that are shown to create a query that uses tags but does not report virtual machines on 5.x servers as **Failed**.

- Use another field to limit tag evaluation to the supported vCenter Server versions.
  Example: `vCenterVersion GreaterEqual "6.0.0" AND Tag Equal "Production"`
  Example: `vCenter Equal "vcenter-123" AND tag Equal "Production"`
- Use the **VMware Server List** option under the **Advanced Attributes** on the **VMware** tab to restrict the policy to a supported list of vCenter Servers.
  See Table 5-7 on page 81.
- Enable the **Treat Tags as unset if unable to evaluate** option under the **Advanced Attributes** on the **VMware** tab.
  See Table 5-7 on page 81.

Place tag clause at the end of the VMware Intelligent Policy query

Place the tag clause toward the end of the VMware Intelligent Policy query. This configuration allows NetBackup to eliminate as many virtual machines as possible before it evaluates the tag portion of the query. This organization optimizes the performance of discovery and selection of virtual machines.

Consider the query: `Powerstate Equal poweredOn AND Tag Equal "Production"`

In the example, the first clause automatically eliminates all virtual machines that are `poweredOff`. The query does not need to evaluate the tag clause of the query for all of those virtual machines.

Tag backup and restore are best effort

Tag associations are part of the metadata of the virtual machine. NetBackup considers virtual machine tag association protection a best effort backup. Any tag collection errors are shown in the Activity Monitor for the virtual machine snapshot job.

Further assistance with NetBackup for VMware

Table 13-1 Sources of information on NetBackup for VMware

Topic	Source
Snapshot Client configuration	*NetBackup Snapshot Client Administrator's Guide*.
List of supported combinations of platforms and snapshot methods	NetBackupSnapshot Client Compatibility List
Support information on NetBackup for VMware	NetBackup Software Compatibility List

Chapter 14

Troubleshooting

This chapter includes the following topics:

- Notes on troubleshooting NetBackup for VMware
- Beware of unsupported backup host
- How to determine the ESX network that NetBackup used for the backup or restore
- NetBackup logging for VMware
- Configuring VxMS logging
- Format of the VxMS core.log and provider.log file names
- Configuring the VDDK logging level
- Preventing browsing delays caused by DNS problems
- Changing the browsing timeout for virtual machine discovery
- Changing timeout and logging values for vSphere
- Credentials for VMware server are not valid
- Snapshot error encountered (status code 156)
- The origin of the snapshot failure: NetBackup or VMware?
- Conflict between NetBackup and VMware Storage vMotion with vSphere 5.0 or later
- Incremental backups of the VM may fail if the NTFS file system in the guest OS is corrupted and the backup uses MSDP storage
- The restore fails when you restore individual files to a virtual machine that has NetBackup client software

- Backup or restore job hangs
- VMware SCSI requirements for application quiesce on Windows
- Mount point missing on a restored Windows virtual machine
- Mount points not available when restoring files from a Linux virtual machine
- Invalid client error when you restore files using NetBackup BAR interface installed on the virtual machine
- VMware virtual machine does not restart after restore
- A restored VM may not start or its file system(s) may not be accessible
- NetBackup job fails due to update tasks on the VMware server
- The vSphere interface reports that virtual machine consolidation is needed
- The Enable file recovery from VM backup option does not work if a volume disk set contains a mixture of disk types
- Linux VMs and persistent device naming
- For a VMware virtual machine with Windows dynamic disks, a restore from incremental backup fails with a Windows restore host and the hotadd transport mode
- Simultaneous hotadd backups (from the same VMware backup host) fail with status 13
- Troubleshooting VMware tag usage
- Ensuring that guest customizations can be restored in vCloud Director
- Troubleshooting vmdk restore to existing VM
- Errors for backups of virtual machines on Virtual Volumes (VVols)
- Issues with the CA certificate during installation of the NetBackup client on VMware Cloud (VMC)

Notes on troubleshooting NetBackup for VMware

Note the following:

- Make sure that the VMware Tools are installed and up to date on each virtual machine. Otherwise, communication problems and other issues can result. For example:

- When you select virtual machines on the policy **Clients** tab, NetBackup cannot obtain the host name, IP address, or DNS name of the virtual machine. Policy validation may fail.
- The virtual machine cannot be quiesced in preparation for the snapshot.

- You cannot restore individual VMware files onto the virtual machine itself, except under certain conditions.
  See "About restore of individual files" on page 223.

Beware of unsupported backup host

Ensure that NetBackup supports your VMware backup host. For supported backup host platforms, see the *NetBackup Enterprise Server and Server OS Software Compatibility List* available from the following location:

NetBackup Primary Compatibility List

For further VMware documentation on the backup host, see the information on backup proxy in the following VMware article:

Best practices when using advanced transport for backup and restore

How to determine the ESX network that NetBackup used for the backup or restore

If a virtual machine's disks are accessible to multiple ESX hosts, the disks can be accessed through any of the ESX hosts. The ESX host that is used for the access may or may not be the ESX host where the virtual machine is running or registered. All of the following must be accessible to each other and should have DNS configured:

- The vCenter server.
- All ESX hosts under the vCenter that have access to the virtual machine's vmdk files.
- The backup host.

If all hosts are not accessible to each other, the backup or restore may not succeed. In that case, you must determine which network NetBackup used for the backup or restore.

Note: For an NBD transport mode backup through vCenter, NetBackup uses the ESX network over which the ESX host was added or registered to the vCenter. For an NBD transport mode backup directly from the ESX host, NetBackup uses the ESX host's DNS/IP network.

The VxMS provider logs contain information on the network that NetBackup used.

See "Configuring VxMS logging" on page 290.

Check the VxMS provider logs for messages similar to those in this example:

```
10:49:21.0926 : g_vixInterfaceLogger:libvix.cpp:1811 <INFO> : Opening file
[MYDATASTORE] TestVM/TestVM-000001.vmdk (vpxa-nfc://[MYDATASTORE]
TestVM/TestVM-000001.vmdk@MyESX.xxx.xxx.com:902)

   10:49:22.0301 : g_vixInterfaceLogger:libvix.cpp:1811 <INFO> : DISKLIB-LINK  :
Opened 'vpxa-nfc://[MYDATASTORE]
TestVM/TestVM-000001.vmdk@MyESX.xxx.xxx.com:902' (0x1e): custom, 41943040
sectors / 20 GB.

   10:49:22.0301 : g_vixInterfaceLogger:libvix.cpp:1811 <INFO> : DISKLIB-LIB   :
Opened "vpxa-nfc://[MYDATASTORE]
TestVM/TestVM-000001.vmdk@MyESX.xxx.xxx.com:902" (flags 0x1e, type custom).

   10:49:22.0301 : vdOpen:VixInterface.cpp:480 <DEBUG> : Done with
VixDiskLib_Open(): 200346144
   10:49:22.0301 : openLeafSnapshotDisks:VixGuest.cpp:475 <DEBUG> : vdOpen()
succeess
   10:49:22.0301 : openLeafSnapshotDisks:VixGuest.cpp:476 <INFO> : Transport
mode in effect = nbd
```

VMware logs the messages starting with `g_vixInterfaceLogger`. Such messages in the example indicate that TestVM-000001.vmdk is opened over the ESX host network `MyESX.xxx.xxx.com`.

The following article contains related information:

- *Best practices when using advanced transport for backup and restore*
  http://kb.vmware.com/kb/1035096

NetBackup logging for VMware

For log messages about VMware backup or VMware restore, see the following NetBackup log directories.

Table 14-1 NetBackup logs that pertain to VMware backup and restore

Log directory	Contains the messages on	Resides on
install_path\NetBackup\logs\bpbrm	Backup and restore	NetBackup primary or media server

Table 14-1 NetBackup logs that pertain to VMware backup and restore *(continued)*

Log directory	Contains the messages on	Resides on
install_path\NetBackup\logs\bptm	Backup and restore	NetBackup media server
install_path\NetBackup\logs\bpfis	Snapshot creation and backup	VMware backup host
install_path\NetBackup\logs\bpcd	Snapshot creation and backup	VMware backup host
install_path\NetBackup\logs\bpbkar	Backup	VMware backup host
install_path\NetBackup\logs\bprd	Restore	NetBackup primary server
install_path\NetBackup\logs\nbfsd	Instant recovery	NetBackup media server and VMware backup host
install_path\NetBackup\logs\bpVMutil	Policy configuration and on restore	VMware backup or recovery host
install_path\NetBackup\logs\bpVMreq	Restore	The client where the Backup, Archive, and Restore interface is running.
install_path\NetBackup\logs\nbproxy	Policy configuration	VMware backup host
install_path\NetBackup\logs\ncfnbcs (originator ID 366) ncfnbcs uses unified logging. See the *NetBackup Logging Reference Guide* for information on how to use unified logs.	Automatic virtual machine selection, and disabling and re-enabling VMware Storage vMotion during backup or restore.	VMware backup host
install_path\NetBackup\logs\ncfnbrestore (originator ID 357) ncfnbrestore uses unified logging. See the *NetBackup Logging Reference Guide* for information on how to use unified logs.	Restore	VMware recovery host
Windows: *install_path*\NetBackup\logs\vxms Linux: /usr/openv/netbackup/logs/vxms	File mapping during backup	VMware backup host See “Configuring VxMS logging” on page 290. **Note:** The use of VxMS logging can reduce the performance of the backup host.

Note: Except for unified logging directories, these log directories must already exist in order for logging to occur. If these directories do not exist, create them.

To create most of these log directories, run the following command on the NetBackup servers and backup host:

Windows:

```
install_path\NetBackup\logs\mklogdir.bat
```

UNIX (on primary or media servers):

```
/opt/openv/netbackup/logs/mklogdir
```

See "Configuring VxMS logging" on page 290.

More detail is available on snapshot logs and logging levels. See the *NetBackup Snapshot Client Administrator's Guide*.

A broader discussion of NetBackup logging is available. See the *NetBackup Logging Reference Guide*.

Configuring VxMS logging

The following procedures describe how to configure VxMS logging for NetBackup.

Except as noted in this topic, you can also use the Logging Assistant (in the NetBackup Administration Console) to configure VxMS logging.

Note: VxMS logging may require significant resources on the VMware backup host.

VxMS logging on a Linux backup host

To configure VxMS logging on a Linux backup host

1. Create the VxMS log directory:

   `/usr/openv/netbackup/logs/vxms`

   Note: For logging to occur, the VxMS directory must exist.

   Note: If you have run the NetBackup `mklogdir` command, the VxMS log directory already exists.

   See "NetBackup logging for VMware" on page 288.

2. Add the following to the `/usr/openv/netbackup/bp.conf` file:

   `VXMS_VERBOSE=<numeric value of 0 or greater>`

   See Table 14-2 for the available logging levels.

3. To change the log location, enter the following in the `bp.conf` file:

   `vxmslogdir=path to new log location`

   Note: If the VxMS log location is changed, the Logging Assistant does not collect the logs.

VxMS logging on a Windows backup host

To configure VxMS logging on a Windows backup host

1 Create the VxMS log directory:

install_path\NetBackup\logs\vxms

Note: For logging to occur, the VxMS folder must exist.

Note: If you have run the NetBackup `mklogdir.bat` command, the VxMS log directory already exists.

See "NetBackup logging for VMware" on page 288.

2 In the Windows registry, create the DWORD registry entry `VXMS_VERBOSE` in the following location:

HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > Config

3 To configure the logging level, set the numeric value of `VXMS_VERBOSE` to 0 or greater. Larger numbers result in more verbose logs.

See Table 14-2 for the available logging levels.

4 To change the log location:

- Open regedit and go to the following location:
  HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion
- Create the registry entry `vxmslogdir` with a string value `(REG_SZ)`. For the string value, specify the full path to an existing folder.

Note: You can use NTFS compression on VxMS log folders to compress the log size. The new logs are written in compressed form only.

Note: If the VxMS log location is changed, the Logging Assistant does not collect the logs.

VxMS logging levels

Table 14-2 lists the VxMS logging levels.

Note: Logging levels higher than 5 cannot be set in the Logging Assistant.

Note: Logging levels higher than 5 should be used in very unusual cases only. At that level, the log files and metadata dumps may place significant demands on disk space and host performance.

Table 14-2 VxMS logging levels

Level	Description
0	No logging.
1	Error logging.
2	Level 1 + warning messages.
3	Level 2 + informative messages.
4	Same as level 3.
5	Highly verbose (includes level 1) + auxiliary evidence files (`.mmf, .dump, VDDK logs, .xml, .rvpmem`). You can set the logging level for the VDDK messages.
6	VIX (VMware virtual machine metadata) dumps only.
7	VHD (Hyper-V virtual machine metadata) dumps only.
> 7	Full verbose + level 5 + level 6 + level 7.

Format of the VxMS core.log and provider.log file names

For the log files `core.log` and `provider.log` created by default during VxMS logging, the NetBackup administrator's user name is inserted into the log file name.

Table 14-3 describes the format of the log file names.

Table 14-3 Format of VxMS core.log and provider.log file names

Platform	VxMS log-file-name format

Windows	`VxMS-`*`thread_id-user_name`*`.`*`mmddyy_tag`*`.log`
	For example:
	`VxMS-7456-ALL_ADMINS.070214_core.log`
	`VxMS-7456-ALL_ADMINS.070214_provider.log`

UNIX, Linux	`VxMS-`*`thread_id-user_name`*`.log.`*`mmddyy_tag`*
	For example:
	`VxMS-27658-root.log.081314_core`
	`VxMS-27658-root.log.081314_provider`

See "Configuring VxMS logging" on page 290.

Configuring the VDDK logging level

The following NetBackup processes capture VDDK log messages:

- `bpbkar, bpbkarv, nbrestore`
  These processes write VDDK messages in the VxMS logs if the VxMS logging level (VxMS_VERBOSE) is 5 or higher. By default, when VXMS_VERBOSE is 5 or higher, the VDDK messages are generated at the highest verbosity.
- `ncfnbcs, bpVMutil`
  These processes write VDDK messages in their own log directories if the NetBackup global logging level is 5. By default, when the NetBackup global logging level is 5, the VDDK messages in the ncfnbcs and bpVMutil logs are generated at minimum verbosity.

To change the logging level (verbosity) of the VDDK messages

1. Check the following on the backup host:
   - Make sure the VxMS log directory exists and that the VXMS_VERBOSE DWORD is set to 5 or higher.
     See "Configuring VxMS logging" on page 290.
   - Make sure the bpVMutil log directory exists and that the NetBackup global logging level is set to 5.

Note: The ncfnbcs process uses unified logging: You do not have to manually create a log directory for ncfnbcs. More information on unified logging is available in the NetBackup Logging Reference Guide.

2 Enter the following on the backup host:

- Windows:
  Create the DWORD registry entry VDDK_VERBOSE in the following location:
  HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > Config
- Linux:
  Add the following to the `/usr/openv/netbackup/bp.conf` file:
  `VDDK_VERBOSE=`*`numeric value`*

3 Set the numeric value of VDDK_VERBOSE as follows:

0	Panic (failure messages only).
1	Level 0 + error logging.
2	Level 1 + warning messages.
3	Level 2 + audit messages.
4	Level 3 + informational messages.
5	Highly verbose; level 4 + additional details.
6	Most verbose; level 5 + debug messages.

Preventing browsing delays caused by DNS problems

NetBackup may be unable to identify virtual machines when you use the **Browse for Virtual Machines** dialog. Virtual machine host names may not be properly configured in your Domain Name Server system (DNS), or the DNS system may be slow. A timeout message may appear, or messages similar to the following may appear in the NetBackup detailed status log:

```
17:25:37.319 [12452.10360] get_vSphere_VMs: Processing vm 002-wcms
17:25:37.319 [12452.10360] get_vSphere_VMs:    uuid
421a8b46-063d-f4bd-e674-9ad3707ee036
```

```
17:25:37.319 [12452.10360] get_vSphere_VMs:    vmxdir [san-05] 002-wcms/
17:25:37.319 [12452.10360] get_vSphere_VMs:    datastore san-05
17:25:37.319 [12452.10360] get_vSphere_VMs:    IpAddress 172.15.6.133
17:25:41.866 [12452.10360] get_vSphere_VMs: retry_gethostbyaddr for
172.15.6.133 failed with The requested name is valid, but no data of
the requested type was found.
```

Note: NetBackup may be unable to determine the host names of the virtual machines from their IP addresses (reverse lookup may fail).

To prevent browsing delays caused by DNS problems (Windows)

1. On the Windows desktop of the backup host, click **Start > Run** and enter `regedit`.
2. To be on the safe side, make a backup of the current registry (**File > Export**).
3. Go to **HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > Config** and create a key that is called `BACKUP`.
4. Create a new DWORD under `BACKUP`, called `disableIPResolution`.

   This registry key causes NetBackup to use the virtual machine's IP address as the virtual machine's host name.
5. Use the NetBackup **Browse for Virtual Machines** screen to rediscover the virtual machines. The host names should now be the IP addresses.

   See "Browse for VMware virtual machines" on page 91.

To prevent browsing delays caused by DNS problems (Linux)

1. On the Linux backup host, create (or open) the following file:

   `/usr/openv/netbackup/virtualization.conf`

2. Add the following to the file:

   ```
   [BACKUP]
   "disableIPResolution"=dword:00000000
   ```

   This entry causes NetBackup to use the virtual machine's IP address as the virtual machine's host name.

   Note: If the file already contains a `[BACKUP]` line, do not add another `[BACKUP]` line. Any other lines that already exist under `[BACKUP]` should remain as they are.

3. Use the NetBackup **Browse for Virtual Machines** screen to rediscover the virtual machines. The host names should now be the IP addresses.

   See "Browse for VMware virtual machines" on page 91.

The following applies if: the **Primary Identifier** in VMware Intelligent Policies is selected as **VM host name** and **Reverse name lookup** is enabled in the configuration setting.

In a large VMware environment, reverse name lookups can be very slow depending on the number of virtual machines being discovered. You can change the `VNET_OPTIONS` option to determine how many items NetBackup can cache. This value is in the `bp.conf` file on UNIX and Linux, and the registry on Windows.

