Dell EMC NetWorker

Version 19.1

VMware Integration Guide

302-005-701
REV 04
August 2019

DELL EMC

Copyright © 1990-2019 Dell Inc. or its subsidiaries. All rights reserved.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Figures 9

Tables 11

Preface 13

Chapter 1 Introduction to NetWorker VMware Protection with the vProxy appliance 17

Introduction to NetWorker VMware Protection with vProxy appliance..... 18
Components in the NetWorker VMware Protection Solution with vProxy appliance..... 18
System requirements..... 19
Compatibility information..... 21
Port requirements..... 22
NetWorker VMware Protection Solution best practices with the vProxy appliance..... 23
Performance and scalability..... 26
Configuration checklist..... 28
Basic configuration..... 28
Data Domain system configuration..... 28
NetWorker configuration..... 29
Virtual machine configuration..... 29
vProxy limitations and unsupported features..... 29
Accessing Knowledge Base Articles..... 33

Chapter 2 Deploy the vProxy appliance and configure the NetWorker datazone 35

Deploying the vProxy appliance..... 36
Deploy the vProxy OVA on a vCenter server..... 36
Deploy the vProxy OVA on an ESXi host..... 38
VMware vCenter server management..... 40
Add the vCenter server using NMC's VMware View..... 40
Add the vCenter server using the NetWorker Management Web UI.. 41
Configuring and registering the vProxy appliance..... 43
Configure and register the vProxy in NMC..... 43
Add and configure the vProxy in the NetWorker Management Web UI..... 45
Installing the vCenter plug-in..... 46
Install the vCenter plug-in using VMware View in NMC..... 46
Install the vCenter plug-in using the NetWorker Management Web UI..... 49
Updating the vCenter plug-in..... 50
Accessing the HTML-5 or flash-based vCenter plug-in as a non-administrator Active Directory user..... 50

Creating a dedicated vCenter user account and VM Backup and Recovery role....51
Create vCenter user account....51
Create a customized role....52
vSphere Client user accounts....55
Migrating policies from VMware Backup appliance to vProxy appliance....57
Migration pre-requisites....57
Policy migration to vProxy by using NMC....57
Policy migration to vProxy by using the command line....59
Renaming a NetWorker server with legacy VMware Backup appliance....59
Resetting the admin account password....59
Upgrading the vProxy appliance....60
Limitations....62
Troubleshooting Redeployment Failures....62

Chapter 3 Protecting virtual machines 65
Overview of protection policies....66
Preparing the NetWorker data zone....67
Configure the Data Domain System....67
VMware backups in the NetWorker Management Web UI....68
Policies, workflows, and actions in NetWorker Management Web UI....68
Create a policy using the NetWorker Management Web UI....69
Create a workflow using the NetWorker Management Web UI....70
Create an action using the NetWorker Management Web UI....72
Create a save set group using the NetWorker Management Web UI....83
Create a VMware group using the NetWorker Management Web UI....84
Create a rule using the NetWorker Management Web UI....85
vProxy backups in NMC....87
Default data protection policies in NMC's NetWorker Administration window....88
Create a VMware policy in NetWorker Administration....88
Create a workflow for a new policy in NetWorker Administration..90
Create a workflow for an existing policy in NetWorker Administration....92
Create or edit a VMware group in NetWorker Administration....94
Enabling a VMware group with Dynamic Association and applying rules....96
Create a VMware backup action in NetWorker Administration....100
Create a clone action in NetWorker Administration....105
Creating an action for Microsoft SQL Server application-consistent protection....108
Starting, stopping, and restarting policies....109
Visual representation of VMware policy and associated actions...109
VMware View in NMC....110
vProxy backup workflows in the vSphere Client's Dell EMC NetWorker interface....115
Connect to the NetWorker server in the vSphere Client....116
Start a vProxy policy in the vSphere Client Dell EMC NetWorker interface....118
Add virtual machines to a vProxy policy in the vSphere Client Dell EMC NetWorker interface....119

vProxy workflows in the vSphere Web Client's VM Backup and Recovery interface..... 121
Connect to the NetWorker server in the vSphere Web Client.....121
Starting a vProxy policy in the vSphere Web Client..... 122
Adding virtual machines to a vProxy policy workflow in the vSphere Web Client..... 123
Additional vProxy backup configuration options.....124
Configure a backup to support VMware encryption..... 124
Configure a backup to support vSAN encryption.....125
Enabling or disabling Changed Block Tracking.....126
Enable the Microsoft VM App Agent for SQL Server application-consistent protection..... 127
Updating the Microsoft VM App Agent and FLR Agent software..... 132
Troubleshooting Data Protection Policies..... 132
Backup operations.....132
Managing command execution for VM Proxy Agent operations on Linux..... 136
vProxy backup log files.....137
NMC function to collect vProxy log bundle information..... 137
Logs for SQL application-consistent data protection..... 138

Chapter 4 Recover virtual machines and data 141
Preparing the NetWorker datazone for recovery..... 142
Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only).....142
File-level restore as an Active Directory user..... 143
Active Directory user access to the vCenter plug-in and NMC.....146
vProxy recovery in NMC.....146
Recovering a virtual machine using the NMC Recovery wizard.... 146
vProxy recovery in the NetWorker Management Web UI.....164
Revert (or rollback) a virtual machine backup..... 165
Recover to a new virtual machine.....166
Instant Restore of a virtual machine..... 167
Virtual Disk (VMDK) recovery..... 168
Emergency Recovery..... 169
File Level recovery..... 170
Monitor recovery operations in the NetWorker Management Web UI 172
vProxy restore from legacy VMware Backup appliance backups.. 172
vProxy file-level restore and SQL restore in the Dell EMC Data Protection Restore Client..... 174
Pre-requisites for file-level restore and SQL restore..... 174
File-level restore and SQL restore limitations.....180
Using the Dell EMC Data Protection Restore Client for file-level restore and SQL restore.....183
vProxy recovery in the vSphere Client's Dell EMC NetWorker interface...196
Connect to the NetWorker server in the vSphere Client..... 196
Recovery to the original virtual machine.....198
Recovery to a new virtual machine..... 200
Virtual disk recovery (restore to an existing virtual machine)..... 203
Instant recovery of a virtual machine.....205
vProxy recovery in the vSphere Web Client's VM Backup and Recovery interface.....207
Connect to the NetWorker server in the vSphere Web Client..... 208
Recovery to the original virtual machine.....208

Recovery to a new virtual machine....210
Virtual disk recovery.... 211
Instant recovery of a virtual machine....213
vProxy recovery log files....215

Chapter 5 VADP Recovery (legacy) 217
Software and hardware requirements.... 218
Limitations and unsupported features.... 218
Limitations to vCenter on non-English versions of Windows.... 219
Limitation for VADP proxy host on non-English versions of Windows 219
Transport modes....219
Independent persistent disks cannot be recovered....220
Configuring the VADP proxy host and Hypervisor resource....220
Creating a Hypervisor resource from the NetWorker server.... 221
Creating a NetWorker client for the VADP Proxy host by using the Client properties windows.... 221
Creating a VADP User role in vCenter.... 223
Creating a VADP Proxy role....223
Assigning the VADP User role to the user specified in the NetWorker Hypervisor resource.... 224
Minimum vCenter permissions needed to recover using VADP.... 224
Recovering VADP Backups....226
File based recovery of a VM.... 226
Image level (single step) recovery of a full VM.... 228
VADP Planning and Best Practices....232
Recommendations and considerations for VADP recovery....233
Selection of physical vs. virtual proxy....233
Recommendations for Data Domain systems....234
Network and Firewall port requirements....235
Support for tape drives in a virtual machine....235
Recommendations and considerations for transport modes....237
VADP proxy access to LUNs....239

Appendix A Backup and recovery of the vCenter server 241
vCenter deployments overview.... 242
Best practices for backup and restore....242
Protecting an embedded PSC.... 243
Restore an embedded PSC with Emergency Recovery....243
Protecting external deployment models.... 244
vCenter server appliance(s) with one external PSC where PSC fails 245
vCenter server appliance is lost but the PSC remains....246
vCenter server appliance with multiple PSCs where one PSC is lost, one remains.... 246
vCenter server appliance remains but all PSCs fail.... 246
vCenter server appliance remains but multiple PSCs fail....247
vCenter server appliance fails.... 247
vCenter server restore workflow....248
Platform Services Controller restore workfow.... 249
Additional considerations....249
Command reference....250
Shutting Down VBA....250

Appendix B **NetWorker VMware Protection in VMware Cloud on Amazon Web Services 253**
Introduction to NetWorker VMware Protection in VMware Cloud on AWS.... 254
Prerequisites..... 254
Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS... 256
NetWorker VMware Protection for VMware Cloud on AWS best practices.... 258
Unsupported NetWorker operations.....259

Appendix C **Regular expressions for NetWorker vProxy dynamic policies rule definitions 261**
Regular expression syntax accepted by dynamic policy rule definition.....262

Appendix D **EMC Backup and Recovery plug-in for Vmware Backup appliance restores 267**
FULLVM (Image-level) Restore.....268
Performing a FULLVM restore.....268
Canceling a FULLVM restore.....269
Instant Access restore (for Data Domain systems only)..... 269
Restore from last backup..... 271
Direct to host recovery.....272

Glossary **275**

FIGURES

1 Components in a NetWorker VMware Protection Solution 18
2 Port requirements for NetWorker VMware Protection with the vProxy appliance..... 23
3 Install vCenter Plugin in NMC..... 47
4 vCenter plug-in for Dell EMC NetWorker in the vSphere Client..... 48
5 vCenter plug-in for Dell EMC NetWorker in the vSphere Client..... 50
6 Hosts and Clusters in the vSphere Web Client..... 56
7 Migrating a VMware Backup appliance policy to vProxy in NMC..... 58
8 Migrate Operation Results dialog..... 58
9 Data Protection Policy..... 67
10 Platinum policy configuration..... 88
11 Changing the Backup Optimization mode in the vProxy protection group..... 96
12 Create a new rule to apply to a VMware group..... 99
13 Specify vProxy Options page..... 102
14 VMware protection policy in the Protection window..... 109
15 VMware protection policy save sets in Media window..... 110
16 Add a vCenter server to VMware View in NMC..... 110
17 Map view of VMware environment in NMC..... 112
18 Cluster with child elements in VMware View..... 113
19 Filtering results in VMware View..... 113
20 VMware table view..... 114
21 Add group in VMware View..... 115
22 Accessing Dell EMC NetWorker in the vSphere Client..... 116
23 NetWorker connection information in the vSphere Client..... 117
24 Dell EMC NetWorker Basic Tasks pane..... 117
25 Policies pane with available vProxy policies..... 118
26 Policy backup options..... 119
27 Recent Tasks pane..... 119
28 Policies pane with available vProxy policies..... 120
29 Edit a vProxy policy..... 120
30 Backup sources in the Editing backup policy dialog..... 121
31 NetWorker connection information in the vSphere Web Client..... 122
32 Backup pane with vProxy policy..... 123
33 Backup sources in the Editing backup policy window..... 124
34 NSR Data Domain Properties..... 142
35 Virtual machine recovery in the NMC Recovery wizard..... 147
36 Select the Virtual Machine to Recover..... 148
37 Select the Target Backup (individual virtual machine)..... 149
38 Select the Target Backup (multiple virtual machines)..... 149
39 Select the Virtual Machine Recovery method..... 149
40 Choose Disks to Revert..... 151
41 Select Alternate Recovery Sources..... 152
42 Configure the Instant Recovery..... 153
43 Configure the virtual machine recovery..... 155
44 Configure the Virtual Disk Recovery..... 156
45 Configure the Emergency Recovery..... 158
46 Select Alternate Recovery Sources for file level recovery..... 160
47 Mount the save set for file level recovery..... 161
48 Select the files and folders to recover..... 162
49 Deploy FLR Agent if not found 174
50 Manage Authentication service users..... 178
51 Application Administrators user group properties 179
52 VMware FLR Users user group properties..... 179
53 Select backups to restore from..... 185

54 Select restore location....185
55 Select items to restore....186
56 Restore Monitoring....186
57 Select the backup(s) to restore from....187
58 Select restore location....188
59 Select items to restore....189
60 Total items available for recovery....189
61 Restore Monitoring....190
62 Select App Backups page....193
63 Restore Target page....193
64 Restore Options page....195
65 Restore Monitoring....196
66 Accessing Dell EMC NetWorker in the vSphere Client....197
67 NetWorker connection information in the vSphere Client....197
68 Dell EMC NetWorker Basic Tasks pane....198
69 Restore pane with available virtual machine backups....199
70 Select Restore from the Action drop-down....199
71 Restore to original location....200
72 Restore pane with available virtual machine backups....201
73 Select Restore from the Action drop-down....201
74 Restore to new virtual machine....202
75 Restore pane with available virtual machine backups....203
76 Select Restore from the Action drop-down....204
77 Restore virtual disks to existing virtual machine....204
78 Restore pane with available virtual machine backups....206
79 Select Restore from the Action drop-down....206
80 Instant Restore....207
81 NetWorker connection information in the vSphere Web Client....208
82 Virtual machines for recovery in the Restore pane....209
83 Select a restore point....209
84 Restore to original location....210
85 Restore options for the new virtual machine recovery....211
86 Select VMDK backup to restore....212
87 Set Restore Options for VMDK recovery....212
88 Set Instant Access restore options....214
89 Finish Instant Access recovery....214
90 Apps and Modules tab in NMC....223
91 Recover Options dialog....227
92 VMware vCenter restore....230
93 vCenter server restore workflow....248
94 PSC restore workflow....249
95 Enable internet access for Forwarders....256
96 Add a vCenter Server to VMware View with Deployed in Cloud enabled....258
97 NSR VMware Proxy Properties....259
98 Restore tab in EMC Backup and Recovery user interface....268
99 Select a backup....270
100 Set instant access options....271
101 Ready to complete....271
102 Emergency Restore window....273

TABLES

1 Revision history....13
2 NetWorker VMware Protection with vProxy appliance requirements....20
3 Incoming port requirements....22
4 Outgoing port requirements....22
5 Performance and scalability factors....26
6 Minimum required vCenter user account privileges....52
7 Location of the vProxy redeployment log files....62
8 Schedule icons....101
9 Schedule icons....106
10 MSVMAPPAGENT binaries called by vProxy....128
11 Supported characters in SQL database names....130
12 SQL Skipped Database Cases and Descriptions....135
13 Backup log files....137
14 FLR privilege requirements....177
15 Recovery log files....215
16 Application information values....221
17 VADP recovery privileges....224

Preface

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

Contact your Dell EMC technical support professional if a product does not function correctly or does not function as described in this document.

Note: This document was accurate at publication time. Go to Dell EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This document describes the integration of VMware with NetWorker.

Audience

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

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
04	August 5, 2019	The following changes are done in the guide: • A new topic on shutting down VBA is added. • The topics“ Data Domain system configuration” and “Performance and scalability” are updated.
03	July 19, 2019	Fixed a few typographical errors.
02	July 09, 2019	The following changes are done in the guide: • A topic is added in “vProxy limitations and unsupported features”. • Data domain requirements are updated in the topic “System Requirement”.
01	March 20, 2019	First release of this document for NetWorker 19.1.

Related documentation

The NetWorker documentation set includes the following publications, available on the Support website:

- *NetWorker E-LAB Navigator*

Provides compatibility information, including specific software and hardware configurations that NetWorker supports. To access E-LAB Navigator, go to https://elabnavigator.emc.com/eln/elnhome.

- *NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *NetWorker Network Data Management Protocol (NDMP) User Guide*
  Describes how to use the NetWorker software to provide data protection for NDMP filers.
- *NetWorker Cluster Integration Guide*
  Contains information related to configuring NetWorker software on cluster servers and clients.
- *NetWorker Installation Guide*
  Provides information on how to install, uninstall, and update the NetWorker software for clients, storage nodes, and servers on all supported operating systems.
- *NetWorker Updating from a Previous Release Guide*
  Describes how to update the NetWorker software from a previously installed release.
- *NetWorker Release Notes*
  Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.
- *NetWorker Data Domain Boost Integration Guide*
  Provides planning and configuration information on the use of Data Domain devices for data deduplication backup and storage in a NetWorker environment.
- *NetWorker Performance Optimization Planning Guide*
  Contains basic performance tuning information for NetWorker.
- *NetWorker Server Disaster Recovery and Availability Best Practices Guide*
  Describes how to design, plan for, and perform a step-by-step NetWorker disaster recovery.
- *NetWorker Snapshot Management Integration Guide*
  Describes the ability to catalog and manage snapshot copies of production data that are created by using mirror technologies on storage arrays.
- *NetWorkerSnapshot Management for NAS Devices Integration Guide*
  Describes how to catalog and manage snapshot copies of production data that are created by using replication technologies on NAS devices.
- *NetWorker Security Configuration Guide*
  Provides an overview of security configuration settings available in NetWorker, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- *NetWorker VMware Integration Guide*
  Provides planning and configuration information on the use of VMware in a NetWorker environment.
- *NetWorker Error Message Guide*
  Provides information on common NetWorker error messages.
- *NetWorker Licensing Guide*

Provides information about licensing NetWorker products and features.

- *NetWorker REST API Getting Started Guide*
  Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.
- *NetWorker REST API Reference Guide*
  Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.
- *NetWorker 19.1 with CloudBoost 19.1 Integration Guide*
  Describes the integration of NetWorker with CloudBoost.
- *NetWorker 19.1 with CloudBoost 19.1 Security Configuration Guide*
  Provides an overview of security configuration settings available in NetWorker and Cloud Boost, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- NetWorker Management Console Online Help
  Describes the day-to-day administration tasks performed in the NetWorker Management Console and the NetWorker Administration window. To view the online help, click **Help** in the main menu.
- NetWorker User Online Help
  Describes how to use the NetWorker User program, which is the Windows client interface, to connect to a NetWorker server to back up, recover, archive, and retrieve files over a network.

CHAPTER 1

Introduction to NetWorker VMware Protection with the vProxy appliance

This chapter contains the following topics:

- Introduction to NetWorker VMware Protection with vProxy appliance 18
- Components in the NetWorker VMware Protection Solution with vProxy appliance 18
- System requirements 19
- Compatibility information 21
- Port requirements 22
- NetWorker VMware Protection Solution best practices with the vProxy appliance 23
- Performance and scalability 26
- Configuration checklist 28
- vProxy limitations and unsupported features 29
- Accessing Knowledge Base Articles 33

Introduction to NetWorker VMware Protection with vProxy appliance

NetWorker provides you with the ability to perform virtual machine protection and recovery by using the NetWorker VMware Protection solution with the vProxy appliance, also known as NVP.

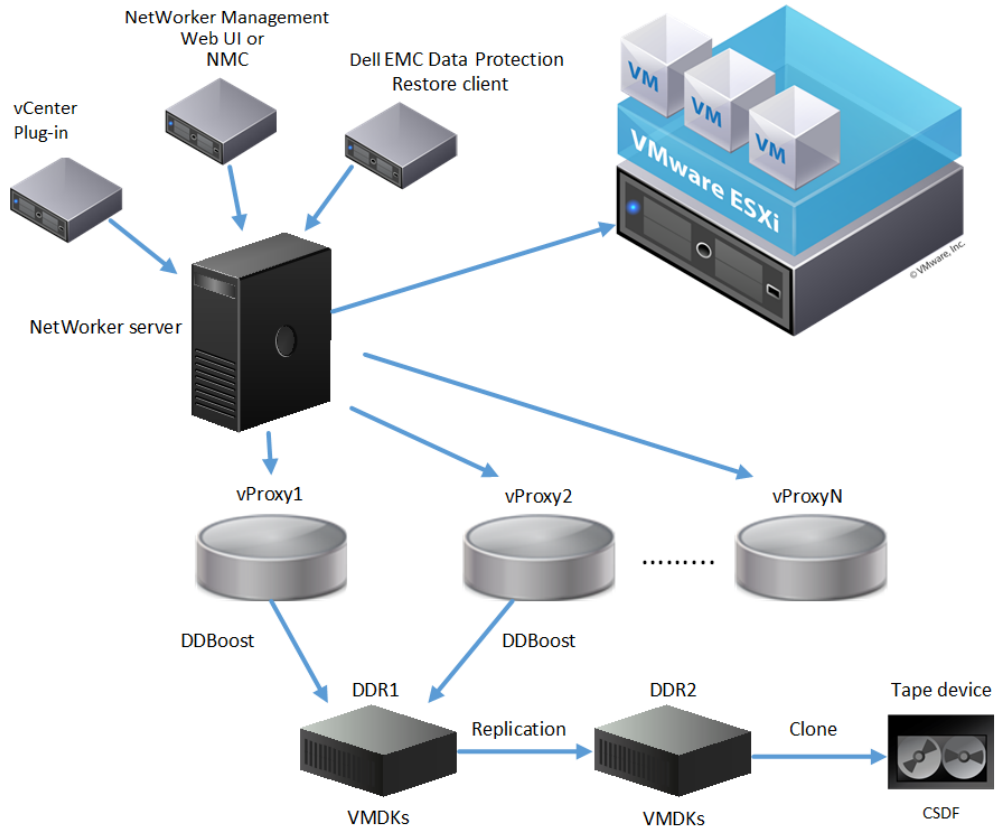
NVP features the following:

- Uses standalone data-mover proxy appliances, or vProxy appliances, to backup and restore virtual machines that run in a virtualized infrastructure, with the ability to offload the data mover from NetWorker and run the backup as a virtual workload.
- NetWorker directly manages the vProxy appliances without the use of an external node for proxy management and load balancing.
- Stores the virtual machine backups as raw virtual machine disk files (VMDKs) on the Data Domain device, which reduces overhead. NetWorker does not convert the backup to any backup streaming formats.
- Provides the ability to clone virtual machine backups. When you use streaming devices such as tape, NetWorker converts the save set directories format (SSDF) to Common Data Storage Format (CDSF) during a clone operation, and converts back to SSDF on Data Domain for recovery from streaming devices.
- Provides user interfaces to perform image-level recovery or file-level recovery.

Components in the NetWorker VMware Protection Solution with vProxy appliance

The following section provides a high-level overview of the components in the NetWorker VMware Protection Solution with the vProxy appliance.

Figure 1 Components in a NetWorker VMware Protection Solution



The solution contains the following components:

- vProxy appliances—Provide the data movement services between the VMware host and the target protection storage, for example Data Domain.
- NetWorker server—Provides the ability to manage vProxy appliances, configure data protection policies for backup and clone operations. Integrates with file-level restore to provide centralized management in a virtual environment.
- NetWorker Management Web UI and NMC—Provides the ability to start, stop, and monitor data protection policies and perform recovery operations.
- Dell EMC Data Protection Restore client—Provides the ability to perform file-level restore by using a web interface.
- vCenter plug-in—Backup and recovery operations for VMware policies. Displays as Dell EMC NetWorker in the vSphere Client or VM Backup and Recovery in the vSphere Web Client.
- DDR1 and DDR2—Data Domain appliances that receive and clone backup data in SSDF format.
- Tape device—Media that receives backup data in CDSF format.

System requirements

The following table lists the required components for NetWorker VMware Protection with the vProxy appliance.

When you install or upgrade NetWorker and deploy the vProxy appliance, ensure that the NetWorker server and storage node are at the same version, and that you use the latest version of the vProxy appliance.

Note: For more compatibility details and the most up-to-date versions supported, refer to the NetWorker compatibility matrix at https://elabnavigator.emc.com/eln/modernHomeDataProtection

Table 2 NetWorker VMware Protection with vProxy appliance requirements

Component	Requirements
NetWorker	• NetWorker 19.1 server software with NMC. The NetWorker storage node should be the same version as the NetWorker server. • The vCenter plug-in (HTML5 or flash-based) requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.
vProxy Appliance	Version 4.0. System requirements for the vProxy include: • CPU: 4 * 2 GHz (4 virtual sockets, 1 core for each socket). • Memory: 8GB. • Disks: 2 disks (59 GB and 98 GB). • Internet Protocol: IPv4 only. • SCSI controller: Maximum 4. • NIC: One vmxnet3 NIC with one port.
vCenter server	• 6.0, 6.0U1, 6.0U2, 6.0U3, 6.5, 6.5U1, 6.5U2, 6.7, 6.7U1, 67U2. • Version 6.5 and later is required to perform Microsoft SQL Server application-consistent protection. • Linux or Windows platform, or VC appliance. **Note:** The NetWorker compatibility matrix at https://elabnavigator.emc.com/eln/modernHomeDataProtection provides detailed information on NetWorker and vCenter/vSphere version compatibility.
ESX/ESXi server	• 6.0, 6.0U1, 6.0U2, 6.0U3, 6.5, 6.5U1, 6.5U2, 6.7, 6.7U1, 67U2. • Version 6.5 and later is required to perform Microsoft SQL Server application-consistent protection. • Automatically enables Changed Block Tracking (CBT) on each virtual machine. **Note:** The NetWorker compatibility matrix at https://elabnavigator.emc.com/eln/modernHomeDataProtection provides detailed information on NetWorker and vCenter/vSphere version compatibility.
VMware Tools	• VMware Tools version 10 or later. VMware Tools version 10.1 or later is required to perform Microsoft SQL Server application-consistent protection.

Table 2 NetWorker VMware Protection with vProxy appliance requirements (continued)

Component	Requirements
	• Open VM Tools, version support as outlined in the VMware Software Compatibility Guide.

Data Domain	• A minimum of one configured DD Boost device is required. Additionally, you must specify one pool that contains the DD Boost device.
	• Data Domain system OS at DDOS version 6.0.x, 6.1.x, 6.2.x.
	• A Data Domain user account with administrator privileges, which you will use to manage file-level restore and instant access restore.
	• NFS v3 is enabled and running. This is required for the file-level restore and instant recovery operations.
	Note:
	• The NetWorker compatibility matrix at https://elabnavigator.emc.com/eln/modernHomeDataProtection provides detailed information on NetWorker and DD Boost version compatibility
	• Ensure that the NFS "default-export-version" is set to 3 on the Data Domain by running the following command on Data Domain console:
	`sysadmin@XXXXXXXX# nfs option set default-export-version 3`
	You can check the default-export-version value by running the following CLI command on the Data Domain console
	`sysadmin@XXXXXXXX# nfs option show all`

Compatibility information

The NetWorker Online Compatibility matrix provides software compatibility information for the NetWorker release, which includes NetWorker VMware Protection with the vProxy appliance.

The guide is available at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

Note: For compatibility information related to the Microsoft VM App Agent for SQL Server application-consistent protection, refer to the NMM support matrix.

Port requirements

The NetWorker VMware Protection solution requires the ports outlined in the following tables.

Note: The vProxy appliance does not support the use of a non-default vCenter HTTPS port. To perform data protection operations using the vProxy appliance, ensure that your vCenter server uses the default 443 HTTPS port.

Table 3 Incoming port requirements

From	To	Port	Purpose
NetWorker server	vProxy appliance	9090	NetWorker VMware Protection web service calls to initiate and monitor backups, image recoveries, and granular recoveries.
NetWorker server	vCenter server	443	**VMware View** in NMC **NetWorker Administration**.
NetWorker server	ESXi server	443	Emergency restore, vProxy redeployment
vCenter server	NetWorker server	9090	vSphere Client's **VM Backup and Recovery** plug-in
Dell EMC Data Protection Restore Client interface	NetWorker server	9090	File-level recovery in the **Dell EMC Data Protection Restore Client**
ESXi servers	Data Domain	111, 2049, 2052	File-level recovery and instant recovery
Virtual machines	Data Domain	111, 2049	SQL application-consistent backup

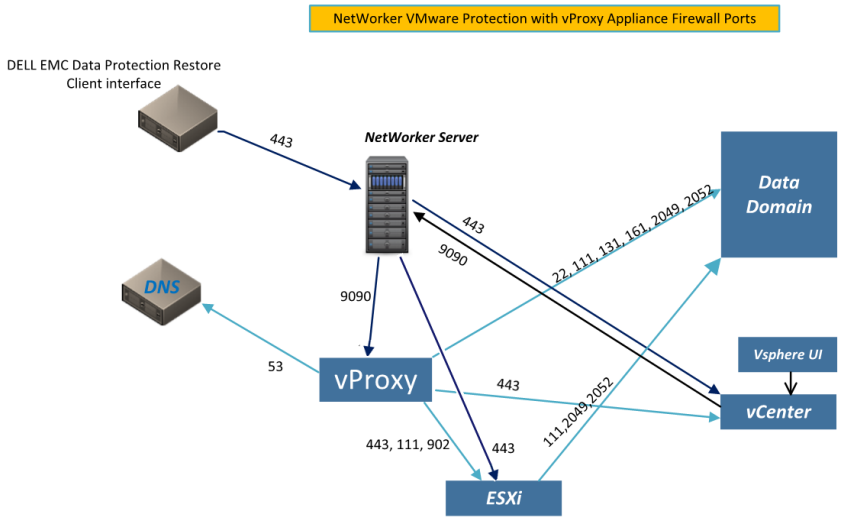
Table 4 Outgoing port requirements

From	To	Port	Purpose
vProxy Appliance	DNS	53	Name resolution
vProxy Appliance	Data Domain	22, 111, 131, 161, 2049, 2052	Data Domain management
vProxy Appliance	ESXi server	443, 902	Backup and recovery operations
vProxy Appliance	vCenter server	443	vProxy registration, backup and recovery operations.

Table 4 Outgoing port requirements (continued)

From	To	Port	Purpose
			Note: Using a non-default vCenter port for HTTPS is not supported.

Figure 2 Port requirements for NetWorker VMware Protection with the vProxy appliance



NetWorker VMware Protection Solution best practices with the vProxy appliance

Observe the following best practices when using the NetWorker VMware Protection Solution with the vProxy appliance.

Software recommendations

Review the following software recommendations:

- Ensure that the NetWorker server and storage node are at the same version, and that all the vProxy appliances you deploy are compatible with this version.
- The vCenter plug-in (HTML5 or flash-based) requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.
- Install **VMware Tools** on each virtual machine by using the **vSphere Web Client**. VMware Tools adds additional backup and recovery capabilities that quiesce certain processes on the guest operating system prior to backup. For Linux operating systems, ensure that you install a supported **Open VM Tools** package, as outlined in the VMware Software Compatibility Guide.
- Installation of third-party tools or applications in the virtual appliance for the purposes of monitoring the appliance status and protecting the appliance from computer viruses can have a negative impact on system performance. Therefore,

it is recommended that you do not install any additional tools or applications in the appliance.

Configuration recommendations

- Ensure that the vCenter server's **Datastore Browser** feature (`enableHttpDatastoreAccess`) is enabled to allow the backup and restore operations to browse the datastores in the vSphere environment. The feature is enabled by default, but you can verify that the vCenter `vpxd.cfg` file does not contain the `enableHttpDatastoreAccess` entry or that it is set to **True**. For further details, refer to the VMware Knowledge Base article at https://kb.vmware.com/s/article/2101567.
- vProxy remote site configurations with a storage node communication latency greater than 50 ms require a storage node in the remote site.
- For best practices related to SQL Server application-consistent protection, review the software and security requirements in the section Enable the Microsoft VM App Agent for SQL Server application-consistent protection.
- During policy configuration, assign virtual machines to a protection group based on logical grouping to allow for better scheduling of backups that will help you avoid resource contention and create more organized logs for review.
- When you plan the backups, ensure that NetWorker VMware Protection supports the disk types that you use in the environment. Currently, NetWorker VMware Protection does not support the following disk types:
  - Independent (persistent and non-persistent)
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode

  For RDM Dependent - Virtual Compatibility Mode, vProxy supports backup and restore with the following limitations:
  - Recover to New Virtual Machine will recover the vRDM disk as a regular thick eager zeroed VMDK disk to the datastore selected during the restore.
  - Instant Restore of Virtual Machine will recover the vRDM disk as a regular thick eager zeroed VMDK disk.
  - Revert a Virtual Machine does not support the **Revert VM configuration** option if the backup includes a vRDM disk. Ensure that you do not select this option during such restores.
- The vProxy Appliance leverages Changed Block Tracking (CBT) by default. If CBT is disabled on the virtual machine, then it will enable CBT automatically. If you add a disk to the virtual machine after the first full backup, for the next policy run a full backup will be performed automatically for the newly added disk, and an incremental backup will be performed for the existing disk. For information on disabling CBT, refer to the section Enabling or disabling Changed Block Tracking.
- When backing up thin-provisioned Virtual Machines or disks for Virtual Machines on NFS datastores, an NFS datastore recovery does not preserve thin provisioning. VMware knowledge base article 2137818 at http://kb.vmware.com/kb/2137818 provides more information.
- It is recommended that you set an appropriate NetWorker server/storage parallelism value, according to the available resources, to reduce queuing. For example, 5 vProxy appliances with backup and clone operations will require more than 125 parallel sessions. Therefore, setting the parallelism for the NetWorker server to 128 or higher (while also setting the server with 32+ GB memory and 8+

CPUs) will suit such an environment. The *NetWorker Performance Optimization Planning Guide* provides more details.

- If you require a larger number of parallel image backups, also consider setting the maximum number of vCenter SOAP sessions to larger value. Note that this requires careful planning and additional resources on the vCenter Server You can configure this by modifying the following line in the vCenter `vpxd.cfg` file:
  `<vmacore><soap><maxSessionCount> N </maxSessionCount></soap></vmacore>`

  This applies specifically to SDK sessions as opposed to VI client sessions.
- Each Virtual Machine backup to a Data Domain system consumes more than one session on the Data Domain device. The default device configuration is `target sessions=20` and `max session=60`, however it is recommended that you configure additional devices for more than 10 parallel backups.
- Virtual Machines with extremely high IO may face hangs during consolidation due to the ESXi forced operation called synchronous consolidate. Plan your backups of such Virtual Machines according to the amount of workload on the Virtual Machine.
- When you work with the vCenter database either directly or by using scripts, do not change the name attribute for the `vmfolder` object. VMware knowledge base article at https://support.emc.com/kb/190755 provides more information.
- Resource contention can occur at various points during the backup cycle. When NetWorker runs larger policies, issues due to contention of resources can occur, which impact all running operations. Adjust your resources and times for other larger policies to avoid overlaps, and avoid resource contention.
  For example, you configure one pool named Bronze, with one device. If you set up a policy where every day at 10 pm two policies called 'Bronze1' and 'Bronze2' with 400 virtual machines each start writing to the device in the 'Bronze' pool, then the long wait for device availability may cause unexpected delays or timeouts. To fix this, set the policy start times 4 hours apart and add more devices, to allow for stable backups.

Transport mode recommendations

Review the following recommendations for transport mode settings:

- Use hotadd transport mode for faster backups and restores and less exposure to network routing, firewall, and SSL certificate issues. The vProxy appliance currently supports a maximum of 25 concurrent hotadd sessions. To support hotadd mode, deploy the vProxy on an ESXi host that has a path to the storage that holds the target virtual disk(s) for backup.
- Hotadd mode requires VMware hardware version 7 or later. Ensure that all virtual machines that you back up with Hotadd mode are using Virtual Machine hardware version 7 or later.
- For sites that contain a large number of virtual machines that do not support hotadd requirements, NBD transport mode will be used. This can cause congestion on the ESXi host management network. Plan your backup network carefully for large scale NBD installs. You may consider configuring one of the following options:
  - Set up Management network redundancy.
  - Set up backup network to ESXi for NBD.

  - Set up storage heartbeats. http://www.vmware.com/files/pdf/techpaper/vmw-vsphere-high-availability.pdf provides more information.
- Avoid deploying VMs with IDE virtual disks; using IDE virtual disks degrades backup performance. Use SCSI virtual disks instead whenever possible.
  Note: You cannot use hotadd mode with IDE Virtual disks and therefore backup of these disks will be performed using NBD mode.
- If you have vFlash-enabled disks and are using hotadd transport mode, ensure that you configure the vFlash resource for the vProxy host with sufficient resources (greater than or equal to the virtual machine resources), or migrate the vProxy to a host with vFlash already configured. Otherwise, backup of any vFlash-enabled disks will fail with the error "VDDK Error: 13: You do not have access rights to this file," and the error "The available virtual flash resource '0' MB ('0' bytes) is not sufficient for the requested operation" on the vCenter server.
- If you only want to use one transport mode, ensure that you set the maximum sessions value for the other transport mode to 0. For example, if you want to use hotadd mode only set hotadd = 25 and nbd = 0. If you want to use NBD mode only, set hotadd = 0 and nbd = 10.
- In order for backup and recovery operations to use Hotadd mode on a VMware Virtual Volume (VVol) datastore, the vProxy should reside on the same VVol as the virtual machine.

Performance and scalability

Performance and scalability of the NetWorker VMware Protection Solution depends on several factors, including the number of vCenter servers and proxies and the number of concurrent virtual machine backups. The following table provides information on these scalability factors and maximum recommendations, in addition to concurrency recommendations for sessions created from backups of the vProxy appliance. The count of sessions is driven by the number of proxies, clone jobs, and other backups running through this server. Each vProxy Appliance can run up to 25 sessions.

Table 5 Performance and scalability factors

Component	Maximum limit	Recommended count	Notes
Number of concurrent hotadd backups per proxy	25	13	It is recommended to use 13 hotadd sessions to achieve optimal performance.
Number of concurrent NBD backups per proxy	25		It is recommended to use hotadd transport mode for optimal performance. When using VMware NBD mode, use of 10G network is recommended.
Number of concurrent NBD backups per vCenter server	50 (10G network)		VMware uses Network File Copy (NFC) protocol to read VMDK using NBD transport mode. You need one VMware NFC connection for each VMDK file being backed up. The VMware Documentation provides more information on vCenter NFC session connection limits.
Virtual machines concurrent backups per vCenter server	100	100	Can be achieved with a combination of the number of proxies multiplied by the number of configured hotadd sessions per vProxy.

Table 5 Performance and scalability factors (continued)

Component	Maximum limit	Recommended count	Notes
Number of proxies per vCenter		8	8 proxies with 12-13 hotadd sessions on each proxy can protect 100 virtual machines concurrently. If more than 8 proxies are required per vCenter, configure the hotadd limits on the proxies to ensure that no more than 100 proxy streams run concurrently against any given vCenter.
Number of workflows per VMware policy	64	8	Ensure that you do not to exceed 2000 virtual machines per VMware policy.
Number of virtual machines per workflow	2000		Ensure that you do not to exceed 2000 virtual machines per VMware policy. Note that the maximum of 2000 virtual machines per workflow is only applicable to the first FULL backup to Data Domain, and does not apply to CBT-based incremental backups of the virtual machines. However, ensure that you do not exceed 100 connections per vCenter at any time during the backup window.
Number of vCenter servers per policy	5	3	Per policy you can use 5 vCenter servers in the respective workflows and trigger concurrent backups.
Number of concurrent recoveries		50	It is recommended to use hotadd transport mode for recoveries. For large concurrent restores, it is highly recommended that multiple target datastores are used for optimal performance
Number of files/directories per file level recovery (User and Admin mode)	20000 or less		File-level recovery is recommended for quickly recovering a small set of files. Image-level or VMDK-level recoveries are optimized and recommended for recovering a large set of files/folders.
Number of parallel instant access sessions	32		You can perform up to 32 parallel instant recovery sessions using `nsrvproxy_recover`, provided that you satisfy the following prerequisites: • For the backups being restored, you must select **Performance** backup optimization mode during VMware type group creation in NMC. • If you are using DDOS version 6.0.x, then minimum Data Domain OS version 6.0.0.30 is required • Data Domain platforms supported include DD6300 (EOS-T2), DD6800 (EOS-T3), DD9300 (EOS-T4), and DD9800. • The ESXi host requires the following default values to be updated to the maximum supported: Under NFS, update **NFS.MaxVolumes**. Under Net, update **Net.TcpipHeapSize**. Under Net, update **Net.TcpipHeapMax**.

Table 5 Performance and scalability factors (continued)

Component	Maximum limit	Recommended count	Notes
			The VMware knowledgebase article at https://kb.vmware.com/kb/2239 provides more information. Additionally, refer to the VMware Documentation for concurrent virtual machine migration limits.
Total number of virtual machines in a single NetWorker policy	2000	1000	You can run multiple vProxy policies concurrently as long as the total number of concurrent backup streams does not exceed the vCenter limits indicated in this table. In the case of a single vCenter, stagger the schedules for policies to ensure that all the backups for a policy complete before the backups of the next policy begin.
Backup Optimization modes			During creation of a VMware type group in NMC, you can select a backup optimization mode of either **Capacity** or **Performance**. **Performance** mode results in additional space use on the Data Domain device (around 20%) but significantly improves random I/O performance for instant access restores.

Configuration checklist

The following configuration checklist provides best practices and troubleshooting tips that might help resolve some common issues.

Basic configuration

- Synchronize system time between vCenter, ESX/ESXi/vSphere, and the vProxy appliance
- Assign IPs carefully — do not reuse any IP address
- Use FQDNs (Fully Qualified Domain Names) everywhere
- For any network related issue, confirm that forward and reverse DNS lookups work for each host in the datazone.

Data Domain system configuration

- All Data Domain systems should be upgraded to a supported DDOS version for the NetWorker VMware Protection solution.
- The Data domain Retention Lock feature for vProxy backup and clone actions requires DDOS version 6.1.
- Ensure that the Data Domain system does not reach the MTree limit and max-streams limit.
- Ensure that only devices from the same Data Domain system host appear in Data Domain system pool when used in any Action.

- Check the NFS settings and ensure that NFS v3 is enabled and running. If NFS v4 is enabled, ensure NFS v3 is also set to enabled in order to avoid issues with file-level restore operations or instant recovery operations.
- For virtual machines within in application-consistent data protection policy, network zoning must be configured to enable network connectivity between the virtual machines and the Data Domain system.

NetWorker configuration

- Ensure that the relevant devices are mounted.
- Ensure that vProxy IP addresses are populated in DNS, and that the NetWorker server has name resolution for the vProxy host names.
- The vCenter plug-in requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.
- Wait until you successfully configure a policy before you run the policy.
- A message appears after successful vProxy registration in NMC.

Virtual machine configuration

- Ensure that the virtual machine network is zoned for access to Data Domain.
- Ensure that the virtual machine has name resolution for the Data Domain system, if applicable.
- Ensure that the virtual machine firewall has port rules for Data Domain.
- Ensure that Microsoft SQL Server instances are enabled for data protection using a SYSTEM account, as described in the software and security requirements section of the topic Enable the Microsoft VM App Agent for SQL Server application-consistent protection.

vProxy limitations and unsupported features

Before you deploy the NetWorker VMware Protection Solution with the vProxy appliance, review the following limitations and unsupported features.

vCenter server using non-default HTTPS port is not supported

The vProxy appliance does not support the use of a non-default vCenter HTTPS port. To perform data protection operations using the vProxy appliance, ensure that your vCenter server uses the default 443 HTTPS port.

VMware limitations by vSphere version

VMware limitations for vSphere 6.0 and later versions are available at https://configmax.vmware.com/home.

vCenter plug-in requires NetWorker server and NetWorker Authentication services running on the same machine

The vCenter plug-in (HTML5 or flash-based) does not support running the NetWorker server and NetWorker Authentication service on different machines. Ensure that both are running on the same machine.

Limitations to SQL Server application consistent data protection

Review the SQL Server application-consistent protection support limitations in the section Enable the Microsoft VM App Agent for SQL Server application-consistent protection.

Network configuration settings do not get restored with virtual machine after recovery of a vApp backup

Network configuration settings are not backed up with the virtual machine as part of a vApp backup in NetWorker. As a result, when you restore a vApp backup, you must manually reconfigure the network settings.

vCenter version not updated in RAP database after upgrade

When you upgrade vCenter, the vCenter version does not get updated immediately in the RAP database since NetWorker does not periodically query vCenter. After the upgrade, refresh **VMware View** in NMC's **Administration** window for the vCenter version to update.

Concurrent vProxy workflows on the same virtual machine is not supported when not using a vCenter server

NetWorker does not support running multiple vProxy workflows concurrently (backup, image-level recovery, or file-level restore operations) on the same virtual machine when not using a vCenter server in your environment.

Data Domain system requires REPLICATION license when clone of VMware backup performed to same system as the backup

When cloning VMware backups using NetWorker VMware Protection with the vProxy appliance, if the clone is performed to the same Data Domain system as the backup, a REPLICATION license is required on the Data Domain system.

No new policies can be created or run with VMware Backup appliance

After upgrading to a NetWorker 18.x release with the vProxy appliance, new policies can only be created with the vProxy appliance. You cannot run or edit existing VMware Backup Appliance policies, and once you delete a VMware Backup appliance policy, it is no longer available.

Virtual machine alert "VM MAC conflict" may appear after successful recovery of virtual machine

After performing a successful recovery of a virtual machine through vCenter version 6, an alert may appear indicating a "VM MAC conflict" for the recovered virtual machine, even though the new virtual machine will have a different and unique MAC address. You must manually acknowledge the alert or clear the alert after resolving the MAC address conflict. Note that this alert can be triggered even when the MAC address conflict is resolved.

The VMware release notes at http://pubs.vmware.com/Release_Notes/en/vsphere/60/vsphere-vcenter-server-60u2-release-notes.html provide more information.

Emergency recovery cannot be performed until vProxy registration event successful with NetWorker

When deploying a new vProxy that is not yet registered with NetWorker, wait for the registration event to complete successfully with NetWorker before performing an emergency recovery in the NMC Recovery wizard. The event will appear in the logs and in NMC.

Datastore names cannot contain special characters

Using special characters in datastore names can cause problems with the vProxy, such as failed backups and restores. Special characters include the following: `% & * $ # @ ! \ / : * ? " < > | ;`, and so on.

Backups fail for resource pools recreated with the same name as deleted pool

When you delete a resource pool in vCenter and then recreate a resource pool with the same name, backups fail. Re-configure the protection group with the newly created resource pool.

Data Domain Boost over fibre channel not supported

The NetWorker VMware Protection Solution does not support Data Domain Boost over fibre channel (DFC).

Data Domain SMT not supported

The NetWorker VMware Protection Solution does not support Data Domain SMT. You can create different DDBoost users to segregate access to specific DD Boost devices. However DD Admin credentials are required for performing instant access and file-level restore workflows.

Only hotadd and NBD transport modes supported

The NetWorker VMware Protection Solution supports only the hotadd and NBD transport modes. The hotadd mode is the default transport mode. If you want to use both modes, the *maximum sessions* value for each must be set to the same non-zero value. For example, set hotadd = 13 and nbd = 13. If you only want to use one transport mode, ensure that you set the maximum sessions value for the other transport mode to 0. For example, if you want to use hotadd mode only, set hotadd = 25 and nbd = 0.

Note: If upgrading to NetWorker 18.1 and later from a previous release where the hotadd and nbd transport modes were configured with different non-zero values for *maximum sessions*, ensure that you change these settings to the same non-zero value. Setting different non-zero values for both transport modes is not supported in NetWorker 18.1 and later.

Specify NBD for datastores if proxies should use NBD mode only

For proxies that only use NBD transport mode (proxies where you specify a value greater than 0 for the NBD maximum sessions limit), you must also specify the datastores for which you want the proxy to perform only NBD backups to ensure that any backups of virtual machines running on these datastores are always performed using NBD mode. This also ensures that the same NBD-only proxies are never used for backups of virtual machines residing on any other datastores.

Backup of individual folders within a Virtual Machine is not supported

The NetWorker VMware Protection Solution only supports image-level backup and disk-level backup. You cannot perform backups of individual folders within the Virtual Machine.

Retries, Retry Delay, and the Inactivity Timeout options for VMware backup action are not supported

The **Retries**, **Retry Delay**, and the **Inactivity Timeout** options that appear during creation of a VMware backup action in the **NetWorker Management Web UI** and **NMC** are not supported. You can ignore these options when creating the backup action.

VMware View in the NetWorker Administration map view does not display when configuration for Virtual Machines within the vCenter is incomplete

When you use VMware View, the map view does not appear when the configuration for one or more Virtual Machines in the vCenter is incomplete. To

avoid this issue, remove the incomplete Virtual Machine configurations from vCenter.

I/O contention when all Virtual Machines on a single data store

I/O contention may occur during snapshot creation and backup read operations when all Virtual Machines reside on a single datastore.

No automatic migration tool to move from previous solution to NetWorker VMware Protection with the vProxy appliance

An automatic migration tool to move from the previous virtual machine backup solution to the NetWorker VMware Protection with vProxy appliance solution does not exist.

VMware snapshot for backup is not supported for independent disks

When using independent disks you cannot perform VMware snapshot for backup.

Cannot select a vProxy or the cloned vProxy when you create a VMware group

When you create a new protection group, you cannot select vProxy or clones of the vProxy from the hosts list. To use the clone vProxy as a normal virtual machine, clear the annotation string `This is EMC Backup and Recovery vProxy Appliance` in the **Notes** section of the cloned vProxy virtual machine.

Restricted data zones not supported

NetWorker VMware Protection with the vProxy appliance does not currently support the protection of virtual machines within a Restricted Data Zone. When you create a VMware policy in NMC, ensure that you leave the **Restricted Data Zone** field blank.

RDM Dependent - Virtual Compatibility Mode limitations

For RDM Dependent - Virtual Compatibility Mode, vProxy supports backup and restore with the following limitations:

- Recover to New Virtual Machine will recover the vRDM disk as a regular thick eager zeroed VMDK disk to the datastore selected during the restore.
- Instant Restore of Virtual Machine will recover the vRDM disk as a regular thick eager zeroed VMDK disk.
- Revert a Virtual Machine does not support the **Revert VM configuration** option if the backup includes a vRDM disk. Ensure that you do not select this option during such restores.

Datastore cluster does not display in the Datastore selection drop-down of NMC Recovery wizard for Virtual Machine Recovery or Virtual Disk Recovery types

If a vCenter server contains a datastore cluster, the datastore cluster name does not display for selection during image-level recoveries using either the **Virtual Machine Recovery** or **Virtual Disk Recovery** types in the NMC **NetWorker Administration Recovery** wizard. When performing the recovery to a datastore cluster, ensure that you select any valid datastore within the cluster that contains enough free space to accommodate the virtual machine.

File level restore, emergency restore or Instant access restore on dual NIC vProxy is supported only if VMkernel port is connected to backup subnet/VLAN

In order to use Instant Access restore, emergency restore, and file-level restore with vproxy having dual NIC or multiple isolated VLANs configured, the destination ESXi requires a VMkernel port connected to the backup subnet/ VLAN.

Registration of a vProxy to multiple NetWorker servers is not supported

You cannot register a vProxy to multiple NetWorker servers. You must unregister the vProxy from previous Networker server before registering it to another NetWorker server. If you are unable to register the vProxy with another Networker server, then check vProxy state and ensure that it is in the UNREGISTERED state.

Accessing Knowledge Base Articles

Additional troubleshooting information is available through the Featured VMware Documentation Sets website at https://www.vmware.com/support/pubs/. Select **Support > Search Knowledge Base**.

CHAPTER 2

Deploy the vProxy appliance and configure the NetWorker datazone

This chapter contains the following topics:

- Deploying the vProxy appliance 36
- VMware vCenter server management 40
- Configuring and registering the vProxy appliance 43
- Installing the vCenter plug-in 46
- Accessing the HTML-5 or flash-based vCenter plug-in as a non-administrator Active Directory user 50
- Creating a dedicated vCenter user account and VM Backup and Recovery role 51
- Migrating policies from VMware Backup appliance to vProxy appliance 57
- Resetting the admin account password 59
- Upgrading the vProxy appliance 60

Deploying the vProxy appliance

You can deploy the vProxy appliance from either of the following:

- The vCenter server.
- The ESXi host.

Registration and configuration of the vProxy appliance must then be completed in the NMC **NetWorker Adminstration** window's **VMware Proxy Configuration wizard**, or the NetWorker Management Web UI.

Deploy the vProxy OVA on a vCenter server

When deploying the vProxy OVA on a vCenter server, configure the host with a trusted SSL certificate, and then perform the following steps to deploy the OVA for the vProxy host from a vCenter server by using the vSphere Web Client.

Before you begin

Install or upgrade to the latest version of the VMware Client Integration Plug-in. This plug-in is required to run the vSphere Web Client. Download information is provided in the knowledgebase article at https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2145066.

Procedure

1. Log in to the **vSphere Client** with an administrator account.
2. In the Main menu, expand **vCenter** and then expand **Hosts**.
3. Right-click the ESXi host on which you will deploy the OVA and select **Deploy OVF template**.
4. On the **Source** window, type a URL path to the OVA package or click **Browse** and navigate to the OVA package location, and then click **Next**.
5. On the **Review details** window, review the product details such as the product name, version, vendor, publisher, and download size, and then click **Next**.
6. On the **Accept License Agreements** window, the EULA appears. Review the EULA and then click **Accept**.
7. On the **Select name and folder** window, specify a name for the virtual appliance, and optionally the inventory location, for example a datacenter or VM folder. Click **Next**.
8. On the **Select storage** window, select disk format and the destination datastore on which to store the virtual appliance files and then click **Next**.

   It is recommended that you select **Thick Provision Lazy Zeroed** to ensure that amount of storage space allocated to the virtual appliance is available.
9. (Optional) On the **Select resource** window, select the host, vApp, or resource pool in which to deploy the OVA, and then click **Next**.
10. On the **Select networks** window, select the **Source** and **Destination** networks to use with the appliance.

    Note: Ensure that the destination network(s) are mapped to the correct source network, otherwise vProxy will fail to register to the NetWorker server. The source network **VM Network** should map to your “vProxy Production network” portgroup, which is the network portgroup with access to the backup application server, vCenter, and ESXi hosts. If your

Data Domain backup data also uses the same "vProxy Production network" portgroup, then you can ignore **VM Network 2**. Otherwise, ensure that you assign the networks according to the following considerations:

- If the Data Domain backup data uses a separate private or isolated physical network, use the optional **VM Network 2** and map this network to your desired destination network portgroup.
- If the Data Domain backup data uses a separate private or isolated physical network, **VM Network 2** should map to the "vProxy Backup Data network" portgroup, which is the network with access to the Dell EMC Data Domain, as indicated in the description when the network is selected.

11. Select **IPv4** from the **IP protocol** drop-down, and then click **Next**.
12. On the **Customize template** window, specify the following attributes, and then click **Next**.
    a. Expand **Networking properties**, and then perform the following tasks:
    - In the **Network IP address** field, specify an IPv4 address for the vProxy appliance.
    - In the **Default gateway** field, specify the IP address of the gateway host.
    - In the **Network Netmask/Prefix** field, specify the netmask for an IPv4 Network IP address.

    Note: Similar to the **Select networks** window, if dual NIC is configured, specify values for both **VM Network** and **VM Network 2**. If a single NIC is configured, then specify a value only for **VM Network** and ignore **VM Network 2**.

    b. Expand **DNS settings**, and then perform the following tasks:
    - In the **DNS** field, specify the IP address of the DNS servers, separated by commas.
    - In the **FQDN** field, specify the fully qualified domain name of the vProxy appliance.

    c. Expand **Timezone settings** and then perform the following tasks:
    - In the **Timezone setting** field, select the timezone.

      Note: To set a timezone outside of the list supported by the vProxy appliance, you need to change the timezone manually. SSH into the vProxy appliance using root credentials and run the following command: `/usr/bin/timedatectl set-timezone new-timezone`.
    - (Optional) In the **NTP** field, specify the NTP server address if you want to time sync the vProxy with the NTP server. If you do not specify the NTP server address, then the vProxy will time sync with the ESXi host.

    d. Expand **Password settings**, and then perform the following tasks:
    - In the **Root password** field, specify a new password for the root account.
    - In the **Admin password** field, specify a new password for the admin account.

> **Note:** The passwords for the root and admin account should be between 8 and 20 characters in length. Specifying a new password is mandatory when deploying the vProxy using vCenter, otherwise the vProxy appliance fails to power on. Ensure that you change the default passwords of both the root and admin account during deployment.

13. On the **Ready to Complete** window, review the deployment configuration details. If you will immediately configure the appliance, select **Power on after deployment**, and then click **Finish**.

    The **Deploying** window appears and provides status information about the deployment.

    > **Note:** If you are deploying vProxy on an ESXi 6.0 directly using vSphere client then you have to use the default passwords to configure once deployed. The default password for root account is “changeme” and for admin account is “a3dp@m8n”.

Deploy the vProxy OVA on an ESXi host

Perform the following steps to deploy the OVA for the vProxy host from an ESXi host.

Before you begin

Download the vProxy OVA package specific to your platform from the NetWorker downloads page at https://support.emc.com/downloads/1095_NetWorker.

Procedure

1. Log into the ESXi host with an administrator account.
2. From the **File** menu, select **Deploy OVF Template**.
3. On the **Source** window, type a URL path to the OVA package or click **Browse** and navigate to the OVA package location, and then click **Next**.
4. On the **OVF Template Details** window, review the product details such as the product name, version, vendor, publisher, and download size, and then click **Next**.
5. On the **Accept License Agreements** window, the EULA appears. Review the EULA and then click **Accept**.
6. On the **Name and Location** window, specify a name for the virtual appliance, and optionally the inventory location, for example a datacenter or VM folder. Click **Next**.
7. If the location you selected in the previous step has more than one available host, the **Host / Cluster** window appears. Select the ESXi host or cluster on which you want to deploy the virtual appliance, and then click **Next**.
8. On the **Resource Pool** window, perform one of the following tasks, and then click **Next**.
   - When you deploy the virtual appliance in a cluster with multiple hosts, select the specific host in the cluster on which to deploy the virtual appliance.
     > **Note:** If DRS is enabled, the target host is automatically selected.
   - When you deploy the virtual appliance on a host with a resource pool or vApp, select the resource pool or vApp on which to deploy virtual appliance.
9. On the **Storage** window, select the destination datastore on which to store the virtual appliance files, and then click **Next**.

10. On the **Disk Format** window, select the disk format.

    It is recommended that you select **Thick Provision Lazy Zeroed** to ensure that amount of storage space allocated to the virtual appliance is available.

11. On the **Network Mapping** window, select the Source and Destination networks to use with the appliance, and then click **Next**.

12. On the **Ready to Complete** window, review the deployment configuration details. If you will immediately configure the appliance, select **Power on after deployment**, and then click **Finish**.

    The **Deploying** window appears and provides status information about the deployment.

    Note: If you are deploying vProxy on an ESXi 6.0 directly using vSphere client then you have to use the default passwords to configure once deployed. The default password for root account is “changeme” and for admin account is “a3dp@m8n”.

Configure the network settings

After you deploy the vProxy appliance on the ESXi host, configure the network settings from a console window.

Procedure

1. From the **vSphere Client** application, open a console window on the vProxy appliance or use `ssh` to connect to the appliance from a host that has network access to the vProxy appliance.

2. Log in to the appliance with the root account.

   The default password for the root account is specified during vProxy deployment.

3. Use the `/opt/emc/vproxy/bin/config_network.sh` command to configure the network settings.

   For example: `/opt/emc/vproxy/bin/config_network.sh` ***fqdn IP address netmask/prefix gateway "dns_server1, dns_server2, ... dns_serverN"***
   where:

   - *fqdn* is the Fully Qualified Domain Name of the appliance.
   - *IP address* is the IPv4 address of the appliance.
   - *netmask/prefix* is the IPv4 netmask of the appliance.
   - *gateway* is the name or IP address of the gateway host.
   - *" dns_server1, dns_server2, ... dns_serverN"* is a comma-separated list of IP addresses or host names for the DNS servers, enclosed in quotes.

   The `config_network.sh` man page provides more information about how to use the `config_network.sh` command.

   Note: After you configure these settings, any subsequent network configuration changes, including DNS name resolution, require a restart of all vProxy services.

VMware vCenter server management

Add the vCenter server to create the client resource for configuring vProxy backups.

Networker provides two options to add, edit or delete the vCenter server:

- **VMware View** in NMC's **NetWorker Administration** window.
- The NetWorker Management Web UI.

When you add a vCenter server, the NetWorker server also creates a client resource for the vCenter server. You will use this client resource to configure VMware backups.

Add the vCenter server using NMC's VMware View

You can also use **VMware View** in NMC's **NetWorker Administration** window to add a vCenter server. To add the vCenter server, perform the following.

Before you begin

Ensure that the vCenter server is added to NetWorker using either the FQDN matching the one configured in the vCenter server, or the actual IP address of the vCenter server. Using a different FQDN alias or shortname alias for the vCenter server when adding it to NetWorker is not supported for the vCenter plug-in.

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the left navigation pane, expand the NetWorker server, right-click **VMware View**, and then select **Add vCenter**.

   The **Add vCenter** window appears.
3. In the **Host Name** field, specify the FQDN of the vCenter server.
4. In the **User Name** field, specify a vCenter user account that has permissions to perform backups.
5. In the **Password** field, specify the password for the account for the vCenter server.
6. If the vCenter server is deployed in the Cloud, select the **Deployed in Cloud** checkbox, and then click **OK**.

   Note: When you select **Deployed in Cloud**, a parameter displays in the backup action logs that indicates `HypervisorMode: VMC`. When the checkbox is not selected, the parameter indicates `HypervisorMode: vSphere`.
7. Click **OK**.

Edit a vCenter server using VMware View in NMC

You can also use **VMware View** in NMC's **NetWorker Administration** window to edit a vCenter server that has been registered with NetWorker to update the credentials stored in the vCenter resource.

Procedure

1. In the left pane of the **Protection** window, expand **VMware VIew** to view the vCenter servers.
2. Right-click the desired vCenter server and select **Modify vCenter**.

The **Modify vCenter** dialog displays, with the **Hostname** field greyed out as this field cannot be changed in this dialog.

3. In the **Username** field, specify a new vCenter user account that has permissions to perform backups.
4. In the **Password** field, specify the password for this vCenter user account.
5. If the vCenter server is deployed in the Cloud and this option is currently unselected, select the **Deployed in Cloud** checkbox.

   Note: When you select **Deployed in Cloud**, a parameter will appear in the backup action logs that indicates `HypervisorMode: VMC`. When the checkbox is not selected, the parameter indicates `HypervisorMode: vSphere`.

6. Click **OK**.

Results

The changes will appear automatically in the visual representation of the vCenter in the right pane of **VMware View**.

Note: If you want to delete a vCenter resource from NetWorker, right-click the vCenter under **VMware View** and select **Remove**.

Add the vCenter server using the NetWorker Management Web UI

You can use the NetWorker Management Web UI to add a vCenter server to perform data protection of vProxy virtual machines and objects, edit an existing vCenter server's configuration options, or delete a vCenter server. To add the vCenter server, perform the following.

Before you begin

Ensure that the vCenter server is added to NetWorker using either the FQDN matching the one configured in the vCenter server, or the actual IP address of the vCenter server. Using a different FQDN alias or shortname alias for the vCenter server when adding it to NetWorker is not supported for the vCenter plug-in.

Procedure

1. If not already logged in to the NetWorker Management Web UI, open a web browser and type an address that points to the NetWorker server or NetWorker Management Console IP and indicates nwui, for example, `https://<NetWorker server IP address>:9090/nwui`.

   The NetWorker login page displays.

2. In the NetWorker login page:
   a. Type the **Username** and **password** credentials for the administrator user.
   b. Type the NetWorker server IP address.
   c. Type the port that will be used for communication between the NetWorker server and the vCenter server.
   d. Click **Log in**.

   The landing page displays options for **Monitoring**, **Protection**, and **Recovery** in the left pane.

3. Select **Protection** > **VMware vCenters**.
4. In the **Protection** window's **VMware vCenters** pane, click **+ Add**.

   The **Add vCenter** dialog displays.

5. In the **Hostname** field, specify the FQDN or IP address of the vCenter server.
6. In the **Username** field, specify a vCenter user account that has permissions to perform backups.
7. In the **Password** field, specify the password for the vCenter user account.
8. If the vCenter server is deployed in the Cloud, select the **Deployed in Cloud** checkbox.

   Note: When you select **Deployed in Cloud**, a parameter will appear in the backup action logs that indicates `HypervisorMode: VMC`. When the checkbox is not selected, the parameter indicates `HypervisorMode: vSphere`.
9. Click **Save**.

   An entry for the added vCenter server will appear automatically in the **Protection** window's **VMware vCenters** pane. If an entry for the added vCenter does not appear, click the **Refresh** icon. You can also use the **Refresh** icon to refresh the vCenter inventory.

Results

When you select one of the available vCenter resources, the vCenter inventory displays in the right pane of the window in a tree structure that allows you to view all virtual machines and entities, and select individual items to view the entity's properties. Additionally, you can toggle a switch to displays all entities (protected and unprotected) in the tree, display only entries that are currently protected by a policy, or display only unprotected entities. An entity that is already protected appears blue and bolded.

Edit a vCenter server using the NetWorker Management Web UI

You can also use the NetWorker Management Web UI to edit a vCenter server that has been registered with NetWorker to update the credentials stored in the vCenter resource.

Procedure

1. Select **Protection** > **VMware vCenters** in the left pane.
2. Select the desired vCenter server, and then click **Edit**.

   The **Edit vCenter** dialog displays, with the **Hostname** field greyed out as this field cannot be changed in this dialog.
3. In the **Username** field, specify a new vCenter user account that has permissions to perform backups.
4. In the **Password** field, specify the password for this vCenter user account.
5. If the vCenter server is deployed in the Cloud and this option is currently unselected, select the **Deployed in Cloud** checkbox.

   Note: When you select **Deployed in Cloud**, a parameter will appear in the backup action logs that indicates `HypervisorMode: VMC`. When the checkbox is not selected, the parameter indicates `HypervisorMode: vSphere`.
6. Click **Save**.

Results

The changes will appear automatically in the **VMware vCenters** pane. If the changes do not appear, click the **Refresh** icon.

Note: If you want to delete a vCenter resource from NetWorker, select the entry in the **VMware vCenters** pane and click the **Delete** icon.

Configuring and registering the vProxy appliance

Networker provides multiple options to configure and register a deployed vProxy appliance:

- The NMC **NetWorker Administration** window's **VMware Proxy Configuration wizard**.
- The NetWorker Management Web UI.

Configure and register the vProxy in NMC

To complete the configuration of a vProxy OVA that was deployed on an ESXi host or a vCenter server, use the NMC **NetWorker Administration** window's **VMware Proxy Configuration wizard** wizard.

About this task

Note that you can also use the procedure described in the section Additional method to add and configure the vProxy in NMC.

Procedure

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. On the taskbar, click the **Enterprise** icon .
3. In the navigation tree, highlight a host:
   a. Right-click **NetWorker**.
   b. Select **Launch Application**. The **NetWorker Administration** window appears.
4. On the taskbar, click the **Devices** button .
5. In the **Device** window's left navigation pane, right-click **VMware Proxies** and select **New VMware Proxy Wizard**.

   The **VMware Proxy Configuration wizard** wizard opens on the **Select the Configuration Method** page.
6. On the **Select the Configuration Method** page, select **Register VMware Proxies**, and then select the vCenter/ESXi server. Click **Next**.

   The **Select the VMware Proxies to Configure and Register** page displays. On this page, the **VMware Proxy Selection** pane displays the location of the deployed but unregistered vProxy appliance(s) within the vCenter/ESXi server.
7. Select the checkbox next to the vProxy appliance(s) you want to configure.
8. (Optional) If you want to override the common configuration options for the selected vProxy, click the **Edit** button to open the **Configure VMware Proxy** dialog. When finished, click **OK** to save the settings.

   VMware Proxy Configuration Wizard reports the status as failed if total hotadd sessions exceeds 100 per vCenter. Registering of vProxy using the VMware Proxy Configuration Wizard through NWUI or NMC incorrectly reports the status as failed if total hotadd sessions for all the vProxies combined exceeds 100 per vCenter. This failed status can be ignored because the registration actually succeeds. The status appears as failed in order to alert the user that the total hotadd sessions have exceeded the recommended limit of 100 hotadd

sessions per vCenter. Refer to the section "Performance and Scalability" for recommended limits.

9. Click **Next**.

   The **VMware Proxies Configuration and Registration Summary** page displays.

10. Verify that the details are correct, and then click **Configure**.

Results

The jobs created for all vProxy registrations display in a table on the **Check Results** page, where you can view the status, as well as the logs, for each entry. If you want to close the wizard, you can also monitor the progress in the **Monitoring** pane of the **Devices** window. To view the details of the job at any time, right-click an entry in the **Monitoring** pane and select **View Log**.

Additional method to add and configure the vProxy in NMC

You can also use the following method in NMC to add and configure the deployed VMware proxy host as a device on the NetWorker server. Note that this procedure is not required if you already configured the vProxy by using the **VMware Proxy Configuration wizard**.

Procedure

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. On the taskbar, click the **Enterprise** icon .
3. In the navigation tree, highlight a host:
   a. Right-click **NetWorker**.
   b. Select **Launch Application**. The **NetWorker Administration** window appears.
4. On the taskbar, click the **Devices** button .
5. In the expanded left navigation pane, right-click **VMware Proxies** and select **New**.

   The **Create NSR VMware Proxy** dialog displays.
6. On the **General** tab, specify the FQDN of the vProxy appliance in the **Name** field.

   Note: Any additional fields on this tab are optional.
7. On the **Configuration** tab, configure the following options:
   a. From the **vCenter** menu, select the vCenter server on which you deployed the vProxy appliance.
   b. Specify a value in the **Maximum NBD sessions** or **Maximum hotadd sessions** attribute, using the guidelines in the section "Performance and Scalability."
      - **Maximum NBD sessions**—Defines the maximum virtual machine sessions that the vProxy appliance supports when you use the NBD transport. Datastores should be defined in the vProxy properties when using this setting to restrict NBD to these datastores only.

- **Maximum hotadd sessions**—Defines the maximum number of virtual disks that NetWorker can concurrently hotadd to the vProxy appliance. The default value is 13. The maximum value for this attribute is 25.

When specifying the maximum sessions value for the transport modes, ensure that at least one transport mode is set to a value greater than 0. If you want to enable only one of the transport modes, set the maximum sessions for the transport mode you do not want to use to 0. NetWorker displays a warning message if you are exceeding 100 hotadd sessions per vCenter. Refer to the section "Performance and Scalability" for recommended limits.

c. In the **User ID** field, specify the `admin` user account.

d. In the **Password** field, specify the password for the `admin` user account on the vProxy appliance. This will be the password that was used during the vProxy deployment.

Note: Any additional fields on this tab not specified here are optional.

8. Click **OK**.

Add and configure the vProxy in the NetWorker Management Web UI

After deploying the OVA for the vProxy host, perform the following steps to add and configure the vProxy by using the NetWorker Management Web UI.

Before you begin

Before adding the vProxy, ensure that you add the vCenter server by using the steps in the section Add the vCenter server using the NetWorker Management Web UI.

Procedure

1. In the NetWorker Management Web UI, select **Protection** in the left pane, and then select **VMware Proxies**.

   The **VMware Proxies** pane opens on the **Proxies** tab, which displays any vProxies that have already been configured. You can choose to display hidden columns by clicking the blue icon in the lower left corner of the table.

2. In the **Proxies** tab, click **+ Add**.

   The **Selection** page appears.

3. On the **Selection** page, ensure that you select the correct vCenter.

   All vProxies in that vCenter inventory will display.

4. Use the **Select Proxies** field to select one or more vProxies, and then click **Next**.

5. On the **Configuration** page, configure the host names for the vProxies you want to register and specify the following configuration options:

   a. Select the vCenter server on which you deployed the vProxy appliance.

   b. Specify the `admin` user account.

   c. Specify the password for the `admin` user account on the vProxy appliance. This is the password that was used during the vProxy deployment.

   d. Specify a value in the **Maximum NBD sessions** or **Maximum hotadd sessions** attribute, using the guidelines in the section "Performance and Scalability."

- **Maximum NBD sessions**—Defines the maximum virtual machine sessions that the vProxy appliance supports when you use the NBD transport. Datastores should be defined in the vProxy properties when using this setting to restrict NBD to these datastores only.
- **Maximum hotadd sessions**—Defines the maximum number of virtual disks that NetWorker can concurrently hotadd to the vProxy appliance. The default value is 13. The maximum value for this attribute is 25.

When specifying the maximum sessions value for the transport modes, ensure that at least one transport mode is set to a value greater than 0. If you want to enable only one of the transport modes, set the maximum sessions for the transport mode you do not want to use to 0.

VMware Proxy Configuration Wizard reports the status as failed if total hotadd sessions exceeds 100 per vCenter. Registering of vProxy using the VMware Proxy Configuration Wizard through NWUI or NMC incorrectly reports the status as failed if total hotadd sessions for all the vProxies combined exceeds 100 per vCenter. This failed status can be ignored because the registration actually succeeds. The status appears as failed in order to alert the user that the total hotadd sessions have exceeded the recommended limit of 100 hotadd sessions per vCenter. Refer to the section "Performance and Scalability" for recommended limits.

6. Click **Finish**.

Results

When vProxy registration is initiated, a notification displays at the top of the window that a request was submitted. You can monitor the status and progress of the registration from the **Tasks** tab on this page.
Once registration is complete, you can use the vProxy for backups of VMware protection policies. You can also edit the configuration settings for the vProxy by clicking the **Edit** icon, or remove the vProxy by clicking the **Delete** icon.

Installing the vCenter plug-in

After you add the vCenter host, install either the HTML5 or flash-based vCenter plug-in to enable virtual machine backup and recovery in the **vSphere Client** or **vSphere Web Client**.

NetWorker provides two options to install the vCenter plug-in:

- The NetWorker Management Web UI.
- **VMware View** in NMC's **NetWorker Administration** window.

Install the vCenter plug-in using VMware View in NMC

Perform the following steps when using **VMware View** in NMC to install either the HTML5 or flash-based vCenter plug-in to enable virtual machine backup and recovery in the **vSphere Client** or **vSphere Web Client**.

Before you begin

- Ensure that the vCenter server is added to NetWorker using either the FQDN matching the one configured in the vCenter server, or the actual IP address of the vCenter server. Using a different FQDN alias or shortname alias for the vCenter server when adding it to NetWorker is not supported for the vCenter plug-in.

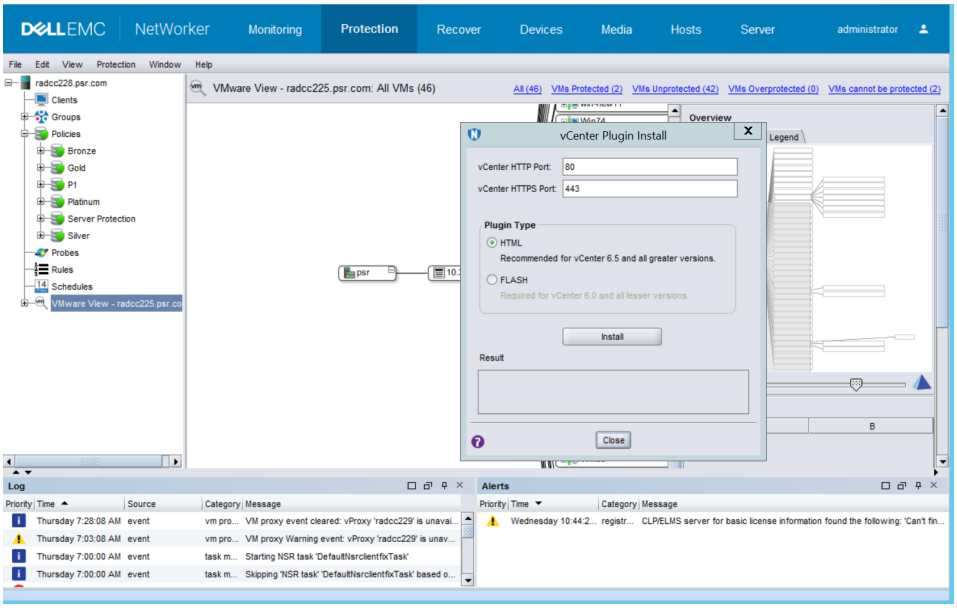
- The vCenter plug-in (HTML5 or flash-based) requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the left navigation pane, expand the NetWorker server and click **VMware View**.
3. In VMware View, right-click on the vCenter you added and select **Install vCenter plugin**.