The third value 200 is the default number of entries to be cached. Each entry takes about 1 kilobyte in memory. Available memory needs to be taken into account when you change this value. The maximum number of allowed entries is 100000.

```
VNET_OPTIONS = 120 3600 200 40 3 1 30 10 1793 32 0 0
```

Use the `nbgetconfig` command to view the configuration settings. Use `nbsetconfig` to change the settings.

Changing the browsing timeout for virtual machine discovery

When browsing for virtual machines in the **Browse for Virtual Machines** dialog, the browsing timeout value may need to be increased.

To change the browsing timeout value

1. On the host that runs the NetBackup Administration Console, open the following file:

   `/usr/openv/java/nbj.conf`

2. Change the value of the `NBJAVA_CORBA_DEFAULT_TIMEOUT` parameter.

   By default, this parameter is set to 60 seconds:

   `NBJAVA_CORBA_DEFAULT_TIMEOUT=60`

   Increase the value to a higher number.

   For more information on the `nbj.conf` file, see the *NetBackup Administrator's Guide, Volume I*:

Http://www.veritas.com/docs/DOC5332

See "Browse for VMware virtual machines" on page 91.

Changing timeout and logging values for vSphere

Table 14-4 lists the vSphere keys and their default values for various timeouts. These values can be changed on the backup host (see the procedure in this topic).

Table 14-4 DWORD keys and defaults for vSphere timeouts

DWORD key name	Default value (in seconds)
`jobtimeout`	900
`poweroptimeout`	900
`snapshottimeout`	900
`registertimeout`	180
`browsetimeout`	180
`connecttimeout`	300

The key and default for the vSphere API logging level are the following.

Table 14-5 DWORD key and default for vSphere API log level

DWORD key name	Default value
`vmcloglevel`	0 (no logging)

Changes to the vSphere API logging level affect the following logs on the backup host:

- For backups (snapshot creation): `bpfis` log
- For restores: `bpVMutil` log
- For virtual machine discovery: `ncfnbcs` log (originator ID 366)

The logs are in the following location on the backup host:

Windows: *install_path*\NetBackup\logs\

Linux: /usr/openv/netbackup/logs

To change vSphere timeouts and logging values on Windows

1. On the Windows desktop of the backup host, click **Start > Run** and enter `regedit`.
2. To be on the safe side, make a backup of the current registry (**File > Export**).
3. Go to **HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > CONFIG** and create a key that is called `BACKUP`.
4. To change a timeout value, create a new DWORD under `BACKUP`, using the appropriate registry name (such as `jobtimeout` or `poweroptimeout`).

   Enter a value for the timeout.
5. To change the level of vSphere API logging, create a new DWORD called `vmcloglevel` and enter the new logging value.

   The allowed values are 0 through 6, where 0 is no logging and 6 is the highest log level.

To change vSphere timeouts and logging values on Linux

1. On the Linux backup host, create (or open) the following file:

   `/usr/openv/netbackup/virtualization.conf`

2. To change a timeout value, enter a new `dword` line under `[BACKUP]`, using the appropriate name (such as `jobtimeout` or `poweroptimeout`). Include a value for the timeout.

   For example:

   ```
   [BACKUP]
   "jobtimeout"=dword:60
   ```

   This example sets the job timeout to 60 seconds.

   Note: If the file already contains a `[BACKUP]` line, do not add another `[BACKUP]` line. Any other lines that already exist under `[BACKUP]` should remain as they are.

3. To change the level of vSphere API logging, enter a `dword` line for `vmcloglevel` with a logging value, under `[BACKUP]`. For example:

   ```
   "vmcloglevel"=dword:6
   ```

   The allowed values are 0 through 6, where 0 is no logging and 6 is the highest log level.

Credentials for VMware server are not valid

A number of issues can prevent NetBackup from gaining access to the ESX server or vCenter server. When you add credentials for a VMware server (**Add Virtual Machine Server** dialog), NetBackup validates the credentials when you click OK. If the credentials do not pass validation, a pop-up message appears.

Problems can result for a variety of reasons, including the following:

- An incorrect virtual machine server name. Make sure that the server name is entered correctly.
  More information is available about changing the server name that is stored in NetBackup.
  See “Changing the host name of a VMware server in NetBackup” on page 50.
- An invalid user name or password. Make sure that a valid user name and password were entered correctly.
- An incorrect port number. Make sure that the port number is correct on the NetBackup **Change Virtual Machine Server** dialog. If the VMware server uses

the default port, no port specification is required. You can uncheck the **Connect using port number** box.

- You do not have enough privileges to perform backups or restores. (Note however that lack of sufficient privileges may not cause the credential validation to fail.)
  For the minimum permissions needed to back up and restore with vStorage, see the following:
  http://www.veritas.com/docs/TECH130493

See "Adding NetBackup credentials for VMware" on page 45.

Snapshot error encountered (status code 156)

The following table describes the VMware issues that relate to NetBackup status code 156.

Table 14-6 Possible causes of status code 156

Causes of status code 156	Description and recommended action
NetBackup cannot obtain the volume ID of a drive	NetBackup may not be able to obtain the volume ID of a drive. In that case, none of the virtual machine drives are backed up. The backup fails with NetBackup status code 156. The drive may be down.
A backup of the virtual machine is already active	You cannot run more than one backup per virtual machine at a time. If you start a second backup of the virtual machine while the first backup is active, the second job fails with a status 156. Recommended action: Wait until the first job completes, then run the second one.
Cannot find virtual machine name	NetBackup cannot find the host name or VM display name of a virtual machine that is listed in the backup policy. The detailed status log may include the following error message: `Critical bpbrm (pid=<pid number>) from client <client name>: FTL - snapshot creation failed, status 156.)` If the virtual machines do not have static IP addresses, you can configure NetBackup to identify virtual machines by their VM display names or UUIDs. Examples of the environments that do not use static IP addresses are clusters, and the networks that assign IP addresses dynamically. Note that NetBackup may have been configured to identify virtual machines by their VM display names. In that case, make sure that the display names are unique and that they do not contain special characters. See "Primary VM identifier options (VMware)" on page 76.

Table 14-6 Possible causes of status code 156 *(continued)*

Causes of status code 156	Description and recommended action
The virtual machine is powered off	Through a vCenter server, NetBackup can back up the virtual machines that are turned off. You must provide credentials for NetBackup to access the vCenter server. See "Adding NetBackup credentials for VMware" on page 45. If NetBackup uses credentials for an ESX server instead of vCenter, it may not be able to identify a turned off virtual machine. Note the following: ■ If the policy uses VM host name or VM DNS name as the Primary VM identifier, NetBackup may not find the virtual machine. The backup fails. ■ If the policy uses VM display name or VM UUID as the Primary VM identifier, NetBackup can identify the virtual machine. The backup succeeds.
The virtual machine has one or more independent disks and is in a suspended state	If a virtual machine with independent disks is in a suspended state, snapshot jobs fail. Messages similar to the following appear in the job details log: `01/12/2015 17:11:37 - Critical bpbrm (pid=10144) from client <client name>: FTL - VMware error received: Cannot take a memory snapshot, since the virtual machine is configured with independent disks.` This issue results from a VMware limitation (SR#15583458301). More information is available in the following VMware article: http://kb.vmware.com/kb/1007532 As a workaround, change the state of the virtual machine to powered on or powered off, and rerun the backup. **Note:** Data on independent disks cannot be captured with a snapshot. The rest of the virtual machine data is backed up.
The virtual machine's disk is in raw mode (RDM)	The RDM is ignored (not backed up) and any independent disk is recreated but empty. See "Configurations for backing up RDMs" on page 370.
The attempt to create a snapshot exceeded the VMware timeout	If the attempt to create a snapshot of the virtual machine exceeds the VMware timeout of 10 seconds, the snapshot fails with NetBackup status 156. This timeout may occur if the virtual machine is configured with a large number of volumes. Note that the timeout may be encountered even if the **Virtual machine quiesce** option was disabled. Do one of the following: ■ Reduce the number of volumes within the virtual machine. ■ Install a NetBackup client on the virtual machine and select another backup method for the policy (not the VMware snapshot method).

Table 14-6 Possible causes of status code 156 *(continued)*

Causes of status code 156	Description and recommended action
The virtual machine has no vmdk file assigned	The snapshot fails if the virtual machine has no vmdk file. Virtual machines without vmdk files can occur in a vCenter Site Recovery Manager (SRM) environment. If a replicated virtual machine has never been active, it is in passive mode and may have no vmdk file(s). You can enable the **Ignore diskless VMs** option on the **VMware Advanced Attributes** tab of the policy. If this option is enabled: NetBackup does not back up a replicated (passive) virtual machine in an SRM environment if that virtual machine has no vmdk files. More information is available on the **Ignore diskless VMs** option. See "VMware - Advanced Attributes dialog" on page 81.

The vmdk file has too many delta files	Whenever a VMware snapshot occurs, a delta.vmdk file is created for each vmdk. If 32 or more such delta files exist for a single vmdk file, a NetBackup backup of that VM may fail (status 156). The NetBackup Activity Monitor job details contain messages similar to the following:
	
	`02/06/2015 10:33:17 - Critical bpbrm (pid=15799) from client fl5vm1_2012: FTL - vSphere_freeze: Unable to proceed with snapshot creation, too many existing delta files(44).`
	`02/06/2015 10:33:17 - Critical bpbrm (pid=15799) from client fl5vm1_2012: FTL - VMware_freeze: VIXAPI freeze (VMware snapshot) failed with 25: SYM_VMC_FAILED_TO_CREATE_SNAPSHOT`
	`02/06/2015 10:33:17 - Critical bpbrm (pid=15799) from client fl5vm1_2012: FTL - vfm_freeze: method: VMware_v2, type: FIM, function: VMware_v2_freeze`
	
	To back up the VM, do the following:
	
	1 Consolidate the VM's snapshots.
	
	In the VMware interface, right-click on the VM and select **Snapshot > Consolidate**. For more information, see your VMware documentation.
	
	2 Verify that each of the VM's vmdk files now has fewer than 32 delta files.
	
	If the snapshot consolidation was not successful, see the following VMware article for further assistance:
	
	Committing snapshosts in vSphere
	
	3 Rerun the NetBackup backup.

VMware snapshot quiesce operation failed	If the NetBackup policy is enabled for virtual machine quiesce (the default), the VMware snapshot operation in vSphere initiates a quiesce of the virtual machine. If snapshot quiesce fails, the NetBackup job fails with status 156.

The origin of the snapshot failure: NetBackup or VMware?

When a NetBackup snapshot job fails with status 156, the problem may originate in your VMware environment rather than in NetBackup. You can begin to isolate the problem to one environment or the other by using vSphere Client to take a snapshot of the VM. NetBackup support often uses this approach to investigate a snapshot issue.

To identify the environment in which the snapshot error occurred

1. In the vSphere interface, right-click on the VM and click **Snapshots > Take Snapshot**.
2. In the **Take VM Snapshot for** dialog, click **Quiesce guest file system** if the NetBackup policy was enabled for virtual machine quiesce (the default).

   In the NetBackup policy, the **Virtual machine quiesce** option is in the **VMware - Advanced Attributes** dialog.

   Note: In the **Take VM Snapshot for** dialog, make sure the **Snapshot the virtual machine's memory** option is not selected. NetBackup does not use that option.

3. Start the snapshot and check the **Recent Tasks** pane for snapshot status.
   - If the snapshot does not complete, the problem with the NetBackup snapshot may be in the VMware environment. Consult your VMware documentation.
   - If the VMware snapshot is successful, the issue may be with NetBackup. For relevant error messages, consult the NetBackup bpfis logs.
     See “NetBackup logging for VMware” on page 288.
     The following topic summarizes some common causes of 156 errors:
     See “ Snapshot error encountered (status code 156)” on page 301.

Conflict between NetBackup and VMware Storage vMotion with vSphere 5.0 or later

To avoid conflicts with Storage vMotion in vSphere 5.0 or later, NetBackup should conduct backups through the vCenter server, not through the ESX host. A backup directly through the ESX server may fail if Storage vMotion simultaneously migrates the virtual machine’s files. In addition, the virtual machine’s snapshot files may be

stranded or other problems with the virtual machine may result. VMware has acknowledged this issue.

If the backup fails, the NetBackup job details contain a message similar to the following:

```
Error opening the snapshot disks using given transport mode: Status 23.
```

To back up a virtual machine while its files are in the process of migration, NetBackup must conduct the backup through the vCenter server.

To back up a virtual machine while its files are in the process of migration

1. In the NetBackup Administration Console, under **Media and Device Management > Credentials > Virtual machine servers**, add NetBackup credentials for the vCenter server.

   Select a server type of VMware VirtualCenter Server.
2. Delete the credentials that are currently defined under the server type VMware ESX server, and add those credentials as type VMware Restore ESX Server.
3. Rerun the backup.

Incremental backups of the VM may fail if the NTFS file system in the guest OS is corrupted and the backup uses MSDP storage

This error may occur in the following case:

- The VMware or Hyper-V backup policy specifies Media Server Deduplication Pool (MSDP) storage.
- The backup schedule includes incrementals (differential or cumulative).
- The NTFS file system in the VM's guest OS is corrupted. For example, the file system contains orphaned file record segments. The `bptm` debug log contains messages similar to the following:

  ```
  16:24:04.604 [5720.7068] <16> 6:bptm:5720:win2012-2.hrous.sen.com:
  [ERROR] PDSTS: fbu_fill_bitmap: (1945) stream_offset(610848768)
  + length(8192) > (1946) stream_offset(610848768)
  16:24:04.604 [5720.7068] <16> 6:bptm:5720:win2012-2.hrous.sen.com:
  [ERROR] PDSTS: fbu_scan_buf: fbu_fill_bitmap() failed
  (2060022:software error)
  ```

  The incremental backups fail with status 84, media write error.

Use the `chkdsk` command to examine the file system in the guest OS and repair it as needed. Then restart the VM and rerun the backup.

The restore fails when you restore individual files to a virtual machine that has NetBackup client software

When you restore individual files to a virtual machine that has a NetBackup client, make sure that a firewall does not interfere with the restore. If a firewall stops the restore, turn off the firewall and retry the restore.

Backup or restore job hangs

NetBackup may have exceeded the maximum number of allowed VMware NFC connections to the ESX server when it used the transport modes `nbd` or `nbdssl`. Note that NetBackup uses one NFC connection per virtual disk on the ESX or ESXi server.

If NetBackup is configured to access the ESX server directly (not through a vCenter or VirtualCenter server), fewer connections are allowed. The following are the maximum connections as set by VMware:

Table 14-7 VMware NFC connection limits for `nbd` or `nbdssl` transfers

ESX version	Type of access to the ESX server	Maximum NFC connections allowed
ESX 4	Directly to ESX server	9
ESX 4	Through vCenter	27
ESXi 4	Directly to ESX server	11
ESXi 4	Through vCenter	23
ESXi 5	Directly to ESX server	The maximum total for all NFC connection buffers to an ESXi host is 32 MB
ESXi 5	Through vCenter	52

Try a different transport type (such as SAN or hotadd). If a different transport type is not available and NetBackup accesses the ESX servers directly, set up access through a vCenter (or VirtualCenter) server. Use of a server increases the maximum

number of allowed connections. For example: With 27 connections, NetBackup can access a virtual machine that has up to 27 disks, if the ESX 4 server is behind a vCenter server.

Note that the connection limits are per-host (that is, per vCenter or ESX server).

For example, assume the following environment:

- An ESX 4.0 server with three virtual machines.
- Each virtual machine has ten virtual disks.
- The virtual machines are behind a vCenter 4.0 server.

For a simultaneous backup of the three virtual machines, NetBackup requires 30 NFC connections. With a limit of 27 NFC connections per vCenter server, any of the three backup jobs may hang.

These limits are described in the *VMware Virtual Disk API Programming Guide*:

VMware Virtual Disk API Programming Guide

See also the following section of the *VMware vSphere 5 Documentation Center*:

Virtual Disk Transport Methods

VMware SCSI requirements for application quiesce on Windows

For a snapshot that quiesces an application on a Windows VM, VMware imposes the following disk requirements:

- The VM's disks must be SCSI, not IDE.
- The SCSI disks on the VM's SCSI controller must not occupy more than half of the total number of slots in the controller. Since the controller has a total of 15 slots, the number of disks in that controller must not exceed 7.
  If these conditions are not met and the NetBackup VMware policy enables the **Virtual machine quiesce** option, the backup may fail with status code 156.
  For more information on this VMware requirement, refer to the following article in the *VMware vSphere 6.0 Documentation Center*:
  Windows Backup Implementations

Mount point missing on a restored Windows virtual machine

A Windows virtual machine may fail to write its mount point configuration to disk (the mount point configuration remains in RAM). In that case, the mount point information cannot be backed up. When the virtual machine is restored, the data from the mounted volume is restored, but the mount point is absent from the restored virtual machine.

Reassign the mount point on the restored virtual machine. To make sure the mount point is correctly configured, restart the virtual machine.

Mount points not available when restoring files from a Linux virtual machine

For Linux virtual machines, only the ext2, ext3, and ext4 file systems are supported for individual file restore. If a partition is formatted with some other file system, the backup succeeds but NetBackup cannot map the file system addresses of the files. As a result, NetBackup cannot restore individual files from that partition. Only the files that were on ext2, ext3, or ext4 partitions can be individually restored.

Note also: To restore individual files from their original mount points, the "/" (root) partition must be formatted as ext2, ext3, or ext4. If the "/" (root) partition is formatted with a different file system (such as ReiserFS), the mount points cannot be resolved. In that case, you can restore ext2, ext3, or ext4 files from the /dev level (such as /dev/sda1). You cannot restore the files from their original mount point level.

Invalid client error when you restore files using NetBackup BAR interface installed on the virtual machine

If the virtual machine was backed up by display name or UUID, and the display name is not the same as the host name, note: You cannot restore individual files by means of the Backup, Archive, and Restore (BAR) interface if the interface is installed on the virtual machine itself. The files can be restored if BAR is installed on the primary server or media server. In this case, BAR must not be installed on the virtual machine that you want to restore to.

To restore files, the **Destination client for restores** field in the BAR interface must have a valid host name or IP address.

VMware virtual machine does not restart after restore

The virtual machine may have been configured as follows:

- At the time of the backup, the virtual machine had a combination of SATA and SCSI disks, or of SATA, SCSI, and IDE disks.
- The guest OS resided on one of the SCSI disks.