   The **vCenter Plugin Install** dialog displays.

   Figure 3 Install vCenter Plugin in NMC

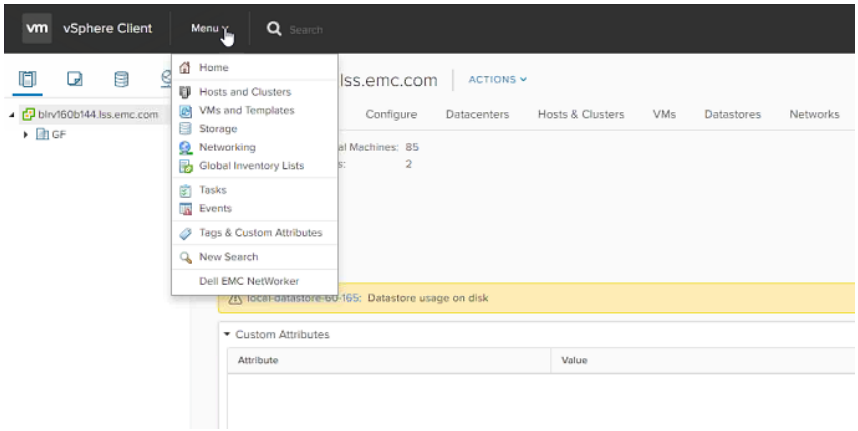


4. If a security warning appears, click **Continue** to dismiss the warning.
5. Select the **Plugin Type** that you want to install. **HTML5** will install the **Dell EMC NetWorker** interface in the **vSphere Client**. **FLASH** will install the **VM Backup and Recovery** interface in the **vSphere Web Client**.
6. Provide the required HTTP port configured for the vCenter server, and leave the default value of 443 for the HTTPS port. Note that the vProxy appliance only supports the 443 port for HTTPS.
7. Click **Install**.

Results

When the vCenter plug-in is validated, log in to the **vSphere Client** for the vCenter to verify the installation. If the installation was successful, depending on the plug-in type selected an entry for **Dell EMC NetWorker** or **VM Backup and Recovery** appears in the **Menu** drop-down in the task bar, as shown in the following, and also appears in the left navigation pane when you select **Home**.

Figure 4 vCenter plug-in for Dell EMC NetWorker in the vSphere Client



Note: If you installed the HTML-5 based plug-in, you can use the `vcui` log file available at `/nsr/authc/logs/vcui.log` to assist with troubleshooting issues with the **Dell EMC NetWorker** interface. If you installed the flash-based plug-in, you can use the `ebr-server` log file available at `/nsr/authc/logs/ebr-server.log` to assist with troubleshooting issues with the **VM Backup and Recovery** interface.

Remove and reinstall the HTML5-based vCenter plug-in from the vSphere Client

In vSphere version 6.5 and later, the html-5 based vCenter plug-in appears as **Dell EMC NetWorker** in the **vSphere Client**. If you need to remove the HTML5-based plug-in and then reinstall the plug-in, perform the following steps.

Procedure

1. Stop the **vSphere Client** services.
2. Log into vCenter Server's MOB at `http://vcenter-server/mob`.
3. Click the **content** link.
4. Click the **ExtensionManager** link.
5. Click the **UnregisterExtension** link.
6. Enter the value `com.dell.emc.nw` and click the **Invoke Method** link.
7. Enter the value `com.emc.networker.backup` and click the **Invoke Method** link.
8. Enter the value `com.emc.networker.recover` and click the **Invoke Method** link.
9. On the vCenter server, manually remove the plug-in from the `/vsphere-client-serenity` folder. The path is `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` on Linux, and `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` on Windows.
10. Restart the **vSphere Client** services.
11. Perform the steps in the section Install the vCenter plug-in for the vSphere Client to re-install the HTML5-based plug-in, and verify that the **Dell EMC NetWorker** interface appears in the **vSphere Client**.

Remove the flash-based vCenter plug-in from the vSphere Web Client

In NetWorker 9.2.x and earlier versions, the vCenter plug-in for vProxy backup and recovery is a flash-based plug-in that appears as **VM Backup and Recovery** in the left

pane of the **vSphere Web Client**. vSphere versions 6.5 and later and NetWorker 18.x both this plug-in and the html-5 based vCenter plug-in that appears as **Dell EMC NetWorker** in the **vSphere Web Client**. If upgrading to NetWorker 18.x and you no longer require the flash-based plug-in, perform the following steps in order to manually remove **VM Backup and Recovery** from the **vSphere Web Client**.

Procedure

1. Stop the **vSphere Web Client** services.
2. Log into vCenter Server's MOB at `http://vcenter-server/mob`.
3. Click the **content** link.
4. Click the **ExtensionManager** link.
5. Click on the **UnregisterExtension** link.
6. Enter the value `com.emc.networker` and click the **Invoke Method** link.
7. Enter the value `com.emc.networker.backup` and click the **Invoke Method** link.
8. Enter the value `com.emc.networker.recover` and click the **Invoke Method** link.
9. On the vCenter server, manually remove the plug-in from the `/vsphere-client-serenity` folder. On vCenter 6.0 and 6.5, the path is `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` on Linux, and `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` on Windows.
10. Restart the **vSphere Web Client** services.

Install the vCenter plug-in using the NetWorker Management Web UI

You can use the NetWorker Management Web UI to install either the HTML or flash-based vCenter plug-in to enable virtual machine backup and recovery in the **vSphere Client** or **vSphere Web Client**. Perform the following steps.

Before you begin

- Ensure that the vCenter server is added to NetWorker using either the FQDN matching the one configured in the vCenter server, or the actual IP address of the vCenter server. Using a different FQDN alias or shortname alias for the vCenter server when adding it to NetWorker is not supported for the vCenter plug-in.
- The vCenter plug-in (HTML5 or flash-based) requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.

Procedure

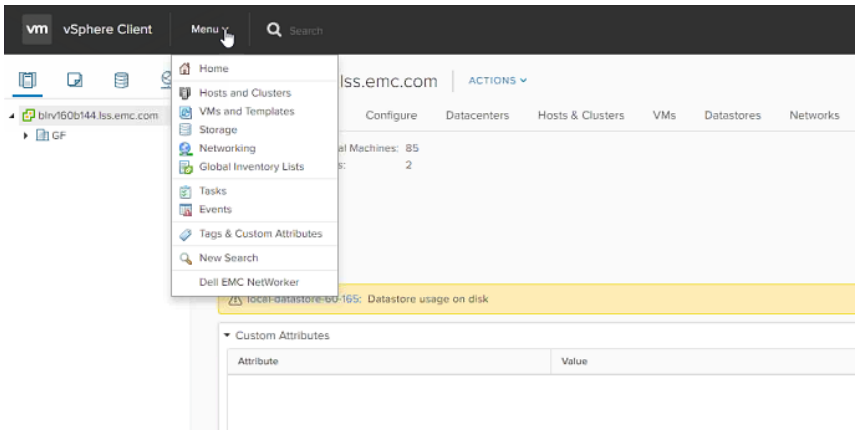
1. Select **Protection** > **VMware vCenters**in the left pane.
2. In the **Protection** window's **VMware vCenters** pane, click the **Install** icon.

   The **Install vCenter Plugin** dialog displays.
3. Select the **Plugin Type** that you want to install. **HTML** will install the **Dell EMC NetWorker** interface in the **vSphere Client** for vSphere version 6.5. **Flash** will install the flash-based **VM Backup and Recovery** interface in the **vSphere Web Client** for vSphere versions 6 and earlier.
4. For the HTTPS port that is configured for the vCenter server, leave the default value of 443. Note that vProxy only supports using port 443 for HTTPS.
5. Type the username and password for the NetWorker administrator user.
6. Click **Install**.

Results

When the vCenter plug-in is validated, log in to the **vSphere Client** for the vCenter to verify the installation. If the installation was successful, depending on the plug-in type selected an entry for **Dell EMC NetWorker** or **VM Backup and Recovery** appears in the **Menu** drop-down in the task bar, as shown in the following, and also appears in the left navigation pane when you select **Home**.

Figure 5 vCenter plug-in for Dell EMC NetWorker in the vSphere Client



Note: If you installed the HTML-5 based plug-in, you can use the `vcui` log file available at `/nsr/authc/logs/vcui.log` to assist with troubleshooting issues with the **Dell EMC NetWorker** interface. If you installed the flash-based plug-in, you can use the `ebr-server` log file available at `/nsr/authc/logs/ebr-server.log` to assist with troubleshooting issues with the **VM Backup and Recovery** interface.

Updating the vCenter plug-in

When you upgrade the NetWorker server to NetWorker 19.1, you must also upgrade the HTML-5 or flash-based vCenter plug-in to the latest version for NetWorker 19.1.

The steps to upgrade the vCenter plug-in are the same as the installation procedure, as described in the sections Install the vCenter plug-in using VMware View in NMC and Install the vCenter plug-in using the NetWorker Management Web UI. Note that the plug-in installation process will automatically initiate an upgrade of the plug-in if an earlier version already exists on the vCenter server.

Accessing the HTML-5 or flash-based vCenter plug-in as a non-administrator Active Directory user

You can only access the HTML-5 or flash-based vCenter plug-in if you are an NetWorker administrator or a non-administrator Active Directory user with appropriate privileges in NetWorker. The following procedure describes how to access the plug-in as a non-administrator Active Directory user.

Before you begin

Install the vCenter plug-in. The section Installing the vCenter plug-in provides instructions.

Procedure

1. Create a **vmwareAdmin** group in NetWorker that contains the following privileges at a minimum:
   - View Security Settings
   - View Application Settings
   - Remote Access All Clients
   - Operate NetWorker
   - Monitor NetWorker
   - Operate Devices and Jukeboxes
   - Recover Local Data
   - Recover Remote Data
   - Backup Local Data
2. Create an Active Directory user within your desired security group.
3. Add the user and group to the NetWorker Management Console's **External Roles** attribute. For example:

   `CN=VMwareTeam,CN=Users,DC=vproxy,DC=com`
   `cn=VMwareUser,cn=Users,dc=vproxy,dc=com`
   where *VMwareTeam* is the security group name, and *VMwareUser* is the Active Directory user name.
4. Log in to the **vSphere Web Client** as the Active Directory user, in the format `<tenant>\<domain>\<userid>`. For example:

   `default\vproxy\VMwareUser`

Results

The Active Directory user that you create using these steps will only have access to the HTML-5 or flash-based vCenter plug-in, and cannot be used to log in to the **Dell EMC Data Protection Restore Client** or the **NetWorker Management Console**. If you also need to provide access to these applications, then add those required privileges as described in the section File-level restore as a domain user.

Creating a dedicated vCenter user account and VM Backup and Recovery role

It is strongly recommended that you set up a separate vCenter user account at the root level of the vCenter that is strictly dedicated for use with NetWorker VMware Protection. Use of a generic user account such as “Administrator” might make future troubleshooting efforts difficult as it might not be clear which “Administrator” actions are actually interfacing, or communicating, with the NetWorker server. Using a separate vCenter user account ensures maximum clarity if it becomes necessary to examine vCenter logs.

Create vCenter user account

Procedure

1. From a web browser, type the following:

   `https://<IP_address_vCenter_Server>:5480`

The **VMware vCenter Server Appliance** login page appears.

2. Enter the vCenter root user credentials to log in.
3. In the **VMware vCenter Server Appliance** Console, click the **Summary** tab, and then click the **Stop** button next to the Server service in the **vCenter** pane.
4. Click the **SSO** tab, and then select **Embedded** from the **SSO deployment type** drop-down list.
5. Assign a password, and click **Save settings**.
6. Click the **Summary** tab, and then click the **Start** button next to the Server service in the **vCenter** pane.
7. Log out of the session.
8. From a web browser, enter the following to connect to the vSphere Web Client:

   `https://<IP_address_vCenter_Server>:9443/vSphere-client/`

9. Login as user administrator@vsphere.local with the password you created in step 5.
10. Navigate to **Home** > **Administration** > **SSO Users and Groups**.
11. On the **Users** tab, click the green **+**.

    The **New User** window appears.
12. In the **Username** field, specify a username (for example, VM Backup and Recovery).
13. In the **Password** and **Confirm Password** fields, specify a password.

    You can leave the First name, last name and password fields blank.
14. Click **OK**.

Create a customized role

Procedure

1. In the **vSphere Web Client**, open **Administration** > **Role Manager** and click on the green **+**.

   The Create Role dialog appears.
2. Type the name of this role (for example, `Admin1`).
3. Select all the privileges listed in the following table and click **OK**. This vCenter user account must have these privileges at a minimum.

   Table 6 Minimum required vCenter user account privileges

Setting	vCenter required privileges
Alarms	• Create alarm • Modify alarm
Datastore	• Allocate space • Browse datastore • Configure datastore • Low level file operations

Table 6 Minimum required vCenter user account privileges (continued)

Setting	vCenter required privileges
	• Move datastore • Remove datastore • Remove file • Rename datastore
Extension	• Register extension • Unregister extension • Update extension
Folder	• Create folder
Global	• Cancel task • Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Settings • Set custom attribute
Host	• Configuration > Storage partition configuration
Network	• Assign network • Configure
Resource	• Assign virtual machine to resource pool • Migrate powered off virtual machine • Migrate powered on virtual machine
Sessions	• Validate session
Tasks	• Create task • Update task
vApp	• Export • Import • vApp application configuration
Virtual Machine	
Configuration	• Add existing disk • Add new disk • Add or remove device

Table 6 Minimum required vCenter user account privileges (continued)

Setting	vCenter required privileges
	• Advanced • Change CPU count • Change resource • Configure managed by • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Set annotation • Settings • Swapfile placement • Upgrade virtual machine compatibility
Guest Operations	• Guest operation modifications • Guest operation program execution • Guest operation queries
Interactions	• Configure CD media • Console interaction • Device Connection • Guest operating system management by VIX API • Power off • Power on • Reset • VMware Tools install
Inventory	• Create new • Register • Remove • Unregister

Table 6 Minimum required vCenter user account privileges (continued)

Setting	vCenter required privileges
Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Mark as Template
Snapshot Management	• Create snapshot • Remove Snapshot • Revert to snapshot

vSphere Client user accounts

Before you can use the vCenter user account with NetWorker VMware Protection, or before you can use the Single Sign-on (SSO) admin user with the vProxy appliance, you must add these users as **administrator** on the vCenter root node. Users who inherit permissions from group roles are not valid.

About this task

Note: In high-security environments, you can restrict the vCenter user account permissions required to configure and administer the vProxy appliance. Table 6 on page 52 provides the account permission categories.

The following steps allow you to configure a VM Backup and Recovery user or SSO admin user by using the **vSphere Web Client**.

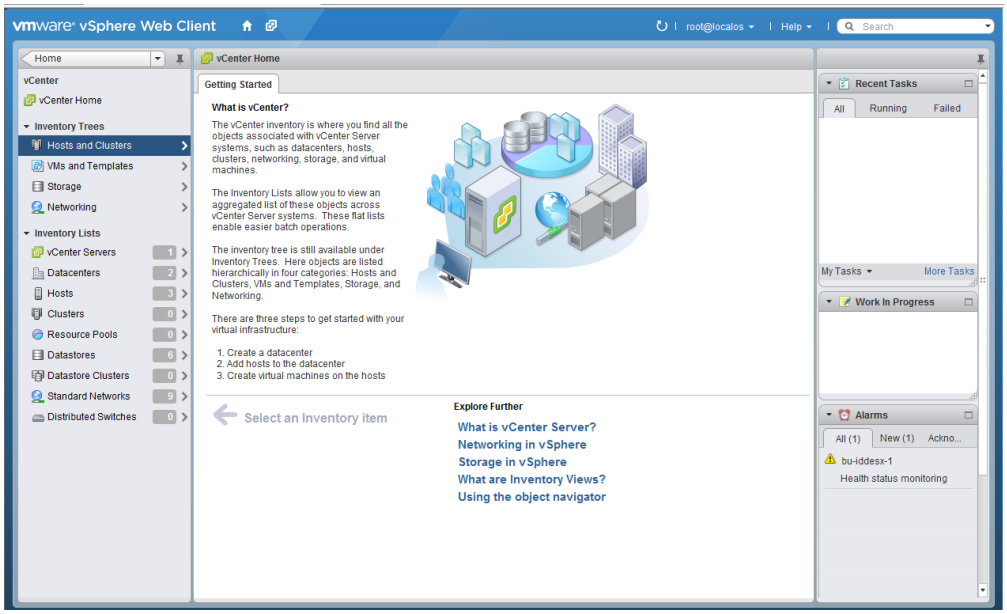
Procedure

1. From a web browser, access the vSphere Web Client using the following URL:

   `https://<Ip_address_vCenter_server>:9443/vsphere-client/`

2. Log in with administrative rights.
3. In the left panel of the **vSphere Web Client** window, select **vCenter** > **Hosts and Clusters**.

Figure 6 Hosts and Clusters in the vSphere Web Client



4. Select the **Manage** tab and then click **Permissions**.

   Note: When assigning permissions, the **vSphere Web Client** places the curser in the location last used. Depending on what level was selected the last time you used this window, permissions might not get applied to the root level of the vCenter. For example, if the last item you selected in this window was Cluster Name, permissions will be assigned at the Cluster level. Review carefully to ensure that permissions get assigned at the root level of the vCenter.

5. Click the **Add permission** (+) icon.

   The **Add Permission** dialog box opens.

6. In the **Users and Groups** pane, click **Add...**.

   The **Select Users/Groups** dialog box appears.

7. From the **Domain** drop-down list, select *domain*, *server*, or *SYSTEM-DOMAIN*.
8. Select the user that will administer VM Backup and Recovery, or the SSO admin user, and then click **Add**.

   If the VM Backup and Recovery user belongs to a domain account, the account appears in the format "SYSTEM-DOMAIN\admin" format. If the user name appears in the format "admin@SYSTEM-DOMAIN", then tasks related to the backup job may not appear on the **Running** tab of the **Recent Tasks** window.

9. Click **OK**.
10. From the **Assigned Role** drop-down list, select the role you created.
11. Confirm that the **Propagate to children** box is checked.
12. Click **OK**.

Migrating policies from VMware Backup appliance to vProxy appliance

New NetWorker installations only use the NetWorker VMware Protection solution with the vProxy appliance. Backup operations with the VMware Backup appliance (VBA) are not supported, although you can use the vProxy appliance to perform recoveries from VBA backups within the **NetWorker Management Web user interface**. When you upgrade from a NetWorker 9.0.x and earlier release, you must migrate to use only the vProxy appliance, which requires workflow migration is required to convert existing VMware Backup appliance policies to vProxy appliance policies.

This migration involves two stages—a check that occurs prior to migration to ensure all the compatibility prerequisites are satisfied, and then the actual migration to convert existing VMware Backup appliance protection groups and policies to the vProxy appliance. You can initiate the policy migration by using the command line or NMC.

Note: NetWorker does not support the migration of workflows and policies from a VMware Backup appliance deployed in a NetWorker release previous to NetWorker 9.0 that uses GSAN internal storage.

Migration pre-requisites

When you migrate a VMware Backup appliance policy to a vProxy policy, a pre-check occurs automatically to determine that compatibility requirements are met.

These requirements include verification of the following items:

- The Data Domain OS (DD-OS) is DDOS version 6.0.0.30, 6.0.1-10, or 6.1.x and later DDOS versions. Note that use of the DD Retention Lock feature on vProxy backup and clone actions requires DDOS 6.1.x and later.
- The NetWorker server and storage node version are the same.
- The vProxy is available on the vCenter server, and is the correct version for the NetWorker release. For NetWorker 19.1, this is version 4.0.x.
- The vCenter server is a minimum of version 6.0.

If this check discovers any compatibility issues that can cause problems migrating all policies, the issues are reported and migration is cancelled. If using the command line to migrate policies, you can specify a force flag (-f) to ignore these errors and proceed with the migration to correct any issues afterwards, however it is recommended that the pre-check requirements be met prior to proceeding with the migration. Issues discovered during the pre-check will be logged and displayed even when using the force flag.

Policy migration to vProxy by using NMC

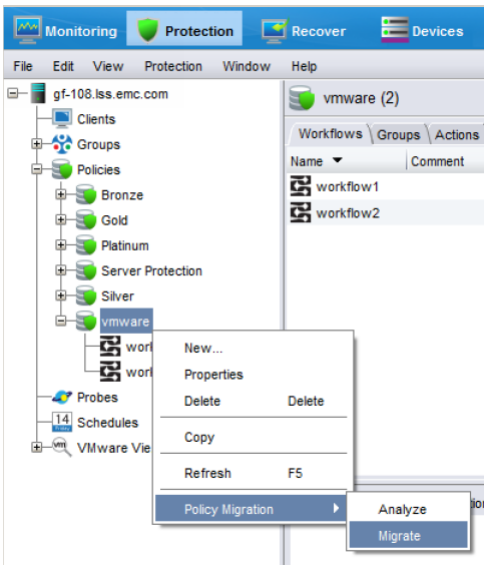
You can use the NetWorker Management Console (NMC) Administration window to migrate VMware Backup appliance policies and workflows to vProxy, or perform a pre-check before migrating.

Procedure

1. In the NMC **Administration** window, click **Protection**.
2. In the left pane, expand **Policies** to view the VMware policy.

3. (Optional) Right-click the **vmware** policy and select **Policy Migration** > **Analyze** from the drop-down if you want to perform a compatibility pre-check before migration.
4. Right-click the **vmware** policy and select **Policy Migration** > **Migrate** to start the migration.

Figure 7 Migrating a VMware Backup appliance policy to vProxy in NMC

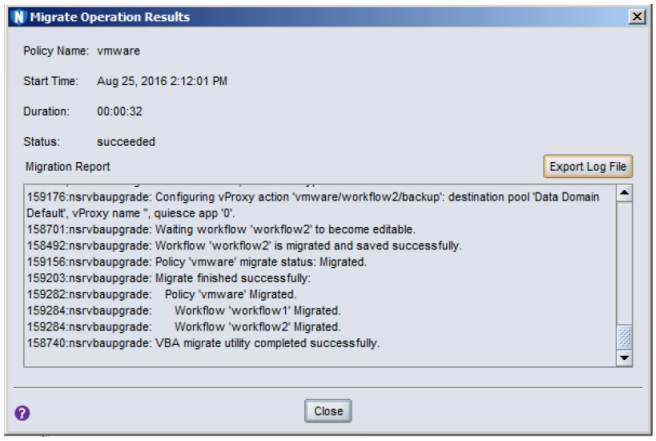


Note: If a pre-check failure occurs upon initiating the migration, a prompt appears to confirm that you want to ignore the errors and proceed. It is recommended that you resolve any pre-check errors, including unsupported software versions, before completing the migration in order for backups to complete successfully.

Results

A **Migrate Operation Results** dialog box opens which provides a real-time report of the analyzation and the migration until the process completes. You can then choose to export a log of the analyzation or migration as a report by clicking **Export Log File**.

Figure 8 Migrate Operation Results dialog



Policy migration to vProxy by using the command line

You can also migrate VMware Backup appliance policies and workflows to vProxy by using the `nsrvbaupgrade` command line utility, which additionally allows you to perform a pre-migration check before migrating. The command line supports multiple policies for each run.

Before you begin

To perform a pre-check only before migrating, run `nsrvbaupgrade -c`. It is recommended that you resolve any pre-check errors, including unsupported software versions, before completing the migration in order for backups to complete successfully.

Procedure

1. Open a command prompt.
2. Specify the `nsrvbaupgrade` command in the following format:

   `nsrvbaupgrade -p` *policy* `[-c] [-f] [-v]` where:

   - -p *policy* specifies one or more policies to migrate
   - -c runs the pre-check only
   - -f forces the migration to ignore a pre-check failure
   - -v specifies verbose mode

Renaming a NetWorker server with legacy VMware Backup appliance

When a NetWorker 8.2.x release is upgraded to NetWorker 9.1 or later, if you plan to change the NetWorker server name or domain name, restore of legacy backups using the VMware Backup appliance will fail. This occurs because when you change the name, the NetWorker sever is in the new domain and the VMware Backup appliance is in the old domain.

In order to ensure that the new domain can access the legacy VMware Backup appliance backups, perform the Disaster Recovery procedures for the VMware Backup appliance, which are provided in NetWorker 18.1 and earlier versions of the *NetWorker VMware Integration Guide*.

Resetting the admin account password

The vProxy appliance locks the admin account when you try to log in to the appliance with an incorrect password three consecutive times.

About this task

Perform the following steps to unlock the admin account and reset the password.

Procedure

1. From the **vSphere Client** application, open a console window on the vProxy appliance or use `ssh` to connect to the appliance from a host that has network access to the vProxy appliance.
2. Log in to the appliance with the root account.

   The default password for the root account is specified during vProxy deployment.

3. Use the `pam_tally2` command to unlock the admin account.

   For example:

   ```
   pam_tally2 --user admin --reset
   ```

   Output similar to the following appears:

   ```
   Login Failures Latest failure From
   admin 5 04/22/13 21:22:37 123.456.789
   ```

4. Use the `passwd` command to reset the admin password

   For example:

   ```
   passwd admin
   ```

The `pam_tally2` man page provides more information about the `pam_tally2` command and how to configure the maximum number of login attempts for a user account.

Upgrading the vProxy appliance

When you upgrade the NetWorker server to NetWorker 19.x, you must also upgrade the vProxy appliance to the latest version for NetWorker 19.x. You can automatically update the vProxy appliance version from the NetWorker server CLI.

Before you begin

Ensure that the root and admin password length of the previously deployed vProxy is in between 8 to 20 characters. You must also update the vProxy resource in NetWorker with the updated vProxy admin password.

About this task

The `nsrvproxy_mgmt` command supports out-of-place upgrade of any version of vProxy. The command ensures that the same configurations are retained post redeployment such as, vProxy VM name in the vCenter, user configured specific MAC addresses in the firewall restrictions in the datazone, dual NIC configurations, hotadd and NBD session limits.
The `nsrvproxy_mgmt redeploy` command performs the following operations:

- Unregister the original vProxy from the NetWorker Server.
- Power off the original vProxy in the vCenter.
- Disconnects all the network connections of the vProxy.
- Renames the vProxy to a temporary name of <originalvProxyName.timestamp> in the vCenter.
- Resets the MAC address of all the network adapters of the original vProxy. The original vProxy MAC address is assigned to the redeployed vProxy.
- Redeploy the vProxy with same configuration as that of original vProxy using the latest OVA and power it on.
- On a successful redeployment, original vProxy is deleted, and the updated vProxy is registered on the NetWorker Server.
- If there is redeployment failure, the command performs a rollback, reverts to original vProxy configuration and registers the old vProxy to NetWorker server.

Procedure

1. Download the ova file from the support site and place it in the following location:

Operating System	Location
Windows	`C:\Program Files\EMC NetWorker\nsr\vproxy \vproxy_ova\ovas\`
Linux	`/nsr/vproxy_ova/ovas/`

   - In Windows, you must manually create the `ovas` folder.
   - In Linux, you must manually create the `vproxy_ova/ovas` directory.

2. Redeploy the vProxy:

Deployment type	Procedure
Single vProxy deployment	For a single vProxy deployment, open a command prompt, and then run the `nsrvproxy_mgmt` command in the following format: **`nsrvproxy_mgmt redeploy -h vProxy-host-name -z vProxy-root-password [-x] [-f] [-u comments] [-t timeout in minutes] [-D debug-level]`**

Sequential deployment	For sequential redeployment, you must create a batch file or a shell script. For example, to initiate three sequential deployments run the following batch file or shell script.
	• On a windows platform, to initiate sequential redeployment you must create a batch file.
	`nsrvproxy_mgmt redeploy -h blrv027b075 -z Welcome@123 -f`
	`nsrvproxy_mgmt redeploy -h blrv027b076 -x -f`
	`nsrvproxy_mgmt redeploy -h blrv027b077 -z P@ssw0rd123 -f`
	• On a linux platform, to initiate sequential redeployment you must create a shell script.
	`[root@blrv160b181 /]# cat sample.sh`
	`#!/bin/bash`
	`nsrvproxy_mgmt redeploy -h blrv027b075 -z Welcome@123 -f`
	`nsrvproxy_mgmt redeploy -h blrv027b076 -x -f`
	`nsrvproxy_mgmt redeploy -h blrv027b077 -z P@ssw0rd123 -f`

   Where

   - -t specifies the maximum timeout value for any active vProxy session to get over and then start the redeployment. The default timeout value is ten minutes.
   - -x can be used when the vProxy admin password is same as that of root.
   - -z is used when specifying the vProxy root password

- -h *vProxyIP/FQDN* is the vProxy hostname that was used for registration and exists in the RAP resource.
- -f is used to disable the confirmation prompt.
- -D is used to set the debug level. By default, the debug level is 0.
- -u is used to display the comments.

Results

vProxy is successfully redeployed.

Limitations

The vProxy redeployment using `nsrvproxy_mgmt redeploy` command has a few limitations.

- Redeployment is performed in thin provisioning mode only. If the original vProxy is on thick provisioning, then post deployment the disk mode is changed to thin provisioning.
- Concurrent vProxy redeployment is not supported. You can sequentially redeploy multiple vProxy using a script.
- vProxy redeployment is not supported for vProxies that are directly deployed in the ESXi bypassing the vCenter. If the vProxy is deployed on the ESXi bypassing the vCenter, then you must manually redeploy the vProxy.
- The root and admin password length of the vProxy should be in between 8–20 characters only. Before redeployment, you must change the root and admin password and update the vProxy resource in NetWorker with the updated vProxy admin password.
- Deploying new vProxies using CLI is not supported

Troubleshooting Redeployment Failures

You can use the vProxy redeployment log files on the NetWorker server to troubleshoot redeployment failures.

Table 7 Location of the vProxy redeployment log files

Log file	Location on NetWorker server	Description
<job-uuid>.log	• Linux: `/nsr/logs/adhoc/nsrvproxy_mgmt` • Windows: `C:\Program Files\EMC NetWorker\nsr\logs\adhoc\nsrvproxy_mgmt`	vProxy management job log file is created during the redeployment of the associated vProxy.
vproxy_upgrade_session_<vProxy-identifier>_<job-uuid>	• Linux: `/nsr/logs/adhoc/nsrvproxy_mgmt` • Windows: `C:\Program Files\EMC NetWorker\nsr\logs\adhoc\nsrvproxy_mgmt`	Associated nsrvisd log file is created during redeployment of the vProxy.
nsrvisd-daemon.log	• Linux: `/opt/nsr/vproxy/logs/nsrvisd`	Associated nsrvisd detailed log file is created.

Table 7 Location of the vProxy redeployment log files (continued)

Log file	Location on NetWorker server	Description
	• Windows: `C:\Program Files\EMC NetWorker\nsr\vproxy\logs\nsrvisd`	
ProxySessions-<uuid>.log	• Linux: `/opt/nsr/vproxy/logs/nsrvisd` • Windows: `C:\Program Files\EMC NetWorker\nsr\vproxy\logs\nsrvisd`	Associated ProxySessions log file is created during redeployment of the vProxy.

CHAPTER 3

Protecting virtual machines

This chapter contains the following topics:

- Overview of protection policies 66
- Preparing the NetWorker data zone 67
- VMware backups in the NetWorker Management Web UI 68
- vProxy backups in NMC 87
- vProxy backup workflows in the vSphere Client's Dell EMC NetWorker interface 115
- vProxy workflows in the vSphere Web Client's VM Backup and Recovery interface 121
- Additional vProxy backup configuration options 124
- Enable the Microsoft VM App Agent for SQL Server application-consistent protection 127
- Updating the Microsoft VM App Agent and FLR Agent software 132
- Troubleshooting Data Protection Policies 132

Overview of protection policies

A protection policy allows you to design a protection solution for your environment at the data level instead of at the host level. With a data protection policy, each client in the environment is a backup object and not simply a host.

Data protection policies enable you to back up and manage data in a variety of environments, as well as to perform system maintenance tasks on the NetWorker server. You can use either the **NetWorker Management Web UI** or the NMC **NetWorker Administration** window to create your data protection policy solution.

A data protection policy solution encompasses the configuration of the following key NetWorker resources:

Policies

Policies provide you with a service-catalog approach to the configuration of a NetWorker datazone. Policies enable you to manage all data protection tasks and the data protection lifecycle from a central location.

Policies provide an organizational container for the workflows, actions, and groups that support and define the backup, clone, management, and system maintenance actions that you want to perform.

Workflows

The policy workflow defines a list of actions to perform sequentially or concurrently, a schedule window during which the workflow can run, and the protection group to which the workflow applies. You can create a workflow when you create a new policy, or you can create a workflow for an existing policy.

A workflow can be as simple as a single action that applies to a finite list of Client resources, or a complex chain of actions that apply to a dynamically changing list of resources. In a workflow, some actions can be set to occur sequentially, and others can occur concurrently.

You can create multiple workflows in a single policy. However, each workflow can belong to only one policy. When you add multiple workflows to the same policy, you can logically group data protection activities with similar service level provisions together, to provide easier configuration, access, and task execution.

Protection groups

Protection groups define a set of static or dynamic Client resources or save sets to which a workflow applies. There are also dedicated protection groups for backups in a VMware environment or for snapshot backups on a NAS device. Review the following information about protection groups:

- Create one protection group for each workflow. Each group can be assigned to only one workflow.
- You can add the same Client resources and save sets to more than one group at a time.
- You can create the group before you create the workflow, or you can create the group after you create the workflow and then assign the group to the workflow later.

Actions

Actions are the key resources in a workflow for a data protection policy and define a specific task (for example, a backup or clone) that occurs on the client resources in the group assigned to the workflow. NetWorker uses a work list to define the task. A

work list is composed of one or several work items. Work items include client resources, virtual machines, save sets, or tags. You can chain multiple actions together to occur sequentially or concurrently in a workflow. All chained actions use the same work list.

When you configure an action, you define the days on which to perform the action, as well as other settings specific to the action. For example, you can specify a destination pool, a retention period, and a target storage node for the backup action, which can differ from the subsequent action that clones the data.

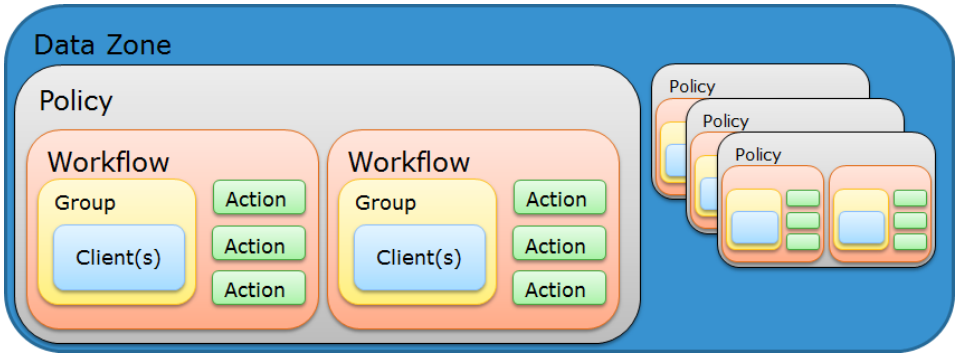
When you create an action for a policy that is associated with the virtual machine backup, you can select one of the following data protection action types:

- Backup — Performs a backup of virtual machines in vCenter to a Data Domain system. You can only perform one VMware backup action per workflow. The VMware backup action must occur before clone actions.
- Clone — Performs a clone of the VMware backup on a Data Domain system to any clone device that NetWorker supports (including Data Domain system or tape targets). You can specify multiple clone actions. Clone actions must occur after the Backup action.

You can create multiple actions for a single workflow. However, each action applies to a single workflow and policy.

The following figure provides a high level overview of the components that make up a data protection policy in a datazone.

Figure 9 Data Protection Policy



Preparing the NetWorker data zone

Review the following requirements.

- Before you configure backup and clone operations, create a DD Boost device and configure the Data Domain management host in NetWorker.
- Before you use file-level restore and instant access restore, enable NFS on the Data Domain System.

Configure the Data Domain System

The Data Domain system must be configured with DD Boost and NFS before configuring vProxy policies.

Procedure

1. Use a web browser to log in to the **Data Domain System Manager** as the system administrator user.

2. In the left navigation pane, select **Protocols** > **DD Boost**.
3. On the **Settings** tab that is located near the top of the page, perform the following tasks:
   a. Ensure that the **DD Boost Status** is **Enabled**.
   b. If it does not appear, add the appliance to the **Allowed Clients** table:
      a. Click the **+** (Add) button that is located above the table and to the right.
      b. In the **Client** field, specify the fully qualified domain name (FQDN) of the host.
      c. In the **Authentication mode** list, select **None**.
      d. In the **Encryption Strength** list, select **None**.
      e. Click **OK**.

      Note: By default, all clients (*) are allowed to access DD Boost.

   c. If it does not exist, add the DD Boost user to the **Users with DD Boost Access** table:
      a. Click the **+** (Add) button that is located above the table and to the right.
      b. In the **User** list, select an existing local user, or select **Create a new Local User** and then create a user account.
      c. Click **Add**, and then click **Close**.
4. For file-level restore and instant access restore only, on **Protocols**, select **NFS**, ensure that **NFS status** is enabled, and then click **OK**.

   The vProxy appliance dynamically creates and deletes the NFS shares, as required.

VMware backups in the NetWorker Management Web UI

You can use the **NetWorker Management Web UI** to create VMware protection policies for the vProxy appliance, and then schedule backups of these policies.

Setting up and configuring data protection policies for the vProxy appliance in NetWorker involves the following tasks:

- Create a policy.
- Creating a VMware protection group.
- (Optional) Create rules.
- Create a workflow.
- Creating one or more action(s).

Policies, workflows, and actions in NetWorker Management Web UI

In NetWorker Management Web UI, you must use the **Policy** wizard to create policies, workflows, and actions.

The following topics provide more information:

- Create a policy using the NetWorker Management Web UI

- Create a workflow using the NetWorker Management Web UI
- Create an action using the NetWorker Management Web UI

Create a policy using the NetWorker Management Web UI

You can use the NetWorker Management Web UI to create data protection policies.

Procedure

1. Select **Protection** > **Policies**.

   The available data protection policies that you can use appears. The details of the selected policy appear in the right pane.

2. Click **ADD**.

   The **Create Policy** wizard appears.

3. Under **Basic Configuration**, in the **Name** field, type a name for the policy.
4. In the **Description** box, type a description for the policy.
5. Select **Enable Protection Period** to specify the protection period.
6. Enter the protection period value in minutes, hours, days, months, or years.
7. Click **NEXT**.
8. Under **Notifications**, from the **Notify** list, select an appropriate notification option.
   - To avoid sending notifications, select **Ignore**.
   - To send notifications with information about each successful and failed workflow and action after all the actions in the policy complete, select **On Completion**.
   - To send a notification with information about each failed workflow and action after all the actions in the policy complete, select **On Failure**.
9. Under **Notify**, when you select the **On Completion** option or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file.

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the Protecting virtual machines `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.
   Use the default mailer program on Linux to send email messages or the smtpmail application on Windows:
   - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:
     `nsrlog -f policy_notifications.log`
   - On Linux, to send an email notification, type the following command:
     `mail -s subject recipient`
   - For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:
     `/usr/sbin/sendmail -v recipient_email "subject_text"`
   - On Windows, to send a notification email, type the following command:
     `smtpmail -s subject -h mailserver recipient1@mailserver recipient2@mailserver...`

where:

- *-s subject*—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the smtpmail program assumes that the message contains a correctly formatted email header and nothing is added.
- *-h mailserver*—Specifies the hostname of the mail server to use to relay the SMTP email message.
- *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

10. Click **FINISH**.

After you finish

You can now create the workflow, group, and actions for the policy.

Edit a policy using the NetWorker Management Web UI

To edit a policy using the NetWorker Management Web UI, perform the following:

Procedure

1. Select **Protection** > **Policies**.

   The available data protection policies that you can use appears.

2. Select the policy that you want to modify, and click **EDIT**.
   - Under **Basic Configuration**, make the required changes.
   - Under **Notification**, make the required changes.
3. Click **Save**.

   Note: If you want to delete a policy, select the policy that you want to delete, and click **Delete**.

Create a workflow using the NetWorker Management Web UI

You can create a workflow after you create a new policy, or you can create a workflow for an existing policy.

Procedure

1. Select **Protection** > **Policies**.

   The available data protection policies that you can use appears.

2. Click on an existing policy or the policy that you created.

   The details of the selected policy appear in the right pane.

3. Click **ADD**.
4. Under **Basic Configuration**, in the **Name** field, type a name for the workflow, or use the default name.

   The maximum number of allowed characters for the Name field is 64. This name cannot contain spaces or special characters such as + or %.

5. In the **Description** box, type a description for the workflow.
6. Under **Schedule**, do the following:

   a. Select **AutoStart** to start the workflow at the time that is specified in the Start time attribute.

b. Use the **Start Time** spin boxes to specify the time to start the actions in the workflow.

c. Use the **Interval** attribute spin boxes to specify how frequently to run the actions that are defined in the workflow over a 24-hour period. The default Interval attribute value is 24 hours, or once a day. When you select a value that is less than 24 hours, the **Interval End** attribute appears. To specify the last start time in a defined interval period, use the spin boxes.

d. Use the **Restart Window** attribute spin boxes to specify the duration of time in which NetWorker can manually or automatically restart a failed or canceled workflow.

7. Under **Notifications**, from the **Notify** list, select an appropriate notification option.
   - To use the notification configuration that is defined in the policy resource to specify when to send a notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action after all the actions in the policy complete, select **On Completion**.
   - To send a notification with information about each failed workflow and action after all the actions in the policy complete, select **On Failure**.
8. Under **Notify**, when you select the **On Completion** option or **On failure** option, the **Command** field appears. Use this field to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file.

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the Protecting virtual machines `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.
   Use the default mailer program on Linux to send email messages or the smtpmail application on Windows:

   - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:
     `nsrlog -f policy_notifications.log`
   - On Linux, to send an email notification, type the following command:
     `mail -s subject recipient`
   - For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:
     `/usr/sbin/sendmail -v recipient_email "subject_text"`
   - On Windows, to send a notification email, type the following command:
     `smtpmail -s subject -h mailserver recipient1@mailserver recipient2@mailserver...`

     where:

     - *-s subject*—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the smtpmail program assumes that the message contains a correctly formatted email header and nothing is added.
     - *-h mailserver*—Specifies the hostname of the mail server to use to relay the SMTP email message.

- *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

9. Click **NEXT**.
10. Under **Associate Group**, do one of the following to assign the workflow to a group:
    - Select an existing group, and click **FINISH** to create a workflow.
    - Click **ADD** to create a group. The section Create a VMware group using the NetWorker Management Web UI provides more information on creating groups.

After you finish

Create the actions that will occur in the workflow.

Edit a workflow using the NetWorker Management Web UI

To edit a workflow using the NetWorker Management Web UI, perform the following:

Procedure

1. Select **Protection** > **Policies**.

   The available data protection policies that you can use appears.
2. Click on an existing policy to view the workflows associated with the policy.
3. Select the workflow that you want to modify, and click **EDIT**.
   - Under **Basic Configuration**, make the required changes.
   - Under **Notification**, make the required changes.
   - Under **Associate Group**, make the required changes.
4. Click **Save**.

   Note: If you want to delete a workflow, select the workflow that you want to delete, and click **Delete**.

Create an action using the NetWorker Management Web UI

Actions are the key resources in a workflow for a data protection policy and define a specific task, for example, a backup or a clone. An action is the task that occurs on the client resources in the group assigned to the workflow. You can chain multiple actions together to occur sequentially or concurrently in a workflow.

Before you begin

Create the required policy and workflow.

About this task

To create an action:

Procedure

1. Select **Protection** > **Policies**.

   The available data protection policies that you can use appears. The details of the selected policy appear in the right pane.
2. Click on an available policy to create a new workflow or view existing workflows.

3. Click on an existing workflow to create an action. The action type can be one of the following:
   - Backup (Backup Subtype—VMware (vProxy))—Performs a backup of virtual machines in vCenter to a Data Domain system. You can only perform one VMware backup action per workflow. The VMware backup action must occur before clone actions.
   - Clone—Performs a clone of the VMware backup on a Data Domain system to any clone device that NetWorker supports (including Data Domain system or tape targets). You can specify multiple clone actions. Clone actions must occur after the Backup action.

   Note:
   - If you have a VMware group associated with the workflow, the first action that you can create is always a backup action, followed by any number of clone actions.
   - If you have a clone protection group (for example, Save Set ID) associated with the workflow, you can only create clone actions.
   - If you do not have any groups associated with the workflow, you can either create a backup or a clone action.

   - The section Create a VMware backup action using the NetWorker Management Web UI provides more information on creating VMware backup actions.
   - The section Create a clone action using the NetWorker Management Web UI provides more information on creating clone actions.

Create a VMware backup action using the NetWorker Management Web UI

You can use the NetWorker Management Web UI to create a VMware backup action.

Before you begin

Create the required policy and workflow.

Procedure

1. Select **Protection** > **Policies**.

   The available data protection policies that you can use appears. The details of the selected policy appear in the right pane.
2. Click on an available policy to create a new workflow or view existing workflows.
3. Click on an existing workflow with the appropriate group association, or create a new workflow, and click **ACTION**.
4. From the **ACTION** list, select **Backup** > **VMWare** to create a VMware backup action.
5. Under **Basic Configuration**, in the **Name** field, type the name of the action, or use the default name.

   The maximum number of characters for the action name is 64.
6. In the **Description** field, type a description for the action.
7. To ensure that the action runs when the policy or workflow that contains the action is started, select **Enabled**. To prevent the action from running when the

policy or workflow that contains the action is started, clear this option. By default, this option is selected.

8. Click **NEXT**.
9. From the **Destination Storage Node** list, select the storage node that contains the devices where you want to store the backup data.

   Note: When you deploy the vCenter server in the Cloud, a parameter displays in the backup action logs that indicates HypervisorMode: VMC. When not deployed in the Cloud, the parameter indicates HypervisorMode: vSphere.

10. From the **Destination Pool**, select the media pool in which to store the backup data.
11. Specify the **NetWorker Retention Period** value.

    After the retention period expires, the save set is removed from the client file index and marked as recyclable in the media database during an expiration server maintenance task.

12. Select **Apply Lock** under **DD Retention Lock** to enable retention lock for the virtual machines included in this backup action. Note that the device used for backing up these virtual machines must also have DD Retention lock enabled.
13. Use the **Lock Period** spin boxes to specify the duration the virtual machines will remain on the Data Domain device before the retention lock expires.
14. Click **NEXT**.
15. Under **VMware-specific Configuration**, select one of the following vProxy options:

    - **Automatic**—Select this option to allow NetWorker to choose the vProxy host for backups.
    - **Manual**—Specify this option to select the vProxy host that NetWorker users for backups. Provide the name of the vProxy host in the **vProxy Name** field.

16. Under **Application Consistency**, select **Quiesce Application** to enable application-consistent protection as part of the policy backup action, which includes protection of the Microsoft SQL Server. You can then select from the **Basic** and **Advanced** options.

    - Select the **Basic** option to create a backup copy for applications during virtual machine quiescing. No additional processing is performed.
    - Select the **Advanced** option to create an SQL server application-consistent backup during virtual machine quiescing, and optionally create a transaction log backup for all SQL Server instances.

    When you select the **Advanced** option, the following additional options appear:

    - **Transaction Log Backup**—Select this option, if you want to perform a transaction log backup of SQL databases in the virtual machine as part of the policy backup action.

      Note: During SQL Server configuration, the NT AUTHORITY\SYSTEM login must be granted SQL login and SQL sysadmin role rights in order to perform transaction log backups.

    - **Quiesce Timeout**—Specify the amount of time, in minutes, to wait for the quiesce operation on the virtual machine to time out before failing. If not selected, the backup action proceeds even if quiescing was not performed,

unless a validation problem occurs. If an application-consistent backup cannot complete due to a problem with validation, the backup action fails even if this option is not selected.

- **System Administrator Username** and **System Administrator Password**—Specify the virtual machine credentials for a user with administrative privileges. All virtual machines in the workflow must use the same System Administrator username/password.

Note: If you select the Advanced option, application-consistent processing is applied for all virtual machines within the parent workflow. When selecting this option, ensure that the policy's workflow and client groups are provisioned specifically for virtual machines that require advanced application-consistent protection. NetWorker will always attempt to perform advanced application processing for virtual machines in a workflow that contains a backup action with advanced application processing enabled.

17. Click **NEXT**.
18. Select a schedule configuration:
    - **Select**—Allows you to select a pre-defined schedule that is applicable to the selected action type, or create a new schedule. Click **ADD SCHEDULE** to create a new schedule. The section Create a schedule using the NetWorker Management Web UI provides more information on creating schedules.
      Note: For VMware backup actions, you can only select or create a VMware type schedule.
    - **Define**—Allows you to define a schedule.

    For **Define**, do the following:

    a. Specify a weekly or monthly recurrence schedule for the action.
       - To specify a schedule for each day of the week, select **Weekly**.
       - To specify a schedule for each day of the month, select **Monthly**.

    b. Click on each day to specify the type of backup to perform.

       The backup levels for NetWorker includes the following:

       - **Full**—Perform a full backup on the specified day. Full backups include all files, regardless of whether the files changed.
       - **Incr**—Perform an incremental backup on the specified day. Incremental backups include files that have changed since the last backup of any type (full or incremental).
       - **Logs Only**—Perform a backup of only database transaction logs.
       - **Skip**—Do not perform a backup on the specified day.

       To perform the same type of backup on each day, click , and select one of the following:

       - Make All Full
       - Make All Incremental
       - Make All Logs Only

- Make All Skip

c. (Optional) Select **Override Options** to configure overrides for the task that is scheduled on a specific day.

Note: If you select this option, you must configure the overrides using either fixed dates or recurring dates.

d. Click **NEXT**.

19. Under **Schedule Overrides**, do the following:

a. In the **Recurring Pattern** attribute, if the status is **Not Available**, click **ADD**. Otherwise, click **VIEW/EDIT** to specify recurring patterns. Then, select the backup level, and define the override schedule to occur on a specific day, week, month, quarter, or year.

The selected date is highlighted with a different color and an asterisk (*).

b. To specify a fixed date pattern, select the month and year, and then click on each day to specify the backup level.

The selected date is highlighted with a different color.

Note:

- You can select multiple override dates.
- In the case of a fixed date pattern, to clear an override schedule, click on the day that you want to clear the override for and select **Clear Selection**. The Clear Selection option is not applicable in the case of a recurring pattern.
- If the fixed and the recurring pattern is on the same day, the fixed pattern gets preference. However, if you clear the fixed override schedule, the recurring pattern is displayed.
- When creating overrides, you cannot select the previous month and year. You also cannot create fixed overrides for the days before the current day because the option to change the level is disabled.
- When editing overrides, you can clear existing fixed overrides for the days before the current day. However, you cannot set any new overrides because the option to change the level is disabled.

20. Click **NEXT**.
21. Under **Notifications**, from the **Notify** list, select an appropriate notification option.
    - To avoid sending notifications, select **Ignore**.
    - To send notifications on completion of the action, select **On Completion**.
    - To send a notification only if the action fails to complete, select **On Failure**.
22. Specify the **Command** to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file.

    The default notification action is to send the information to the `policy_notifications.log` file. By default, the Protecting virtual machines `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

Use the default mailer program on Linux to send email messages or the smtpmail application on Windows:

- To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:
  `nsrlog -f policy_notifications.log`
- On Linux, to send an email notification, type the following command:
  `mail -s subject recipient`
- For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:
  `/usr/sbin/sendmail -v recipient_email "subject_text"`
- On Windows, to send a notification email, type the following command:
  `smtpmail -s subject -h mailserver recipient1@mailserver recipient2@mailserver...`

  where:

  - *-s subject*—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the smtpmail program assumes that the message contains a correctly formatted email header and nothing is added.
  - *-h mailserver*—Specifies the hostname of the mail server to use to relay the SMTP email message.
  - *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

23. Click **NEXT**.
24. From the **Start Time** list, select one of the following options to specify the time to start the action. Use the spin boxes to set the hour and minute values.
    - **Set at Workflow level**—Do not enforce an action start time. The action will start at the time defined by the workflow.
    - **Absolute**—Start the action at the time specified by the values in the spin boxes.
    - **Relative**—Start the action after the period of time defined in the spin boxes has elapsed after the start of the workflow.
25. Although the **Retries**, **Retry Delay**, and the **Inactivity Timeout** options appear, this action does not support these options and you can ignore these values.
26. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. The default value is 100.
27. From the **On Failure** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort Action**.
    - To abort the entire workflow if there is a failure with one of the jobs in the action, select **Abort Workflow**.
28. In the **Soft Limit** field, select the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no amount of time.
29. In the **Hard Limit** field, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.

30. Click **NEXT**.

    The Action Configuration Summary appears.

31. Review the settings that you have configured, and then click **FINISH**.

After you finish

(Optional) Create a clone action to automatically clone the save sets after the backup. A clone action is the only supported action after a backup action in a workflow.

Create a clone action using the NetWorker Management Web UI

You can use the NetWorker Management Web UI to create a clone action.

Procedure

1. Select **Protection** > **Policies**.

   The available data protection policies that you can use appears. The details of the selected policy appear in the right pane.

2. Click on an available policy to create a new workflow or view existing workflows.
3. Click on an existing workflow with the appropriate group association, or create a new workflow, and click **ACTION**.
4. From the **ACTION** list, select **Clone** to create a clone action.
5. Under **Basic Configuration**, in the **Name** field, type the name of the action, or use the default name.

   The maximum number of characters for the action name is 64.

6. In the **Description** box, type a description for the action.
7. To ensure that the action runs when the policy or workflow that contains the action is started, select **Enabled**. To prevent the action from running when the policy or workflow that contains the action is started, clear this option. By default, this option is selected.
8. If the action is part of a sequence of actions in a workflow path, from the **Driven By** list, select the action that should precede this action.
9. Click **NEXT**.
10. Select the **Delete source save sets after clone completes** option to instruct NetWorker to delete the data from the source volume after cloning to the destination volume completes. This is equivalent to staging the save sets.
11. Under **Devices and Volumes**, define the volumes and devices to which NetWorker sends the cloned data:

    a. From the **Source Storage Node** list, select the source storage node for a clone action, that is, the storage node from which clone data is read.

    b. From the **Destination Storage Node** list, select the storage node with the devices on which to store the cloned save sets.

    c. From the **Destination Pool** list, select the target media pool for the cloned save sets.

12. Specify the **NetWorker Retention Period** value.

    After the retention period expires, the save set is removed from the client file index and marked as recyclable in the media database during an expiration server maintenance task.

13. If you want to have the same retention period as that of the backup action, select **Keep Retention Same as Backup**.

    Note: If you select this option, you cannot configure the NetWorker retention period.

14. Select **Apply Lock** under **DD Retention Lock** to enable retention lock for the virtual machines included in this clone action.
15. Use the **Lock Period** spin boxes to specify the duration the virtual machines will remain on the Data Domain device before the retention lock expires.
16. Click **NEXT**.
17. (Applicable only for a second clone action) In the **Filter Savesets** section, you can do the following:

    a. To define the criteria that NetWorker uses to create the list of eligible save sets to clone, select **Define Filters**. The eligible save sets must match the requirements that are defined in each filter. NetWorker provides the following filter options:

    - **Time** —In the Time section, specify the time range in which NetWorker searches for eligible save sets to clone in the media database. Use the spin boxes to specify the start time and the end time. The Time filter list includes the following options to define how NetWorker determines save set eligibility, based on the time criteria:
        - **Accept**—The clone save set list includes save sets that are saved within the time range and meet all the other defined filter criteria.
        - **Reject**—The clone save set list does not include save sets that are saved within the time range and meet all the other defined filter criteria.
    - **Backup Levels** —In the Backup Levels section, specify the backup levels that you want to include or exclude, when NetWorker searches for eligible save sets to clone in the media database. The Levels filter list includes the following options, which define how NetWorker determines save set eligibility, based on the backup level filter criteria:
        - **Accept**—The clone save set list includes eligible save sets with the selected backup levels.
        - **Reject**—The clone save set list does not include eligible save sets with the selected backup levels.
    - **Save Sets** —In the Save Sets section, specify whether to include or exclude ProtectPoint and Snapshot save sets, when NetWorker searches for eligible save sets to clone in the media database. The Save Set filter list includes the following options, which define how NetWorker determines save set eligibility, based on the save set filter criteria:
        - **Accept**—The clone save set list includes eligible ProtectPoint save sets or Snapshot save sets, when you enable the ProtectPoint checkbox or Snapshot checkbox.
        - **Reject**—The clone save set list does not include eligible ProtectPoint save sets and Snapshot save sets when you enable the ProtectPoint checkbox or Snapshot checkbox.
    - **Clients** —In the Client section, specify a list of clients to include or exclude, when NetWorker searches for eligible save sets to clone in the media database. The Client filter list includes the following options, which

define how NetWorker determines save set eligibility, based on the client filter criteria:

- **Accept**—The clone save set list includes eligible save sets for the selected clients.
- **Reject**—The clone save set list does not include eligible save sets for the selected clients.

18. If you do not want to define a filter criteria, select **Do Not Filter**, and click **NEXT**.

    Note: The Filter Savesets feature is available only in the case of a second clone action.

19. Specify a weekly or monthly schedule for the action.
    - To specify a schedule for each day of the week, select **Weekly**.
    - To specify a schedule for each day of the month, select **Monthly**.
20. Click on each day to specify the type of backup to perform.
    - **Execute**—Perform a clone action on the specified day.
    - **Skip**—Do not perform a clone action on the specified day.

    To perform the same type of backup on each day, click , and select one of the following:
    - Make All Execute
    - Make All Skip
21. (Optional) Select **Override Options** to configure overrides for the task that is scheduled on a specific day.

    Note: If you select this option, you must configure the overrides using either fixed dates or recurring dates.

22. Click **NEXT**.
23. Under **Schedule Overrides**, do the following:
    a. In the **Recurring Pattern** attribute, if the status is **Not Available**, click **ADD**. Otherwise, click **VIEW/EDIT** to specify recurring patterns. Then, select the backup level, and define the override schedule to occur on a specific day, week, month, quarter, or year.

       The selected date is highlighted with a different color and an asterisk (*).

    b. To specify a fixed date pattern, select the month and year, and then click on each day to specify the backup level.

       The selected date is highlighted with a different color.

       Note:
       - You can select multiple override dates.
       - In the case of a fixed date pattern, to clear an override schedule, click on the day that you want to clear the override for and select **Clear**

Selection. The Clear Selection option is not applicable in the case of a recurring pattern.

- If the fixed and the recurring pattern is on the same day, the fixed pattern gets preference. However, if you clear the fixed override schedule, the recurring pattern is displayed.
- When creating overrides, you cannot select the previous month and year. You also cannot create fixed overrides for the days before the current day because the option to change the level is disabled.
- When editing overrides, you can clear existing fixed overrides for the days before the current day. However, you cannot set any new overrides because the option to change the level is disabled.

24. Click **NEXT**.
25. Under **Notifications**, from the **Notify** list, select an appropriate notification option.
    - To avoid sending notifications, select **Ignore**.
    - To send notifications on completion of the action, select **On Completion**.
    - To send a notification only if the action fails to complete, select **On Failure**.
26. Specify the **Command** to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file.

    The default notification action is to send the information to the `policy_notifications.log` file. By default, the Protecting virtual machines `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.
    Use the default mailer program on Linux to send email messages or the smtpmail application on Windows:

    - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:
      `nsrlog -f policy_notifications.log`
    - On Linux, to send an email notification, type the following command:
      `mail -s subject recipient`
    - For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:
      `/usr/sbin/sendmail -v recipient_email "subject_text"`
    - On Windows, to send a notification email, type the following command:
      `smtpmail -s subject -h mailserver recipient1@mailserver recipient2@mailserver...`

      where:

      - *-s subject*—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the smtpmail program assumes that the message contains a correctly formatted email header and nothing is added.
      - *-h mailserver*—Specifies the hostname of the mail server to use to relay the SMTP email message.
      - *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

27. Click **NEXT**.
28. From the **Start Time** list, select one of the following options to specify the time to start the action. Use the spin boxes to set the hour and minute values.
    - **Set at Workflow level**—Do not enforce an action start time. The action will start at the time defined by the workflow.
    - **Absolute**—Start the action at the time specified by the values in the spin boxes.
    - **Relative**—Start the action after the period of time defined in the spin boxes has elapsed after the start of the workflow.
29. (Optional) Select **Concurrent** to enable concurrent operations for the action.
30. From the **On Failure** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort Action**.
    - To abort the entire workflow if there is a failure with one of the jobs in the action, select **Abort Workflow**.
31. In the **Soft Limit** field, select the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no amount of time.
32. In the **Hard Limit** field, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.
33. Click **NEXT**.

    The Action Configuration Summary appears.
34. Review the settings that you have configured, and then click **FINISH**.

After you finish

(Optional) Create a clone action to automatically clone the save sets again after this clone action.

Edit an action using the NetWorker Management Web UI

To modify an action, perform the following:

Procedure

1. Select **Protection** > **Policies**.

   The available data protection policies that you can use appears. The details of the selected policy appear in the right pane.
2. Click on an available policy to view existing workflows.
3. Click on an existing workflow to view the actions associated with the workflow.
4. Select the action that you want to modify, and click **EDIT**.
5. Make the required changes, and click **SAVE**.

   The action is successfully updated.

Create a save set group using the NetWorker Management Web UI

A save set group defines a static list of save sets for cloning or for snapshot index generation.

Procedure

1. Select **Protection** > **Groups**.

   Groups that have already been created appears. The details of the selected group appears in the right pane.

2. Click **ADD**.

   The **Create Group** wizard appears.

3. In the **Name** field, type a name for the group.
4. (Optional) In the **Description** box, type a description of the group.
5. From the **Type** list, select **Save Set**.
6. (Optional) From the **Policy** list, select a policy that you want to assign the group to.
7. (Optional) From the **Workflow** list, select a workflow that you want to assign the group to.

   Note: The applicable workflows corresponding to the selected policy are only available for selection.

8. Specify a **Filter Type**.
   - **Static**- Represents the save set ID list.
   - **Dynamic** - Represents the save set query.

   If the filter type is **Static**:

   a. Click **NEXT**.

   b. Enter a list of comma separated save set IDs, and click **ADD**.

   Note: You can also use the search function to filter the save set IDs from the **Selected Saveset ID List**.

   c. Click **FINISH**.

   If the filter type is **Dynamic**:

   a. Use the **Maximum number of Clones** spin boxes to specify the number of clones that can be created for the save set.

   b. Click **NEXT**.

   c. (Optional) Specify one or more of the basic save set criteria.

Filter criteria	Description
Time	Specify the start date and time range for the save sets. To specify the current date and time as the end date for the range, select **Up To Now**.

Filter criteria	Description
	To specify a time period, select **Up to**.
Levels	Specify a backup level.
Name	Specify a list of comma separated save set names.

d. Click the **+** icon to add a filter, and click the **-** icon to remove a filter.

e. Click **NEXT**.

f. (Optional) Select the save set resource filter.

Resource filter	Description
Clients	Select client resources associated with the save set.
Workflows	Select the workflow used to generate the save set.
Policies	Select the policy used to generate the save set.
Actions	Select the action used to generate the save set.
Groups	Select the group associated with the save set.
SourcePools	Select the pool on which the save set is stored.

g. Click **FINISH**.

Create a VMware group using the NetWorker Management Web UI

A VMware group allows you to define the virtual machines or virtual disk files to back up within the policy/workflow.

Procedure

1. Select **Protection** > **Groups**.

   Groups that have already been created appears. The details of the selected group appears in the right pane.

2. Click **ADD**.

   The **Create Group** wizard appears.

3. In the **Name** field, type a name for the group.
4. (Optional) In the **Description** box, type a description of the group.
5. From the **Type** list, select **VMware**.
6. (Optional) From the **Policy** list, select a policy that you want to assign the group to.
7. (Optional) From the **Workflow** list, select a workflow that you want to assign the group to.

> **Note:** The applicable workflows corresponding to the selected policy are only available for selection.

8. Select a backup optimization mode.
   - **Capacity** - Use for variable segment sizing.
   - **Performance** - Use for fixed segment sizing.
9. (Optional) Select the Dynamic Association checkbox if you plan to apply rules that will determine which virtual machines and containers are dynamically included in the group based upon the rule criteria.
10. Click **NEXT**.
11. From the **vCenter** list, select a vCenter server that contains the VMware objects that you want to protect, or click **ADD VCENTER** to add a vCenter server.
12. Select a pre-defined rule that you want to apply for any VMware objects that are dynamically included in the group based upon the rule criteria, or click **ADD RULE** to create a new rule and click **EDIT RULE** to modify an existing rule. The section Create or edit a rule using the NetWorker Management Web UI provides more information on creating and editing rules.
13. Under **Include/Exclude Resources**, select the objects (Datacenter, ESXi host, virtual machine, resource pool, vApp, or disk) to include in the group and to view a consolidated list of virtual machines selected statically and evaluated by a rule. You can also exclude virtual machines or disks.
14. Click **Preview** to view a list of the static and dynamic virtual machines and objects that have been added to the group.
15. Click **Finish**.

Edit a group using the NetWorker Management Web UI

To edit a group using the NetWorker Management Web UI, perform the following:

Procedure

1. Select **Protection** > **Groups**.

   Groups that have already been created appears.
2. Select the group that you want to modify.

   The details of the group such as the type, sub type, the backup optimization mode, and the VMware resources appears in the right pane.

   > **Note:** You cannot change the name of the group.
3. Click **EDIT**, and make the required changes.
4. Click **Save**.

   > **Note:** If you want to delete a group, select the group that you want to delete, and click **Delete**.

Create a rule using the NetWorker Management Web UI

You can use the NetWorker Management Web UI to create a rule.

About this task

To create a rule, perform the following:

Procedure

1. Select **Protection** > **Rules**.

   Rules that have already been created appears. The details of the rule such as the datasource type, condition, and usage also appears in the right pane.

2. Click **ADD**.

   The **Add Rules** wizard appears.

3. In the **Name** field, type a name for the rule.
4. Select the **Datasource Type** from the drop-down. The default Datasource Type is VMware.
5. (Optional) In the **Description** box, you can specify more information about the rule.
6. Specify a matching condition. You can select **All** as the match type, if the item has to meet all of the rules criteria or select **Any** to include the item, if the item meets any of the criteria.

   a. Specify the VMWare object type. You can select one of the following:

   - Virtual Machine
   - ESXi Host/Cluster
   - Virtual App
   - Virtual Machine Folder
   - Datacenter
   - Resource Pool

   b. Specify the object type properties that the rule uses to determine a match. It can be the object's name, path, or tag. The available properties depend on the object type.

   - Virtual Machine - name, vSphere tag
   - ESXi Host/Cluster - path, vSphere tag
   - Virtual App - name, vSphere tag
   - Virtual Machine Folder - name, path, vSphere tag
   - Datacenter - name, path, vSphere tag
   - Resource Pool - path, vSphere tag

   c. Select an operator to further define how a match is made based on the selected object type property. The operator value can be one of the following:

   - equals
   - not equals
   - contains
   - not contains
   - starts with
   - does not start with
   - ends with
   - does not end with

- regular expression

d. Click the **Browse** icon to select the vCenter server and vSphere tag and click **OK** to exit the dialog.

> **Note:** This option is available only if you select the vSphere tag property type in the definition.

e. Click the **+** icon to add a rule definition, and click the **-** icon to remove a rule definition.

7. Click **Create**.

   The Rule is successfully created.

8. Repeat steps 1 through 7 for any additional rules that you want to create.

> **Note:** You can associate a rule to a group, if dynamic selection is enabled when creating groups. The section Create a VMware group using the NetWorker Management Web UI provides more information on creating groups.

Edit a rule using the NetWorker Management Web UI

To edit a rule, perform the following:

Procedure

1. Select **Protection** > **Rules**.

   Rules that have already been created appears. The details of the rule such as the datasource type, condition, and usage also appears in the right pane.

2. Select the rule that you want to modify, and click **EDIT**.
3. Make the required changes, and click **SAVE**.

   The rule is successfully updated.

> **Note:**
>
> - You cannot change the name of a rule.
> - If you want to delete a rule, select the rule that you want to delete, and click **Delete**. However, a rule cannot be deleted, if it is associated with a group.

vProxy backups in NMC

You can use the NMC **NetWorker Administration** window to create VMware protection policies for the vProxy appliance, and then schedule backups of these policies.

Setting up and configuring data protection policies for the vProxy appliance in NetWorker involves the following tasks:

- Create a policy.
- Create a workflow.
- Create a VMware protection group.

- (Optional) Create dynamic associations to apply rules.
- Create one or more action(s).

Default data protection policies in NMC's NetWorker Administration window

The NMC **NetWorker Administration** window provides you with pre-configured data protection policies that you can use immediately to protect the environment, modify to suit the environment, or use as an example to create resources and configurations. To use these pre-configured data protection policies, you must add clients to the appropriate group resource.

Note: NMC also includes a pre-configured Server Protection policy to protect the NetWorker and NMC server databases.

Platinum policy

The Platinum policy provides an example of a data protection policy for an environment that contains supported storage arrays or storage appliances and requires backup data redundancy. The policy contains one workflow with two actions, a snapshot backup action, followed by a clone action.

Figure 10 Platinum policy configuration

Gold policy

The Gold policy provides an example of a data protection policy for an environment that contains virtual machines and requires backup data redundancy.

Silver policy

The Silver policy provides an example of a data protection policy for an environment that contains machines where file systems or applications are running and requires backup data redundancy.

Bronze policy

The Bronze policy provides an example of a data protection policy for an environment that contains machines where file systems or applications are running.

Create a VMware policy in NetWorker Administration

If you do not want to use the default "Gold" policy for the protection of virtual machines, you can create a new VMware policy by using the following procedure in the NMC **NetWorker Administration** window.

Procedure

1. On the **NetWorker Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Policies**, and then select **New**.

   The **Create Policy** dialog box appears.
3. On the **General** tab, in the **Name** field type a name for the policy.

   The maximum number of characters for the policy name is 128.

Note: This name cannot contain spaces or special characters such as + or %. After you create a policy, the **Name** attribute is read-only.

4. In the **Comment** box, type a description for the policy.
5. From the **Send Notifications** list, select whether to send notifications for the policy:
   - To avoid sending notifications, select **Never**.
   - To send notifications with information about each successful and failed workflow and action after all the actions in the policy complete, select **On Completion**.
   - To send a notification with information about each failed workflow and action after all the actions in the policy complete, select **On Failure**.
6. In the **Send notification** attribute, when you select the **On Completion** option or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file or you can send an email notification.

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

   Use the default mailer program on Linux to send email messages or the `smtpmail` application on Windows:

   - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

     `nsrlog -f policy_notifications.log`
   - On Linux, to send an email notification, type the following command:

     `mail -s` ***`subject recipient`***
   - For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:

     `/usr/sbin/sendmail -v` ***`recipient_email`*** **`"`*****`subject_text`*****`"`**
   - On Windows, to send a notification email, type the following command:

     `smtpmail` **`-s`** ***`subject`*** **`-h`** ***`mailserver recipient1@mailserver recipient2@mailserver...`***

     where:

     - **`-s`** ***`subject`***—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the `smtpmail` program assumes that the message contains a correctly formatted email header and nothing is added.
     - **`-h`** ***`mailserver`***—Specifies the hostname of the mail server to use to relay the SMTP email message.
     - *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

7. In the **Restricted Data Zones** tab, leave the **Restricted Data Zone** field blank. NetWorker VMware Protection with the vProxy appliance does not currently support the protection of virtual machines within a Restricted Data Zone.
8. Click **OK**.

After you finish

You can now create the workflow, group, and actions for the policy.

Create a workflow for a new policy in NetWorker Administration

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the left pane, expand **Policies**, and then select the policy that you created.
3. In the right pane, select **Create a new workflow**.
4. In the **Name** field, type the name of the workflow.

   The maximum number of allowed characters for the **Name** field is 64.

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

5. In the **Comment** box, type a description for the workflow.

   The maximum number of allowed characters for the **Comment** field is 128.
6. From the **Send Notifications** list, select how to send notifications for the workflow:
   - To use the notification configuration that is defined in the policy resource to specify when to send a notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after the workflow completes all the actions, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after the workflow completes all the actions, select **On Failure**.
7. In the **Send notification** attribute, when you select the **On Completion** option or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file or you can send an email notification.

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

   Use the default mailer program on Linux to send email messages, or use the `smtpmail` application on Windows:

   - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

     ```
     nsrlog -f policy_notifications.log
     ```

   - On Linux, to send an email notification, type the following command:

     ```
     mail -s subject recipient
     ```

- For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:

  /usr/sbin/sendmail -v *recipient_email* "*subject_text*"

- On Windows, type the following command:

  smtpmail **-s *subject* -h *mailserver* *recipient1@mailserver* *recipient2@mailserver...***

  where:

  - **-s *subject***—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the smtpmail program assumes that the message contains a correctly formatted email header and nothing is added.
  - **-h *mailserver***—Specifies the hostname of the mail server to use to relay the SMTP email message.
  - *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

8. In the **Running** section, perform the following steps to specify when and how often the workflow runs:

   a. To ensure that the actions that are contained in the workflow run when the policy or workflow starts, in the **Enabled** box, leave the option selected. To prevent the actions in the workflow from running when the policy or workflow that contains the action starts, clear this option.

   b. To start the workflow at the time that is specified in the **Start time** attribute, on the days that are defined in the action resource, in the **AutoStart Enabled** box, leave the option selected. To prevent the workflow from starting at the time that is specified in the **Start time** attribute, clear this option.

   c. To specify the time to start the actions in the workflow, in the **Start Time** attribute, use the spin boxes.

      The default value is 9:00 PM.

   d. To specify how frequently to run the actions that are defined in the workflow over a 24-hour period, use the **Interval** attribute spin boxes. If you are performing transaction log backup as part of application-consistent protection, you must specify a value for this attribute in order for incremental transaction log backup of SQL databases to occur.

      The default **Interval** attribute value is 24 hours, or once a day. When you select a value that is less than 24 hours, the **Interval End** attribute appears. To specify the last start time in a defined interval period, use the spin boxes.

   e. To specify the duration of time in which NetWorker can manually or automatically restart a failed or canceled workflow, in the **Restart Window** attribute, use the spin boxes.

      If the restart window has elapsed, NetWorker considers the restart as a new run of the workflow. NetWorker calculates the restart window from the start of the last incomplete workflow. The default value is 24 hours.

      For example, if the **Start Time** is 7:00 PM, the **Interval** is 1 hour, and the **Interval End** is 11:00 PM., then the workflow automatically starts every hour beginning at 7:00 PM. and the last start time is 11:00 PM.

9. To create the workflow, click **OK**.

After you finish

Create the actions that will occur in the workflow, and then assign a group to the workflow. If a workflow does not contain a group, a policy does not perform any actions.

Create a workflow for an existing policy in NetWorker Administration

A policy can contain one or more unique workflows.

Before you begin

- Create a policy for the workflow.
- (Optional but recommended) Create a group of client resources or save sets to assign to the workflow.

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the expanded left pane, select **Policies**.
3. Select the policy for the workflow.
4. In the right pane of the window, select the **Workflows** tab.
5. Right-click an empty area of the **Workflows** tab and select **New**.

   The **New Workflow** dialog box appears.
6. In the **Name** field, type the name of the workflow.

   The maximum number of allowed characters for the **Name** field is 64.

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}
7. In the **Comment** box, type a description for the workflow.