The virtual machine when restored may attempt to boot from the SATA or the IDE disk. The boot attempt fails with the message "Operating system not found."

VMware has identified this problem and will address it in a future release.

As a workaround, reconfigure the BIOS on the virtual machine to boot from the correct SCSI disk.

A restored VM may not start or its file system(s) may not be accessible

A restored VM may not boot up or its file system(s) may not be accessible in the following case:

- The VM's guest operating system is Windows 8,
- The VM is restored from a block-level incremental backup image,
- And the restore uses the hotadd transport mode.

As a result of a VMware issue in VDDK 5.5.x, the Windows NTFS Primary File Table on the restored VM may be corrupted. As a workaround, use a different transport mode to restore the VM (not hotadd).

NetBackup job fails due to update tasks on the VMware server

Certain virtual machine update tasks on the VMware server may cause a NetBackup job to fail. For example, a restore may fail when you use the nbrestorevm command to restore multiple VMs at the same time. If the failed restore job creates the VM, the VM is deleted.

On the backup or restore host, the `bpVMutil` log may contain a message similar to the following:

```
Detail: <ManagedObjectNotFoundFault xmlns="urn:vim25"
xsi:type="ManagedObjectNotFound"><obj type="VirtualMachine">
vm-14355</obj>
        </ManagedObjectNotFoundFault>
```

As a workaround, rerun the job for the operation that failed.

Note: If possible, avoid VMware maintenance activities during backup or restore operations.

The vSphere interface reports that virtual machine consolidation is needed

When NetBackup begins a virtual machine backup, it requests a VMware snapshot of the virtual machine in vSphere. If the NetBackup policy is enabled for virtual machine quiesce (the default), the VMware snapshot operation initiates a quiesce of the virtual machine. If snapshot quiesce fails, the NetBackup job fails with status 156 and VMware snapshot delta files may be left behind in vSphere. Note: As a result of leftover snapshot delta files, the vSphere status for the virtual machine may warn that virtual machine consolidation is needed.

VMware has acknowledged the problem of leftover delta files after a snapshot quiesce failure. VMware has fixed this issue in certain ESXi versions. See the following VMware article for more information on this issue:

Delta disk files (REDO logs) are left uncommitted after a failed quiesced snapshot operation (2045116)

For a workaround for leftover delta files, see the following VMware article:

Committing snapshots when there are no snapshot entries in the Snapshot Manager (1002310)

The Enable file recovery from VM backup option does not work if a volume disk set contains a mixture of disk types

If a VM is configured on a logical volume (LVM or LDM): Individual file recovery does not work if the volume disk set contains a mixture of disk types:

- Some of the logical volume disks are regular virtual disks (normal VMDKs).

- Some of the disks in the same volume are independent disks or are physical disks in raw device mapping mode (RDM).

The backup job succeeds but files cannot be individually restored from the file systems that reside on the disk set (LVM or LDM). To be able to restore files individually, reconfigure the VM's logical volumes to reside on regular virtual disks (vmdk) only. Note that VMware does not make snapshots of independent disks or RDM disks.

Linux VMs and persistent device naming

For Linux VMs without persistent device naming, multiple disk controllers (such as IDE, SCSI, and SATA) may complicate the recovery of individual files. This issue occurs because non-persistent device naming, such as `/dev/sda` and `/dev/sdb`, may cause unexpected mount point changes after a restart. If the VM has a SCSI disk and SATA disk, the Backup, Archive, and Restore interface may show incorrect mount points for the VM's files. For example, the files originally under `/vol_a` might appear under `/vol_b` when you browse to restore them. The restore is successful, but the restored files may not be in their original directories.

As a workaround, search for the files on the restored VM and move them to the proper locations.

To prevent this issue on Linux VMs with multiple disk controllers, it is recommended a persistent device-naming method for mounting the file systems. When persistent naming is in place, device mounting is consistent and this issue does not occur when you restore files from future backups.

For persistent device naming, you can mount devices by UUIDs. The following is an example of the `/etc/fstab` file that contains the devices that are mounted by UUIDs:

```
UUID=93a21fe4-4c55-4e5a-8124-1e2e1460fece /boot  ext4  defaults  1 2
UUID=55a24fe3-4c55-4e6a-8124-1e2e1460fadf /vola  ext3  defaults  0 0
```

To find the device UUIDs, you can use either of the following commands:

```
blkid
```

```
ls -l /dev/disk/by-uuid/
```

Note: NetBackup also supports the by-LABEL method for persistent device naming.

For a VMware virtual machine with Windows dynamic disks, a restore from incremental backup fails with a Windows restore host and the hotadd transport mode

A restore of a Windows virtual machine by means of the hotadd transfer mode may fail in the following case:

- A backup is taken of a Windows virtual machine that has a dynamic disk group.
- After the backup, another dynamic disk is added to the virtual machine's disk group.
- After the dynamic disk is added, an incremental backup is taken of the virtual machine.
- A Windows restore host is used with the hotadd transport mode to restore the virtual machine from the incremental backup.

The restore fails when the Windows restore host tries to mount the dynamic disk that was added after the first backup. Depending on the data that has already been restored, Windows may detect the dynamic disk as `Invalid` or `Foreign`. Further writes to an `Invalid` or `Foreign` disk are unsuccessful and the restore fails.

The restore fails with status 1, "the requested operation was partially successful." Messages similar to the following may appear in the VxMS provider logs:

```
14:10:18.0854 : vdWrite:../VixInterface.cpp:760 <ERROR> : Error
24488361628532739 in write with vdhandle 48870608 startsector
128 numsectors 1 14:10:18.0854 : write:VixFile.h:333 <ERROR>
: Returned error 3, offset 0x0000000000010000, length
0x0000000000000200   14:10:18.0854 : write:VixFile.h:334
<ERROR> : Returning: 11
 14:10:18.0854 : vixMapWrite:../VixCoordinator.cpp:1259 <ERROR>
: Returning: 11
14:10:18.0854 : vix_map_write:../libvix.cpp:1826 <ERROR>
: Returning: 11
```

When they are enabled, VxMS logs are written in the following directory:

Windows:

install_path\NetBackup\logs\vxms

Linux:

/usr/openv/netbackup/logs/vxms

Note: For successful restores from future incremental backups, run backups with the **Use Accelerator** option in the policy.

Try any of the following workarounds to restore from the current incremental backup:

- Use a Linux restore host (not Windows).
- Use a different transport mode, such as NBD, NBDSSL, or SAN (not hotadd).
- When the dynamic disk (the one that was added after the first backup) is mounted for restore, manually set the disk to offline. When the disk is offline, NetBackup can write data to it and successfully complete the restore.
  See the remainder of this tech note for assistance with this workaround.

To determine when the dynamic disk is mounted for restore

- Use the Windows Disk Management utility (**Control Panel > Administrative Tools > Computer Management > Disk Management**), or run `diskpart` in administrator mode and enter the `list disk` option.

  When Windows attempts to mount the disk, it labels the disk as `Invalid` or `Foreign`.

To use diskpart to take the dynamic disk offline

1. On the Windows restore host, run `diskpart` in administrator mode.
2. Enter `list disk` to list all disks and find the `Invalid` or `Foreign` disk.

3 Enter `select disk disk ###` to select the disk that is `Invalid` or `Foreign`.

4 Enter `offline disk` to offline the disk.

Example session:

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          100 GB  1024 KB
  Disk 1    Online          256 GB    56 GB        *
  Disk 2    Invalid          40 MB    40 MB   *    *
  Disk 3    Offline          40 MB    40 MB

DISKPART> select disk 2

Disk 2 is now the selected disk.

DISKPART> offline disk

DiskPart successfully taken offline the selected disk.
```

Simultaneous hotadd backups (from the same VMware backup host) fail with status 13

During simultaneous backups from the same VMware backup host, some of the backups may fail with status 13, "file read failed." A hotadd backup of multiple disks may take more time than the client-read timeout allows (the default is 300 seconds). The delay may be caused by locking timeouts in the VMware VDDK.

In the NetBackup Activity Monitor, the detailed status log may include messages similar to the following:

```
12/05/2014 06:43:53 - begin writing
12/05/2014 06:48:53 - Error bpbrm (pid=2605) socket read failed:
errno = 62 - Timer expired
12/05/2014 06:48:55 - Error bptm (pid=2654) media manager terminated
by parent process
```

The `/NetBackup/logs/vxms` log may include repeated instances of a VDDK message similar to the following:

```
12/08/2014 05:11:35 : g_vixInterfaceLogger:libvix.cpp:1844 <DEBUG> :
[VFM_ESINFO] 2014-12-08T05:11:35.146-06:00 [7F1B1163F700 info Libs']
FILE: FileLockWaitForPossession timeout on '/var/log/vmware/hotAddLock.
dat.lck/M34709.lck' due to a local process '15882-26732358(bpbkarv)'
```

To prevent this issue, do one of the following:

- Reduce the number of hotadd backups that run simultaneously.
- Increase the client-read timeout on the media server as appropriate (15 minutes or more):
  In the NetBackup Administration Console, click **NetBackup Management > Host Properties >** Double-click on media server **> Timeouts > Client read timeout**.

Troubleshooting VMware tag usage

Tag associations are backed up and restored as part of the VMware backup process. Backup and restore of tag associations is a best effort. Any tag collection errors are shown in the Activity Monitor for the virtual machine snapshot job.

Because of the best effort on backup and restore of tag associations, you may receive unexpected behavior. Please be aware of the following:

- You can receive a NetBackup Status Code 0 even if the tag associations are not captured during the backup. Because tag backup is best effort, this error is not considered a failure that halts a backup. Any tag collection errors that occur in the backup are shown in the Activity Monitor for the virtual machine snapshot job.
- You can receive a NetBackup Status Code 0 on a restore even if tag associations are not restored. Any tag collection errors that occur in the backup are shown in the Activity Monitor for the virtual machine snapshot job.
- Restores receive a NetBackup Status Code 1 when:
  - The tag doesn't exist on the target vCenter Server. Be aware that NetBackup restores tag associations to virtual machines by the tag identifier not tag name.
  - The virtual machine was restored to a pre-6.0 vCenter Server.
  - Other VMware failures.

Query behavior with unsupported versions of VMware

Table 14-8 NetBackup query behavior for tag field keyword with unsupported versions of VMware

Version of VMware	Behavior	Additional information
vCenter earlier than 5.1	Virtual machines are evaluated as if tags are not set.	N/A
vCenter 5.1 and 5.5	Virtual machine selection is marked as **Failed**.	If tag information is required to determine virtual machine selection, the virtual machine is marked as **Failed** with NetBackup Status Code 4266.
ESX server	Virtual machine selection is marked as **Failed**.	If tag information is required to determine virtual machine selection, the virtual machine is marked as **Failed** with NetBackup Status Code 4265.

List of possible Tag values not displayed in Query Builder

If the list of possible values does not return any results when the **Tag Field** is selected in the **Policy Query Builder**, there are several causes of this problem.

- Confirm that your version of vCenter Server is 6.0 or later.
  NetBackup support for tags starts with VMware vCenter Server 6.0.
  See "Notes and limitations for tag usage in VMware Intelligent Policy queries" on page 41.
- Confirm there are tags defined using the vSphere Web Client.
- Confirm that all tags and categories have descriptions.
  If one of the tags does not have a description, when you attempt to browse for tags in the VMware Intelligent Policy, no tags are displayed.
  Veritas has confirmed that this issue is resolved in vCenter Server 6.0 Update 1.
  VMware Knowledge Base article: http://kb.vmware.com/kb/2124204
- Confirm the system times of the discovery host and the vCenter Server are synchronized.
  VMware Knowledge Base article: http://kb.vmware.com/kb/2125193

Timeout issues in discovery job

In large VMware environments, you may experience timeout issues during the discovery job or the test query. Review the NetBackup Activity Monitor for this message:

```
09/21/2015 10:23:05 - Error nbpem (pid=13064) VMware vCloud Suite
SDK API Failed, msg = [This method requires authentication.], display
name = [display_name], server = [server_name]
```

This message indicates that the discovery job exceeded the bearer timeout. You need to increase this timeout for the job to complete successfully.

To adjust the timeout on the vCenter

1. Open the VMware vSphere Web Client.
2. Select **Administration > Single Sign-On > Configuration > Policies > Token Policy**.
3. Increase **Maximum bearer token lifetime** from the default 300 seconds. Because each environment is unique, Veritasdoes not have any recommendations on this value. Increase the value until the problem is eliminated.

Ensuring that guest customizations can be restored in vCloud Director

NetBackup can back up VMware vCloud Director environments and restore virtual machines into vCloud Director.

See "About NetBackup for vCloud Director" on page 262.

To ensure that any VM guest customizations are restored into vCloud Director, you must set a NetBackup parameter, as follows:

- On Windows, you must set a registry value.
  See "To ensure that guest customizations can be restored in vCloud Director on Windows" on page 318.
- On UNIX and Linux, you must edit a NetBackup configuration file.
  See "To ensure that guest customizations can be restored in vCloud Director on Linux" on page 318.

The parameter value specifies a wait period in seconds so that the guest customizations can be restored successfully. (The VMware API requires that the VMware Tools are installed and running, but the state of the VMware Tools cannot be identified after the restore. Therefore, we wait the specified amount of time so that the VMware Tools are running in the initial restore environment.)

To ensure that guest customizations can be restored in vCloud Director on Windows

1. On the Windows desktop of the backup host, click **Start > Run** and enter `regedit`.
2. To be on the safe side, make a backup of the current registry (**File > Export**).
3. Go to **HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > CONFIG** and create a key that is called `BACKUP`.
4. Create a new DWORD under `BACKUP` and name it `powerCycleInterval`.

   Enter a decimal value of `60` for the timeout.
5. Close the Windows Registry Editor.

To ensure that guest customizations can be restored in vCloud Director on Linux

1. On the Linux backup host, create (or open) the following file:

   `/usr/openv/netbackup/virtualization.conf`
2. Create a line in the file named `[BACKUP]` and then on a separate line create a `powerCycleInterval dword` parameter with a value of `60`, as follows:

   For example:

   ```
   [BACKUP]
   "powerCycleInterval"=dword:60
   ```

   Note: If the file already contains a `[BACKUP]` line, do not add another `[BACKUP]` line. Any other lines that already exist under `[BACKUP]` should remain as they are.
3. Save the file and then close it from the text editor.

Troubleshooting vmdk restore to existing VM

For virtual disk restores and in-place restores to an existing VM, be aware of the following:

- If the VMDKs cannot be attached to the target VM, the restored VMDKs are retained on the temporary VM. The name of the temporary VM is available in the job details in NetBackup. In the following job details example, the temporary VM name is `vCenter60vm1_rhel6.4_1465584674`:

  ```
  06/10/2016 13:51:17 - Info bpVMutil (pid=3400) Restoring [datastore1]
   vCenter60vm1_rhel6.4/vCenter60vm1_rhel6.4_4.vmdk to [datastore1]
  ```

```
 vCenter60vm1_rhel6.4/vCenter60vm1_rhel6.4_4-1465584677.vmdk
06/10/2016 13:51:38 - Info bpVMutil (pid=3400) Successfully created
 virtual machine vCenter60vm1_rhel6.4_1465584674 with specified disks.
06/10/2016 13:51:41 - requesting resource @aaaab
```

You can access the data on the temporary VM.
If the temporary VM is retained after a restore failure, the restore job contains a message similar to the following:

```
06/14/2016 15:29:06 - Info bpVMutil (pid=5225) attachDisksToExistingVM:
 Unable to attach restored disks to target VM vCenter60vm2_rhel6.4
06/14/2016 15:29:06 - Info bpVMutil (pid=5225) attachDisksToExistingVM:
 Temporary VM  with restored virtual disks was left in place, it can be
 used to access restored data
```

By default, NetBackup retains the temporary VM if the disks are not attached. To change that behavior, set the `DeleteRestoredVMOnError` field to `Yes` in the restore parameters file.

- After a restore to an existing VM, the next backup of the VM backs up the restored virtual disks. This backup may show a warning during collection of the Changed Block Tracking (CBT) information.
- For an In-place disk restore, raw devices (RDMs) and independent disks are not deleted or replaced during restore. If the controller for these disks conflicts with the disks being restored, the restore fails. The following example messages are job details from a failed in-place restore:

```
May 07, 2020 10:26:21 AM - Warning bprd.sfr (pid=2425) Unable to
 attach the restored disks to requested VM
May 07, 2020 10:26:21 AM - restored from image
 InPlaceDiskRestoreDemo_1588837243; restore time: 0:00:50
May 07, 2020 10:26:21 AM - end Restore; elapsed time 0:00:50
May 07, 2020 10:26:21 AM - Info bpVMutil (pid=2673)
 attachDisksToExistingVM: Controller scsi0-1 not available
 to perform in-place disk restore. Aborting restore.
 The requested operation was partially successful(1)
```

Errors for backups of virtual machines on Virtual Volumes (VVols)

When troubleshooting backups of virtual machines on VVols, note the following:

- Each NetBackup snapshot job creates a vSphere snapshot of the virtual machine.

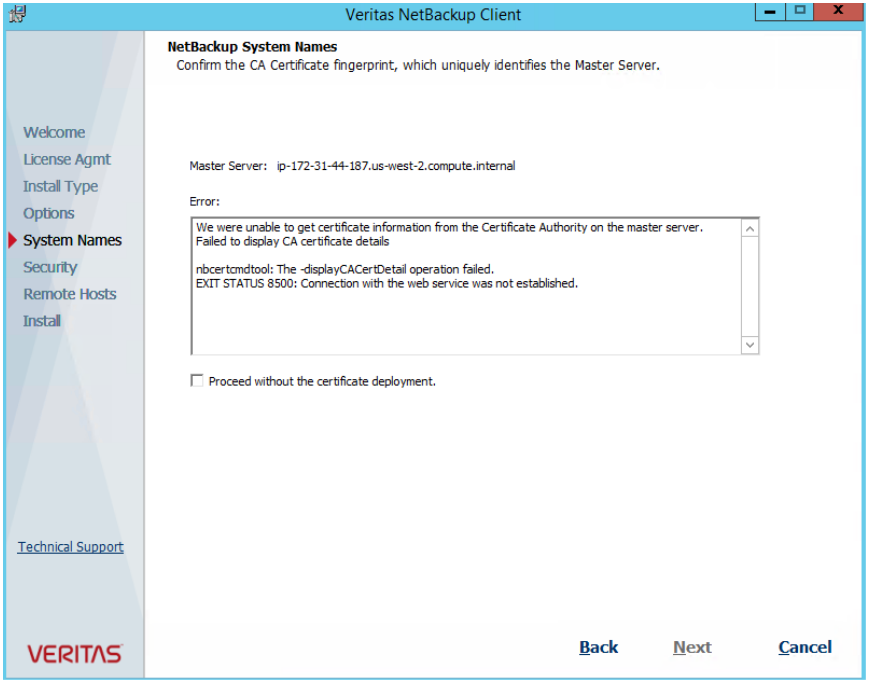
- To investigate snapshot failures, check the storage array's VASA provider logs as well as the vSphere error messages. (VASA is vSphere API for Storage Awareness.)

Table 14-9 Errors for backups of virtual machines on VVols

Error message or cause	Explanation and recommended action
vSphere snapshot creation fails for a backup of a VM on VVol.	Ensure that you have the required snapshot license from the array vendor. Licensing requirements for vSphere snapshots vary from one type of VVol storage to another, depending on the array vendor. Each NetBackup snapshot job creates a vSphere snapshot of the virtual machine.
	There is insufficient space in VVol storage. Space requirements vary from one array vendor to another. Consult the storage array documentation.

Issues with the CA certificate during installation of the NetBackup client on VMware Cloud (VMC)

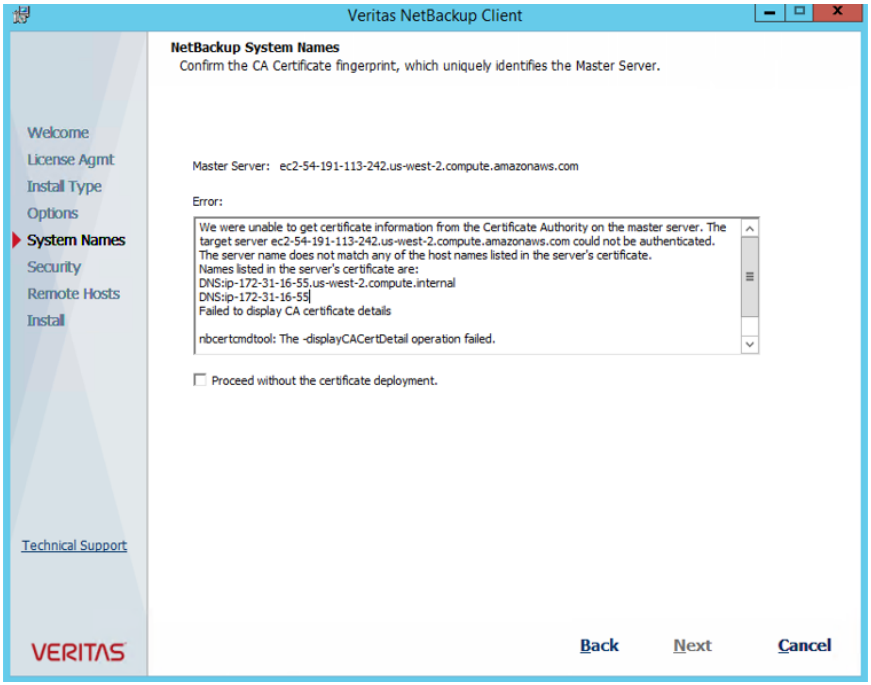
Failed to display CA certificate details



To fix this problem, do the following:

1. Click **Cancel** to cancel the installation.
2. Make sure the private DNS name was used to install the primary server.
3. In the hosts file of the primary server installed in AWS and of the backup host installed in VMC, add the following:
   - The private IP and private DNS name of the NetBackup primary server.
   - The IP and the DNS name of the backup host.
     The hosts file location on Windows:
     `C:\Windows\System32\drivers\etc\hosts`
     The hosts file location on Linux:
     `/etc/hosts`
4. Begin the NetBackup client installation again.

The target NetBackup server cannot be authenticated, or the server name does not match any of the host names that are listed in the server's certificate



To fix this problem, do the following:

1. Click **Cancel** to cancel the installation.
2. Follow the previous steps under "Failed to display CA certificate details."
3. If the error persists, see the following article:

   Host validation fails when a NetBackup client tries to connect to the primary server
4. Begin the NetBackup client installation again.

Appendix A

NetBackup commands to back up and restore virtual machines

This appendix includes the following topics:

- Using NetBackup commands to create a VMware policy
- Using the nbdiscover command to search the virtual environment
- Using the nbrestorevm command to restore virtual machines into vSphere
- Using the nbrestorevm command to restore virtual machines into vCloud Director
- Using the nbrestorevm command to restore virtual machines with Instant Recovery
- Using the nbrestorevm command to restore virtual machine disks
- The nbrestorevm -R rename file for restoring virtual machines
- Logs for troubleshooting the nbrestorevm command
- Query format and examples for searching virtual machine backups
- Allowing other servers or clients to restore virtual machines

Using NetBackup commands to create a VMware policy

This topic describes how to use NetBackup commands to create a policy to back up virtual machines.

The NetBackup commands for policy creation are in the following directory:

Windows:

install_path\Veritas\NetBackup\bin\admincmd

UNIX or Linux:

usr/openv/netbackup/bin/admincmd

Run these commands on the NetBackup primary server.

To use NetBackup commands to create a VMware policy

1. Create a blank policy.

   bppolicynew *policyName* -M *primaryServer*

   For example:

   bppolicynew policy1 -M nbserver.acme.com

2. Configure the VMware policy type and set the VMware snapshot options.

   This step requires running the initialize form of the bpplinfo command in two stages.

   First stage: bpplinfo *policyName* -set -pt VMware

   Example for the first stage of bpplinfo:

   bpplinfo policy1 -set -active -pt VMware -residence stu1

Second stage:

```
bpplinfo policyName -modify -use_virtual_machine 1
-alt_client_name VMware_backup_host -snapshot_method
"VMware_v2" -snapshot_method_args
keyword=value,keyword=value,...
```

The `-alt_client_name` specifies the VMware backup host (NetBackup access host). You can specify a particular backup host on this option, or specify MEDIA_SERVER (a media server acts as the backup host).

The `-use_virtual_machine`, `-alt_client_name`, `-snapshot_method "VMware_v2"`, and `-snapshot_method_args` must be specified with all parameters set. (Otherwise, the snapshot job fails.)

Note: `-snapshot_method_args` is a comma-delimited list of keywords that define the VMware snapshot and policy. The keywords are described in a separate topic:

See "VMware policy: bpplinfo options and keywords" on page 327.

Example for the second stage of bpplinfo (for a policy for vCloud Director):

```
bpplinfo policy1 -modify -use_virtual_machine 1 -alt_client_name
backuphost1.acme.com -application_discovery 1 -snapshot_method
"VMware_v2" -snapshot_method_args "file_system_optimization=1,
snapact=2,drive_selection=0,Virtual_machine_backup=2,
enable_vCloud=1,multi_org=0,disable_quiesce=0,nameuse=0,
exclude_swap=1,skipnodisk=0,post_events=1,ignore_irvm=0,
rLim=10,rTO=0,rHz=10,trantype=san:hotadd:nbd:nbdssl"
```

To back up virtual machines in vCloud Director, the `bpplinfo` command must include the following:

- `-application_discovery 1`
- The *snapshotMethodArgs* list must include `enable_vCloud=1`.

In addition, NetBackup credentials must be specified for a vCloud Director server.

3 Create a schedule for the policy.

```
bpplsched policyName -add scheduleLabel -st scheduleType
```

For example:

```
bpplsched policy1 -add Full -st FULL
```

4 Modify the schedule attributes.

```
bpplschedrep policyName scheduleLabel -(0..6) start duration
```

For example:

```
bpplschedrep policy1 Full -0 0 604800
```

5 Select the virtual machines to back up.

This step requires two commands: `bpplclients` and `bpplinclude`.

```
bpplclients policyName -add VM_to_back_up hardware operating_System

bpplinclude policyName -add ALL_LOCAL_DRIVES | filter_to_select_VMs
```

- To back up a virtual machine through manual selection (for example):

  ```
  bpplclients policy1 -add prvm1.acme.com Windows-x64 Windows2008
  bpplinclude example -add ALL_LOCAL_DRIVES
  ```

  In this example, `prvm1.acme.com` is the virtual machine to back up, including all of its local drives (`-add ALL_LOCAL_DRIVES`). `ALL_LOCAL_DRIVES` is the only file list option available for the VMware policy type.

- To automatically select virtual machines through a query rule (for example):

  ```
  bpplclients policy1 -add MEDIA_SERVER VMware VMware
  bpplinclude pol1 -add "vmware:/?filter= Displayname Contains
  'prvm'"
  ```

  MEDIA_SERVER allows NetBackup to use a media server to discover and select the virtual machines. As an alternative, you can use -add to specify a particular discovery host.
  In the `bpplinclude` example, the query rule `"vmware:/?filter= Displayname Contains 'prvm'"` selects the virtual machines with the display names that contain `prvm`. (Other characters can also appear in the display names.)

Note: To back up virtual machines in vCloud Director, the policy must use a query rule on the bpplinclude command to select virtual machines automatically. For vCloud, do not specify a virtual machine on the bpplclients command.

`bpplinclude` has options for modifying the query rules in an existing policy.

See "bpplinclude options for modifying query rules in a VMware policy" on page 330.

To test the bpplinclude query rule (`vmware:/?filter`) before you run the backup

- Run the following:

  Windows:

  ```
  install_path\NetBackup\bin\nbdiscover -noxmloutput -policy
  policyName -noreason
  ```

  UNIX, Linux:

  ```
  /usr/openv/netbackup/bin/nbdiscover -noxmloutput -policy
  policyName -noreason
  ```

  A + sign appears before the virtual machines that the query rule selects for the backup: these virtual machines are included in the backup when the policy runs.

  The virtual machines to be excluded from the backup appear with a - sign.

  The -noreason option omits explanations as to why the query excluded a virtual machine or why the query failed. For explanations, do not include -noreason.

  For more details on most of the command options, see the man page or the *NetBackup Commands Reference Guide*.

Notes on creating a VMware policy for vCloud Director

Note the following when you create a policy for vCloud Director:

- NetBackup credentials must be specified for a vCloud Director server.
- The bpplinfo command must include the following option and value, to enable the policy for automatic selection of virtual machines: -application_discovery 1
- On the bpplinfo command, the *snapshotMethodArgs* list must include the following attribute: `enable_vCloud=1`.
- The policy must use a query rule, on the bpplinclude command, to select virtual machines automatically.

For the complete steps--including these points--use the following procedure:

See "Using NetBackup commands to create a VMware policy" on page 323.

VMware policy: bpplinfo options and keywords

Table A-1 describes the options that are available on the `bpplinfo` command. These options are set to default values if not specified.

Table A-1 bpplinfo options

Option	Values	Keyword label in policy GUI
-ignore_client_direct	0 enables client deduplication, 1 disables client deduplication	The **Attributes** tab > **Disable client side deduplication**
-application_discovery	0 disabled, 1 enabled	**Clients** tab > **Select automatically through VMware Intelligent Policy query**
-discovery_lifetime	seconds	**Clients** tab > **Reuse VM selection query results for**
-ASC_apps_attr	`exchange`, `mssql`, `sharepoint` truncatelogs=0 disabled, 1 enabled (for Exchange or SQL Server only) To enable Exchange file recovery: -ASC_apps_attr exchange: To enable Exchange, SQL, and SharePoint file recovery: -ASC_apps_attr exchange:,mssql:,sharepoint: To enable exchange recovery with truncate logs: -ASC_apps_attr exchange:;truncatelogs=1 To enable exchange without truncate logs and mssql with truncate logs: -ASC_apps_attr exchange:,mssql:;truncatelogs=1 To enable exchange with truncate logs and mssql without truncate logs (note the final colon): -ASC_apps_attr exchange:;truncatelogs=1,mssql: To enable both exchange and mssql with truncate logs: -ASC_apps_attr exchange:;truncatelogs=1,mssql:;truncatelogs=1	Enables the file-level recovery of database data. **VMware** tab > **Application Protection**: **Enable Exchange Recovery**, **Enable SQL Server Recovery**, or **Enable SharePoint Recovery**
-snapshot_method_args	*keyword=value,keyword=value,* ... See Table A-2 on page 329.	

Table A-2 describes the keywords that must be included in `-snapshot_method_args`.

Table A-2 Keywords and values for -snapshot_method_args

Keyword	Value	Name of keyword in policy GUI
disable_quiesce=	0 virtual machine quiesce is enabled, 1 virtual machine quiesce is disabled	VMware tab > Advanced > Virtual machine quiesce
drive_selection=	0 Include all disks, 1 Exclude boot disk, 2 Exclude data disks	Exclude Disks tab
enable_vCloud=	0 disabled, 1 enabled	Clients tab > Enable vCloud Director integration (only available with automatic selection of client)
exclude_swap=	0 disabled, 1 enabled	VMware tab > Exclude swap and paging files
file_system_optimization=	0 disabled, 1 enabled	VMware tab > Exclude deleted blocks
ignore_irvm=	0 disabled, 1 enabled	VMware tab > Advanced > Ignore Instant Recovery VMs
multi_org=	0 disabled, 1 enabled	VMware tab > Advanced > Multiple organizations per policy
nameuse=	0 VM host name, 1 VM display name, 2 VM BIOS UUID, 3 VM DNS Name, 4 VM instance UUID	VMware tab > Primary VM identifier
post_events=	0 No Events, 1 All Events, 2 Error Events	VMware tab > Advanced > Post vCenter events
rHz=	0 - 3600	VMware tab > Advanced > Snapshot creation interval (seconds)
rLim=	0 - 100	VMware tab > Advanced > Snapshot retry
rTO=	0 - 1440	VMware tab > Advanced > Snapshot timeout (minutes)

serverlist=	VMware server names. Use a colon to separate the names. For example:
	`serverlist=vc1.acme.com:vc2.acme.com`
	To specify no server list, enter
	`serverlist=`
		VMware tab > Advanced > VMware server list

skipnodisk=	0 disabled, 1 enabled	VMware tab > Advanced -> Ignore diskless VMs

Table A-2 Keywords and values for -snapshot_method_args *(continued)*

Keyword	Value	Name of keyword in policy GUI
snapact=	0 Continue backup 1 Abort if any snapshot(s) exist 2 Remove NetBackup snapshot(s) and continue backup 3 Abort if NetBackup snapshot(s) exist	VMware tab > Existing snapshot handling
trantype=	san, hotadd, nbd, or nbdssl If more than one, separate each with a colon. Order of modes indicates priority. Example: `trantype=nbd:hotadd` This example selects these two modes and tries nbd first.	VMware tab > Transport modes
Virtual_machine_backup=	1 disabled, 2 enabled	VMware tab > Enable file recovery from VM backup
vmdk_ca=	The name of the VMware custom attribute that specifies the disk(s) to exclude from backups. For example, `vmdk_ca=NB_DISK_EXCLUDE_LIST`. Set the value for the custom attribute on each virtual machine or managed host, as appropriate. The custom attribute must have comma separated values of device controls for the disks to be excluded. For example: `scsi0-0,ide0-0,sata0-0`.	Exclude Disks tab > Perform custom attribute based selection
vmdk_list=	Colon separated values of device controllers for the disks to be excluded. For example: `scsi0-0:ide0-0:sata0-0`.	Exclude Disks tab > Specific disk(s) to be excluded

bpplinclude options for modifying query rules in a VMware policy

The bpplinclude command has options for modifying the query rules in an existing policy.

Table A-3 bpplinclude options for modifying query rules

Option	Description

-addtoquery *query_string* ...	Adds the specified query string to the end of the policy query rules, or creates a query if none exists.
	Quotes (") must be escaped (\).
	Examples:
	To add `vm17` to the list of values in the query rules of policy1:
	`bpplinclude policy1 -addtoquery ,\"vm17\"`
	To create a query in a policy that does not have a query:
	`bpplinclude policy1 -addtoquery vmware:/?filter=Displayname AnyOf \"grayfox7\",\"grayfox9\"`
	Note: Each quote (") is escaped with a backslash (\).

-addtoquery -f *file_name*	Adds the entries to the query rules from the specified file, or creates a query if none exists.
	In the file, quotes (") do not need to be escaped.
	Example:
	To create a query in a policy that does not have a query:
	`bpplinclude policy1 -addtoquery -f qfile1`
	where the contents of `qfile1` are:
	`vmware:/?filter=vCenter Contains "ROS" AND ESXserver Equal "VM_test1" AND Powerstate Equal poweredOn`
	Note: The values "ROS" and "VM_test1" are not escaped.
	Note: You can place entries on multiple lines in the file. All entries are added to the end of the query (if a query already exists).

Table A-3 bpplinclude options for modifying query rules *(continued)*

Option	Description

-deletefromquery *query_string* ...	Deletes the specified query string from the policy query rules.
	Examples:
	To delete `vm27` from the list of values in the query rule of policy1:
	`bpplinclude policy1 -deletefromquery \"vm27\"`
	This example also deletes the comma preceding vm27 if such a comma exists in the query rules.
	Note: The -deletefromquery option deletes a comma if: the phrase in the query_string does not begin or end with a comma and the character preceding the deleted string is a comma.
	To delete an entire query from the policy:
	`bpplinclude policy1 -deletefromquery vmware:/?filter=Displayname AnyOf "grayfox7","grayfox9"`

-deletefromquery -f *file_name*	Deletes the file entries from the query rules.
	Example:
	To delete a query from a policy:
	`bpplinclude policy1 -deletefromquery -f qfile1`
	where the contents of `qfile1` are:
	`vmware:/?filter=vCenter Contains "ROS" AND ESXserver Equal "VM_test1" AND Powerstate Equal poweredOn`
	Note: The values "ROS" and "VM_test1" are not escaped.

Note: paths that contain wildcards must be enclosed in quotes.

Using the nbdiscover command to search the virtual environment

To search for VMs, run nbdiscover on the primary server.

UNIX and Linux:

`/usr/openv/netbackup/bin/nbdiscover -noxmloutput "`*query*`"`

Windows:

install_path`\NetBackup\bin\nbdiscover.exe -noxmloutput "`*query*`"`

where -noxmloutput displays one VM per line. The *query* specifies either a filter-based search rule or a browse operation.

See "Query format and examples for searching virtual machine backups" on page 347.

For example, to search for the backups of virtual machines that have "prod1" in their display names:

```
nbdiscover -noxmloutput
"vmsearch:/;reqType=search?filter=VMDisplayName Contains 'prod1'"
```

For further descriptions of the command options, see the command's man page or the *NetBackup Commands Reference Guide*.

Using the nbrestorevm command to restore virtual machines into vSphere

To restore VMs, run the nbrestorevm command on the primary server or recovery host. The command is located in the following directory:

UNIX and Linux:

```
/usr/openv/netbackup/bin/nbrestorevm
```

Windows:

```
install_path\NetBackup\bin\nbrestorevm.exe
```

The following nbrestorevm options are used in these examples:

- `-vmw`
  Required for all VMware virtual machine restores.
- `-C virtual_machine_to_restore`
  The VM name must match the type of name that was selected in the **Primary VM identifier** option of the backup policy. For example, if the VM was backed up by its VM display name, specify the display name on the `-C` option.
- `-R absolute_path_to_rename_file`
  Restores to a different location. The required entries in the rename file depend on the destination for the restore. See each example in this topic. Further notes are available on the rename file.
  See "The `nbrestorevm -R` rename file for restoring virtual machines" on page 343.
- `-O`
  Overwrites the VMs and associated resources if they already exist.
- `-S primary_server`

Specifies the primary server that made the backup (if different from the current primary).

- `-vmserver` *`vCenter_server`*
  Specifies a different vCenter server for the restore destination.
- `-vmproxy` *`VMware_recovery_host`*
  Specifies a different VMware recovery host (overrides the default backup host that backed up the VMs).

Note: Storage lifecycle policies (SLPs) can use Auto Image Replication to replicate a virtual machine backup image to another NetBackup domain. To restore the virtual machine from the replicated image, you must include the `-vmproxy` option. Use `-vmproxy` to specify the backup host (access host) that is in the domain where the virtual machine was replicated.

- `-vmkeephv`
  Retains the hardware version upon recovery.
- `-vmid`
  Retains the BIOS UUID of the original virtual machine.
- `-vmInstanceId`
  Retains the Instance UUID of the original virtual machine (note that the Instance UUID is a vCenter specific unique identifier of a virtual machine).
- `-vmsn`
  Removes the network from the restored VM.
- `-vmvmxd`
  Restores the .vmdk files to the vmx datastore (the configuration datastore).
- `-vmpo`
  Turns on the VM after the restore.

Following are examples of nbrestorevm, for various restore destinations and options.

A. Restore to the original location and overwrite the VM.

```
nbrestorevm -vmw -C VM_to_restore -O
```

B. Restore to the original location, overwrite the VM, and retain the BIOS UUID.

```
nbrestorevm -vmw -C VM_to_restore -O -vmid
```

C. Restore to the original location, overwrite the VM, and retain the instance UUID.

```
nbrestorevm -vmw -C VM_to_restore -O -vmInstanceId
```

D. Restore to the original location, overwrite the VM, and remove the network.

```
nbrestorevm -vmw -C VM_to_restore -O -vmsn
```

E: Restore to the original location from a VM backup that a different primary server made, and overwrite the VM.

```
nbrestorevm -vmw -C VM_to_restore -S primary_server -O
```

F: Restore to the original vCenter and ESX, but to a different datastore that also contains the VM configuration files.

```
nbrestorevm -vmw -C VM_to_restore -R absolute_path_to_rename_file
-vmvmxd
```

For the `-R` rename file, create a text file with the following entry:

```
change datastore to new_vmx_datastore
```

where *new_vmx_datastore* specifies the path to the vmx datastore (configuration datastore) for the restored VM. After the restore, this datastore contains the .vmdk files of the restored VM.

Note: In the rename file, the change line must end with a carriage return.

G: Restore to a different vCenter server.

```
nbrestorevm -vmw -C VM_to_restore -R absolute_path_to_rename_file
-vmserver vCenter_server
```

For the `-R` rename file, create a text file with the following entries. Replace the italicized values with the actual name for the restored VM and for the other vSphere objects in this list:

```
change vmname to new_display_name
change esxhost to new_ESX_host
change datacenter to /new_datacenter
change folder to /new_datacenter/new_folder
change resourcepool to new_datacenter/host/new_ESX_host/resources
/new_resource_pool
```

```
change datastore to new_vmx_datastore
change /original_vmdk_path to /new_datastore/
```

Note: In the rename file, each change line must end with a carriage return.

The last change entry in this list (change */original_vmdk_path* to */new_datastore/*) designates the following: the original path to the .vmdk file, and the new datastore for the .vmdk file of the restored VM. This change entry is required when you restore to a different datastore (unless you use the nbrestorevm –vmvmxd option). Depending on your VMware environment, this change entry may take the following form:

```
change /original_datastore/original_VM_folder/original_vmdk.vmdk to
/new_datastore/
```

Note: If the change vmdk directive specifies a different path for some of the VM's vmdk files, the other vmdk files are restored to their original datastore.

See "The nbrestorevm -R rename file for restoring virtual machines" on page 343.

H: Restore to a different vCenter server that has multiple networks.

```
nbrestorevm -vmw -C VM_to_restore -R absolute_path_to_rename_file
-vmserver vCenter_server
```

Create a rename file with the change entries listed for example G. Add the following change entry:

```
change network to new_network, new_network(n)
```

Note: In the rename file, each change line must end with a carriage return.

I: Restore by means of a different recovery host, to a different ESX server under the same vCenter Server. After recovery, turn on the VM.

```
nbrestorevm -vmw -C VM_to_restore -R absolute_path_to_rename_file
-vmproxy VMware_recovery_host -vmpo
```

The –vmpo option turns on the restored VM.

Include the following in the rename file:

```
change esxhost to new_ESX_host
```

To restore the .vmdk files to a different datastore, include the following entry in the rename file:

```
change /original_vmdk_path to /new_datastore/
```

Note: In the rename file, each change line must end with a carriage return, even if the file contains only one line.

Note: The rename file may require other change entries, depending on your vSphere environment. See the available entries under example G.

Note: Configure the recovery host as a VMware Access Host on the primary server. Communication between the primary server and the backup host or recovery host (client) should be established before the restore.

J. Restore to a different location, to a standalone ESX server

```
nbrestorevm -vmw -C VM_to_restore -R absolute_path_to_rename_file
```

Include the following in the rename file:

```
change esxhost to new_ESX_host
change datacenter to None
change folder to None
change resourcepool to /ha_datacenter/host/new_ESX_host/Resources
change datastore to new_datastore
change /original_vmdk_path to /new_datastore/
change network to new_network
```

Note: For restore to a standalone ESX server, the resource pool entry must include the literal string ha-datacenter in the pool path.

Note: The rename file may require other change entries, depending on your vSphere environment. See the available entries under example G.

K. Restore to a different location in a vSphere cluster, retaining the VM hardware version

```
nbrestorevm -vmw -C VM_to_restore -R absolute_path_to_rename_file
-vmkeephv
```

Include the following in the rename file:

```
change resourcepool to
/new_datacenter/host/cluster/resources/new_resource_pool
```

Note: The rename file may require other change entries, depending on your vSphere environment. See the available entries under example G.

For further descriptions of the nbrestorevm options, see the command's man page or the *NetBackup Commands Reference Guide*.

The following topics contain additional information:

See "Logs for troubleshooting the nbrestorevm command" on page 346.

See "The `nbrestorevm -R` rename file for restoring virtual machines" on page 343.

Using the nbrestorevm command to restore virtual machines into vCloud Director

To search the virtual environment for VMs, use the nbdiscover command.

See "Using the nbdiscover command to search the virtual environment" on page 332.

To restore the virtual machines, run nbrestorevm on the primary server or backup host. The nbrestorevm command is located in the following directory:

UNIX and Linux:

```
/usr/openv/netbackup/bin/nbrestorevm
```

Windows:

```
install_path\NetBackup\bin\nbrestorevm.exe
```

The following command options are used in these examples:

- `-vmw`
  Required for all VMware virtual machine restores.
- `-vcd`
  Required for all virtual machine restores into vCloud.
- `-C virtual_machine_to_restore`
  The VM name must match the type of name that was selected in the **Primary VM identifier** option of the backup policy. For example, if the VM was backed up by its VM display name, specify the display name on the `-C` option.
- `-R absolute_path_to_rename_file`

Restores to a different location. The entries that are required in the rename file depend on the destination for the restore. See each example in this topic. Further notes are available on the rename file:

See "The `nbrestorevm -R` rename file for restoring virtual machines" on page 343.

- `-vcdovw`
  Overwrites an existing vApp.
- `-vcdrte`
  Restores to an existing vApp. (If this option is set but the vApp does not exist, the restore fails.)
- `-vcdtemplate`
  Restores a vApp as a template.
- `-vcdlfree`
  Restores to the datastore that has the most free space.
- `-vcdremv`
  Removes a vApp after capture to a template.
- `-vmid`
  Retains the BIOS UUID of the original virtual machine.
- `-vmInstanceId`
  Retains the Instance UUID of the original virtual machine (note that the Instance UUID is a vCenter specific unique identifier of a virtual machine).

A: Restore to the original vApp in vCloud and overwrite the VM.

```
nbrestorevm -vmw -vcd -C VM_to_restore -vcdrte -O -vmInstanceId
```

The -O option overwrites the VM.

B: Restore to the original vApp in vCloud, overwrite the VM, and retain the BIOS UUID.

```
nbrestorevm -vmw -vcd -C VM_to_restore -vcdrte -O -vmid
```

The -O option overwrites the VM, and the -vmid option retains the original Instance UUID.

C: Restore to the original vApp in vCloud, overwrite the VM, and retain the instance UUID.

```
nbrestorevm -vmw -vcd -C VM_to_restore -vcdrte -O -vmInstanceId
```

The -O option overwrites the VM, and the -vmInstanceId option retains the original Instance UUID.

D: Restore to the original vCloud location to an existing vApp. Remove the existing vApp and create a new vApp.

```
nbrestorevm –vmw –vcd –C VM_to_restore –vcdovw
```

The –vcdovw option deletes the vApp and the VMs inside it, and creates a new vApp.

Note: For restore to the original location, you must use either the –vcdovw option or the –O option.

E: Restore to the original vCloud location in a vApp template.

```
nbrestorevm –vmw –vcd –C VM_to_restore –vcdovw
```

Note: To restore a VM that resides in a vApp template to its original location, use the –vcdovw option. If you use –O option, the restore fails with status 2820.

F: Restore to a different vCloud vApp but to the same vCloud organization.

```
nbrestorevm –vmw –vcd –C VM_to_restore –R absolute_path_to_rename_file
–vcdrte
```

For the `-R` rename file, create a text file with the following entries. These entries describe the restore location. Replace the italicized values with the actual values:

```
change vcdvapp to new_vcdvapp
change orgvdc to new_organization_VDC
```

Note: In the rename file, each change line must end with a carriage return.

Note: If you want to associate the restored VM with a different organization VDC, use the `change orgvdc` entry to specify the organization VDC.

G: Restore to a different vCloud organization.

```
nbrestorevm –vmw –vcd –C VM_to_restore –R absolute_path_to_rename_file
–vcdrte
```

Include the following in the rename file:

```
change organization to new_organization
change orgvdc to new_organization_VDC
```

```
change vcdvapp to new_vcdvapp
change resourcepool to /new_datacenter/host/new_ESX_host/resources
/new_resource_pool
change datastore to new_vmx_datastore
```

Note: To create the organization on a different vCenter, include the `-vmserver vCenter_server` option on the command. You must also include other change directives, such as for datacenter and ESX server.

See "The `nbrestorevm -R` rename file for restoring virtual machines" on page 343.

H: Restore to a different vCloud Director.

```
nbrestorevm -vmw -vcd -C VM_to_restore -R absolute_path_to_rename_file
-vcdrte -vmserver vCenter_server
```

Include the following in the rename file:

```
change vcdserver to new_vcdserver
change organization to new_organization
change orgvdc to new_organization_VDC
change vcdvapp to new_vcdvapp
change vcdvmname to new_vcdvmname
change esxhost to new_ESX_host
change datacenter to /new_datacenter
change resourcepool to /new_datacenter/host/new_ESX_host/resources
/new_resource_pool
change datastore to new_vmx_datastore
```

I: Restore to a different vCloud vApp and capture it as a template in a catalog.

```
nbrestorevm -vmw -vcd -C VM_to_restore -R absolute_path_to_rename_file
-vcdtemplate
```

Include the following in the rename file:

```
change vcdvapp to new_vcdvapp
change vcdcatalog to new_vcdcatalog
```

The vApp is restored to the original organization and organization VDC. To associate the vApp with a different organization VDC, include this directive:

```
change orgvdc to new_organization_VDC
```

Note: After the template is created, no other VMs can be added to the template.

J: Restore to a different vCloud vApp, capture the vApp as a template, and remove the vApp.

```
nbrestorevm –vmw –vcd –C VM_to_restore –R absolute_path_to_rename_file
–vcdtemplate –vcdremv
```

Include the following in the rename file:

```
change vcdvapp to new_vcdvapp
change vcdcatalog to new_vcdcatalog
```

The -vcdremv option removes the non-template vApp; the new vApp template is retained.

Note: After the template is created, no other VMs can be added to the template.

K: Restore a vCloud vApp template that has multiple virtual machines.

First, restore a virtual machine to a non-template vApp:

```
nbrestorevm -vmw -vcd -C VM_to_restore -vcdrte
```

Run this command for each VM but do not restore the last VM.

Next, restore the last VM, create a vApp template, and copy all the restored VMs into that template:

```
nbrestorevm -vmw -vcd -C VM_to_restore -R absolute_path_to_rename_file
-vcdtemplate -vcdremv -vcdlfree
```

Include the following in the rename file:

```
change vcdvapp to vApp_template
```

The change directive provides the name for the new vApp template into which the VMs are to be restored.

The -vcdremv option removes the non-template vApp into which you initially restored the virtual machines. The -vcdlfree option selects the datastore that has the largest available space.

Note: After the template is created, no other VMs can be added to the template.

Using the nbrestorevm command to restore virtual machines with Instant Recovery

Instant Recovery for VMware is described in the "Restore virtual machines with Instant Recovery" chapter of this guide.

See “About Instant Recovery for VMware” on page 237.

See “Notes on Instant Recovery for VMware” on page 242.

See “Instant Recovery options on the nbrestorevm command” on page 244.

See “Restoring a virtual machine with Instant Recovery for VMware” on page 249.

Using the nbrestorevm command to restore virtual machine disks

Virtual Machine Disk restore for VMware is described in other topics.

See “About VMware virtual machine disk restore” on page 196.

See “Restoring VMware virtual machine disks by using NetBackup commands” on page 204.

The `nbrestorevm -R` rename file for restoring virtual machines

The `-R` option on the nbrestorevm command is for restoring a VM to a different location. It identifies a text file that is called the rename file. This file describes the restore location by means of `change` directives. Each change directive provides information about a VMware attribute or object that defines the VM when it is restored. For example: the change directives can set the display name for the restored VM, the name of the datastore, and the name of the ESX server.

Note the following about the `-R` rename file:

- The `-R` option must specify the absolute path to the rename file.
- The `-R` option and rename file are not required when you restore the VM to its original location with all its original settings.
- Each change directive in the `-R` rename file must end with a carriage return. If the file contains only one change directive, that line must end with a carriage return.

- The change directives to include in the rename file depend on the VMware environment.
  Unlike the Backup, Archive, and Restore interface, the nbrestorevm command does not have its own validation checks. When you use the `nbrestorevm -R` option, you must include all the `change` entries that the VMware environment requires. Otherwise, the restore does not succeed or the VM does not function correctly.
- The change directives can be placed in any order in the file.
- The change directive should be entered exactly as shown in Table A-4, except for the variable at the end (such as *new_display_name*). Replace that variable with the new name.
- If a vSphere object does not apply to the restore destination, enter `None` as its value. For example: For restore to a standalone ESX, enter `change datacenter to None`.
- The rename file overrides the nbrestorevm -vmsn and -vmvmxd options:
  - If the rename file includes a change directive for a .vmdk path and nbrestorevm includes the –vmvmxd option, the –vmvmxd option is ignored. The change directive determines the .vmdk path of the restored VM.
  - If the rename file includes a change directive to designate a network for the restored VM and nbrestorevm includes the –vmsn option, –vmsn is ignored.

Table A-4 `-R` rename file change directives

-R rename file directives	Description and notes
`change vmname to new_display_name`	Sets the display name for the restored VM. If this entry is omitted, the original display name is used.
`change esxhost to new_ESX_host`	Designates the ESX server to restore to. This entry is required when you restore to a different ESX server.
`change datacenter to /new_datacenter`	Designates the datacenter in which to restore the VM. If the destination does not have a datacenter, enter None as the value: `change datacenter to None`
`change folder to /new_datacenter/new_folder`	Designates the folder in which to restore the VM. If the destination does not have a folder, enter None as the value: `change folder to None`

Table A-4 `-R` rename file change directives *(continued)*

-R rename file directives	Description and notes
`change resourcepool to /new_datacenter/host/new_ESX_host/resources/new_resource_pool`	For restore to a different ESX server, specify a different resource pool. (The original resource pool cannot be used to create a VM on a different ESX server.) You must specify a resource pool by including the following line in the rename file: For restore to a standalone ESX server, the `change resourcepool` entry must include the literal string `ha-datacenter` in the path: `change resourcepool to /ha_datacenter/host/new_ESX_host/Resources`
`change datastore to new_vmx_datastore`	Designates the vmx datastore (configuration datastore) of the restored VM. The vmx datastore contains the configuration files that describe the virtual machine. This change entry is required when you use the –vmvmxd option on the nbrestorevm command. The -vmvmxd option allows the vmdk files to be restored to the same datastore where the vmx file is specified. **Note:** See the change */original_vmdk_path* to */new_datastore/* directive in this table.

`change /original_vmdk_path to /new_datastore/`	Designates the original path to the .vmdk file, and the new datastore for the .vmdk file of the restored VM. As a rule, this change entry is required when you restore to a different datastore. Depending on your VMware environment, this change entry may take the following form:
	
	change */original_datastore/original_VM_folder/original_vmdk.vmdk* to */new_datastore/*
	
	Note: If you use the -vmvmxd option on nbrestorevm to restore the .vmdk files to the vmx datastore, do not use this change directive. By specifying the datastore for the vmdk files, this change directive overrides the -vmvmxd option.
	
	Note: If the change vmdk directive specifies a different path for some of the VM's vmdk files, the other vmdk files are restored to their original datastore.
	
	To restore more than one vmdk file to a specified datastore:
	
	`change /first_vmdk_path to /new_first_datastore/`
	`change /second_vmdk_path to /new_second_datastore/`
	`change /nth_vmdk_path to /new_nth_datastore`

Table A-4 `-R` rename file change directives *(continued)*

-R rename file directives	Description and notes
`change network to new_network`	Designates the new network for the restored VM. To designate multiple networks, enter the following: `change network to new_network, new_network(n)`
`change organization to new_organization`	Designates the vCloud Director organization to restore to.
`change orgvdc to new_organization_virtual_datacenter`	Designates the virtual datacenter in the vCloud Director organization to restore to.
`change vcdserver to new_vcdserver`	Designates the vCloud Director server to restore to.
`change vcdvapp to new_vcdvapp`	Designates the vCloud Director vApp to restore to.
`change vcdvapptemplate to new_vcdvapptemplate`	Designates the vCloud Director vApp template to restore to.
`change vcdvmname to new_vcdvmname`	Sets the display name for the restored VM in vCloud Director.
`change vcdcatalog to new_vcdcatalog`	Designates the vCloud Director catalog to restore to.

See "Logs for troubleshooting the nbrestorevm command" on page 346.

Logs for troubleshooting the nbrestorevm command

The following logs may contain helpful messages on nbrestorevm.

Table A-5 Logs with messages on nbrestorevm

Log directory	Contains the messages on	Resides on
Windows *install_path*\NetBackup\logs\bprd Linux, UNIX /usr/openv/netbackup/logs/bprd	The restore operation, such as for status code 2820.	Primary server

Table A-5 Logs with messages on nbrestorevm *(continued)*

Log directory	Contains the messages on	Resides on
Windows *install_path*\NetBackup\logs\bpVMutil Linux, UNIX /usr/openv/netbackup/logs/bpVMutil	The restore operation, such as for status code 2820.	Recovery host
Windows *install_path*\NetBackup\logs\nbrestorevm Linux, UNIX /usr/openv/netbackup/logs/nbrestorevm	Incorrect usage of the nbrestorevm command, such as omission of a required option.	Host where nbrestorevm is run

If the restore job reaches the point of creating the virtual machine, the job's detailed status should contain a specific error message. vSphere Client shows an attempt to create the virtual machine and displays an associated failure message.

Query format and examples for searching virtual machine backups

From the primary server, the nbdiscover command can search virtual machine backups based on a query rule. Compose the query manually and enclose it in double quotes.

For example: Search for backups of the virtual machines that have "vm1" as their display names:

```
nbdiscover "vmsearch:/;reqType=search?filter=VMDisplayName Equal
'vm1'"
```

Table A-6 Query format with examples

Element	Description
`vmsearch:/`	Specifies that the query searches virtual machine backups.

Table A-6 Query format with examples *(continued)*

Element	Description
`reqType`	The request type. The following request types are supported: ■ `search` Specifies that the query is used for search. Requires a query rule ■ `browse` Displays the hierarchy of the virtual machines that were backed up. Requires the `viewType`. ■ `listFields` Lists the supported field names and their attributes. ■ `listOps` Lists the operations that a field supports. Requires the `fieldName` option.

`viewType`	Specifies the type of hierarchical view (`vcloud` or `vsphere`). Used with the browse option.
	Example - Show the hierarchy of vCloud:
	`nbdiscover "vmsearch:/;reqType=browse;viewType=vcloud"`
	Example - Show the hierarchy of vSphere:
	`nbdiscover "vmsearch:/;reqType=browse;viewType=vsphere"`

`fieldName`	Specifies the name of the field for which supported operators are to be listed. Used with the `listOps`. Example - List supported operators for `VMDisplayName` `nbdiscover "vmsearch:/;reqType=listOps;fieldName=VMDisplayName"`
`filter`	The query rule. nbdiscover searches virtual machine backups based on the rule. Example: `nbdiscover -noxmloutput "vmsearch:/;reqType=search?filter=ScheduleType Equal '0'"`

See the following examples with sample output.

Example 1: Search for the virtual machines that have full backups.

```
nbdiscover -noxmloutput "vmsearch:/;reqType=search?filter=ScheduleType
Equal '0'"

+ "demovm%20(8c879391-2917-4416-9373-bea7ec727717)"
+ "smallvm2%20(10a16222-8532-46ff-bd6a-9661240392f4)"
```

Example 2: Search backups of the virtual machines that have the display names that contain "vm".

```
nbdiscover -noxmloutput
"vmsearch:/;reqType=search?filter=VMDisplayName Contains 'vm'"

+ "demovm%20(8c879791-2917-4428-9373-bea7ec727717)"
+ "small_vm%20(33e85579-7279-411f-b2f9-9fb570583911)"
+ "small_vm_percent_%25%20(33e85579-7279-411f-b2f9-9fb570583911)"
```

Example 3: Search for backups of the vCloud virtual machines that have "test" in their vApp names.

```
nbdiscover -noxmloutput "vmsearch:/;reqType=search?filter= vCDvApp
Contains 'test'"

+ "demovm%20(8c879791-2917-4428-8213-bea7ec727717)"
+ "small_vm%20(61e83479-7246-411f-b1f9-9fb570546755)"
+ "small_vm_percent_%25%20(61e83479-7246-411f-b1f9-9fb570546755)"
```

Example 4: Search the virtual machine backups that occurred before 08/24/2012 11:05:56 AM. Specify the backup time in UTC.

```
nbdiscover -noxmloutput "vmsearch:/;reqType=search?filter=BackupTime
Less '1345871512'"

+ "demovm%20(8c846791-2917-4428-9373-bea7ec727437)"
+ "small_vm%20(22e85813-7246-433f-b2f9-9fb570585387)"
+ "small_vm_percent_%25%20(22e85579-7246-433f-b2f9-9fb570585387)"
```

Example 5: Search backups for virtual machines where the vCloud organization is named "QA" and the vApp name contains "demo".

```
nbdiscover -noxmloutput "vmsearch:/;reqType=search?filter=vCDOrg
Equal 'QA' AND vCDvApp Contains 'demo'"

+ "demovm%20(8c879791-2917-4428-9373-bea7ec727717)"
```

Example 6: Show the hierarchy of a vCloud environment. The output is in XML.

```
nbdiscover "vmsearch:/;reqType=browse;viewType=vcloud"

<Start Iteration="vmsearch:/;reqType=browse;viewType=vcloud">
<VCDSERVER>
     <NBU>
     <NAME>hypervm1.acme.com</NAME>
     </NBU>
     <VCDORG>
          <NBU>
          <NAME>Test Cloud</NAME>
          </NBU>
```