   The maximum number of allowed characters for the **Comment** field is 128.
8. From the **Send Notifications** list, select how to send notifications for the workflow:

   - To use the notification configuration that is defined in the policy resource to specify when to send a notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after the workflow completes all the actions, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after the workflow completes all the actions, select **On Failure**.
9. In the **Send notification** attribute, when you select the **On Completion** option or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file or you can send an email notification.

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

Use the default mailer program on Linux to send email messages or the `smtpmail` application on Windows:

- To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

  `nsrlog -f policy_notifications.log`

- On Linux, to send an email notification, type the following command:

  `mail -s subject recipient`

- On Windows, type the following command: `smtpmail` **`-s subject -h mailserver recipient1@mailserver recipient2@mailserver...`** where:
  - **`-s subject`**—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the `smtpmail` program assumes that the message contains a correctly formatted email header and nothing is added.
  - **`-h mailserver`**—Specifies the hostname of the mail server to use to relay the SMTP email message.
  - *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

10. In the **Running** section, perform the following steps to specify when and how often the workflow runs:
    a. To ensure that the actions that are contained in the workflow run when the policy or workflow starts, in the **Enabled** box, leave the option selected. To prevent the actions in the workflow from running when the policy or workflow that contains the action starts, clear this option.
    b. To start the workflow at the time that is specified in the **Start time** attribute, on the days that are defined in the action resource, in the **AutoStart Enabled** box, leave the option selected. To prevent the workflow from starting at the time that is specified in the **Start time** attribute, clear this option.
    c. To specify the time to start the actions in the workflow, in the **Start Time** attribute, use the spin boxes.

       The default value is 9:00 PM.

    d. To specify how frequently to run the actions that are defined in the workflow over a 24-hour period, use the **Interval** attribute spin boxes. If you are performing transaction log backup as part of application-consistent protection, you must specify a value for this attribute in order for incremental transaction log backup of SQL databases to occur.

       The default **Interval** attribute value is 24 hours, or once a day. When you select a value that is less than 24 hours, the **Interval End** attribute appears. To specify the last start time in a defined interval period, use the spin boxes.

    e. To specify the duration of time in which NetWorker can manually or automatically restart a failed or canceled workflow, in the **Restart Window** attribute, use the spin boxes.

       If the restart window has elapsed, NetWorker considers the restart as a new run of the workflow. NetWorker calculates the restart window from the start of the last incomplete workflow. The default value is 24 hours.

For example, if the **Start Time** is 7:00 PM, the **Interval** is 1 hour, and the **Interval End** is 11:00 PM., then the workflow automatically starts every hour beginning at 7:00 PM. and the last start time is 11:00 PM.

11. In the **Groups** group box, specify the protection group to which the workflow applies.

    To use a group, select a protection group from the **Groups** list. To create a protection group, click the **+** button that is located to the right of the **Groups** list.

12. The **Actions** table displays a list of actions in the workflow. To edit or delete an action in the workflow, select the action and click **Edit** or **Delete**. To create one or more actions for the workflow, click **Add**.

    The **Actions** table organizes the information in sortable columns. Right-click in the table to customize the attributes that appear.

13. To create the workflow, click **OK**.

Create or edit a VMware group in NetWorker Administration

A VMware group allows you to define the virtual machines or virtual disk files to back up within the policy/workflow.

Before you begin

Ensure that you perform the steps in the section Adding the vCenter host to VMware View and creating the vCenter client resource, and confirm that the map appears.

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Groups** and select **New** from the drop-down, or right-click an existing group and select **Edit** from the drop-down.

   The **Create Group** or **Edit Group** dialog box appears, with the **General** tab selected.
3. In the **Name** attribute, type a name for the group.

   The maximum number of characters for the group name is 64.

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

   Note: After you create a group, the **Name** attribute is read-only.

4. From the **Group Type** list, select **VMware**.
5. From the **Sub-Type** list, select **ALL**.

   NetWorker does not support other sub-types in this configuration.
6. From the **Optimization** drop-down, select a backup optimization mode. **Capacity** is for variable segment sizing, while **Performance** is for fixed segment sizing.
7. In the **Comment** field, type a description of the group.
8. From the **Policy-Workflow** list, select the workflow that you want to assign the group to.

> **Note:** You can also assign the group to a workflow when you create or edit a workflow.

9. (Optional) Select the **Dynamic Association** checkbox if you plan to apply rules that will determine which virtual machines and containers are dynamically included in the group based upon the rule criteria. The section Enabling a VMware group with Dynamic Association and applying rules in NMC provides more information on enabling a policy/group with **Dynamic Association** and applying rules.
10. From the **vCenter** drop-down, select the vCenter server that contains the VMware objects that you want to protect, and then select the objects (Datacenter, ESX host, virtual machine, resource pool, vApp, or disk) to include in this group. Any objects selected here will be considered static objects, which means that the items will be included in the group until unselected, even when **Dynamic Association** is enabled.

    > **Note:** If the vCenter list is empty, cancel the task and, using the NMC **Protection** window, right-click **VMware View** in the left pane, and select **Refresh**.

11. (Optional) If the group as **Dynamic Association** enabled, from the **Rule** drop-down, select a pre-defined rule that you want to apply for any VMware objects that will be dynamically included in the group based upon the rule criteria, or click **+** to open the **Create Rule** window and create a new rule. The section Enabling a VMware group with Dynamic Association and applying rules in NMC provides more information on associating a VMware group with rules.
12. Click **Preview All Virtual Machines** to view a list of the static and dynamic virtual machines and objects that have been added to the group. In this window, you can also unselect a virtual machine or VMDK to exclude the item from the backup. When an object is unselected, an entry for the object appears in the **Excluded VM** list.
13. Click **OK** to exit the **Preview Virtual Machines** window, and then click **OK** to finish creating or editing the group.

vProxy backup optimization modes

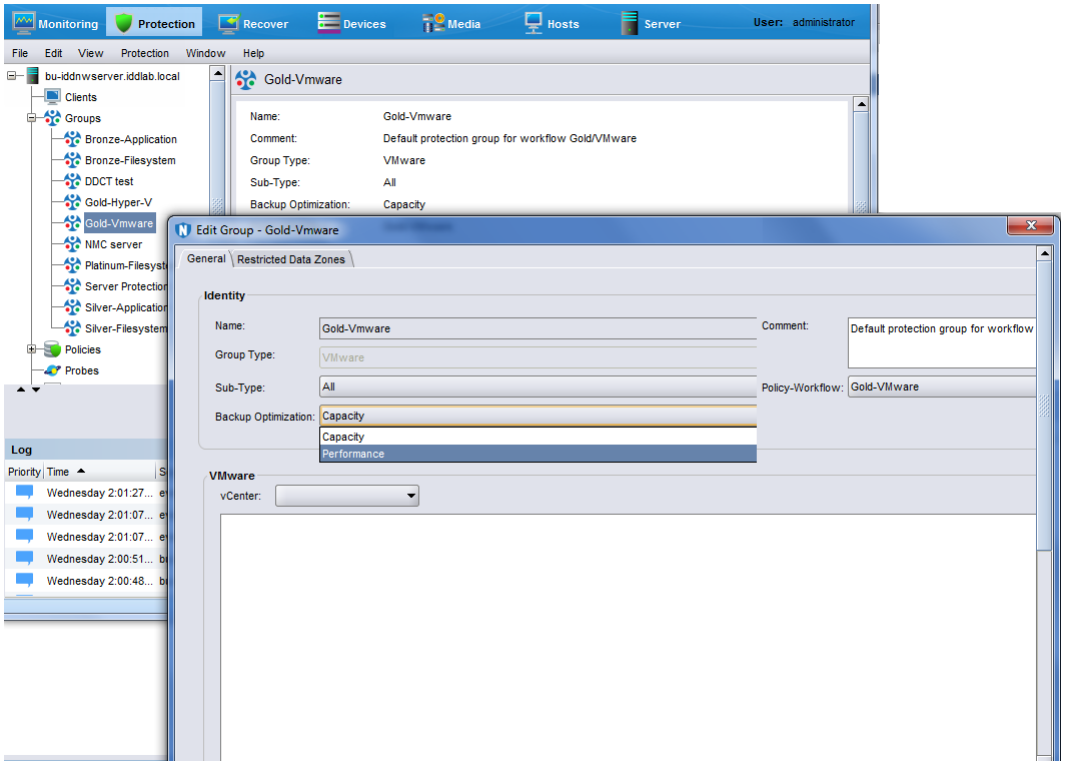
NetWorker supports two types of backup optimization modes for vProxy backup to Data Domain systems—**Optimized for Capacity**, and **Optimized for Performance**. You can apply the optimization mode to vProxy protection groups during backup.

The **Optimized for Capacity** mode uses variable size segmentation, which produces more overhead in data processing due to the higher deduplication rate, but reduces the capacity consumed on the Data Domain system. Virtual machines backed up prior to NetWorker 9.1 use the **Optimized for Capacity** mode.

Optimized for Performance provides performance improvements when you back up virtual machines using Changed Block Tracking (CBT) and replicate data to a Data Domain system, and is particularly effective when backing up large VMDK files. Although **Optimized for Performance** results in additional space use on the Data Domain device (around 20%), this mode significantly improves random I/O performance for instant access restores.

New and upgraded installations of NetWorker use the **Optimized for Capacity** mode by default. For a vProxy protection group, you can change this setting to **Optimized for Performance** by using NMC, `nsradmin`, or `nsrpolicy`. The following figure displays the backup optimization setting within a vProxy protection group in NMC.

Figure 11 Changing the Backup Optimization mode in the vProxy protection group



Software and storage requirements for Optimized for Performance mode

Using **Optimized for Performance** requires DDOS version 6.0.0.30 and later. A warning log message will be generated. Also, cloning of **Optimized for Performance** save sets is supported only between DDOS platforms that natively support this mode.

Requirements when changing backup optimization modes

Changing a virtual machine from one backup optimization mode to another (for example, from **Optimized for Capacity** to **Optimized for Performance**) requires performing a new full level-zero backup as the starting point for subsequent backups. Ensure that the Data Domain device has sufficient capacity. Since backups for each optimization mode must coexist during this period, backups will consume twice the usual storage capacity until the last **Optimized for Capacity** backup expires, as defined by the retention period. After this, storage consumption will return to normal.

Enabling a VMware group with Dynamic Association and applying rules

When you create or edit a VMware protection group, enabling the **Dynamic Association** option for the group will allow you to assign rules. Rules can be used to determine which virtual machines and containers will be protected by the group in addition to any objects that have been manually selected for inclusion. You can use the NMC **NetWorker Administration** window or the **NetWorker Management Web user interface** to create rules and assign rules to a group. These operations are not supported from the command line or the vCenter plug-in.

A VMware group with **Dynamic Association** enabled can include both static and dynamic objects:

- Virtual machines and containers from the vCenter that are manually selected when you create or edit the group in NMC are known as static objects, because their inclusion in the group does not change unless you unselect an item.
- Virtual machines and containers that are only included in the group according to the rules assigned when you create or edit the group in NMC are known as dynamic objects, because their inclusion in the group can change over time based on whether the items continue to match the rule criteria.

When creating or editing the group, you can preview both static and dynamic contents to ensure that the protection policy will include all the virtual machines and containers that you want protect in the backup. Additionally, you can specify a virtual machine exclusion list for the VMware protection group to exclude particular virtual machines or VMDKs from being backed up as part of the group.

When a VMware protection group is associated with one or more rules, the rules are executed against the vCenter inventory when the policy backup is started in order to filter the group contents according to the rule criteria.

Creating and viewing tags in the vSphere Web Client

In order to support the dynamic selection of VMware objects based on the user-defined rules created in NMC, vSphere tags in the **vSphere Web Client** allow you to attach metadata to the objects in the vSphere inventory to make these objects easier to sort and search. Tags are supported in vSphere versions 6.5 and later.

When you create a tag in the **vSphere Web Client**, the tag can be assigned to a category in order to group related tags together. When defining a category, you can also specify the object types the tags will be applied to, and whether more than one tag in the category can be applied to an object. Within a single rule, there is a maximum limit of 50 rule definitions applicable to tags and categories, as shown in the following example where *Category* is the category name and *Bronze* is the tag name:

- Category:*Category*1,Tag:*Bronze*1
- Category:*Category*2,Tag:*Bronze*2
- Category:*Category*3,Tag:*Bronze*3
- and so on up to Category:*Category*50,Tag:*Bronze*50

In the above example, if the number of characters associated with category name or tag name are more than 9 or 7 characters respectively, then the maximum limit for rule definitions in a single rule will be further reduced from 50. Exceeding the maximum limit for rule definitions will result in no virtual machines being backed up as part of this group, since there will be no members associated with the group. As a best practice, it is recommended to keep the number of rule definitions within a single rule to 10 or less and, in cases where there are a large number of rule definitions within a single rule, it is also recommended to keep the number of characters in category/tag names to 10 or less.

The **vSphere Web Client** displays any tags that have been created for the vCenter under Tags & Custom Attributes in the left pane. When you click **Tags & Custom Attributes**, select the **Tags** tab. A table lists the available tags. Click on a tag link in the table to view the objects associated with this particular tag.

Note: Once virtual machines are associated with tags, the association will not be reflected in the NMC **NetWorker Administration** window's **VMware View** until the timeout period has completed. The default timeout for NetWorker to fetch the latest inventory from vCenter is 15 minutes.

Rules in the NMC NetWorker Administration window

Rules are used to automatically map VMware objects (virtual machines and containers) to a group by using one or more filtering mechanisms, according to the following supported rule criteria:

- Type: The VMware object type. Available selections include VM, VApp, VM Folder, Datacenter, Host/Cluster, or Resource Pool.
- Properties: The object type properties that the rule uses to determine a match. These properties include the object's name, path or a tag that you've created, and available properties depend on the object type, as specified below.
  Host/Cluster - Path, tag

  VMfolder - Name, path, tag

  Datacenter - Name, path, tag

  ResourcePool - Path, tag

  VirtualMachine - Name, tag

  vApp - Name, tag
- Operator: Uses the object type properties to further define how a match is made. Available selections include Equals, DoesNotEqual, StartsWith, DoesNotStartWith, Contains, DoesNotContain, EndsWith, DoesNotEndWith, or Regular expression.

For example, for an object type VirtualMachine with the Name property selected, you can select "equals" to create a rule where the virtual machine will only be included in the group when the entire name is specified, or "contains" to include the virtual machine in the group whenever a specific text string appears in the virtual machine name.

Additionally, if you create multiple rules, you can select **All** from the **Match type** drop-down if the item has to meet all of the rules criteria in order to be included in the group, or select **Any** from the drop-down to include the item if the item meets any of the criteria.

Note: Rule definitions for NetWorker vProxy policies with dynamic association enabled can contain regular expressions. The appendix Regular expressions for NetWorker vProxy dynamic policies rule definitionsdescribes the acceptable rules, syntax, and grammar to use when writing such regular expressions.

Create a rule in NMC and associate the rule to a VMware group

To create a rule or access existing rules in NMC, and apply these rules to a VMware group, perform the following.

Before you begin

Create the VMware group and associate the group with a policy/workflow, as outlined in the previous sections.

About this task

Rules can only be applied to VMware groups in NMC when you enable the **Dynamic Association** option. When a group is enabled with **Dynamic Association**, rules are executed against the vCenter inventory to determine which VMware objects will be dynamically added to the VMware protection group's contents, based on matching the rule criteria.

Procedure

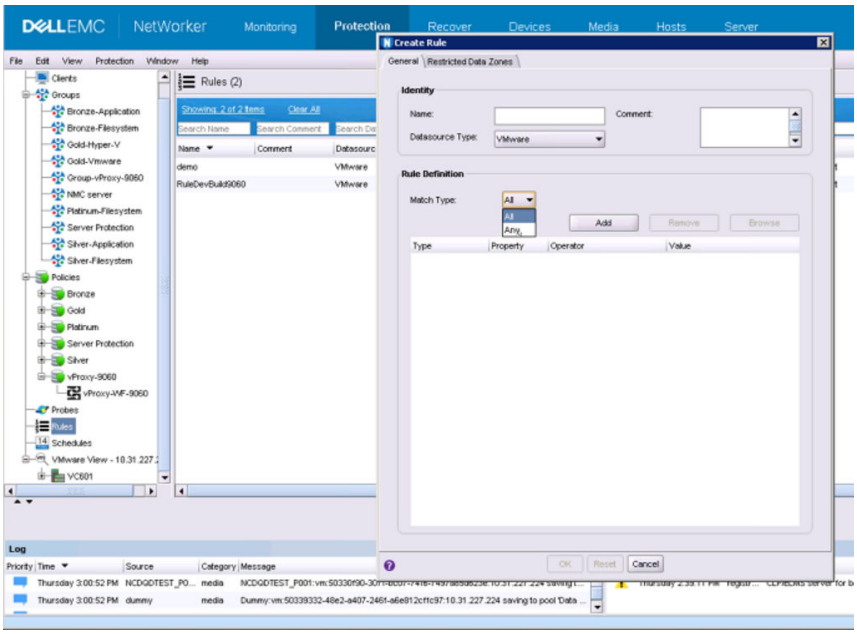
1. In the **NetWorker Administration** window, click **Protection**, and then select **Rules** in the left navigation pane.

   Any rules that have already been created appear in the right pane.

2. Right-click **Rules** and select **New** from the drop-down.

   The **Create Rule** window displays.

Figure 12 Create a new rule to apply to a VMware group



3. In the **General** tab, type a name for the rule, and select the **Datastore Type** from the drop-down. The default Datastore Type is VMware.
4. In the **Rule Definition** pane, click **Add**.
5. In the Rule Definition pane:

   a. For the **Type** column's drop-down, select the object type, for example, **VirtualMachine**.

   b. For the **Property** column's drop-down, select from one of the available options, for example, **Tag**.

   c. For the **Operator** column's drop-down, select from one of the available options, for example, **Equals**.

   d. Click **Browse** to display a list of all the categories and tags that have been created on that vCenter server. Select the tag you want to apply to the rule and click **OK** to exit the dialog.

   Note: Tags are only supported in vSphere versions 6.5 and later.

6. Repeat steps 2 through 5 for any additional rules you want to create.

   Note: If adding multiple rules, in order to specify whether to apply more than one rule to the group, select either **All** or **Any** from the **Match Type** drop-down.

7. When finished adding rules, return to the **Protection** window and right-click the desired group in the left pane, and then select **Properties** from the drop-down. The **Edit Group** window displays.
8. If not already selected, select the **Dynamic Association** checkbox, and then select any virtual machine(s) in this workflow that you want to include in the group regardless of the rules applied. These objects are known as static objects.

9. Select the desired rule from the **Rule** drop-down that you want to apply to the other virtual machines in the workflow to determine which objects will be dynamically included.
10. Click **Preview All Virtual Machines** to view a list of the static and dynamic virtual machines and objects that have been added to the group. In this window, you can also unselect a virtual machine or VMDK to exclude the item from the backup. When an object is unselected, an entry for the object appears in the **Excluded VM** list.
11. Save the changes in the **Edit Group** window, and close the window.

Results

When you select the specific VMware group in the **Protection** window, the **vCenter Objects Selected** field displays the list of virtual machines that are statically selected. Similarly, Protected VMs in **VMware View** only displays the virtual machines that are statically protected.

Create a VMware backup action in NetWorker Administration

A VMware backup is a scheduled backup of virtual machines within a vCenter. The following section provides details for creating a VMware backup action for vProxy. The *NetWorker Administration Guide* provides information about other action types.

Before you begin

Create the policy and workflow that contain the action.

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the expanded left pane, select the policy's workflow, and then perform one of the following tasks in the right pane to start the **Policy Action** wizard:
   - If the action is the first action in the workflow, select **Create a new action**.
   - If the workflow has other actions, right-click an empty area of the **Actions** pane, and then select **New**.

   The **Policy Action** wizard opens on the **Specify the Action Information** page.
3. In the **Name** field, type the name of the action.

   The maximum number of characters for the action name is 64.

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}
4. In the **Comment** field, type a description for the action.
5. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   Note: When you clear the **Enabled** option, actions that occurs after a disabled action do not start, even if the subsequent options are enabled.
6. From the **Action Type** list, select **Backup**.
7. From the secondary action list, select **VMware (vProxy)**.
8. If you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is dimmed.

9. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, in the **Previous** box, select the action that should precede this action.
   - If the action should run concurrently with an action, in the **Previous** box, select the concurrent action, and then select the **Concurrent** checkbox.
10. Specify a weekly, monthly, or reference schedule for the action:
    - To specify a schedule for each day of the week, select **Define** option under **Select Schedule** and period as **Weekly by day**.
    - To specify a schedule for each day of the month, select **Define** option under **Select Schedule** and period as **Monthly by day**.
    - To specify a customized schedule to the action, select **Select** option under **Select Schedule** and choose a customized schedule using the drop down menu that is already created under NSR schedule resource.
11. Click the icon on each day to specify the backup level to perform.

    Backup levels for NetWorker VMware Protection include the following.

    Note: Any backup level that displays in the wizard but is not identified in this table is not supported for VMware.

Table 8 Schedule icons

Icon	Label	Description
	Full	Perform a full backup on this day. Full backups include all files, regardless of whether the files changed. In the case of virtual machine backup, this is a virtual machine disk (VMDK) backup to Data Domain.
	Incr	Uses the previous backup and leverages changed block tracking to write only incremental blocks to a new backup that is independent of other backups. **Note:** Since the backup is performed to Data Domain, the resulting backup on the target device is a new full backup because NetWorker uses Data Domain virtual synthetics technology to create a synthetic full backup.
	Skip	Do not perform a backup on this day.
	Logs only	Perform a backup of only database transaction logs.

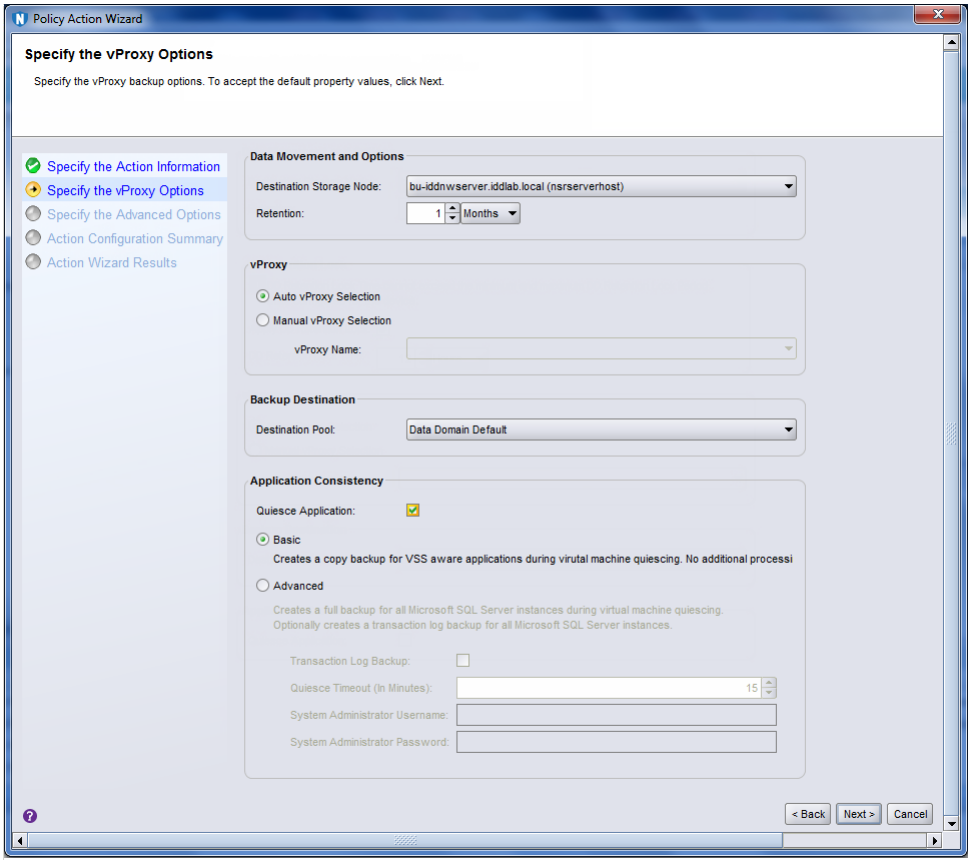
To perform the same type of backup on each day, select the backup type from the list and click **Make All**.

Note: A full backup is required initially if performing application-consistent backup of virtual machines as part of this action.

12. Click **Next**.

    The **Specify vProxy Options** page appears.

Figure 13 Specify vProxy Options page



13. From the **Destination Storage Node** box, select the storage node that contains the devices where you want to store the backup data.

    Note: When you deploy the vCenter server in the Cloud, a parameter displays in the backup action logs that indicates `HypervisorMode: VMC`. When not deployed in the Cloud, the parameter indicates `HypervisorMode: vSphere`.

14. From the **Retention** spin boxes, specify the amount of time to retain the backup data.

    After the retention period expires, the save set is removed from the client file index and marked as recyclable in the media database during an expiration server maintenance task.

15. Select the **Apply DD Retention Lock** checkbox to enable retention lock for the virtual machines included in this backup action. Note that the device used for backing up these virtual machines must also have DD Retention lock enabled in the NMC **Device Properties** window, or DD Retention Lock must be enabled during device creation.

16. In the **DD Retention Lock Time** box, specify the duration the virtual machines will remain on the Data Domain device before the retention lock expires. During this time, these virtual machine backups cannot be overwritten, modified, or deleted for the duration of the retention period, although the backups can be mounted and unmounted. The retention time period set here must fall within the minimum and maximum values set for the Data Domain Mtree, and should be lower than or equal to the NetWorker Retention Period.
17. In the **vProxy** section, select one of the following options:
    - **Auto vProxy Selection**—Select this option to allow NetWorker to choose the vProxy host for backups.
    - **Manual vProxy Selection**—Specify this option to define the vProxy host that NetWorker users for backups. Provide the name of the vProxy host in the **vProxy Name** field.
18. From the **Destination Pool** box, select the media pool in which to store the backup data.

    Only pools configured with a DDBoost device appear in the drop-down.
19. In the **Application Consistency** section, select the **Quiesce Application** checkbox to enable application-consistent protection as part of the policy backup action, which includes protection of the Microsoft SQL Server. You can then select from the **Basic** and **Advanced** options.
    - Select the **Basic** option to create a backup copy for applications during virtual machine quiescing. No additional processing is performed.
    - Select the **Advanced** option to create an SQL server application-consistent backup during virtual machine quiescing, and optionally create a transaction log backup for all SQL Server instances.

    When you select the option, the following fields display:
    - **Transaction Log Backup**—Select this checkbox if you want to perform a transaction log backup of SQL databases in the virtual machine as part of the policy backup action. Note that if you enable transaction log backup, you must also set a value for the **Interval** attribute in the Workflow properties for this action, as specified in the section "Creating a workflow in a new policy."

      Note: During SQL Server configuration, the NT AUTHORITY\SYSTEM login must be granted SQL login and SQL sysadmin role rights in order to perform transaction log backups.
    - **Quiesce Timeout**—Specify the amount of time, in minutes, to wait for the quiesce operation on the virtual machine to time out before failing. If not selected, the backup action will proceed even if quiescing was not performed, unless a validation problem occurs. If an application-consistent backup cannot complete due to a problem with validation, the backup action will fail even if this checkbox is not selected.
    - **System Administrator Username and Password**—Specify the virtual machine credentials for a user with administrative privileges. All virtual machines in the workflow should use the same System Administrator username/password.

    Note: Selecting the **Advanced** option will apply application-consistent processing for all virtual machines within the parent workflow. When selecting this option, ensure that the policy's workflow and client groups are provisioned specifically for virtual machines that require advanced

application-consistent protection. NetWorker will always attempt to perform advanced application processing for virtual machines in a workflow that contains a backup action with advanced application processing enabled. The section Creating an action for application-consistent data protection provides more information.

20. Click **Next**.

    The **Specify the Advanced Options** page appears.

21. Although the **Retries**, **Retry Delay**, and the **Inactivity Timeout** options appear, this action does not support these options and you can ignore these values.
22. In the **Parallelism** field, specify the maximum number of concurrent operations for the action.
23. From the **Soft Limit** list, select the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no amount of time.
24. From the **Hard Limit** list, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.
25. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To specify the month, use the navigation buttons and the month list box. To specify the year, use the spin boxes. You can set an override in the following ways:

    - Select the day in the calendar, which changes the action task for the specific day.
    - Use the action task list to select the task, and then perform one of the following steps:
      - To define an override that occurs on a specific day of the week, every week, select **Specified day**, and then use the lists. Click **Add Rules based override**.
      - To define an override that occurs on the last day of the calendar month, select **Last day of the month**. Click **Add Rules based override**.

    Note:

    - You can edit or add the rules in the **Override** field.
    - To remove an override, delete the entry from the **Override** field.
    - If a schedule is associated to an action, then override option is disabled.

26. From the **Send Notifications** list box, select whether to send notifications for the action:

    - To use the notification configuration that is defined in the Policy resource to send the notification, select **Set at policy level**.
    - To send a notification on completion of the action, select **On Completion**.
    - To send a notification only if the action fails to complete, select **On Failure**.

27. Click **Next**.

    The **Action Configuration Summary** page appears.

28. Review the settings that you specified for the action, and then click **Configure**.

After you finish

(Optional) Create a clone action to automatically clone the save sets after the backup. A clone action is the only supported action after a backup action in a workflow.

Create a clone action in NetWorker Administration

A clone action creates a copy of one or more save sets. Cloning allows for secure offsite storage, the transfer of data from one location to another, and the verification of backups.

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the expanded left pane, select the policy's workflow, and then perform one of the following tasks in the right pane to start the **Policy Action** wizard:
   - If the action is the first action in the workflow, select **Create a new action**.
   - If the workflow has other actions, right-click an empty area of the **Actions** pane, and then select **New**.

   The **Policy Action** wizard opens on the **Specify the Action Information** page.
3. In the **Name** field, type the name of the action.

   The maximum number of characters for the action name is 64.
   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}
4. In the **Comment** field, type a description for the action.
5. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   Note: When you clear the **Enabled** option, actions that occurs after a disabled action do not start, even if the subsequent options are enabled.
6. From the **Action Type** list, select **Clone**.
7. If you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is dimmed.
8. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, in the **Previous** box, select the action that should precede this action.
   - If the action should run concurrently with an action, in the **Previous** box, select the concurrent action, and then select the **Concurrent** checkbox.
9. Specify a weekly, monthly, or reference schedule for the action:
   - To specify a schedule for each day of the week, select **Define** option under **Select Schedule** and period as **Weekly by day**.
   - To specify a schedule for each day of the month, select **Define** option under **Select Schedule** and period as **Monthly by day**.
   - To specify a customized schedule to the action, select **Select** option under **Select Schedule** and choose a customized schedule using the drop down menu that is already created under NSR schedule resource.

10. Specify the days to perform cloning:
    - To clone on a specific day, click the **Execute** icon on the day.
    - To skip a clone on a specific day, click the **Skip** icon on the day.
    - To check connectivity every day, select **Execute** from the list, and then click **Make All**.

    The following table provides details on the icons.

    Table 9 Schedule icons

Icon	Label	Description
	Execute	Perform cloning on this day.
	Skip	Do not perform cloning on this day.

11. Click **Next**.

    The **Specify the Clone Options** page appears.
12. In the **Data Movement** group box, define the volumes and devices to which NetWorker sends the clone data.
    a. From the **Destination Storage Node** list, select the storage node with the devices on which to store the cloned save sets.
    b. In the **Delete source save sets after clone completes**, select the option to instruct NetWorker to remove the source save set information from the client file index, and to mark the save set as recyclable in the media database during a Server expiration maintenance action. Clear this option to allow the source save sets to expire based on the defined retention time.
    c. From the **Destination Pool** list, select the target media pool for the cloned save sets.
    d. From the **Retention list**, specify the amount of time to retain the cloned save sets. After the retention period expires, the save sets are marked as recyclable during an expiration server maintenance task.
13. Click **Next**.

    The **Specify the Advanced Options** page appears.
14. Configure advanced options, including notifications and schedule overrides.

    Note: Although the **Retries**, **Retry Delay**, or the **Inactivity Timeout** options appear, the clone action does not support these options and ignores the values.
15. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. This value should not exceed 25.
16. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the entire workflow if there is a failure with one of the jobs in the action, select **Abort workflow**.

Note: If any of the actions fail in the workflow, the workflow status does not appear as interrupted or cancelled. NetWorker reports the workflow status as failed.

17. From the **Send Notifications** list box, select whether to send notifications for the action:
    - To use the notification configuration that is defined in the Policy resource to send the notification, select **Set at policy level**.
    - To send a notification on completion of the action, select **On Completion**.
    - To send a notification only if the action fails to complete, select **On Failure**.
18. From the **Soft Limit** list, select the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no amount of time.
19. From the **Hard Limit** list, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.
20. Optional, in **Start Time** specify the time to start the action.

    Use the spin boxes to set the hour and minute values, and select one of the following options from the drop-down list:
    - **Disabled**—Do not enforce an action start time. The action will start at the time defined by the workflow.
    - **Absolute**—Start the action at the time specified by the values in the spin boxes.
    - **Relative**—Start the action after the period of time defined in the spin boxes has elapsed after the start of the workflow.
21. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To specify the month, use the navigation buttons and the month list box. To specify the year, use the spin boxes. You can set an override in the following ways:
    - Select the day in the calendar, which changes the action task for the specific day.
    - Use the action task list to select the task, and then perform one of the following steps:
      - To define an override that occurs on a specific day of the week, every week, select **Specified day**, and then use the lists. Click **Add Rules based override**.
      - To define an override that occurs on the last day of the calendar month, select **Last day of the month**. Click **Add Rules based override**.

      Note:
      - You can edit or add the rules in the **Override** field.
      - To remove an override, delete the entry from the **Override** field.
      - If a schedule is associated to an action, then override option is disabled.
22. Click **Next**.

The **Action Configuration Summary** page appears.

23. Review the settings that you specified for the action, and then click **Configure**.

After you finish

(Optional) Create a clone action to automatically clone the save sets again after this clone action. Another clone action is the only supported action after a clone action in a workflow.

Creating an action for Microsoft SQL Server application-consistent protection

You can create a backup action with SQL Server application-consistent protection of virtual machines by using the Policy Action wizard in NMC. When you enable a VMware backup action with this feature, you can run full backups of SQL databases as part of the VMware image-level backup, and also perform incremental backups of the transaction log.

SQL Server application-consistent protection is enabled in the **Specify the vProxy and Application Protection Options** page of the **Policy Action** wizard by selecting the **Application Protection** checkbox and then selecting an **Application Protection Type**, as outlined in the steps for Create a VMware backup action.

SQL Server application-consistent protection enables the following backup operations:

- SQL Server backup—Select this option in the **Policy Action** wizard in NMC to perform image-level (FULL) backup with application-consistent processing. This backup will request VMware Tools to perform a FULL quiesce type for applications running in the virtual machine in order to provide a full backup of the Microsoft SQL Server instances within the virtual machine. Upon completion of the virtual machine image snapshot, the Microsoft VM App Agent is called to catalog this backup, writing the catalog to the Data Domain system.
- Transaction log backup—Select this option in the **Policy Action** wizard in NMC to perform transaction log backups of SQL Server databases for all SQL Server Instances in the virtual machine. Note that if you perform transaction log backup, you must also set the **Interval** attribute in the policy's **Workflow Properties** window in NMC. The transaction log backup of SQL databases is separate from the virtual machine image-level backup, as no virtual machine image-level backup occurs during the transaction log backup. Transaction log backup files will be saved to the backup folder for the current save set on the Data Domain system. Databases that do not support transaction log backup are filtered out.

The process for creating a policy with SQL Server application-consistent protection of virtual machines in NMC is very similar to creating a policy with the VMware backup action, with the following exceptions:

- You must provision a new policy and workflow exclusively for SQL clients that require SQL Server application-consistent protection.
- You must provision a new policy and workflow exclusively for SQL clients that have different security accounts, for example, system administrator username and/or password.
- It is recommended that the virtual machines included in the group for the dedicated workflows are not contained within multiple workflows.

Creating a workflow with an SQL Server application-consistent backup action will perform a full image-level backup. Ad-hoc (on demand) runs of this workflow will also create full backups, even when started at off-schedule times. If you also select transaction log backup in the **Policy Action** wizard, the transaction log backup will

occur as part of incremental backups after the initial full backup, at the interval set in the workflow properties.

Starting, stopping, and restarting policies

The workflows in a policy can run automatically, based on a schedule. You can also manually start, stop, and restart specific workflows by using the the NMC **NetWorker Administration Monitoring** window.

About this task

You can restart any failed or canceled workflow. Note, however, that the restart must occur within the restart window that you specified for the workflow. Additionally, for a VMware backup, if you cancel a workflow from **NetWorker Administration** and then want to restart the backup, ensure that you restart the workflow from the **NetWorker Administration** window. If a workflow that was started from **NetWorker Administration** is restarted from the **vSphere Web Client**, the backup fails.

Procedure

1. In the **Monitoring** window, select the workflow or actions.
2. Right-click and then select **Start**, **Stop**, or **Restart**.