```
            <VCDORGVDC>
                  <NBU>
                  <NAME>Test Org</NAME>
                  </NBU>
                  <VCDVAPP>
                        <NBU>
                        <NAME>TestvApp</NAME>
                        </NBU>
                  </VCDVAPP>
            </VCDORGVDC>
      </VCDORG>
</VCDSERVER>
<StatusMsg NBUStatus="0" Severity="0"></StatusMsg>
</START>
```

This search found the following:

- A vCloud Director server: `hypervm1.acme.com`
- An organization: `Test Cloud`
- A virtual datacenter: `Test Org`
- A vApp: `TestvApp`

Allowing other servers or clients to restore virtual machines

You can configure NetBackup to allow nbrestorevm to run from another host (such as another server, client, or virtual machine). The enabled host can use nbrestorevm to restore the virtual machine. The host must be configured as a peer of the NetBackup primary server that performed the backup.

You can configure the peer in either of the following ways:

- In the NetBackup Administration Console, click **Host Properties > Primary Servers > *double click the primary server* > Servers**. Add the peer on the **Additional servers** tab.
- Add an empty *peer_name* file in the following location:
  UNIX, Linux
  `/usr/openv/netbackup/db/altnames/`*`peer_name`*
  Windows
  `install_path``\NetBackup\db\altnames\`*`peer_name`*
  The name of the file is the name of the server or client to be granted restore privileges.

For instructions, see the topics on allowing clients to perform redirected restores, in the *NetBackup Administrator's Guide, Vol I*.

Appendix B

Configuring services for NFS on Windows

This appendix includes the following topics:

- About installing and configuring Network File System (NFS) for Granular Recovery Technology (GRT)
- About configuring services for NFS on Windows 2012 or 2016 (NetBackup for VMware)
- Disabling the Server for NFS (NetBackup for VMware)
- Disabling the Client for NFS on the media server (NetBackup for VMware)
- Configuring a UNIX media server and Windows backup or restore host for Granular Recovery Technology (NetBackup for VMware)
- Configuring a different network port for NBFSD (NetBackup for VMware)

About installing and configuring Network File System (NFS) for Granular Recovery Technology (GRT)

NetBackup Granular Recovery leverages Network File System, or NFS, to read individual objects from a database backup image. Specifically, the NetBackup client uses NFS to extract data from the backup image on the NetBackup media server. The NetBackup client uses “Client for NFS” to mount and access a mapped drive that is connected to the NetBackup media server. The NetBackup media server handles the I/O requests from the client through NBFSD.

NBFSD is the NetBackup File System (NBFS) service that runs on the media server. NBFSD makes a NetBackup backup image appear as a file system folder to the NetBackup client over a secure connection.

About configuring services for NFS on Windows 2012 or 2016 (NetBackup for VMware)

For instant recovery of virtual machines, the Services for Network File System (NFS) must be installed on Windows media servers.

Table B-1 Configuring NFS in a Windows 2012 or 2016 environment

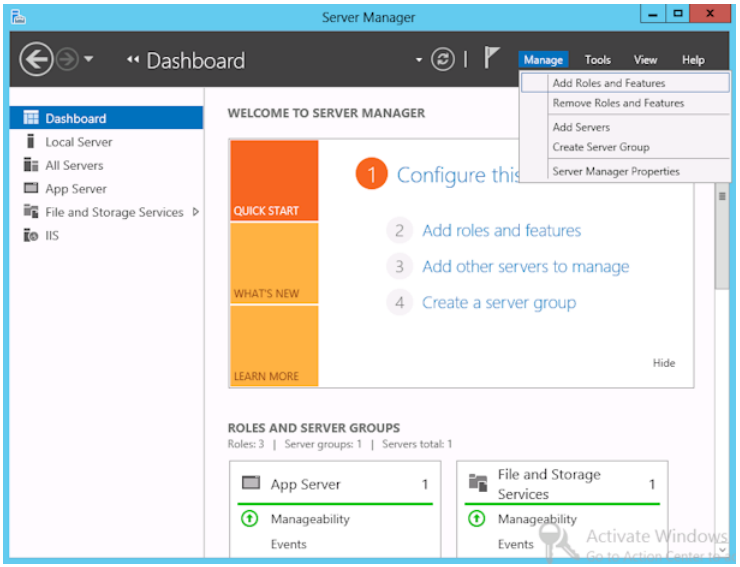
Action	Description
Configure NFS on the media server.	On the media server do the following: ■ Stop and disable the ONC/RPC Portmapper service, if it exists. ■ Enable NFS. See "Enabling Services for Network File System (NFS) on a Windows 2012 or 2016 media server (NetBackup for VMware)" on page 353. ■ Stop the Server for NFS service. See "Disabling the Server for NFS (NetBackup for VMware)" on page 360. ■ Configure the portmap service to start automatically at server restart. Issue the following from the command prompt: `sc config portmap start= auto` This command should return the status `[SC] ChangeServiceConfig SUCCESS`.
Configure NFS on the restore host.	On the restore host, do the following: ■ Enable NFS. See "Enabling Services for Network File System (NFS) on a Windows 2012 or 2016 restore host (NetBackup for VMware)" on page 357. ■ Stop the Server for NFS service. See "Disabling the Server for NFS (NetBackup for VMware)" on page 360.

Enabling Services for Network File System (NFS) on a Windows 2012 or 2016 media server (NetBackup for VMware)

To perform VM instant recovery with a Windows 2012 or 2016 media server, you must enable Services for Network File System. When this configuration is completed, you can disable any unnecessary NFS services.

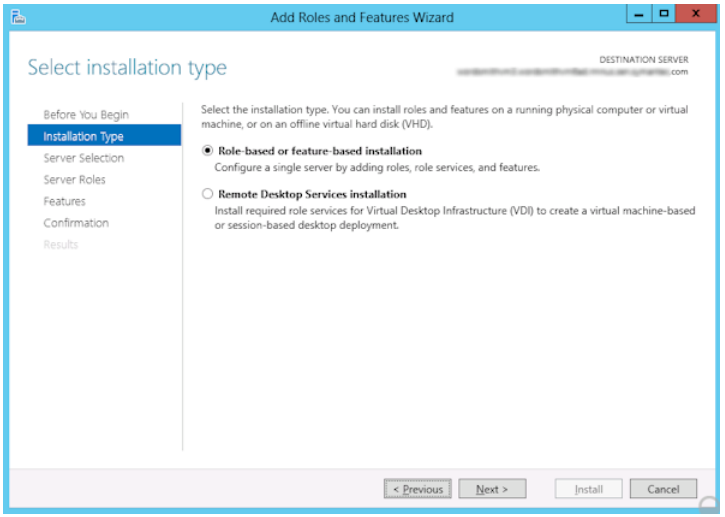
To enable Services for Network File System (NFS) on a Windows 2012 or 2016 media server

1. Open the Server Manager.
2. From the **Manage** menu, click **Add Roles and Features**.



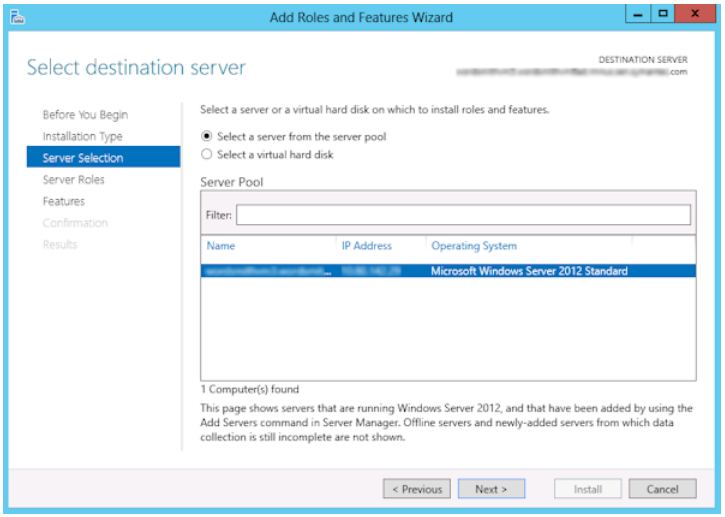
3. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.

4 On the **Select installation type** page, select **Role-based or feature-based installation**.



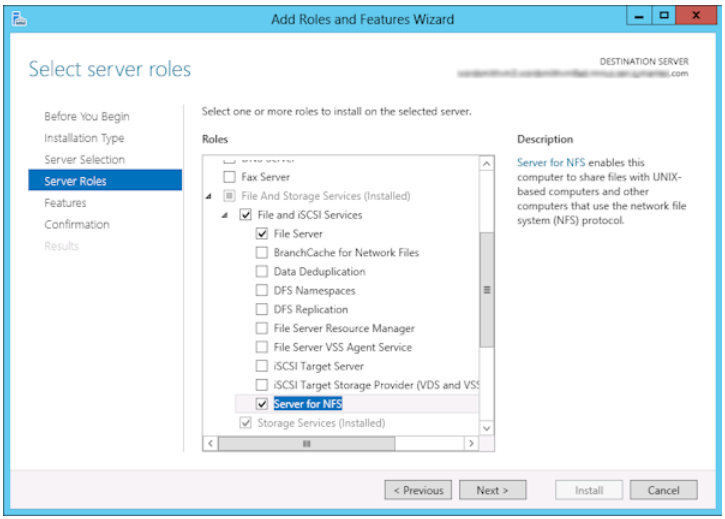
5 Click **Next**.

6 On the **Server Selection** page, click **Select a server from the server pool** and select the server. Click **Next**.

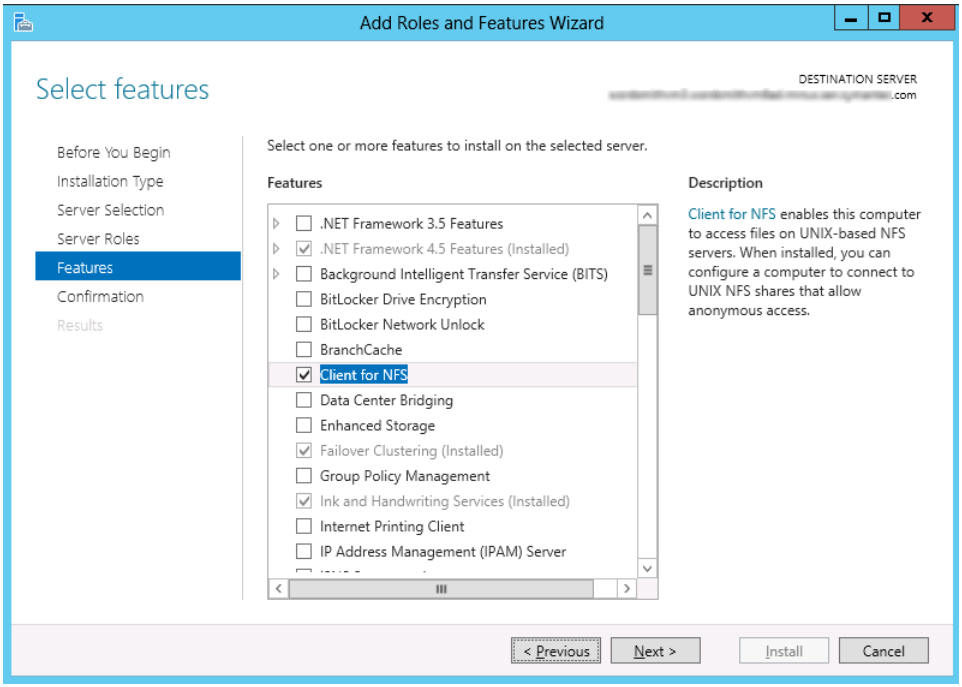


7 On the **Server Roles** page, expand **File and Storage Services** and **File and iSCSI Services**.

8 Click **File Server** and **Server for NFS**. When you are prompted, click **Add Features**. Click **Next**.



9 If the media server is also a restore host, on the **Features** page, click **Client for NFS**. Click **Next**.



10 On the **Confirmation** page, click **Install**.

11 Disable any unnecessary services, as follows:

- If you have a single host that functions as both the media server and the restore host, you can disable the Server for NFS.
- For a host that is only the NetBackup media server, you can disable the Server for NFS and the Client for NFS.

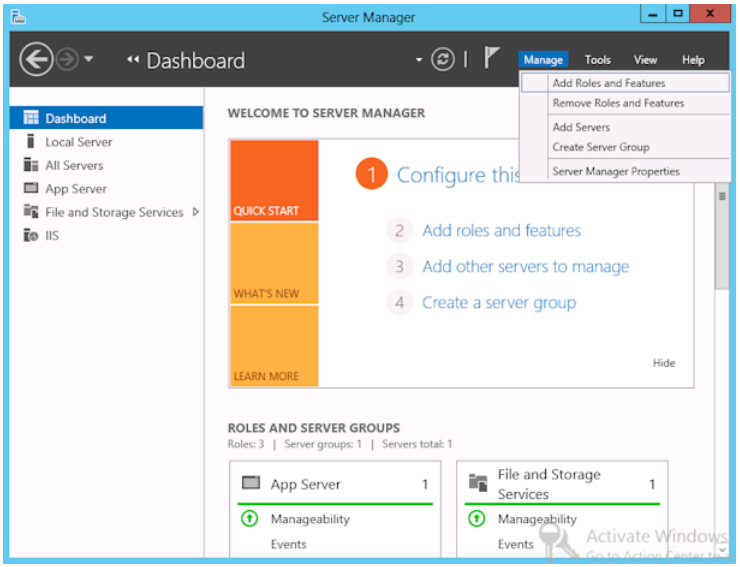
12 Make sure that the portmap service is started and that its startup mode is set to auto.

Enabling Services for Network File System (NFS) on a Windows 2012 or 2016 restore host (NetBackup for VMware)

To perform VM instant recovery with a Windows restore host, you must enable Services for Network File System. When this configuration is complete, you can disable any unnecessary NFS services.

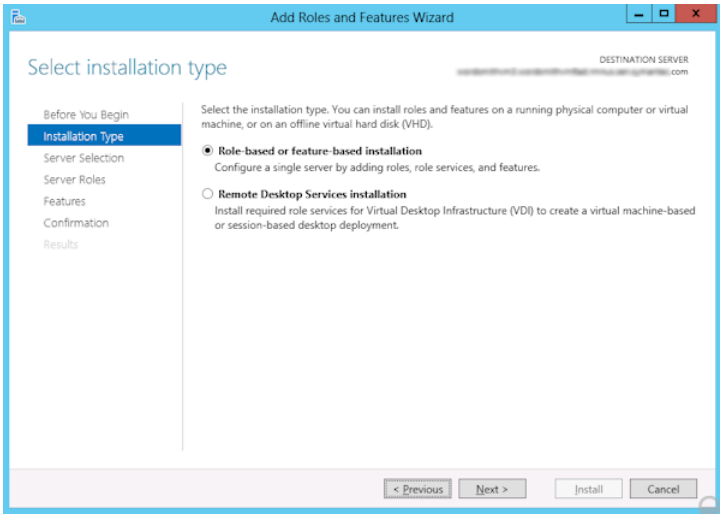
To enable Services for Network File System (NFS) on a Windows 2012 or 2016 restore host

1. Open the Server Manager.
2. From the **Manage** menu, click **Add Roles and Features**.



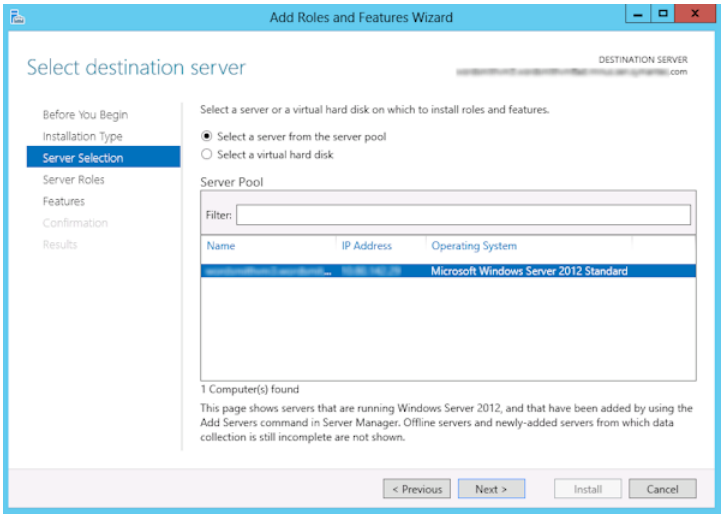
3. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.

4 On the **Select installation type** page, select **Role-based or feature-based installation**.



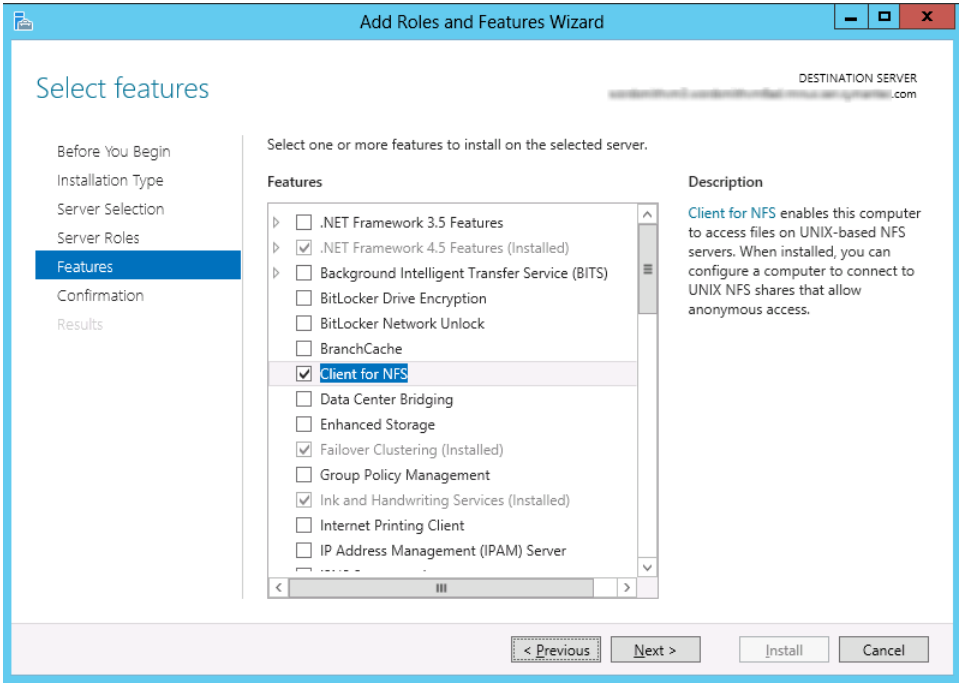
5 Click **Next**.

6 On the **Server Selection** page, click **Select a server from the server pool** and select the server. Click **Next**.



7 On the **Server Roles** page, click **Next**.

8 On the **Features** page, click **Client for NFS**. Click **Next**.



9 On the **Confirmation** page, click **Install**.

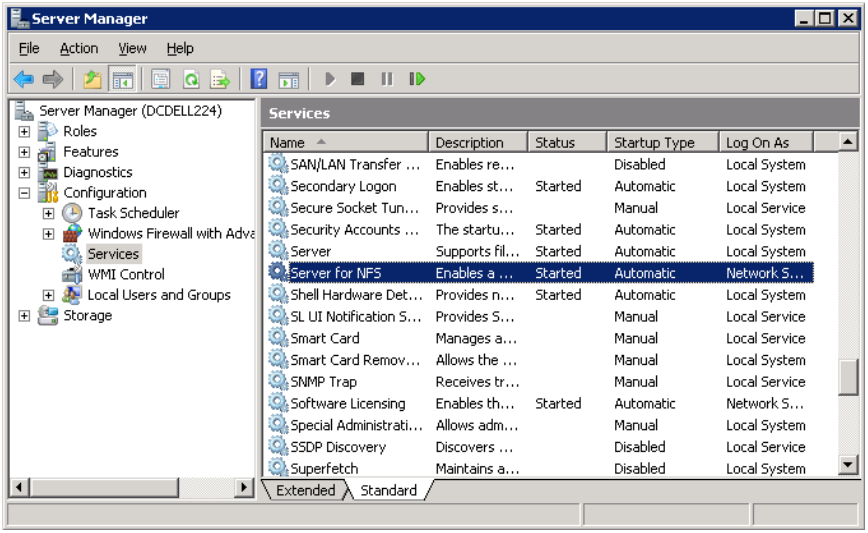
Disabling the Server for NFS (NetBackup for VMware)

To disable the Server for NFS

1 Open the Server Manager.

2 In the left pane, expand **Configuration**.

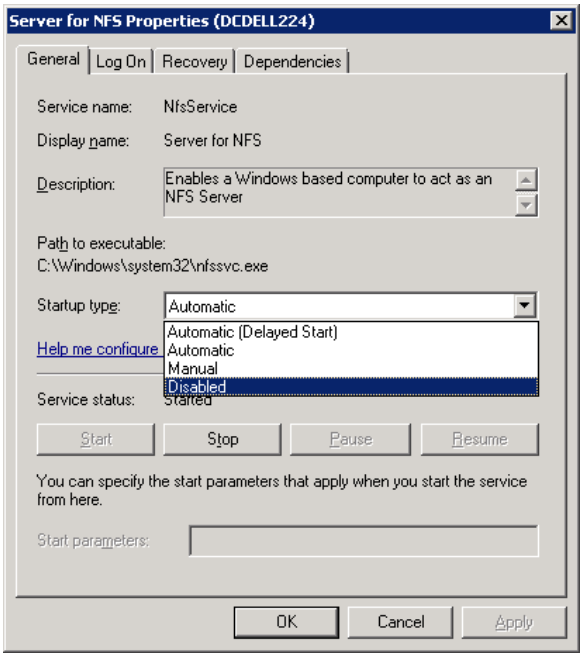
3 Click **Services**.



4 In the right pane, right-click on **Server for NFS** and click **Stop**.

5 In the right pane, right-click on **Server for NFS** and click **Properties**.

6 From the **Startup type** list in the **Server for NFS Properties** dialog box, click **Disabled**.



7 Click **OK**.

8 Do this procedure for each media server and for the restore host.

Disabling the Client for NFS on the media server (NetBackup for VMware)

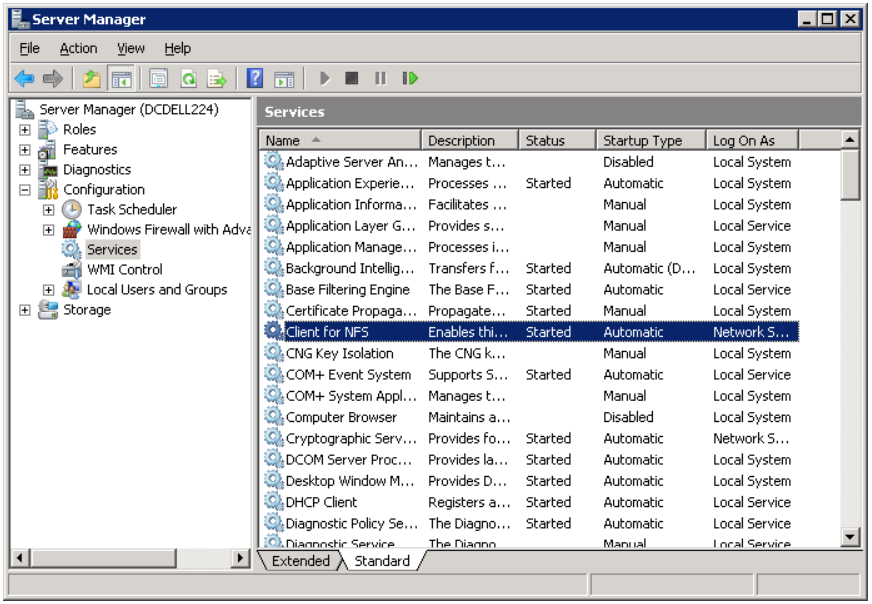
After you enable Services for Network File System (NFS) on a host that is only a NetBackup media server, disable the Client for NFS.

To disable the Client for NFS on the NetBackup media server

1 Open the Server Manager.

2 In the left pane, expand **Configuration**.

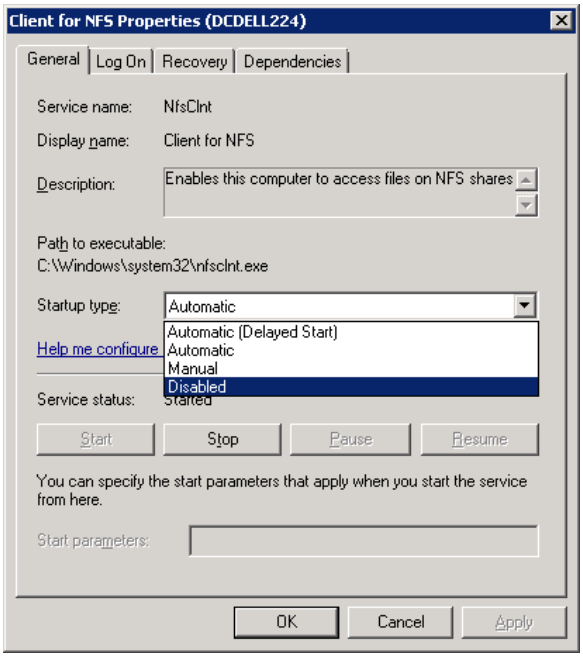
3 Click **Services**.



4 In the right pane, right-click on **Client for NFS** and click **Stop**.

5 In the right pane, right-click on **Client for NFS** and click **Properties**.

6 From the **Startup type** list in the **Client for NFS Properties** dialog box, click **Disabled**.



7 Click **OK**.

Configuring a UNIX media server and Windows backup or restore host for Granular Recovery Technology (NetBackup for VMware)

For backups and restores that use Granular Recovery Technology (GRT), perform the following configuration if you use a UNIX media server and Windows restore host:

- Confirm that your media server is installed on a platform that supports granular recovery.

  For more information about supported platforms, see the *NetBackup Enterprise Server and Server - OS Software Compatibility List* at the following URL:

  http://www.netbackup.com/compatibility

  No other configuration is required for the UNIX media server.

- Enable or install NFS on the restore host.
  See "Enabling Services for Network File System (NFS) on a Windows 2012 or 2016 restore host (NetBackup for VMware)" on page 357.
- You can configure a different network port for NBFSD.

Configuring a different network port for NBFSD (NetBackup for VMware)

`NBFSD` runs on port 7394. If another service uses the standard `NBFSD` port in your organization, you can configure the service on another port. The following procedures describe how to configure a NetBackup server to use a network port other than the default.

To configure a different network port for NBFSD (Windows server)

1. Log on as administrator on the computer where NetBackup server is installed.
2. Open Regedit.
3. Open the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\Config
```

4. Create a new DWORD value named **FSE_PORT**.
5. Right-click on the new value and click **Modify**.
6. In the **Value data** box, provide a port number between 1 and 65535.
7. Click **OK**.

To configure a different network port for NBFSD (UNIX server)

1. Log on as root on the computer where NetBackup server is installed.
2. Open the `bp.conf` file.
3. Add the following entry, where *XXXX* is an integer and is a port number between 1 and 65535.

   FSE_PORT = *XXXX*

See "Configuring a UNIX media server and Windows backup or restore host for Granular Recovery Technology (NetBackup for VMware)" on page 364.

Appendix C

The Reuse VM selection query results option

This appendix includes the following topics:

- About the Reuse VM selection query results option
- The effect of virtual machine discovery on vCenter

About the Reuse VM selection query results option

The NetBackup Test Query screen lists the virtual machines that NetBackup discovered in your virtual environment. Because the automatic selection feature is dynamic, later changes in the environment may affect which virtual machines match the query rules. For example: if virtual machines are added later, the current test results may not be identical to the virtual machines that are selected when the backup runs.

During the period you specify on **Reuse VM selection query results for**, NetBackup reuses the current list of virtual machines as the backup list. It does not consult the Query Builder or rediscover virtual machines.

The less often your virtual machine environment undergoes changes, the more advantageous it may be to reuse the list of virtual machines for backups. In large environments, discovery of virtual machines takes time and consumes resources on the vCenter server.

Note the following about the Reuse VM selection query results option:

- Determines how long the query results are reused (that is, how often the list of discovered virtual machines is refreshed).
- Controls how often NetBackup performs discovery on the vCenter server.

For the environments that contain many virtual machines, the discovery process may increase the load on the vCenter server.

- Has no effect on the NetBackup policy execution schedule.
- Is invalidated if the query rules are changed or if the policy attributes that affect discovery are changed. In that case, NetBackup rediscovers virtual machines the next time the policy runs.

  The following topic describes the policy attributes that affect discovery:

  See "Effect of Primary VM identifier parameter on Selection column in Test Query results" on page 144.

For example: assume that the **Reuse VM selection query results for** option is set to 8 hours and your query selects turned-on virtual machines. If additional virtual machines are turned on during the 8-hour period, they are not added to the policy's backup list. The policy backs up the virtual machines that were last added to the list (such as when the policy was created). After 8 hours, at the next execution of the policy, the recently turned on virtual machines are discovered and added to the backup list.

If the next backup occurs before the Reuse period expires, and a virtual machine was renamed during the Reuse period, NetBackup backs up the renamed virtual machine under its original name. Because the reuse period has not expired, NetBackup does not rediscover virtual machines and therefore cannot identify the virtual machine by its new name. (NetBackup identifies the virtual machine by its instance UUID.) To have backed up the virtual machine with its new name, the Reuse period should have been set to a shorter interval.

Note: The virtual machines that have been selected for backup are not displayed on the policy **Clients** tab. To see which virtual machines NetBackup has selected and backed up, refer to the following topics.

See "Using the Activity Monitor to monitor virtual machine backups" on page 156.

See "Using OpsCenter to report on virtual machine backups" on page 160.

The effect of virtual machine discovery on vCenter

In all but the largest environments, it may be advantageous to set the **Reuse VM selection query results for** option so that discovery occurs more often.

If changes occur to virtual machine configuration (such as adding, deleting, or moving vmdk files), it may be necessary to set **Reuse VM selection query results for** to 0. With a setting of 0, NetBackup rediscovers the virtual machines and their configuration each time the policy runs.

Note: If the vmdk files are reconfigured and the next backup runs without rediscovery, NetBackup is not aware of the vmdk changes. It attempts to back up the virtual machines in their previous configuration. The result may be an incorrect backup.

Appendix D

Backup of VMware raw devices (RDM)

This appendix includes the following topics:

- About VMware raw device mapping (RDM)
- Configurations for backing up RDMs
- About alternate client backup of RDMs
- Requirements for alternate client backup of RDMs
- Configuring alternate client backup of RDMs

About VMware raw device mapping (RDM)

VMware raw device mapping mode (RDM) allows a virtual machine to directly access physical disks. With raw device mapping, a VMware virtual machine can use large storage devices such as disk arrays. Access to the data on an RDM disk is faster than to a fully virtualized disk (vmdk file). An RDM disk can be locally attached to the ESX server or configured on a Fibre Channel SAN.

NetBackup supports the disk arrays that are configured on a virtual machine as RDMs.

Note: NetBackup cannot back up the RDM by means of a VMware backup host.

For notes and restrictions on NetBackup support for VMware RDM, see the following Veritas tech note:

Support for NetBackup in virtual environments

http://www.veritas.com/docs/000006177

Configurations for backing up RDMs

You can use either of the following NetBackup configurations to back up disk arrays as RDMs:

- Without Snapshot Client: Install a NetBackup client on the virtual machine. You can configure NetBackup to back up the virtual machine and any RDMs as if the client was installed on a physical host. Without Snapshot Client software on the virtual machine, the features of Snapshot Client are not available. (This configuration is not discussed in this NetBackup for VMware guide.)
- With Snapshot Client: Install a NetBackup client and Snapshot Client software on the virtual machine. Configure an alternate client backup.

About alternate client backup of RDMs

Alternate client backup of an RDM consists of the following:

- The RDM disk array contains the data to be backed up. Another host containing NetBackup client software and Snapshot Client software must have access to the disk array. This host is the alternate client. In this configuration, the virtual machine is called the primary client.
- A snapshot of the data is created on the disk array and is mounted on the alternate client. The alternate client creates a backup image from the snapshot, using original path names, and streams the image to the NetBackup media server.
- The alternate client handles the backup I/O processing; the backup has little or no effect on the virtual machine. The media server reads the snapshot data from the alternate client and writes the data to storage.
- The virtual machine and alternate client must be running the same operating system, volume manager, and file system. For each of these I/O system components, the alternate client must be at the same level as the primary client, or higher level.
  For complete requirements on alternate client backup, refer to the Policy configuration chapter of the *NetBackup Snapshot Client Administrator's Guide*.

Requirements for alternate client backup of RDMs

To use NetBackup Snapshot Client to back up an RDM, note the following:

- RDM devices must be configured in physical compatibility mode. You select this mode when you create the RDM. Physical compatibility mode is not configured in NetBackup.

  For an introduction to RDM, refer to your VMware documentation. For example, see the following VMware document:

  ESX Server 3 Configuration Guide
- NetBackup may require certain OS and array configuration, depending on the guest OS and the array. For details, see the disk arrays chapter of the *NetBackup Snapshot Client Administrator's Guide*.
- NetBackup client software must be installed on the virtual machine.
- The requirements for the NetBackup for VMware feature (a backup host and the VMware snapshot method) do not apply to backups of RDM disk arrays. To back up RDM disk arrays, you must configure a Snapshot Client alternate client backup.

Configuring alternate client backup of RDMs

This procedure highlights key points in creating a NetBackup alternate client backup of a disk array that is configured as an RDM. For broader details on disk array configuration, refer to the *NetBackup Snapshot Client Administrator's Guide*.

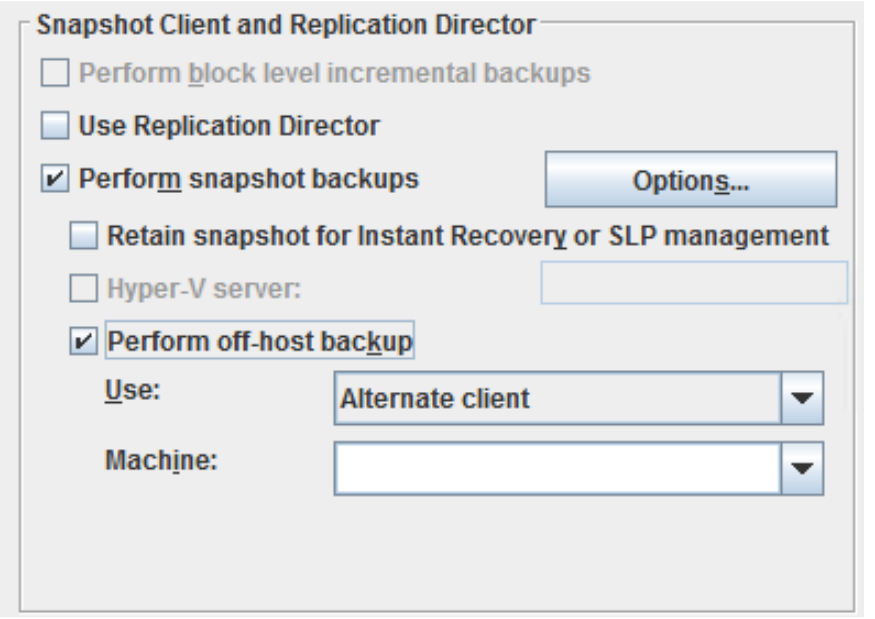
To create an alternate client policy for a disk array that is configured as an RDM

1. Select a policy type that is appropriate for the OS of the virtual machine and for the type of data to back up.

   Refer to the Policy configuration chapter of the *NetBackup Snapshot Client Administrator's Guide*.

2. On the policy **Attributes** tab in the Administration Console, click **Perform snapshot backups** and **Perform off-host backup**.

   The following is a detail from the **Attributes** tab.



3. Select **Alternate Client** from the **Use** pull-down. Do not select **VMware backup host**.

   In the **Machine** field, enter the name of the host that is configured as an off-host backup computer (the alternate client).

4. Click **Options**.

5. Select a snapshot method.

   The VMware method does not apply to alternate client backup and is not available in the list.

Select a snapshot method that is appropriate for the volume or array. For example:

- The HP_EVA_Snapclone method or other EVA method for an HP EVA array.
- The EMC_CLARiiON_Snapview_Clone or other CLARiiON method for an EMC CLARiiON array.
- FlashSnap.
  For FlashSnap, the following must be installed: VxVM 3.2 or later for UNIX, VxVM 4.0 or later for Linux and AIX, or VxVM 3.1 or later for Windows. Also, volumes must be configured over the primary host's disks. The VxVM FlashSnap license must also be installed.
- VSS (for Windows guest operating systems only).

The array may require additional OS and NetBackup configuration as described in the disk arrays chapter of the *NetBackup Snapshot Client Administrator's Guide*. The same guide contains more details on snapshot methods.

6 If required by an array snapshot method that you selected in the previous step, specify the **Snapshot Resources**.

7 In the policy's **Clients** list, select the virtual machine on which the array is configured as an RDM.

8 In the policy's **Backup Selections** tab, specify the disk that you want to back up, or the files or volumes that reside on the disk.

Index

Symbols

156 (status code) 301

A

Accelerator 162
  and the NetBackup catalog 166
  logs for 167
  messages in the backup job details log 167
  policy attribute 163
  replacing image size with network-transferred data in command output 171
  reporting network-transferred data in command output 168
access host 16
Activity Monitor
  to monitor VM backups 156
ALL_LOCAL_DRIVES 301
allowed list
  for dynamic multipathing on Linux 35
alternate client backup
  configure for RDM 371
  of RDM 370
alternate location for restore 188
AND vs OR 123
  Join field in Query Builder 117
automatic selection of virtual machines 72
  about 102
  Basic Mode 111
  cache file for 366
  Clients tab 109
  examples 102, 118
  notes on 105
  requirements 107
  task overview 108
  testing 141
  with multiple policies 121

B

backup
  fault tolerant VM 37
backup *(continued)*
  host 15
  how to configure 68
  how to perform 154
  job hangs 306
  monitoring with Activity Monitor 156
  monitoring with OpsCenter 160
  process overview 20
  reduce size of 150
backup host 73
  adding to configuration 44
  check if supported 287
backup media server 16, 18, 73
backups
  replacing Accelerator image size with network-transferred data in command output 171
  reporting network-transferred data for Accelerator 168
Basic Mode
  edit rule in Query Builder 116
  Query Builder 111
best practices 281
BIOS
  reconfigure for booting 309
BLIB 75, 99, 151
block-level incremental backup. *See* BLIB
blocked list
  for dynamic multipathing on Linux 35
blocks
  exclude deleted 75
browse virtual machines 91
browsing timeout 297

C

cache file
  for browsing virtual machines 93
catalog
  and use of Accelerator 166
change VMware hostname in NetBackup 50
Changed Block Tracking 151

Client Reports
using OpsCenter 160
Clients tab
automatic selection of virtual machines 109
description of fields for queries 129
code 156 error 301
compound query rules 124
configuration
of auto selection of virtual machines 109, 111
overview for backup of VMs 24
configuration datastore 178
credentials
adding for VMware 45
troubleshooting 300
cross-platform restore 175
Cumulative Incremental Backup 71

D

datacenter
for restore 191
datacenter folders
rules in Query Builder 126
datastore
in a datastore cluster 192
restore of 192
deduplication 282
delete
vSphere Client snapshot 152
Differential Incremental Backup 71
disable virtual machine quiesce 81
Discovered Timestamp 93
disk array
configured as RDM 371
display name 76, 93
DNS name 76
drives
and reboot failure 309
dynamic multipathing
in a SAN environment 35

E

edit rules in Query Builder 116
EMM database
remove VM host name from NetBackup 50
Enable block-level incremental backup 75, 151
encrypted drives 27
encryption of snapshot data transport 79, 184
equipment 287
ESX server 16, 45
Exclude deleted blocks option 75
exclude disks from backup 88
exclude list
speed up discovery of virtual machines 93
ext file systems, Linux 179
extended attributes, restore of 179

F

failed virtual machines
in test query 143
fault tolerant VMs 37
FIFO files, Linux 179
file system
Linux, restore of 179
firewall 306

G

grouping rules in Query Builder 124
guest customizations
ensuring their restore 317

H

host name 76, 93
changing in NetBackup 50
host properties
for VMware 44
hotadd transport mode 79, 184
notes on 40
hypervisor 21

I

Ignore diskless VMs 81, 303
in-place disk restore 196–197, 212, 216, 220–221, 318–319
incremental backup
about 99
requirements 71
setting up 100
independent disk 22, 94, 302
how to back up 28
installing and configuring Network File System (NFS) 352
instant recovery 238
Intelligent Policy 102
invalid client 308
IsSet operator examples 120

J

job hangs 306
Join field in Query Builder 117

K

keywords
    in Query Builder 130

L

Last Update 93
Linux
    notes on 34
    notes on restore 179
    quiesce 34
logging
    Accelerator 167
    how to create folders for 290
    VMware 288
    vSphere 298
    VxMS 290
LVM2 volume 34, 179

M

MAC address 179
manual backup 154
monitor backups
    with Activity monitor 156
    with OpsCenter 160
mount point
    missing 308
multiple policies
    for auto selection of VMs 121

N

nbdiscover command 141
    to test a query 106, 108, 110
nbemmcmd 50
nbfsd port 365
NetBackup Accelerator. *See* Accelerator
Network Block Device (NBD) transport 79, 184
Network Block Device (NBD) transport with SSL 79, 184
Network Connections dialog 194
Network File System (NFS), described 352
NFC connections 306
NFS share, Linux 179
NTFS file system
    for USB drives 27

O

OpsCenter
    to monitor VM backups 160
optimized storage 150
order of operations
    Query Builder 123
overview
    configuration steps 24
    of backup process 20
    restore procedure 223
overwrite virtual machine 185

P

parentheses
    for rules in Query Builder 124
path length
    maximum for Linux/UNIX files 35
Perform Recovery dialog 195
policy
    and cache file for auto selection of VMs 366
    configure for auto VM selection 111
    for full virtual machine backup 68
    multiple, for auto VM selection 121
    types 69
    wizard for creating 68
Policy Configuration wizard 68
port number 49, 300
precedence 123
prerequisites 26
Primary VM identifier
    setting 76
Primary VM identifier parameter
    and IsSet operator 120
    and multiple policies 121
    and testing query rules 143–144
    and VM Name column in Test query 146
privileges 301

Q

Query Builder
    and Primary VM identifier parameter 144
    cache file for results 366
    configuration in Advanced Mode 116
    configuration in Basic Mode 111
    description of fields 129

Query Builder *(continued)*
edit rule in 116
enter rules manually 116
escape character 140
examples 118
grouping rules 116
IsSet operator examples 120
keywords 130
operators 139
order of operations 116, 123
quotation marks 140
testing rules for 141, 143
to select virtual machines for backup 102
values 140
wildcards 140
with multiple policies 121
query builder
to filter virtual machines for backup 72
quiesce
Linux file system 179
Linux, notes on 34
quiesce virtual machine 81

R

RDM 22, 302
about 369
alternate client backup of 370–371
configurations supported 370
reboot failure 309
Recovery Destination dialog 183
recovery host 15, 183
Recovery Options dialog 183, 189
recovery wizard. *See* restore from backup. *See* restore into vCloud
reduce size of backup 150
release level
using mixed levels 236
remove VMware host name from NetBackup EMM database 50
reports on backups
using OpsCenter 160
resource pool
for virtual machine restore 192
resource pools
rules in Query Builder 125
restore
about restoring individual virtual machines 204
from backup 182, 188
guest customizations 317
restore *(continued)*
how to 181, 197
individual files 224
into vCloud 275
job hangs 306
maximum path length for Linux/UNIX files 35
notes on 175
procedure overview 223
virtual machine 181, 197
vmdk 204
restore vmdk
Changed Block Tracking warning during subsequent backup 319
create restore parameters file 207
determine backup ID from which to restore 205
restoring individual 213
validate restore parameters file 212
reuse file
for Query Builder results 366
Reuse VM selection query results for 366
rules in Query Builder
about 104
configuring 111
editing 116
examples 104
examples with parentheses 124
for datacenter folders 126
for resource pools 125
IsSet operator examples 120
order of operations 123
testing 141
testing failed 143
run a backup 154

S

SAN transport mode 79, 184
SCSI drives
and reboot failure 309
Select automatically through VMware Intelligent Policy query 72, 102
Select ESX server dialog 192
Select Folder dialog 193
server name
changing in NetBackup 50
size of backups
reducing 150
snapshot
vSphere Client
how to delete 152

socket files, Linux 179
SRM environment and replication 81, 303
SSL encryption of snapshot data 79, 184
start a backup 154
status code 156 301
Storage Destination dialog 193
storage optimization 27, 150
    how to delete snapshot for 152
Storage vMotion
    backup conflict 305

T

tag associations
    support 103
    use 103
template VM 27
terminology 20
Test Query screen 141
    and Primary VM identifier parameter 144, 146
    failed virtual machines 143
    nbdiscover as alternative 106, 108, 110
thin provisioned disks 187
timeout
    browsing 297
timeouts
    vSphere 298
transport modes
    and hung job 306
    for restore 184
    hotadd 40
troubleshooting
    tips 286

U

USB drives
    as the snapshot mount point 27
UUID 76, 93

V

validate
    credentials 45
validate virtualization server's certificate 54
vApp
    browsing virtual machines within 93
    for virtual machine restore 192
vCenter server 16
vCloud
    alternate location for restore 275
vCloud *(continued)*
    NetBackup credentials for 47
Virtual machine quiesce option 81
Virtual Machine recovery wizard
    restore to alternate location 188
    vCloud restore to alternate location 275
virtual machines
    about restoring individual 204
    auto selection from reuse file 366
    browsing 91
    configure backup policy for 68
    configure for auto selection of 111
    how to back up 154
    monitor backups of 156, 160
    notes on query builder 105
    requirements for auto selection 107
    Select automatically through VMware Intelligent Policy query 72, 102
    testing auto selection of 141
virtual network
    select for restore 195
VirtualCenter server 16
VM Name column in Test Query screen 146
vmdk file 23
    backup fails if none assigned 81, 303
vmdk restore
    about 196
    overwrite during restore 203, 222
    process 204
    restore parameters file 214
    troubleshooting 318
VMware
    access host 16
    backup environment 15
    backup host 44
    backup media server 18
    backups 154
    configuration overview 24
    credentials 45
    ESX server 16, 45
    Exclude Disk tab 86
    host properties 44
    introduction 13
    logging 288
    main features 13
    policy configuration 68
    required components 15
    restores 181, 197
    terminology 20

VMware *(continued)*
troubleshooting 288
VMware Intelligent Policy 102
VMware Intelligent Policy query 72
VMware policy 69
VMware policy tab 69
VMware Tools 23
VMX directory 178
vmx-07 71
vNetwork Distributed Switch 195
Volume Manager volumes 100
vSphere Client snapshot
how to delete 152
vStorage 23
incrementals 100
restore into vCloud 275
VxMS logging 290

W

wizard
to create backup policy 68
to recover virtual machine 182, 275