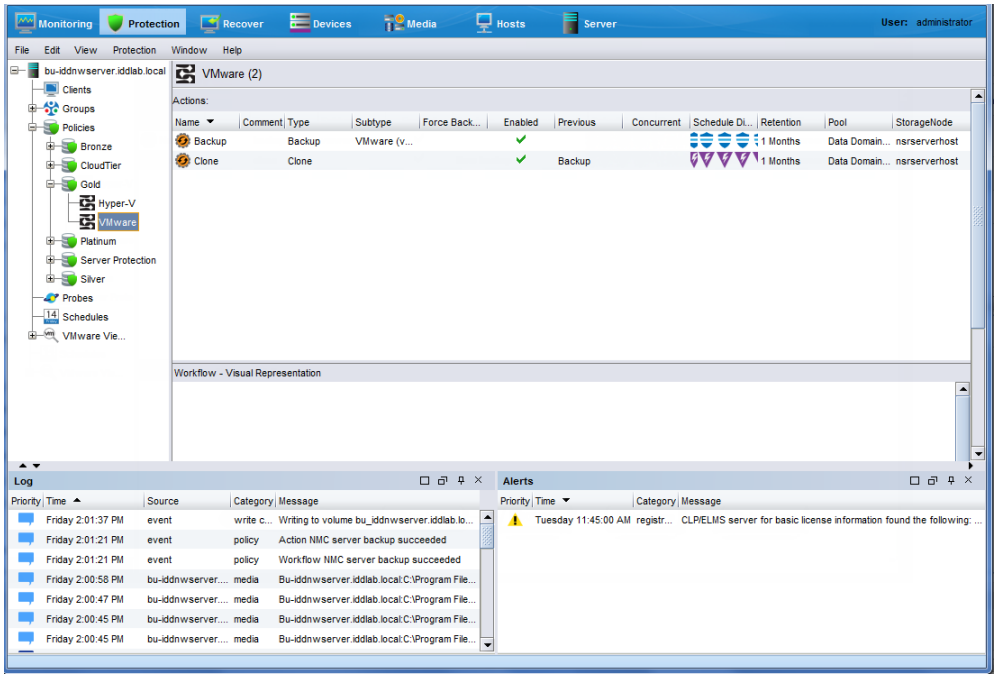
   A confirmation message appears.

   Note: You cannot stop, restart, or start individual actions.
3. Click **Yes**.

Visual representation of VMware policy and associated actions

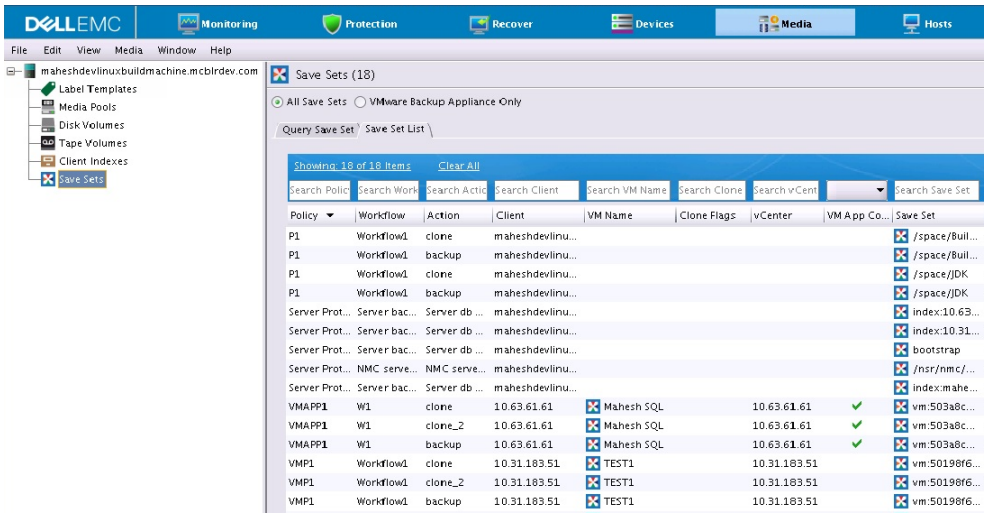
A visual representation of the VMware backup policy with its associated workflow and actions appears in the lower panel of the **Protection** window.

Figure 14 VMware protection policy in the Protection window



The **Media** window displays the save sets contained within the policy. If the save sets are additionally part of an application-consistent policy, a green check mark appears in the **VM App Consistent** column.

Figure 15 VMware protection policy save sets in Media window

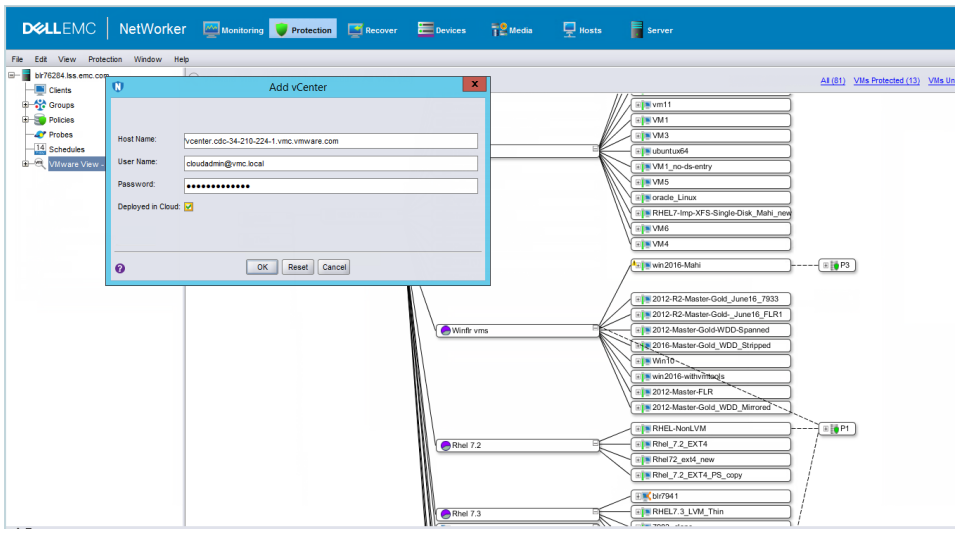


VMware View in NMC

VMware View provides an overview of the vCenter environment. You can access VMware View from the **NetWorker Administration Protection** window.

If you have not yet added a vCenter server to **VMware View**, right-click **VMware View** in the right pane, and select **Add vCenter** from the drop-down. The **Add vCenter** dialog displays.

Figure 16 Add a vCenter server to VMware View in NMC



In the **Host Name** field, type the IP address of the host, and provide the vCenter Server username and password credentials. Additionally, if the vCenter server is deployed in the Cloud, select the **Deployed in Cloud** checkbox, and then click **OK**.

Note: When you select **Deployed in Cloud**, a parameter displays in the backup action logs that indicates `HypervisorMode: VMC`. When the checkbox is not selected, the parameter indicates `HypervisorMode: vSphere`.

When you add the vCenter server to **VMware View**, the following actions occur:

- A visual (map) or tabular representation of the vCenter environment appears in the **VMware View** window.
- A client resource is created for the vCenter server with the vProxy backup type.

Using **VMware View**, you can also assign the policies you created in "VMware data protection policies in NMC." to the vCenter objects.

The following sections describe the options that are available in **VMware View**.

Map view of the VMware environment

When you expand **VMware View**, a hierarchical display of the VMware environment appears. The following containers appear:

- vCenters
- DataCenters within the vCenter
- Clusters within the DataCenter
- ESX servers
- Folders above the DataCenters and folders above ESX hosts/clusters
- vApps
- Resource Pools

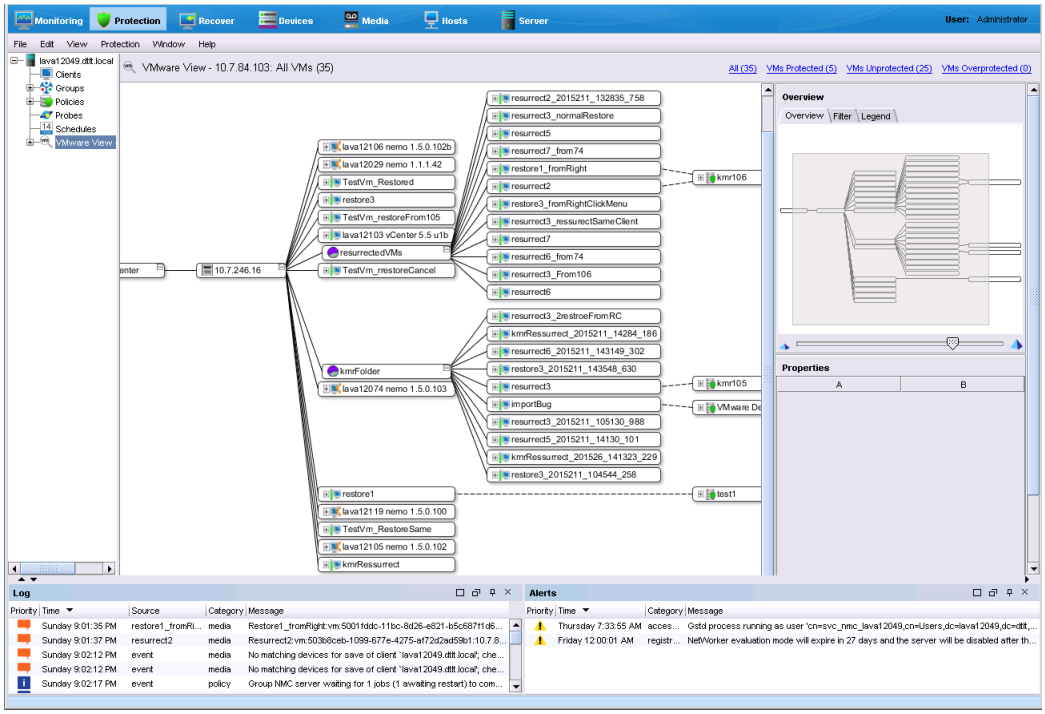
You can use several operations to navigate within the map view:

- To zoom in and out of the map view, select the zoom icons on the map view icon bar or click on the right details pane and scroll with the mouse wheel. You can also click the **Zoom Area** button to select an area to zoom into, or click the **Fit Content** button to fit the entire display into the right details pane. These operations are also available when you right-click the details pane.
- To move the graphical display, left-click in the details pane and drag the mouse cursor.
- To expand or collapse any container in the map view to display or hide the child elements associated with the container, double-click the container.
- To display an overview of the map view, select the **Overview** tab within the **Overview** pane. The overview of the map view is particularly useful for large maps and allows you to quickly drill down to specific areas in the map.
- To limit items displayed and search for specific items in the map view, use the **Filter VM by** and **Show** functions, available from the **Filter** tab within the **Overview** pane.

When you click on any container, the hierarchical tree provides a detailed map view of that container and all of its children. For example, select the top level virtualization node to display a complete view of your VMware environment across all configured vCenters, or select an individual ESX server or Cluster in the hierarchy to display the resource pool with all child elements associated with that ESX server or Cluster including VMs, VMDKs, the vProxy appliance, and any associated VMware backup policies to the right of these containers.

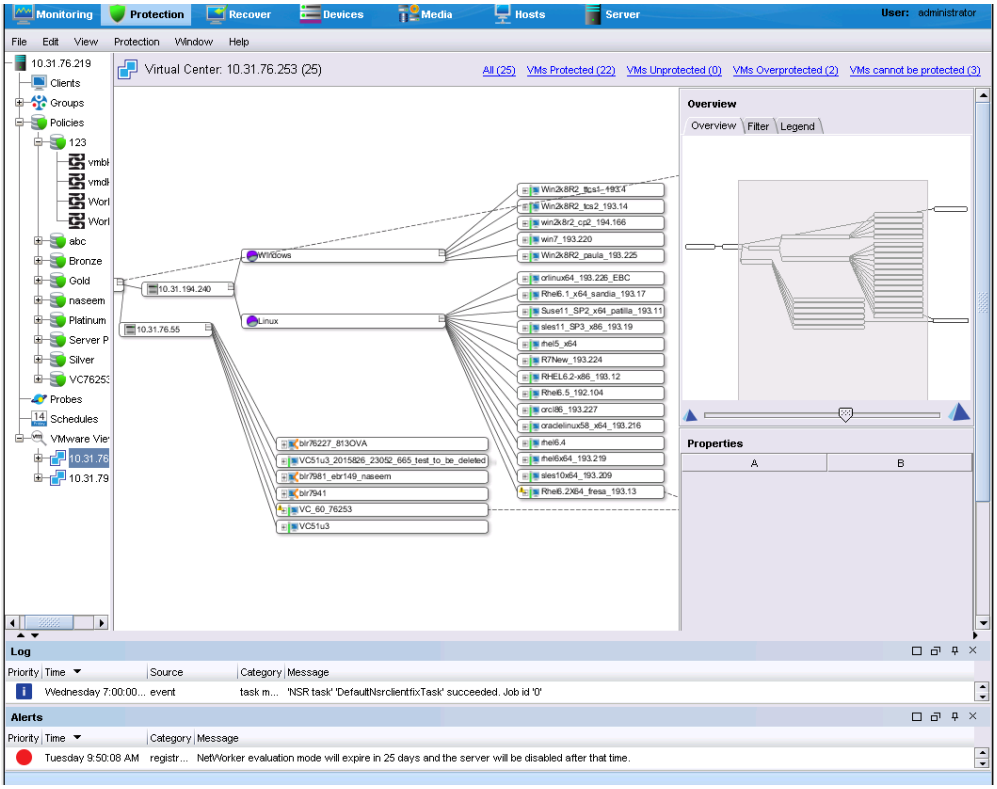
Lines connect each child element to the parent element, with child elements proceeding hierarchically from left to right in the display, as shown in the following figure.

Figure 17 Map view of VMware environment in NMC



To refine items displayed in the right details pane, select containers in the Virtualization node hierarchy in the left pane. For example, if an individual Cluster is selected in the Virtualization node, only child elements associated with that Cluster display.

Figure 18 Cluster with child elements in VMware View



To filter the visible items to show only protected VMs, unprotected VMs, or overprotected VMs, click the links located above the right pane, as shown in the following figure.

Note: When you enable a VMware group with **Dynamic Association**, the protected VMs reflect those virtual machines that are statically protected, and does not include virtual machines that get dynamically added to the group after rules are applied.

Figure 19 Filtering results in VMware View

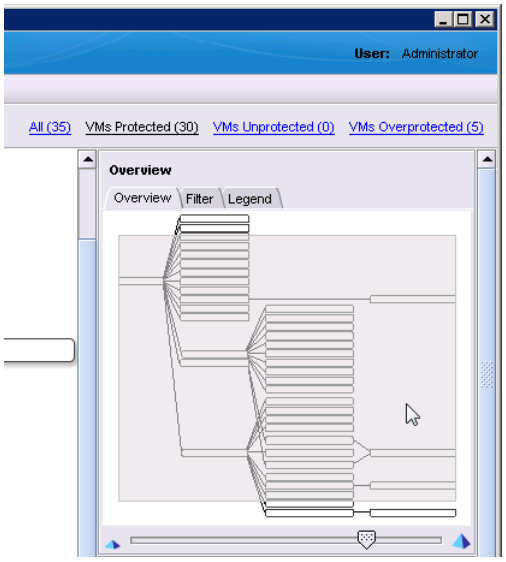
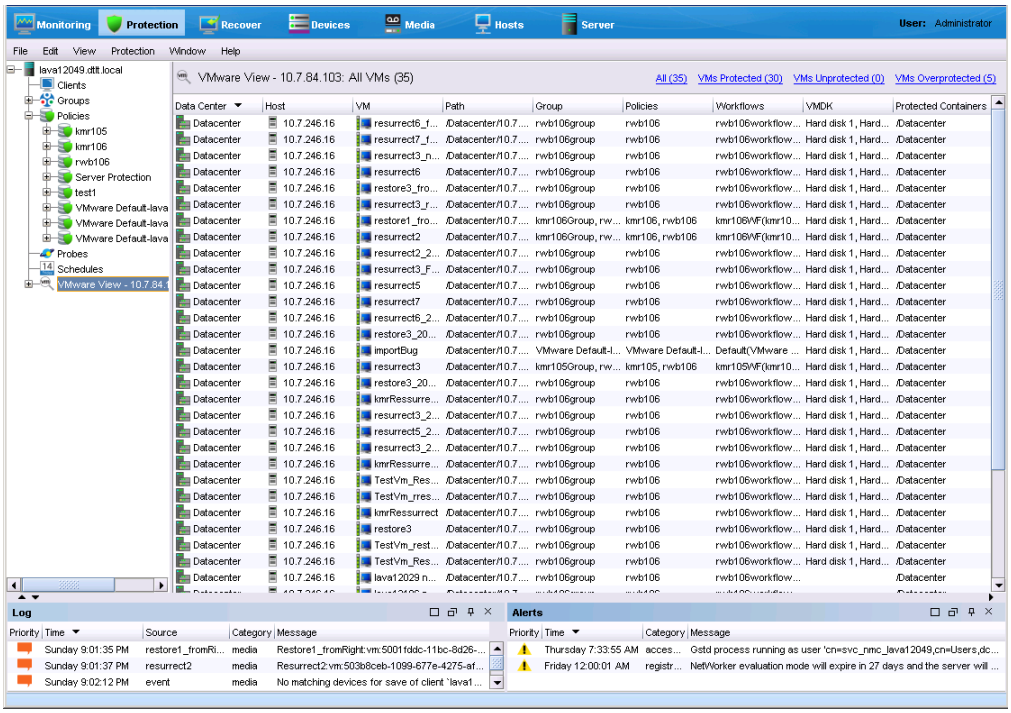


Table view of the VMware environment

To switch to a view of the VMware environment in table form, right-click anywhere in the details pane and select **Table**. The Table view functions like other table views in the **Administration** window.

Note: Table view only displays information for virtual machines. It does not show any details about VMDKs. You must use Map view to display those details.

Figure 20 VMware table view



The filtering function works the same in Table view as in Map view. Links provided above the details pane allow you to display only overprotected virtual machines, unprotected virtual machines, or all virtual machines in the environment. The *NetWorker Administration Guide* provides general information on using tables in the **Administration** window.

Note: In Table view, the **Host** field contains an undefined value for virtual machines or containers that are part of a cluster. The Map view provides a link to the cluster.

Assigning protection groups to virtual machines

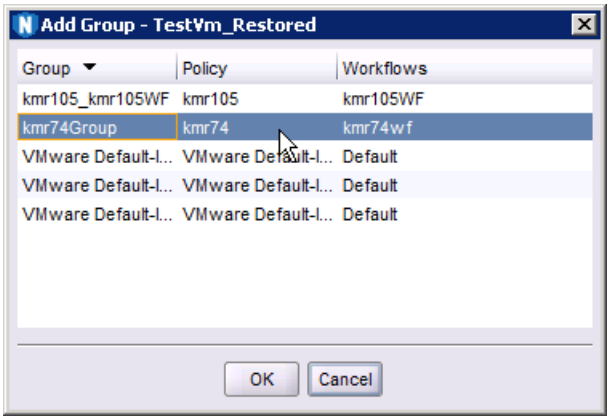
From within the map or table view of the VMware environment, you can assign protection groups at any level, for example, you can assign a group to the entire datacenter, a cluster, a resource pool, a virtual machine, or even a VMDK by using **VMware View**.

Procedure

1. Right-click on any container, or expand the container, and then right-click on an element within **VMware View**.
2. Select **Add to Group**.

   The available groups display, as shown in the following figure.

Figure 21 Add group in VMware View



3. Select a group, and click **OK**.

   VMware View refreshes and displays the new association.

4. To assign a group at the VMDK level, expand a virtual machine, right-click the VMDK that you want to associate to the group, and select **Add to Group**.

Assigning a group to a disconnected ESX server

When you disconnect an ESX host from the vCenter server, the ESX still appears in VMware View. You can assign a group to an ESX host that is disconnected from the vCenter server, however, if you start the group, the group will remain in "interrupted" state until you reconnect the ESX back to the vCenter server and run the group again.

Note: Disconnecting an ESX server from a vCenter server only temporarily disconnects the server and does not remove the server. To permanently remove the ESX server from the vCenter inventory, use the `Remove` command from vCenter.

vProxy backup workflows in the vSphere Client's Dell EMC NetWorker interface

The NetWorker vProxy workflows can only be created in NMC, however, you can perform virtual machine backups of these vProxy workflows, and add virtual machines to the vProxy workflows, by using the **Dell EMC NetWorker** interface within the **vSphere Client**.

Dell EMC NetWorker appears in the left navigation pane of the **vSphere Client** after you install the vCenter plug-in. The section Installing the vCenter plug-in provides instructions.

Note: Backup and recovery operations in the **vSphere Client Dell EMC NetWorker** interface are not supported for SQL Server advanced application-consistent protection policies. Perform these operations from the NMC **NetWorker Administration** window or the **Dell EMC Data Protection Restore Client**.

Connect to the NetWorker server in the vSphere Client

You must establish a connection to the NetWorker server before performing any vProxy backup and recovery operations in the **vSphere Client**.

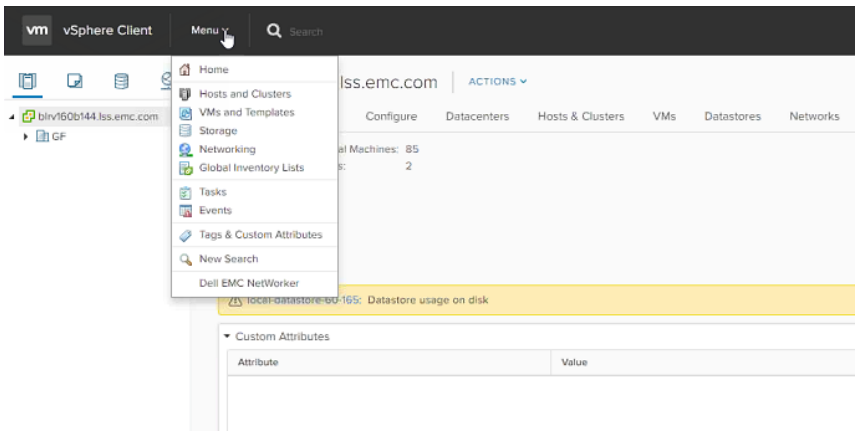
Before you begin

Dell EMC NetWorker only appears in the **vSphere Client** after you install the vCenter plug-in. The section Installing the vCenter plug-in provides instructions.

Procedure

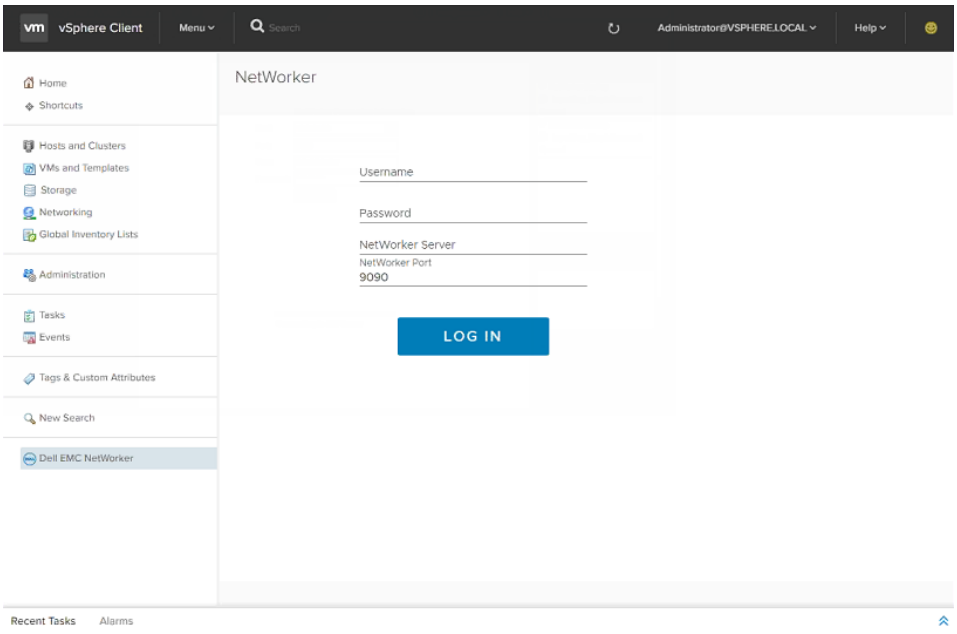
1. Login to the **vSphere Client** as an administrator, or as a non-administrator Active Directory user that you created using the steps in the section Accessing the HTML-5 or flash-based vCenter plug-in as a non-administrator Active Directory user.
2. In the **vSphere Client**, select **Menu** > **Dell EMC NetWorker**, or select **Dell EMC NetWorker** in the left pane.

   Figure 22 Accessing Dell EMC NetWorker in the vSphere Client

   A prompt displays in the right pane with fields required to connect to the NetWorker server.
3. For the NetWorker server, type the following information:
   a. In the **Username** field, type the NetWorker administrator username.
   b. In the **Password** field, type the NetWorker administrator password.
   c. In the **NetWorker Server** field, type the IP address of the NetWorker server.
   d. In the **Port** field, type **9090**.

Figure 23 NetWorker connection information in the vSphere Client



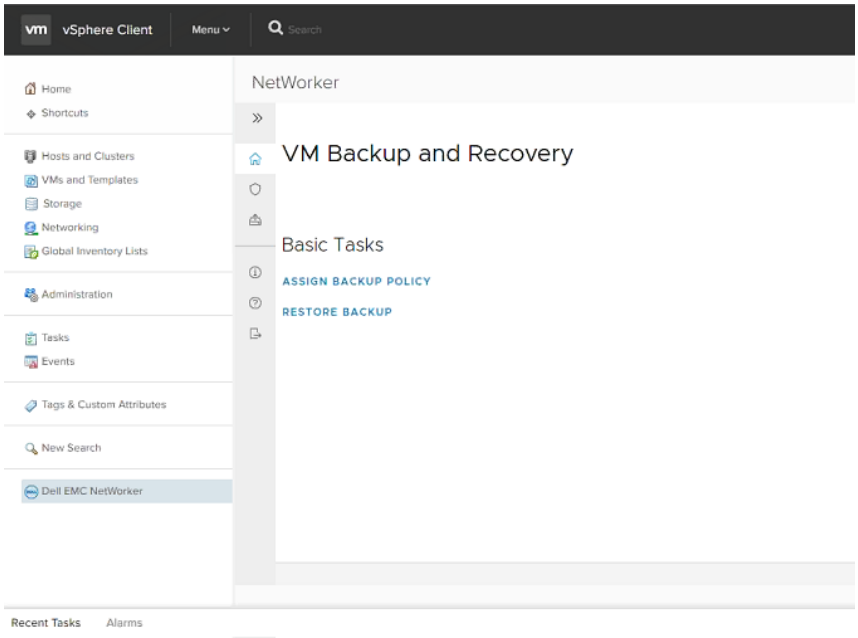
Note: The vCenter plug-in (HTML5 or flash-based) requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.

4. Click **Log in**.

Results

When a connection to the NetWorker server is established, the **Basic Tasks** pane appears, as shown in the following.

Figure 24 Dell EMC NetWorker Basic Tasks pane



Start a vProxy policy in the vSphere Client Dell EMC NetWorker interface

To start a vProxy backup policy by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

Procedure

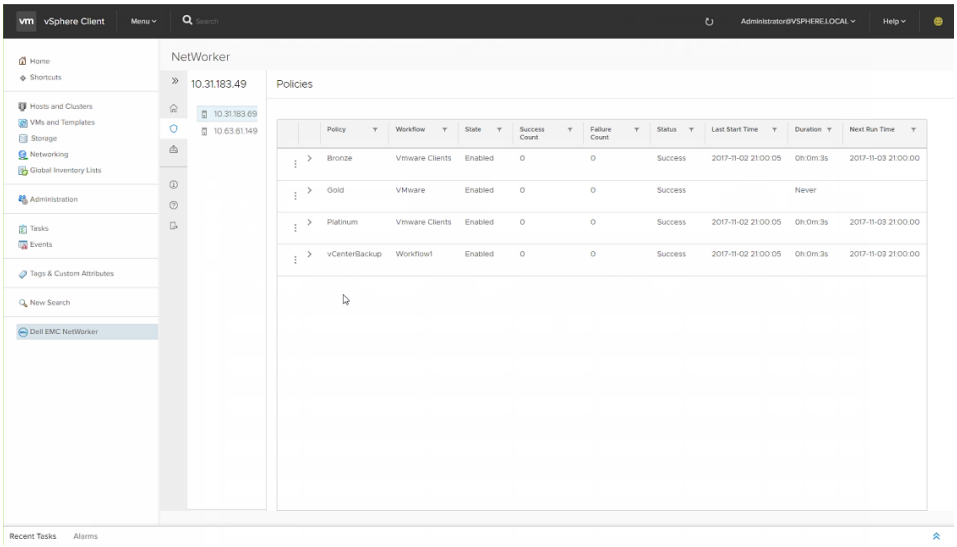
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

   When a connection to the NetWorker server is established, links to **Basic Tasks** appear in the right pane.

2. From the **Basic Tasks** pane, click **Assign Backup Policy**, or click the Protection icon in the vertical navigation bar.

   The vCenter server hosts associated with the NetWorker server display. When you select one of these entries, a list of available vProxy policies that were created in NMC displays in the right pane.

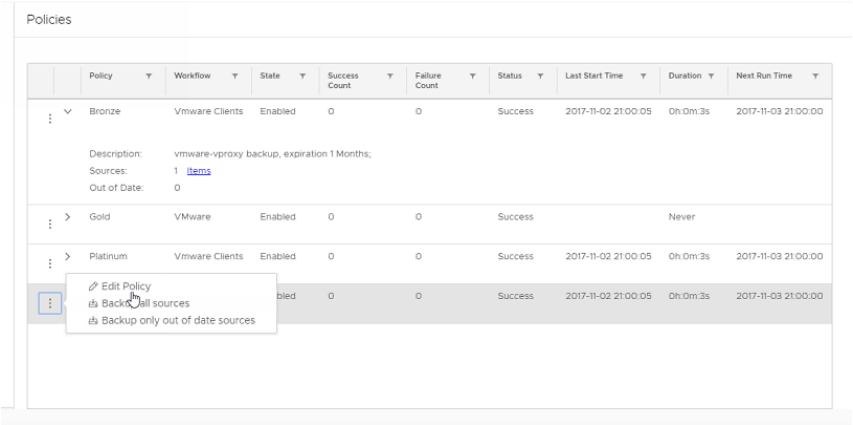
   Figure 25 Policies pane with available vProxy policies



3. Click the arrow to the left of a policy to expand and view the policy and workflow details. You can click the **Items** link under the Workflow to display the virtual machines protected by this workflow.

4. If you do not need to add or remove any virtual machines from the workflow, click the three dots next to the policy and select **Backup all sources** or **Backup only out of date sources** from the drop-down.

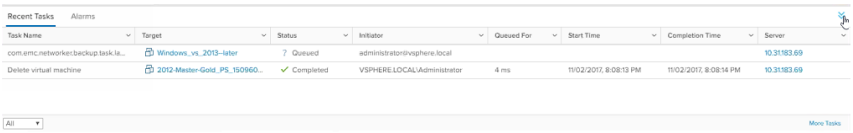
Figure 26 Policy backup options



Results

A dialog displays indicating that the policy was successfully started. To close the dialog, click **OK**. You can then click the blue arrows in the lower right corner of the window to monitor the progress of the policy in the **Recent Tasks** pane.

Figure 27 Recent Tasks pane



Add virtual machines to a vProxy policy in the vSphere Client Dell EMC NetWorker interface

Perform the following steps to edit a vProxy policy to add virtual machines to a workflow by using the **Dell EMC NetWorker** interface in the **vSphere Client**.

Procedure

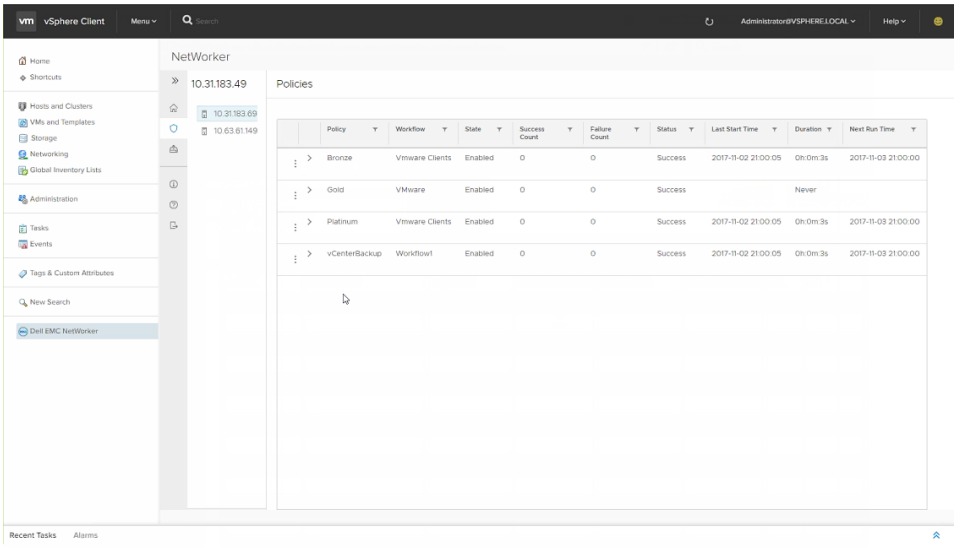
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

   When a connection to the NetWorker server is established, links to **Basic Tasks** appear in the right pane.

2. Click **Assign Backup Policy**.

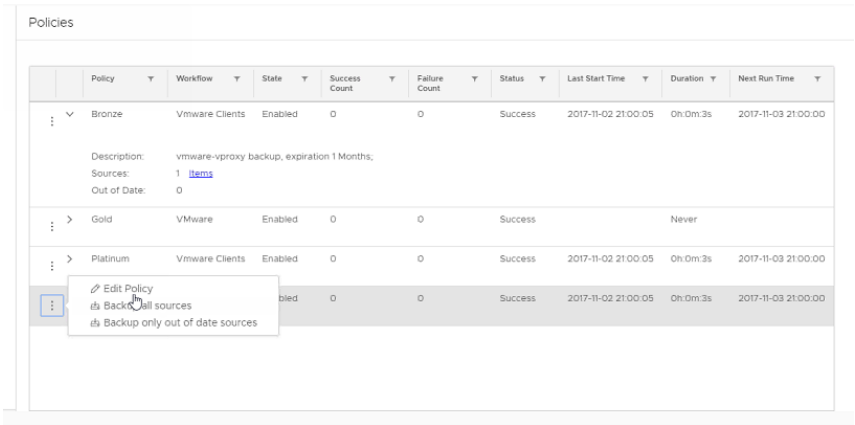
   A list of available vProxy policies that were created in NMC displays in the right pane.

Figure 28 Policies pane with available vProxy policies



3. Click the arrow to the left of a policy to expand and view the policy and workflow details. You can click the **Items** link under the Workflow to display the virtual machines protected by this workflow.
4. To add virtual machines to the workflow, click the three dots next to the policy and select **Edit** from the drop-down.

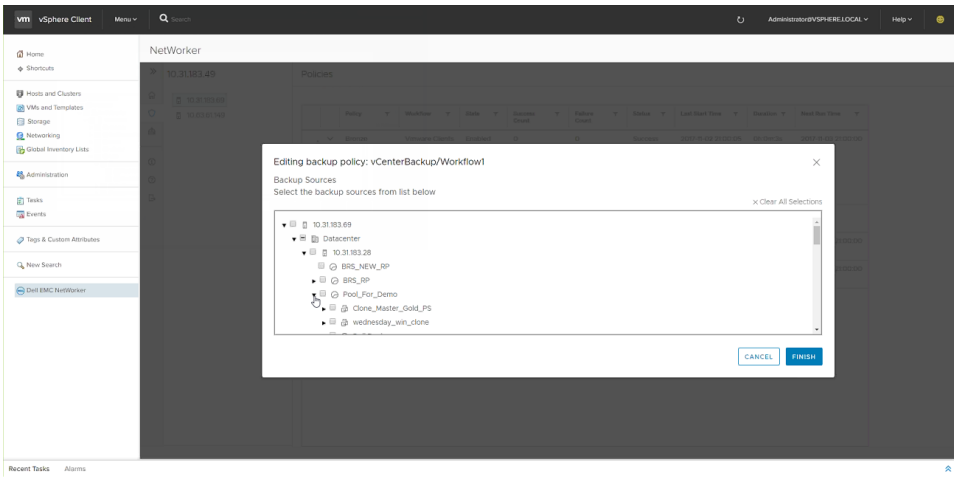
Figure 29 Edit a vProxy policy



The **Editing backup policy** dialog displays with available backup sources.

5. Select any virtual machines or VMDKs in the inventory you want to protect with this workflow, and then click **Finish**.

Figure 30 Backup sources in the Editing backup policy dialog



Results

Any virtual machines or VMDKs added to the workflow now appear when you click the **Items** link under the workflow in the **Policies** pane.

vProxy workflows in the vSphere Web Client's VM Backup and Recovery interface

The flash-based vCenter plug-in, which displays as the **VM Backup and Recovery** interface in the vSphere Web Client, was introduced in NetWorker 9.1. New and upgraded users of NetWorker version 18.x can still use this plug-in to run virtual machine backups from the vProxy workflows created in NMC, and add virtual machines to those vProxy workflows.

VM Backup and Recovery appears in the left navigation pane of the **vSphere Web Client** when you install the flash-based vCenter plug-in. The section Installing the vCenter plug-in provides instructions.

Note: Backup and recovery operations in the **vSphere Web Client VM Backup and Recovery** interface are not supported for SQL Server advanced application-consistent protection policies. Perform these operations from the NMC **NetWorker Administration** window or the **Dell EMC Data Protection Restore Client**.

Connect to the NetWorker server in the vSphere Web Client

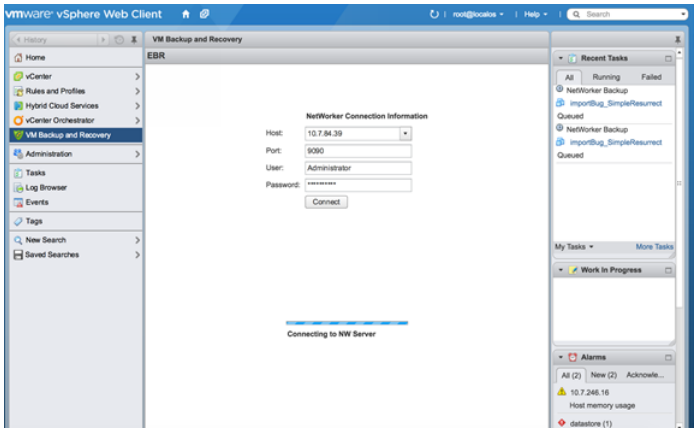
After installing the vCenter plug-in, you must establish a connection to the NetWorker server before performing any vProxy operations in the vSphere Web Client.

Procedure

1. Log in to the **vSphere Web Client** as an administrator, or as a non-administrator Active Directory user that you created using the steps in the section Accessing the HTML-5 or flash-based vCenter plug-in as a non-administrator Active Directory user.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   The required NetWorker connection information appears in the right pane.

Figure 31 NetWorker connection information in the vSphere Web Client



3. Enter the following information for the NetWorker server:
   a. In the **Host** field, type the IP address of the NetWorker server.
   b. In the **Port** field, type **9090**.
   c. In the **User** field, type the NetWorker administrator username.
   d. In the **Password** field, type the NetWorker administrator password.

   Note: The vCenter plug-in (HTML5 or flash-based) requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.

4. Click **Connect**.

Results

When a connection to the NetWorker server is established, the **Getting Started** pane appears.

Starting a vProxy policy in the vSphere Web Client

Perform the following steps to start a vProxy policy and workflow created in NMC by using the vSphere Web Client.

Procedure

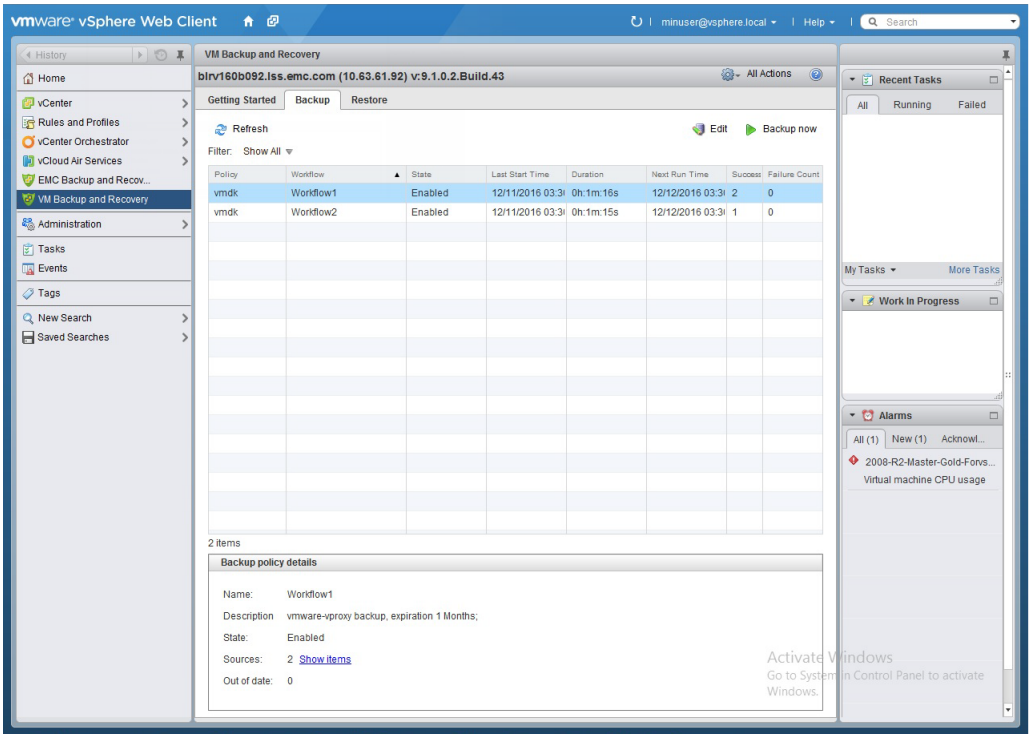
1. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   When a connection to the NetWorker server is established, the **Getting Started** pane appears.

2. Click the **Backup** tab to open the **Backup** pane.

   Any vProxy policies created in NMC display.

Figure 32 Backup pane with vProxy policy



3. Highlight the policy and workflow you want to run and click **Backup now** in the top-right corner.

Results

You can monitor the progress of the backup in the **Running** tab of the **Recent Tasks** pane.

Note: If you cancel a workflow from the **vSphere Web Client** and then want to restart the backup, ensure that you restart the workflow from the **vSphere Web Client**. If a workflow that was started from the **vSphere Web Client** is restarted from the NMC **NetWorker Administration** window, the backup fails.

Adding virtual machines to a vProxy policy workflow in the vSphere Web Client

Perform the following steps to add virtual machines to a vProxy workflow created in NMC by using the vSphere Web Client.

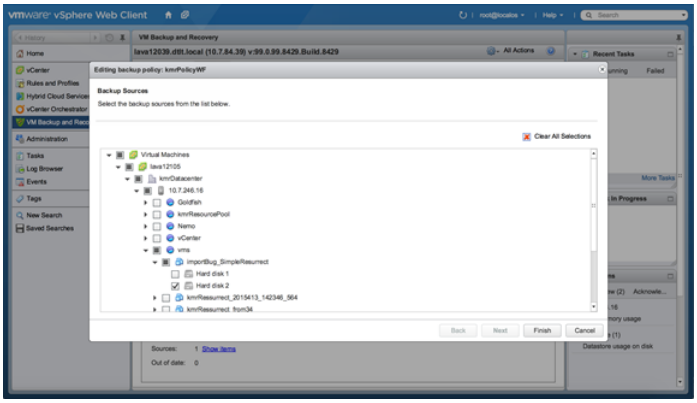
Procedure

1. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane. When a connection to the NetWorker server is established, the **Getting Started** pane appears.
2. Click the **Backup** tab to open the **Backup** pane.

   Any vProxy policies created in NMC display.
3. Highlight the policy whose workflow you want to add virtual machines to and click **Edit** in the top-right corner.

   The **Editing backup policy** window displays with available backup sources.

Figure 33 Backup sources in the Editing backup policy window



4. Select any virtual machines or VMDKs in the inventory you want to protect with this workflow and click **Finish**.

Results

Any virtual machines or VMDKs added to the workflow appear under **Sources** in the bottom of the **Backup** pane.

Additional vProxy backup configuration options

The following section provides additional configuration options for vProxy backups.

Configure a backup to support VMware encryption

NetWorker supports encrypted virtual machine backups. When configuring a virtual machine backup with VMware encryption, perform the following steps.

Before you begin

Review the known limitations for configuring a backup to support VMware encryption. To backup or restore encrypted virtual machines, ensure that the vProxy appliance is also encrypted, and that the vProxy is manually mapped to the backup policy.

About this task

The *VMware vSphere Security Guide* provides more information about virtual machine encryption.

Procedure

1. Establish encryption for the virtual machine.
   a. Set up the Key Management Service (KMS).
   b. Create a VM encryption policy.
   c. Assign the encryption policy to the virtual machine(s) you want to encrypt.
2. Encrypt the vProxy appliance.
3. Open the `/opt/emc/vproxy/conf/VixDiskLib.config` file with a Linux text editor.
4. In the file, search for *vixDiskLib.transport.hotadd.NoNFCSession* and change the value to `0`.

Changing this value to 0 overrides a VMware VDDK bug that inhibits hot-adding an encrypted virtual machine. The *VMware Release Notes* provide more information.

5. Save and close the file.
6. Run the following:

   ```
   systemctl restart vbackupd.service
   ```

7. Set the following additional permissions for the **vCenter user account** role, which is described in the section Create a customized role:

   Cryptographic operations > Add disk

   Cryptographic operations > Direct access

   Cryptographic permissions- Register VM

VMware encryption support limitations

The following limitations apply to backups with VMware encryption enabled.

- As a result of disabling **NoNFCSession**, backup and restore in VMware Cloud on Amazon Web Services (AWS) is not supported. This VMware limitation is addressed in the VDDK update.
- When restoring from an encrypted virtual machine backup, the restored data is unencrypted.
- Restoring virtual machines requires that the target vCenter is configured for the same Key Management Service (KMS) host as the source vCenter.
- Application-consistent quiesce snapshot backups on an encrypted virtual machine will fail back to a file system-consistent snapshot. This process generates an error message in vCenter, which can be ignored. This is a VMware limitation.
- When restoring a virtual machine as a new image, by default, new virtual machines are not encrypted. If you want to apply encryption to the new virtual machine, apply the required storage policy.
  In cases where a boot order other than the default was implemented before the image-level backup was performed, the original boot order is not restored. In this instance, you must select the correct boot device after the restore completes. Alternatively, you can enter the non-default boot order to the VMX file so that the restored virtual machine starts without any reconfiguration. This limitation does not affect virtual machines that use the default boot order.

Configure a backup to support vSAN encryption

Backup and recovery functionality is supported for encrypted vSAN virtual machines, including the restore of an encrypted vSAN virtual machine to a different vCenter that has a non-encrypted datastore. The following steps describe how to configure a virtual machine backup with vSAN encryption.

About this task

When performing backups or restores of virtual machines residing on vSAN datastores, it is highly recommended to deploy the vProxy on a vSAN datastore. A vProxy deployed on any one vSAN datastore can be used for backing up virtual machines from other vSAN or non-vSAN datastores (encrypted or non-encrypted) by using hotadd or nbdssl transport modes, as applicable. Both **Capacity** and **Performance** Optimization modes are fully supported for vSAN encrypted virtual machines.

The *VMware Administering VMware VSAN Guide* provides more information about VSAN encryption.

When configuring a virtual machine backup with vSAN encryption, perform the following steps.

Procedure

1. Set the following permissions for the **vCenter user account** role, which is described in the section Create a customized role:

   ```
   Cryptographic operations > Add disk

   Cryptographic operations > Direct access
   ```

2. Create the backup group.

   Note: To back up the vSAN virtual machine, use the vProxy deployed in the vSAN datastore.

Enabling or disabling Changed Block Tracking

The vProxy appliance uses changed block tracking (CBT) automatically upon the first virtual machine backup so that only changed disk areas on the virtual machine get backed up. Some virtual machines, however, do not support CBT and you may be required to disable CBT for those virtual machines.

A vCenter administrator can control the application of CBT by using the custom field **EMC vProxy Disable CBT**. You can set this custom field to **true** to disable CBT, or **false** to enable CBT. If you do not set this field for a virtual machine, or the field is not present, CBT is enabled by default for that virtual machine.

To set CBT for virtual machines, perform the following:

1. Log into the **vSphere Client** (vSphere versions 6 and earlier) or **vSphere Web Client** (vSphere versions 6.5 and later) as an administrator.
2. Click on a virtual machine in the vCenter tree, and then click the **Summary** tab.
3. Edit the virtual machine attributes:
   - In vSphere versions 6.x and earlier, click **Edit** in the **Annotation** box.
   - In vSphere versions 6.5 and later, click **Edit** under **Custom Attributes**.
4. Locate the **EMC vProxy Disable CBT** field, or create a string for **EMC vProxy Disable CBT**. The string must match the field name exactly and is case-sensitive.
5. Set the value to **true** to disable CBT on the virtual machine, or to **false** (or leave the field blank) to enable CBT on the virtual machine. Setting or resetting the field for one virtual machine does not affect the other virtual machines in the vCenter.
6. Refresh **VMware View** in the NMC **NetWorker Administration** window.

Fixing CBT if corrupted on virtual machine

If CBT becomes corrupted on the virtual machine, warnings similar to the following appear in the backup logs:

```
WARN: Change block tracking needs to be reset.
WARN: Change Block Tracking could not be reset, causing full backup:
Second attempt failed.
NOTICE: Change block tracking cannot be reset by proxy. Please
remediate VM.
```

If these messages appear, you can use PowerCLI commands to disable and then enable CBT without powering off the virtual machines as described in the VMware

knowledgebase article at https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1031873, or perform the following steps to clean up CBT:

1. Power down the virtual machine.
2. Remove CBT flags.
3. Delete CTK files from the datastore.
4. Power ON the virtual machine.

Enable the Microsoft VM App Agent for SQL Server application-consistent protection

The Microsoft Virtual Machine Application Agent (MSVMAPPAGENT) is a component of the vProxy data protection solution that is bundled with the vProxy appliance OVA. **MSVMAPPAGENT** is automatically deployed by the vProxy during a virtual machine application-consistent backup and, if required, when restoring Microsoft SQL databases and SQL instance backups to running virtual machines. After installation, the **MSVMAPPAGENT** package appears in the Windows installer Add-Remove programs list.

The **MSVMAPPAGENT** allows for advanced application data protection of workloads residing on a VMware ESXi server. This includes adding SQL virtual machines to an advanced application-consistent protection policy to perform the following operations:

- SQL Server FULL backup to Data Domain—Configure a NetWorker policy's VMware backup action with the Advanced Application Consistency option to perform SQL Server backup to a Data Domain device as part of a VMware image-level backup. The SQL Server FULL backup is performed during the in-guest quiesce by VMware Tools. After running the policy, the catalog and index information for the SQL server backup is stored on the Data Domain device. When the backup is performed as part of the VMware image-level backup, the SQL data files are backed up as part of the VMDKs during the vProxy image backup. The sections Creating a VMware backup action and Creating an action for Microsoft SQL Server application-consistent protection provide more information.
- Transaction log backup—When configuring a NetWorker policy's workflow and VMware backup action with the Advanced Application Consistency option, select Transaction log backup to enable transaction log backups for SQL Instances running in the virtual machine, and set the Interval attribute in the backup policies workflow properties to specify the frequency of backups. Backups are written directly to Data Domain under the SDSF backup folder that was created by the NetWorker save set session. Transaction log backup is only performed for databases in the proper state, otherwise databases are skipped. The section Create a VMware backup action provides more information.
- Restore of SQL Server instance or individual SQL Server databases—The **Dell EMC Data Protection Restore Client** includes an **App** mode that allows you to restore an entire SQL Server instance to the original virtual machine and original instance, and restore individual SQL Server databases to the original database on the original virtual machine, to multiple instances on the same virtual machine, or to an alternate location (different virtual machines/SQL instances on the same or a different vCenter), as well as the ability to roll-forward transaction log backups. The section Restoring SQL Server application-consistent backups provides more information.

During advanced application-consistent backup for both SQL Server FULL backup and transaction log backup, vProxy installs or upgrades the **vProxy Agent** and

MSVMAPPAGENT software packages. On a new virtual machine without these software packages installed, the **vProxy Agent** uses the VM Administrator Credentials from the backup action to install the vProxy Agent, using the vCenter VIX API to copy packages into the guest virtual machine and run the install. Once the vProxy Agent is installed in the virtual machine, vProxy communicates with the **vProxy Agent** to install the **MSVMAPPAGENT** package.

On a system with vProxy and **MSVMAPPAGENT** already installed, vProxy performs a version check of the **MSVMAPPAGENT** by running the `Msvmagent_discovery.exe` program to report the installed program version and, if necessary, perform an upgrade if the vProxy software repository contains a later version.

Note: Ensure that you manually uninstall in-guest agents (VM app agent for Microsoft Applications) from an alternate virtual machine that is not protected by a SQL application-consistent backup workflow. Also, if you are restoring to an alternate virtual machine that is not protected by a SQL application-consistent workflow, note that the agents will not be automatically uninstalled once the restore is complete. If you want to remove these agents, you must manually uninstall the agents.

The following table provides a list of the **MSVMAPPAGENT** binaries that are called by the vProxy, and the operations these binaries perform.

Table 10 MSVMAPPAGENT binaries called by vProxy

Binary	Purpose	When called
`Msvmagent_discovery.exe`	Provides functions for listing program version and for validating that SQL is installed and for listing SQL Instances and databases.	Called by vProxy to report agent version and determine if an upgrade is required. Also called by vProxy to validate that SQL Server services are running in the virtual machine. Also called by vProxy to report running SQL instances and databases to support SQL alternate restore selection. **Note:** If `Msvmagent_discovery.exe` does not find running SQL Server services, the program returns a failure to the vProxy and the overall NetWorker Application Consistent backup workflow cannot proceed. To resolve the issue, remove virtual machines that do not have SQL from the NetWorker Application Consistent workflow. You can also use the action logs to diagnose the failure, and contact Dell EMC support if required.
`Msvmagentcatsnap.exe`	Catalogs the SQL VSS Full backup that was performed by VMware Tools as an App Agent VSS Full backup of SQL Server instances. Catalog is written to Data Domain.	Called by vProxy once the virtual machine image snapshot has completed.

Table 10 MSVMAPPAGENT binaries called by vProxy (continued)

Binary	Purpose	When called
`Msvmagent_appbackup.exe`	Performs transaction log backup.	Called by vProxy for transaction log backup workflows. The `Msvmagent_appbackup.exe` program will back up all SQL instances in the virtual machine. `Msvmagent_appbackup.exe` performs transaction log backup only, and does not create a virtual machine image backup.
`Msvmagent_snapshotrestore.exe`	Performs restore of SQL VSS Full backup.	Called by vProxy during restore of SQL Database FULL backup. Prior to the restore, the virtual machine image backup is mounted on the target virtual machine. The `Msvmagent_snapshotrestore.exe` copies the VSS manifest documents from the backup, and uses those documents to perform a VSS-aware restore of the SQL database. The SQL database files are copied from the mounted backup VMDK to the original location of the database, and during the VSS post restore, the SQL VSS Writer completes recovery of the backup. If transaction logs are to be restored, or if the NORECOVERY option has been specified, the database will be left in a NORECOVERY state. The msvmagent_snapshotrestore.exe command also supports SQL Alternate restore and instructs SQL the SQL instance to be restored and to change database name and file locations as selected by the customer.
`Msvmagent_apprestore.exe`	Performs restore of individual SQL transaction log backup.	Called by vProxy during restore of the transaction log backup. For each transaction log restore, `Msvmagent_apprestore.exe` receives the Data Domain path for the backup and performs a SQL VDI restore of the transaction log backup. For intermediate transaction logs, the database is left in the NORECOVERY state. For the final transaction log restore, the database is either recovered or left in the NORECOVERY state if you specify this option. The STOPAT feature may also be used for the final transaction log restore if you specify this

Table 10 MSVMAPPAGENT binaries called by vProxy (continued)

Binary	Purpose	When called
		option. The msvmagent_apprestore.exe command also supports SQL Alternate restore and instructs SQL the SQL instance to be restored and to change database name and file locations as selected by the customer.

MSVMAPPAGENT binaries are installed to `C:\Program Files\DPSAPPS\MSVMAPPAGENT\bin`. Logs are located in `C:\Program Files\DPSAPPS\MSVMAPPAGENT\log`.

Software and security requirements

In order to perform SQL Server application-consistent data protection for virtual machines, the **MSVMAPPAGENT** requires the following:

- The**MSVMAPPAGENT** runs under the SYSTEM account for data protection operations. Configure all SQL Server instances in the virtual machine to grant NT AUTHORITY\SYSTEM account rights to perform SQL database backup and recovery operations:
  Add **SYSTEM** account to SQL logins.

  Grant **SYSTEM** account the sysadmin role.
- Network connectivity, host name resolution, and firewall ports between the Data Domain device and the virtual machines that are part of SQL Server application-consistent protection policies and restore to alternate operations. This connectivity is required to allow **MSVMAPPAGENT** to perform client direct operations to Data Domain.
- VMware vCenter server version 6.5 and later.
- VMware ESXi server version 6.5 and later.
- VMware Tools version 10.1 and later.
- Enable the UUID attribute (*disk.EnableUUID=TRUE*) in the **vSphere Client**.
- The virtual machine must use SCSI disks only, and the number of available SCSI slots must at least match the number of disks. For example, a virtual machine with 7 disks will only require one SCSI controller, but a virtual machine with 8 disks will require 2 SCSI controllers.
- The vProxy requires live network connectivity to the ESXi where the targeted SQL virtual machine resides.

Note: The **MSVMAPPAGENT** does not require installation of the NetWorker client.

The following table provides a list of special characters known to be supported in SQL database names for English and non-English locales.

Table 11 Supported characters in SQL database names

Special character	FULL and transaction log backup	FULL and transaction log restore
~ Tilde	Supported	Supported

Table 11 Supported characters in SQL database names (continued)

Special character	FULL and transaction log backup	FULL and transaction log restore
- Hyphen	Supported	Supported
! Exclamation mark	Supported	Supported
{ Open curly bracket	Supported	Supported
% Percentage	Supported	Supported
} Close curly bracket	Supported	Supported
) Close parenthesis	Supported	Supported
(Open parenthesis	Supported	Supported
` Accent grave	Supported	Supported
@ At the rate	Supported	Supported
# Hash	Supported	Supported
_ Underscore	Supported	Supported
& Ampersand	Supported	Supported
^ Caret	Supported	Supported
\ Backslash	Supported	Supported
' Apostrophe **Note:** Restore to an alternate location for a SQL database with an apostrophe in the file name or destination file path will fail to restore.	Supported	Supported
$ Dollar	Supported	Supported
: Colon	Supported	Supported
. Period	Supported	Supported

Unsupported features and configurations

The following features and configurations are not supported for SQL application-consistent protection:

- The **MSVMAPPAGENT** only supports stand-alone SQL Server instances, and does not support SQL Server Always-On Availability Group and SQL Server Clustered Failover instances.
- The **MSVMAPPAGENT** does not support interoperability with other backup agents, including SQL backup products from Dell EMC. If another backup product is running at the same time as **MSVMAPPAGENT**, the **MSVMAPPAGENT** has safeguards to prevent issues. For example, if another product is performing in-guest backups, **MSVMAPPAGENT** may skip databases for transaction log backups.
- If using the **VM Backup and Recovery** user interface in the **vSphere Web Client** for vSphere versions earlier than 6.5, backup and recovery operations are not

supported for SQL Server advanced application-consistent protection policies. For SQL backups, perform these operations from the NMC **NetWorker Administration** window or the **Dell EMC NetWorker** user interface in the **vSphere Client**. For SQL recoveries, perform these operations from the **Dell EMC Data Protection Restore Client**.

Additionally, the following items are not supported due to VMware restrictions and feature limitations:

- Changing pools between backup actions, for example, between a SQL full and transaction log backup.
- Application-consistent quiescing for virtual machines with IDE disks.
- Dynamic disks on the virtual machine.
- Read-only volumes mounted on the SQL virtual machine.
- VMware encrypted virtual machines.
- VMware Fault Tolerant virtual machines.
- RDM storage.

The vProxy appliance performs validation of the environment for these VMware restrictions. If validation fails, the VMware policy with SQL Server application-consistent data protection will not run.

Updating the Microsoft VM App Agent and FLR Agent software

The Microsoft VM App Agent and FLR Agent software required to perform advanced application-consistent data protection and file-level restore operations on the client will be automatically updated on the target virtual machine by the vProxy appliance during the file-level restore operation. The vProxy detects the available software on the client and updates the Agent software with the new version of software from its repository. If the update does not occur automatically, contact a Dell EMC technical support professional for a procedure to update the vProxy software repository with the latest version of the Agent software packages.

Troubleshooting Data Protection Policies

This section provides information about issues related to configuring Data Protection Policy resources and with backup and recovery operations.

Backup operations

The following troubleshooting items provide some direction on how to identify and resolve common issues with vProxy backups.

SQL Server application-consistent backups fail with error "Unable to find VSS metadata files in directory"

SQL Server application-consistent virtual machine backups might fail with the following error when the *disk.enableUUID* variable for the virtual machine is set to **`False`**.

```
Unable to find VSS metadata files in directory C:\Program Files
\DPSAPPS\MSVMAPPAGENT\tmp\VSSMetadata.xxxx.
```

To resolve this issue, ensure that the *disk.enableUUDI* variable for the virtual machines included in an SQL Server application-consistent backup is set to `True`.

Failed to lock Virtual Machine for backup: Another EMC vProxy operation 'Backup' is active on VM

This error message appears when a backup fails for a virtual machine, when previous backups of the virtual machine was abruptly ended and the VM annotation string was not cleared.

To resolve this issue, clear the annotation string value for the virtual machine.

1. Connect to the vCenter server and navigate **Home** > **Inventory** > **Hosts and Clusters**.
2. Select the virtual machine, and then select the **Summary** tab.
3. Clear the value that appears in the **EMC Proxy Session** field.

"Loading backup job data"

This message can appear for up to five minutes when you select a large number of VMs (approximately 100 VMs) for a single backup job. This issue can also apply to lock/unlock, refresh, or delete actions for large jobs. This is expected behavior when you select a very large number of jobs. This message disappears when the action is completed, which can take up to five minutes.

"The following items could not be located and were not selected {client name}."

This error can occur when the backed up VM(s) cannot be located during Edit of a backup job. This is a known issue.

Windows 2008 R2 VMs may fail to backup with "disk.EnableUUID" configured to "true."

Windows 2008 R2 backups may fail if the VM is configured with the *disk.EnableUUID* parameter set to *true*. To correct this problem, manually update the vmx configuration parameter *disk.EnableUUID* to *false* by using the vSphere Web Client:

1. Shut down the VM by right clicking the VM and selecting **Shut Down Guest OS**.
2. Right click the VM and select **Edit Settings**.
3. Click **VM Options**.
4. Expand the **Advanced** section and click **Edit Configuration**.
5. Locate the name *disk.EnableUUId* and set the value to *false*.
6. Click **OK** on the next two pages.
7. Right click the VM and select **Power On**.

After you update the configuration parameter, the backups of the Windows 2008 R2 VM should succeed.

When VMs are moved in or out of different cluster groups, associated backup sources may be lost

When you move hosts into clusters with the option to retain the resource pools and vApps, the containers get recreated, not copied. As a result, the container is no longer the same container even though the name is the same. To resolve this issue, validate or recreate any backup jobs that protect containers after moving hosts in or out of a cluster.

vMotion operations are not allowed during active backup operations

The vSphere vMotion feature enables the live migration of running virtual machines from one physical server to another. You cannot run vMotion operations on the vProxy appliance or VMware Backup appliance during active backup operations. This is expected behavior. Wait until all backup operations have completed prior to performing a vMotion operation.

Backups fail if certain characters are used in the virtual machine name, datastore, folder, or datacenter names

When you use spaces or special characters in the virtual machine name, datastore, folder, or datacenter names, the .vmx file is not included in the backup. The vProxy appliance does not back up objects that include the following special characters, in the format of character/escape sequence:

- & %26
- + %2B
- / %2F
- = %3D
- ? %3F
- % %25
- \ %5C
- ~ %7E
-] %5D

NSRCLONE failed for one or more savesets

This message appears during a clone action and NetWorker does not clone all save sets.

Error messages similar to the following also appear:

```
[CLONE SKIPPED SAVESETS]
ssid/cloneid;
Action clone 'name' with job id 5 is
exiting with status 'failed', exit code 1
NSRCLONE failed for one or more savesets
```

To resolve this issue, increase the values in the **max target sessions** and **target sessions** attributes for the clone device. The *NetWorker Administration Guide* describes how to modify the properties of a device.

Lock placed on virtual machine during backup and recovery operations continues for 24 hours if vProxy appliance fails

During vProxy backup and recovery operations, a lock is placed on the virtual machine. If a vProxy appliance failure occurs during one of these sessions, the lock gets extended to a period of 24 hours, during which full backups and transaction log backups will fail with the following error until the lock is manually released:

```
Cannot lock VM 'W2K8R2-SQL-2014' (vm-522): Another EMC vProxy
operation 'Backup' is active on VM vm-522.
```

Workaround

To manually release the lock on the virtual machine:

1. Open the **vSphere Web Client**.
2. Select the virtual machine and select **Summary**.
3. Select **Custom attribute** and click **Edit**.
4. Remove the attribute **EMC vProxy Session**.

Trailing spaces not supported in SQL database names

Due to a VSS limitation, you cannot use trailing spaces within the names of SQL databases protected by an application-consistent data protection policy.

SQL databases skipped during virtual machine transaction log backup

When an advanced application-consistent policy is enabled with transaction log backup, the `msvmagent_appbackup.exe` program evaluates databases to determine if transaction log backup is appropriate.

If transaction log backup is not appropriate for a database, the database will automatically be skipped. Databases are skipped for the following reasons:

Table 12 SQL Skipped Database Cases and Descriptions

Case	Description
Database has been restored	When a database has been restored, this database will be skipped during transaction log backup because there is no Backup Promotion.
System Database	System databases are automatically skipped for transaction log backup.
Database State	Database is not in a state that allows backup. For example, the database is in the NORECOVERY state.
Recovery Model	Database is in SIMPLE recovery model, which does not support transaction log backup
Other Backup Product	Most recent backup for the database was performed by a different backup product.
New Database	Database was created after most recent full backup.
Backup Failure	Database was in state to allow backup, backup was attempted, but backup failed.

All skipped databases will be backed up as part of the next full backup. Also, a skipped database will not result in `msvmagent_appbackup.exe` failure. The only instance in which `msvmagent_appbackup.exe` would potentially fail is if all databases failed to back up.

The `msvmagent_appbackup.exe` program generates a history report of the databases, if the database backup status was success/skipped/failed, and a reason if they were skipped or failed if applicable. This history report is visible in the action logs for the vProxy, which are available as part of the appbackup logs.

Note: For SQL virtual machine application-consistent data protection, the SQL and operating system versions follow the NMM support matrix available at http://compatibilityguide.emc.com:8080/CompGuideApp/.

Increase the vCenter query timeout before starting a VMware backup action

Before starting a VMware backup action, NetWorker queries the vCenter server to determine if any changes have occurred in the items selected for backup. You can increase the timeout value by setting the *NSR_HYPERVISOR_QUERY_REQUEST_TIMEOUT* environment variable.

The amount of time for the query to complete depends on several factors, including the network response time, the size of the vCenter, and the number of resources free on the NetWorker server. The default timeout of the query is 30 minutes, after which the backup fails with the following error:

```
nsrvproxy_save NSR warning Dispatcher: Request timed out
```

Perform the following steps to set the *NSR_HYPERVISOR_QUERY_REQUEST_TIMEOUT* environment variable to a higher timeout value. Note that the timeout value is in seconds. In this example, a value of 2700 (or 45 minutes) is used.

1. Set up the environment variable:
   - On Linux, add the following lines to the /nsr/nsrrc file:
     ```
     NSR_HYPERVISOR_QUERY_REQUEST_TIMEOUT=2700

     export NSR_HYPERVISOR_QUERY_REQUEST_TIMEOUT
     ```
   - On Windows, add a new variable called *NSR_HYPERVISOR_QUERY_REQUEST_TIMEOUT* under **Environment variables** > **System variables**, and specify a value of `2700`.
2. On the NetWorker server, connect to nsradmin:
   ```
   nsradmin -p nsrexec
   ```
3. Select/Print the 'NSRLA' resource:
   ```
   p type: nsrla
   ```
4. Append to the attribute:
   ```
   append environment variable names:
   NSR_HYPERVISOR_QUERY_REQUEST_TIMEOUT
   ```
5. Select/Print the 'NSRLA' resource again to verify your changes:
   ```
   p type: nsrla
   ```

The last attribute should display as *environment variable names: NSR_HYPERVISOR_QUERY_REQUEST_TIMEOUT*.

Managing command execution for VM Proxy Agent operations on Linux

The **VM Proxy Agent** automatically creates a PAM service file named `vproxyra` in the `/etc/pam.d system` directory, if the file does not already exist.

This file, which allows you to manage command execution through the **VM Proxy Agent**, is modeled on the corresponding `vmtoolsd` file. The settings in this file permit command execution by any user who is able to perform VM Proxy-based operations on the guest virtual machine. A system administrator can further modify this file to specify which users can perform **VM Proxy Agent** operations, for example, file-level restore and SQL application-aware protection. For more information on the configuration of PAM service files, see the system documentation for your specific guest virtual machine operating system.

vProxy backup log files

You can use vProxy session log files to troubleshoot backup failures.

The following table provides information about the vProxy backup log files. located in `/opt/emc/vproxy/runtime/logs/vbackupd/` on the vProxy host. Note that old daemon and session logs are located in `/opt/emc/vproxy/runtime/logs/recycle/`.

Table 13 Backup log files

Log file	Log location	Description
Session logs	`<session-uuid>.log`	Contains processing details for a session. Sessions display as “Recycled” when the session is deleted. The log level is configured in the session request.
Daemon logs	`<daemon>-engine.log`	Records requests and problem events which may require administrative action in vProxy or vCenter. Error and Panic messages from the session logs are also recorded in the daemon log. The log level is set in `/usr/lib/systemd/system/<daemon>.service`, for example, "--engine-log-level <level>".
DD Boost backup log	`<daemon>-boost.log`	The log level is set in `/usr/lib/systemd/system<daemon>.service`, for example, "--boost-log-level <level>"
VDDK backup log	`<daemon>-vddk.log`	The log level is set in `/opt/emc/vproxy/conf/VixDiskLib.config` (vixDiskLib.transport.LogLevel = <level>)

On the NetWorker server, the location of log files for individual backups differ on Windows and LINUX:

- Linux—`/nsr/logs/policy/`*`policy_name`*
- Windows—`C:\Program Files\EMC NetWorker\logs\policy\`*`policy_name`*

where *policy_name* is the name of the policy resource associated with the backup action.

Additional logging with the VMBackup broker

Debug logging of the `vmbackup` broker of `nsrd` is disabled by default. To turn on additional logging, you can touch an empty file at `<nsr>/tmp/vmbackup_logging`. Enabling of additional logging can be performed while other operations are in progress, and a NetWorker restart is not required. To turn off additional logging, you can remove the same file.

NMC function to collect vProxy log bundle information

NetWorker 18.x features an NMC function to collect vProxy log bundle information from a virtual machine. To collect log bundle information, perform the following steps in NMC:

1. From NMC's **NetWorker Administration**, open the **Devices** window.

2. From the left pane, select **VMware Proxies** to display the virtual machine proxy devices.
3. Right-click the virtual machine that you want to collect log bundle information from, and then from the menu, click **Log Bundle**.
4. (Optional) Collect the recycled logs from the pop-up window selection.

Note: Since the temporary log bundle download occurs on the NetWorker server, ensure that there is sufficient space on the drive where the Networker server is installed.
Also, note that NMC cannot collect the log bundle when accessed from a remote machine that cannot communicate with vProxy

Logs for SQL application-consistent data protection

The following section provides location information for all logs associated with SQL application-consistent data protection.

Note: In order to increase the debug level for SQL application-consistent virtual machine (MSVMAPPAGENT) backups, use `dbgcommand`, For example, `dbgcommand -p <nsrd-pid> Debug=9`. Once you complete the debugging session, ensure that you reset the debug level of `nsrd` to zero by running `dbgcommand <nsrd-pid> Debug=0`.

MSVMAPPAGENT logs

You can access logs related to MSVMAPPAGENT from the following locations:

- Discovery log: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmagent_discovery.log`
- FULL backup: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmcatsnap.log`
- Transaction log backup: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmagent_appbackup.log`
- Restore of FULL backup: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmagent_snapshotrestore.log`
- Restore of transaction log backup: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmagent_apprestore.log`

vProxy logs

You can access these vProxy logs from the following locations:

- FULL and transaction log backups: `/opt/emc/vproxy/runtime/logs/vbackupd/BackupVmSessions-sessionnumber.log`
- InspectBackup logs: `/opt/emc/vproxy/runtime/logs/vsessionsd/inspectBackup-sessionnumber.log`
- Mount session logs: `/opt/emc/vproxy/runtime/logs/vflrd/mount-sessionnumber.log`
- Browse session logs: `/opt/emc/vproxy/runtime/logs/vflrd/browse-sessionnumber.log`
- Recover App sessions logs: `/opt/emc/vproxy/runtime/logs/vflrd/application-sessionnumber.log`. Note that a few minutes after

completion, these logs are moved to `/opt/emc/vproxy/runtime/logs/recycle/`.

CHAPTER 4

Recover virtual machines and data

This chapter contains the following topics:

- Preparing the NetWorker datazone for recovery 142
- vProxy recovery in NMC 146
- vProxy recovery in the NetWorker Management Web UI 164
- vProxy file-level restore and SQL restore in the Dell EMC Data Protection Restore Client 174
- vProxy recovery in the vSphere Client's Dell EMC NetWorker interface 196
- vProxy recovery in the vSphere Web Client's VM Backup and Recovery interface 207
- vProxy recovery log files 215

Preparing the NetWorker datazone for recovery

Before performing an image-level or file-level virtual machine recovery with NetWorker, review the following sections.

Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only)

Before you perform an instant recovery of a virtual machine or file-level restore (User mode), ensure that you provide the management credentials for the Data Domain resource. For instant recovery, these credentials are required when performing the recovery using the NMC **Recover** wizard or the **VM Backup and Recovery** interface in the **vSphere Web Client**.

Procedure

1. In the NMC Administration window, click **Devices**.

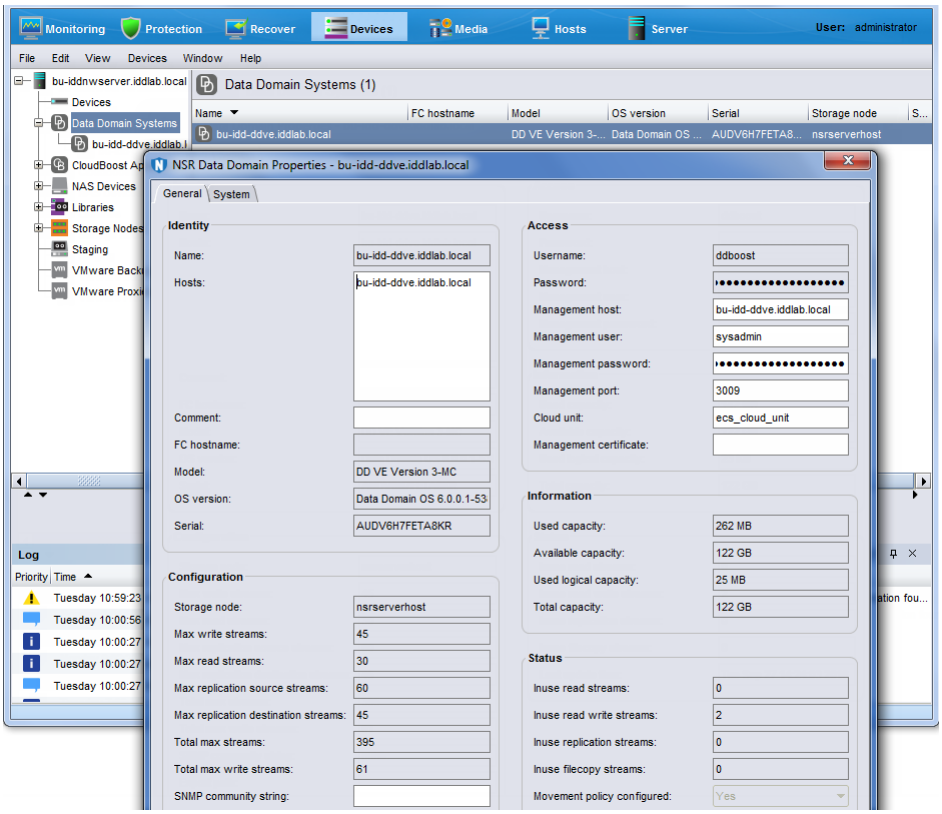
   The **Devices** window displays.

2. In the expanded left navigation pane, select **Data Domain Systems**.

3. In the right details pane, right-click the Data Domain system, and then select **Properties**.

   The **NSR Data Domain Properties** window displays.

Figure 34 NSR Data Domain Properties



4. In the **Access** pane, type the management credentials.

   a. In the **Management host** field, specify the hostname of the Data Domain system that is used for management commands.

b. In the **Management user** field, specify the username for a Data Domain user that has admin access. For example, sysadmin. The Management user should have Data Domain administrator privileges.

c. In the **Management password** field, specify the password of the management user.

d. In the **Management port** field, specify the management port. By default, the port is 3009.

Note: The *NetWorker Data Domain Boost Integration Guide* provides information about the Cloud unit field and use of the Cloud tier device.

5. If required, in the **Configuration** pane, update the export path. It is recommended that you leave this field blank, which sets the export path to the default path. The short name of the NetWorker server is the default path.

   If you do type a path in this field, ensure that the path has NFS permissions. When you log in to the Data Domain resource, browse to the NFS section and add the Mtree device path (the path to the NetWorker backup device) as a valid NFS path.

6. To save the changes, click **OK**.

File-level restore as an Active Directory user

In order to perform a file-level restore as an Active Directory (AD) user in the NMC **NetWorker Administration** window's **Recovery** wizard or the **Dell EMC Data Protection Restore Client**, you need to register a tenant user and provide the FLR AD user required permissions.

About this task

Note: The following steps include high level information for running `authc_config`. More detailed steps might be required if configuring AD authentication in the NetWorker environment. The *NetWorker Security Configuration Guide* provides more information.

Procedure

1. Log in to your AD server, and make note of objects related to this user (such as the Organizational Units (OU) and Groups in the Active Directory server) that will be added as a tenant user of NetWorker. You can use any third party AD viewer/browser to obtain the required objects and their properties.

   For example,

   a. Create an OU **proxy** inside the domain.

   b. Inside the OU **proxy**, create a group named `vmware` and another OU **user**.

   c. Inside the OU **user**, create a user named `ADuser` and make this user a member of the group **vmware**.

   d. If you plan to use the command line to register the AD user to NetWorker, as described in step two below, make note of the values for the following variables as you will require these values for the registration commands:

   - config-name
   - config-server-address
   - config-domain

- config-user-dn
- config-user-dn-password
- config-user-object-class
- config-user-search-path
- config-user-id-attr
- config-group-search-path
- config-group-name-attr
- config-group-object-class
- config-group-member-attr
- config-active-directory

e. If you plan to use the **NetWorker Management Console** to register the AD user to NetWorker, also described in step two below, make note of the following values as you will require these values for the registration:

- Domain
- Port number
- Provider Server name
- User DN
- Group Object Class
- Group Search Path
- Group Name Attribute
- Group Member Attribute
- User Object Class
- User Search Path
- User ID Attribute

2. Register the AD domain user to NetWorker either using the command line or the **NetWorker Management Console** user interface.

   If using the command line:

   a. Create a tenant user on NetWorker by running the `authc_config` command, as in the following:

   authc_config -u administrator -e add-tenant -D tenant-name=*your tenant name* -D tenant-alias *your selected aliases* -p *password*

   For example, to create a tenant user **ADuser** with the alias **FLR**, run **authc_config -u administrator -e add-tenant -D tenant-name=ADuser -D tenant-alias FLR -p *password***

   b. Obtain the tenant ID by running the `authc_config` command using the `find-tenant` parameter. For example:

   authc_config -u administrator -e find-tenant -D tenantname=*ADuser* -p *password*

   c. Register the AD domain user to NetWorker by running the `authc_config` command using the `add-config` parameter and using the values obtained in Step1d, as in the following:

```
authc_config -u administrator -e add-config -D config-tenant-
id=tenant ID number -D config-name=your tenant name -D config-
server-address=ldap IPv4 addressOU=proxy,DC=domain name,DC=com
-D config-domain=domain name -D config-user-
dn=CN=Aduser,OU=user,OU=proxy,DC=domain name,DC=com -D config-
user-dn-password=password -D config-user-object-
class=inetOrgPerson -D config-user-search-path=OU=user -D
config-user-id-attr=cn -D config-group-search-path=OU=user -D
config-group-name-attr=cn -D config-group-object-class=group -
D config-group-member-attr=member -D config-active-directory=y
-p password
```

If using the **NetWorker Management Console**:

a. Click the **Setup** tab.

b. On the left pane of the **Setup** window, expand **Users and Roles**, right-click **External Authority** and select **New** from the drop-down. The **Add External Authentication Authority** dialog displays.

c. Provide a name for the external authority (for example, `Aduser`), select **Active Directory** from the **Server Type** drop-down, and then fill in the required details with the values obtained from Step1e.

d. Click **OK**.

3. In the **NetWorker Management Console**, click the **Server** tab.
4. On the **Server** window, select **User Groups**.
5. Add a user group (for example, `ADuser group`) with the following permissions:
   - View Security Settings
   - View Application Settings
   - Remote Access All Clients
   - Operate NetWorker
   - Monitor NetWorker
   - Operate Devices and Jukeboxes
   - Recover Local Data
   - Recover Remote Data
   - Backup Local Data
6. Edit the new user to add the required **AD user** and **AD group** in the **External Roles** field. For example, for a user named **ADuser** with the domain **rideblr**, add the following in the **External Roles** field:

   ```
   CN=Aduser,OU=user,OU=proxy,DC=rideblr,DC=com
   CN=vmware,OU=proxy,DC=rideblr,DC=com
   ```

7. Log in to the **Dell EMC Data Protection Restore Client** as the AD user, in the format `<tenant>\<domain>\<userid>`. For example, `default\rideblr.com\ADuser`.

Results

You can now perform file-level restore as an Active Directory user.

Active Directory user access to the vCenter plug-in and NMC

The Active Directory (AD) user that you create using the steps in the section "File-level restore as a domain user" will only have access to the **Dell EMC Data Protection Restore Client**, and cannot be used to log in to the **vCenter** plug-in or the **NetWorker Management Console**. If the AD user also needs access to these applications, the following additional privileges are required.

vCenter plug-in additional privileges

If you require access to the **vCenter** plug-in as the same AD user:

1. Launch the NMC **NetWorker Administration** window, and go to **Server** > **User Groups** > **Edit Security Administrators**.
2. Add the AD user and group in the **External Roles** field. For example, for a user named **ADuser** with the domain **rideblr.com**, type `CN=Aduser,OU=user,OU=proxy,DC=rideblr,DC=com` for the user and `CN=vmware,OU=proxy,DC=rideblr,DC=com` for the group.

NetWorker Management Console additional privileges

If you require access to the **NetWorker Management Console** as the same AD user:

1. In the **NetWorker Management Console**, click the **Setup** tab.
2. On the **Setup** window, expand **Users and Roles** in the left navigation pane, and then select **NMC Roles**. The roles display in the right pane.
3. For the Console User NMC Roles, add the AD user and group in the **External Roles** field. For example, for a user named **ADuser** with the domain **rideblr.com**, type `CN=Aduser,OU=user,OU=proxy,DC=rideblr,DC=com`.
4. Navigate to the NMC **Enterprise** window, right-click the server and select **Launch Application** to open the NMC **NetWorker Administration** window.
5. Click the **Server** tab to open the **Server** window, and then click **User Groups** in the left pane to display the users in the right pane.
6. Add the AD user in the **External Roles** field under **Application Administrators**. For example, for a user named **ADuser** with the domain **rideblr.com**, type `CN=Aduser,OU=user,OU=proxy,DC=rideblr,DC=com`.

vProxy recovery in NMC

You can use the **Recovery** wizard in NMC to perform image level recovery, which allows you to recover full virtual machines and VMDKs. You can also use the **Recovery** wizard to perform file-level restore from a primary or cloned backup on a Data Domain device, but only as an administrator.

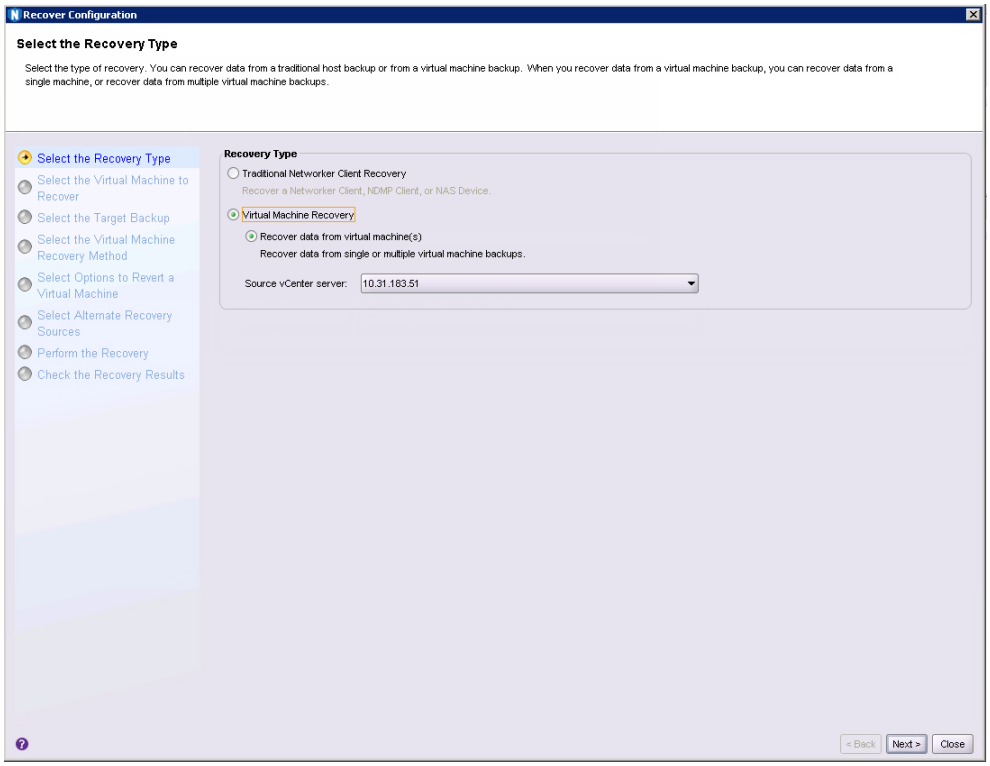
In NMC's **NetWorker Administration** window, click **Recover**. From the **Recover** window, launch the **Recovery** wizard by selecting **Recover** > **New**.

Recovering a virtual machine using the NMC Recovery wizard

About this task

When you click **Recover** in NMC's **NetWorker Administration** window and select **Recover** > **New** from the menu, the **Recovery** wizard launches. **Virtual Machine Recovery** is the second recovery type displayed.

Figure 35 Virtual machine recovery in the NMC Recovery wizard

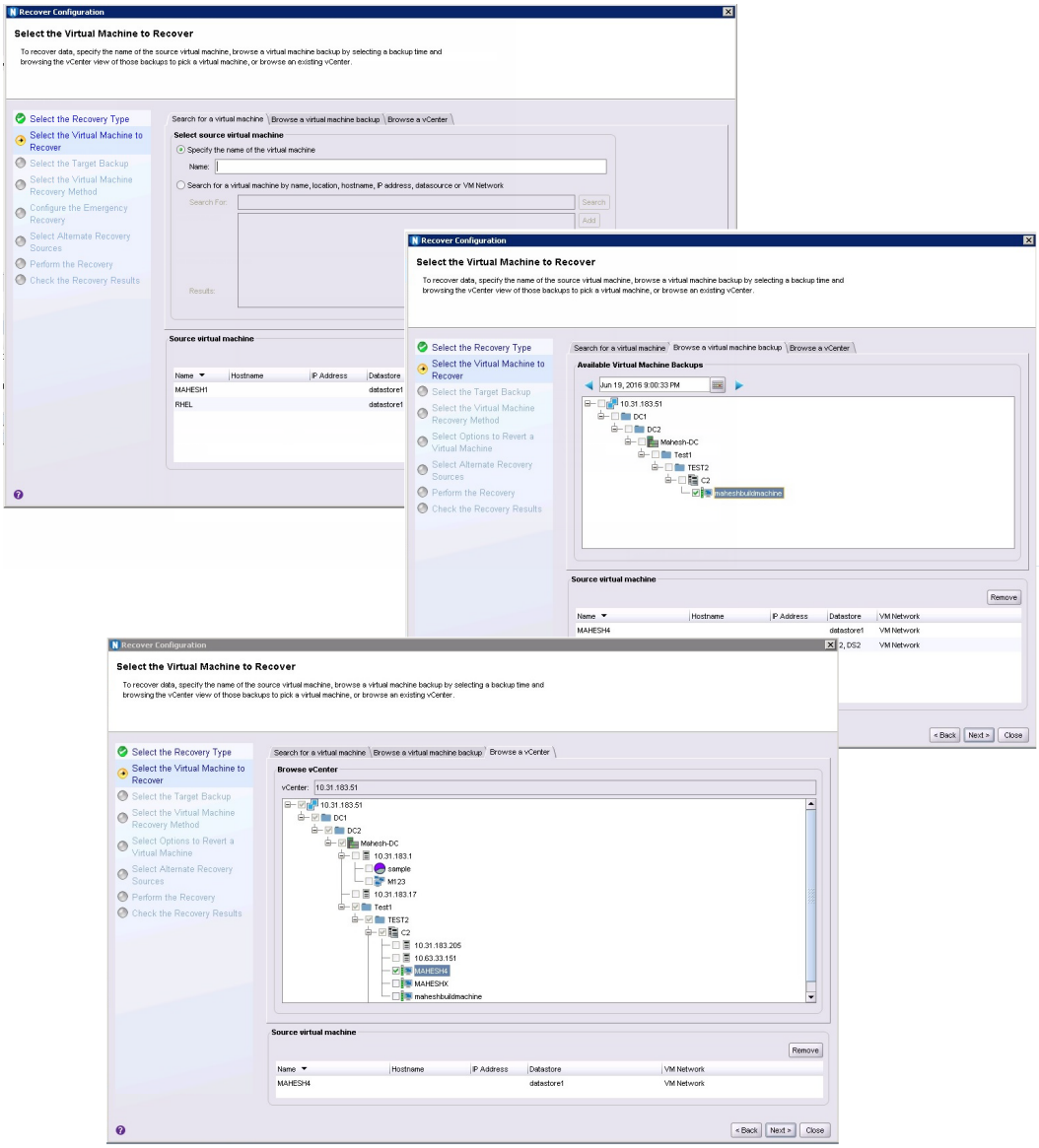


After selecting the **Virtual Machine Recovery** type, you can perform recovery of individual virtual machines, or (for revert and virtual machine recovery options) recovery from multiple virtual machines.

Procedure

1. In the **Select the Recovery Type** page, select **Virtual Machine Recovery**, and then select a vCenter server to recover from using the **Source vCenter server** drop-down. Click **Next**.
2. In the **Select the Virtual Machine to Recover** page, enter the name of the source virtual machine(s) to recover from, or perform a search for the virtual machine. Additionally, you can use the tabs on this page to choose a single virtual machine or multiple virtual machines from a selected backup, or browse the source vCenter to determine the required virtual machine source. When you locate and choose the desired virtual machine(s), click **Next**.

Figure 36 Select the Virtual Machine to Recover



3. In the **Select the Target Backups** page, select the virtual machine backup(s) you want to restore from the **Available Backups** pane. This pane lists both primary backups and, if available, clone copies. If you selected recovery from multiple virtual machines, you can switch between virtual machines to browse each machine's available backups by using the **Virtual Machine Name** drop-down. Click **Next**.

Figure 37 Select the Target Backup (individual virtual machine)

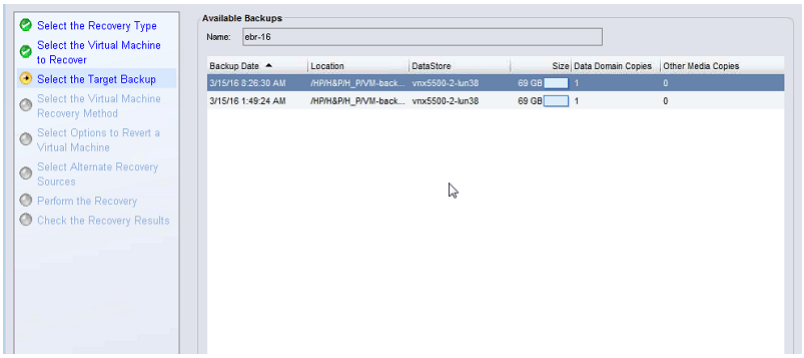
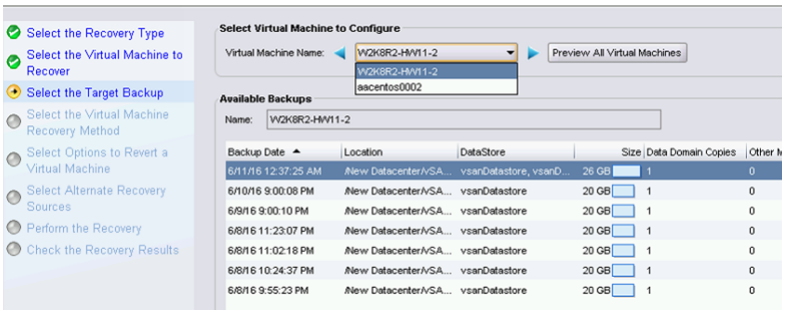
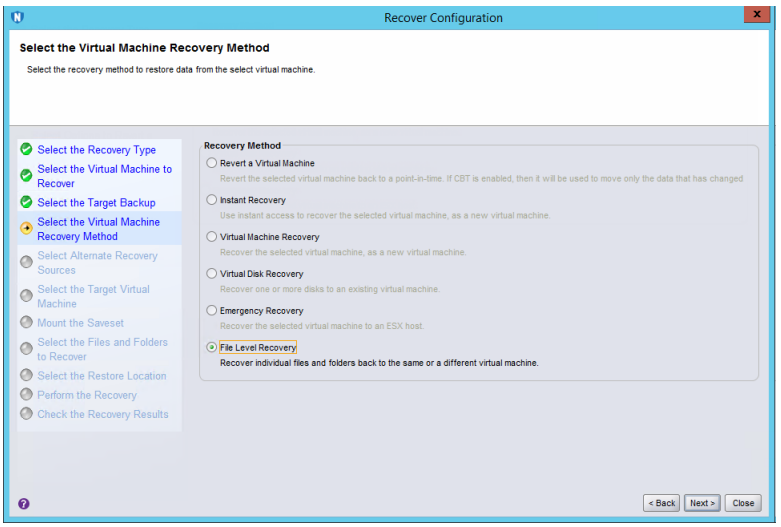


Figure 38 Select the Target Backup (multiple virtual machines)



4. In the **Select the Virtual Machine Recovery method** page, select from one of the available recovery options:
   - Revert (or rollback) a virtual machine
   - Instant Recovery of a virtual machine (direct restore from a Data Domain device)
   - Virtual Machine recovery (recovery to a new virtual machine)
   - Virtual Disk recovery (recover VMDKs to an existing virtual machine)
   - Emergency recovery (recovery to an ESX host)
   - File Level recovery (recover files from VMDKs to a file system, or as a download).

Figure 39 Select the Virtual Machine Recovery method



Results

Subsequent wizard options change based on the recovery option selected, as described in the following sections.

Revert (or rollback) a virtual machine backup

The first virtual machine recovery option available in the NMC Recovery wizard is to revert, or rollback, a virtual machine backup. With a Revert a virtual machine backup recovery, you use an existing virtual machine to rollback the VMDKs as a virtual machine.

About this task

Note: When you revert a virtual machine, the current virtual machine is removed in the process. You cannot use the **Revert a Virtual Machine** recovery option when the ESXi has been removed from the vCenter and then added back to the vCenter. In this case, use the **Virtual Machine recovery** option instead.

To complete the Recovery wizard with the reverting a virtual machine method, perform the following.

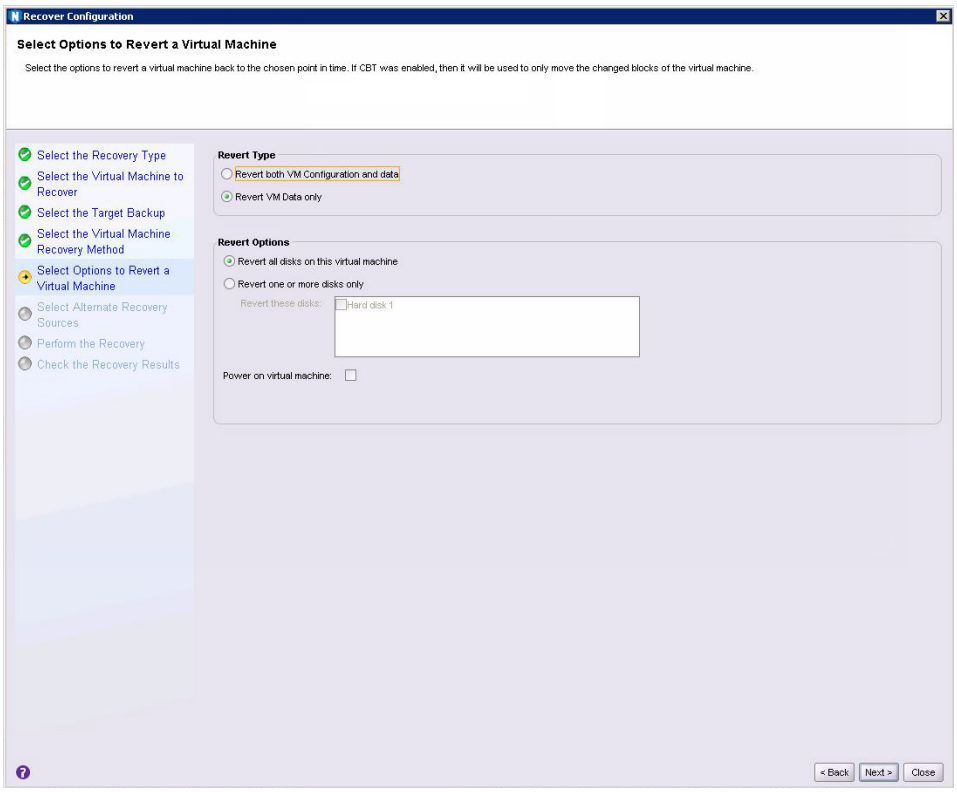
Procedure

1. In the **Select the Virtual Machine Recovery Method** page:
   a. Select **Revert a Virtual Machine**.
   b. Click **Next**.

   The **Select Options to Revert a Virtual Machine** page displays
2. In the **Revert Type** pane of the **Select Options to Revert a Virtual Machine** page:
   a. Select **Revert both VM configuration and data** to revert both the configuration information (such as operating system, virtual machine size) and data for a virtual machine. When you select this revert type, the **Delete existing disk on disk configuration mismatch** option appears in the **Revert Options** pane to allow you to overwrite an existing disk if a configuration mismatch occurs.
   b. Select **Revert VM Data Only** to revert only the virtual machine data without changing the virtual machine configuration.
3. In the **Revert Options** pane of the **Select Options to Revert a Virtual Machine** page, choose from the following options
   a. Select **Revert all disks on this virtual machine** to rollback all VMDKs, or select **Revert one or more disks only** and then select a specific disk drive to rollback only that disk.
   b. Select the **Power on virtual machine** checkbox to power on the virtual machine after the restore.
   c. Select **Delete existing disk on disk configuration mismatch** if you want to be presented with the option of deleting the existing disk if a disk configuration mismatch is detected. Note that this option only appears when you select the **Revert both VM configuration and data** revert type in step two.
   d. Click **Next**.

Note: If the virtual machine is currently powered on, a dialog displays requesting confirmation to power off the virtual machine. Additionally, if a change has occurred in the virtual machine configuration since the backup, a warning message displays.

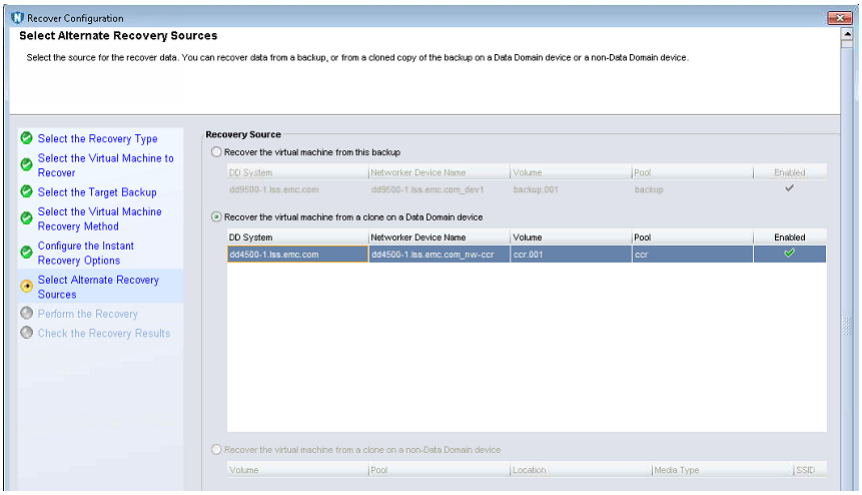
Figure 40 Choose Disks to Revert



Note: The entire VMDK will be rolled back unless you have CBT enabled, in which case only the changed blocks will be moved.

4. In the **Select Alternate Recovery Sources** page:
   a. Select the original backup or a clone copy if one is available.
   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the DD Boost clone pool.
   c. Click **Next**.

Figure 41 Select Alternate Recovery Sources



5. In the **Perform the Recovery** page:

   a. Specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct.

   b. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the reversion is complete.

Instant Recovery of a virtual machine

The next virtual machine recovery option available in the NMC Recovery wizard is instant recovery of a virtual machine backup. With instant recovery, the virtual machine backup is read directly from the Data Domain device and the VMDKs will be restored directly on a Data Domain device. You can perform one instant recovery session at a time.

Before you begin

Before you begin, make note of the following:

- For the Data Domain resource, ensure that you provide the management credentials and, if required, enter the export path appropriately.
- Ensure that the free space on the Data Domain system is equal to or greater than the total disk size of the virtual machine being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target virtual machine fails.
- Ensure that you have at least one proxy that is not restricted to a specific datastore. For the vProxy, select **Properties** and then select **Configuration**, and verify that datastores is left blank.
- Do not perform an instant recovery of virtual machines in resource pools and other similar containers that are part of a currently running protection group.

About this task

To complete the Recovery wizard with the instant recovery method, perform the following steps:

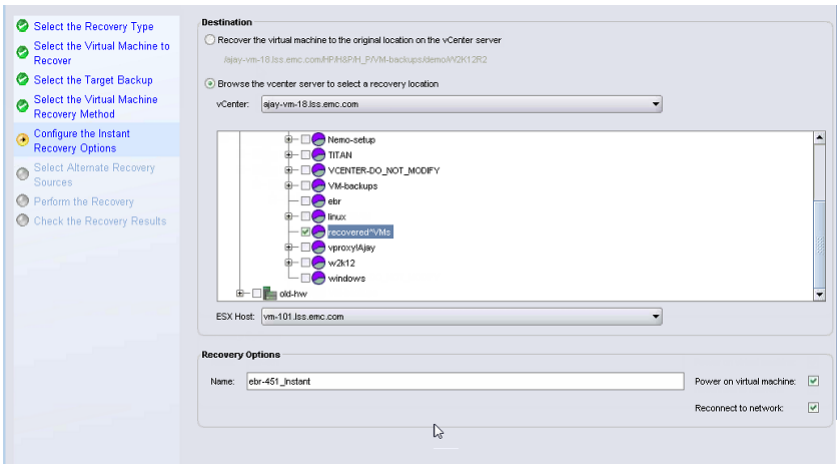
Procedure

1. In the **Select the Virtual Machine Recovery Method** page:
   a. Select **Instant Recovery**.
   b. Click **Next**.
2. In the **Configure the Instant Recovery Options** page:
   a. Select the location where you want to restore the virtual machine in the vCenter environment.

      This does not have to be the original location, and can also be on a different vCenter server.

   b. Ensure that you select the **Power on virtual machine** and **Reconnect to network** options.
   c. Click **Next**.

Figure 42 Configure the Instant Recovery



3. In the **Select Alternate Recovery Sources** page:
   a. Select the original backup, or a clone copy if one is available.
   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the DD Boost clone pool.
   c. Click **Next**.
4. In the **Perform the Recovery** page:
   a. Specify a name for the recovery.
   b. Check the summary at the bottom of the page to ensure all the details are correct.
   c. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the instant recovery is complete. When the instant recovery is complete and ready for use, you can then storage vMotion the virtual machine to a datastore, or perform a file level recovery to the target file system, and then stop the completed instant recovery to free up those resources.
To stop an instant recovery in NMC:

1. Navigate to the **Recover** window.
2. Right-click the entry for the recovery within the Recover sessions pane.
3. Select **Stop** from the drop-down.

Note: To optimize use of NetWorker and Data Domain resources, it is strongly recommended that you stop the instant recovery session once you satisfy your recovery objectives.

Virtual machine recovery

The next virtual machine recovery option available in the NMC Recovery wizard is to perform a recovery of a virtual machine backed up with the vProxy Appliance to a new virtual machine.

About this task

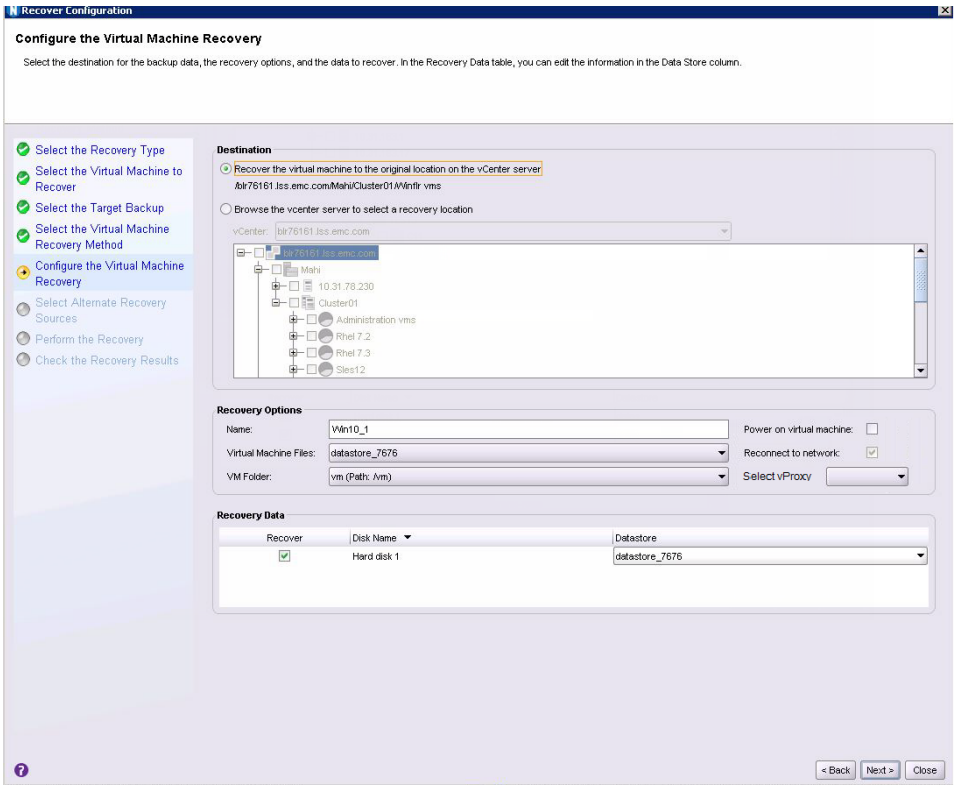
Note: Recoveries of virtual machines backed up with the VMware Backup Appliance should still be performed with the **EMC Backup and Recovery** user interface in the **vSphere Web Client**.

To complete the Recovery wizard with the virtual machine recovery method, perform the following.

Procedure

1. In the **Select the Virtual Machine Recovery Method** page:
   a. Select **Virtual Machine Recovery**.
   b. Click **Next**.
2. In the **Configure the Virtual Machine Recovery** page, select the location where you want to restore the virtual machine in the vCenter environment
   a. In the **Destination** pane, select the option to recover the new virtual machine to the original location, or browse to select a new location on the same vCenter server or a different vCenter server.
   b. In the **Recovery Options** pane, choose a vProxy for the virtual machine recovery from the **Select vProxy** drop-down, specify the name of the new virtual machine, and then optionally select the virtual machine file datastore and folder where you want to recover the files. You can recover the virtual machine to a Blue folder by using the **VM Folder** drop-down, as shown in the following figure. The folder can be the default folder, or a new folder.

Figure 43 Configure the virtual machine recovery



If you have a single disks, or multiple disks with multiple datastores, you can perform the following:

- Choose to recover a collection of all the available hard drives.
- Select a different datastore than the original datastore.
- Select a different datatore for each disk you want to recover.
- Specify the datastore where the virtual machine configuration files reside.

Optionally, select the **Power on virtual machine** and **Reconnect to network** options to power on and reconnect after the recovery, and then click **Next**.

3. In the **Select Alternate Recovery Sources** page:
   a. Select the original virtual machine backup, or a clone copy if one is available.
   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the staging pool.
   c. Click **Next**.

   Note: If selecting a clone from **Select Alternate Recovery Sources**, additionally review the "Selecting alternate recovery sources" section.

4. In the **Perform the Recovery** page:
   a. Specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct.
   b. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the virtual machine recovery is complete.

Virtual Disk Recovery

The next virtual machine recovery option available in the NMC Recovery wizard is to perform a virtual disk, or VMDK, recovery. With VMDK recovery, the disks from the virtual machine backup are recovered to an existing virtual machine.

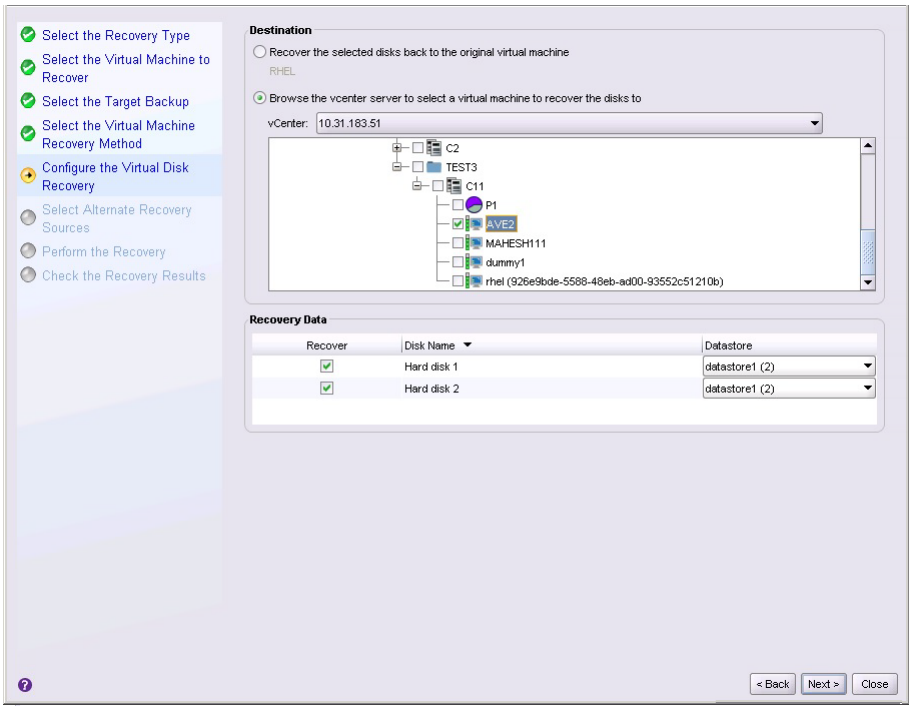
About this task

To complete the Recovery wizard with the virtual disk recovery method, perform the following.

Procedure

1. In the **Select the Virtual Machine Recovery Method** page:
   a. Select **Virtual Disk Recovery**.
   b. Click **Next**.
2. In the **Configure the Virtual Disk Recovery** page:
   a. Select the virtual machine where you want to restore the VMDKs. This can be the original virtual machine, or another existing virtual machine.
   b. Select the desired disks from the **Recovery Data** pane, and select a datastore.
   c. Click **Next**.

Figure 44 Configure the Virtual Disk Recovery



3. In the **Select Alternate Recovery Sources** page:
   a. Select the original virtual disk backup, or a clone copy if one is available.
   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the staging pool.

c. Click **Next**.

4. In the **Perform the Recovery** page:

   a. Specify a name for the recovery.

   b. Check the summary at the bottom of the page to ensure all the details are correct.

   c. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the disk recovery is complete.

Note: When you start a VMDK recovery, the virtual machine will be powered off automatically without issuing a warning message.

Emergency Recovery

The next virtual machine recovery option available in the NMC Recovery wizard is an Emergency Recovery. An Emergency Recovery is required when you need to restore the virtual machine to an ESXi host.

Before you begin

Emergency Recovery requires a vProxy set up on the ESXi host prior to running the recovery.

Additionally, ensure that you disconnect the ESXi host from the vCenter server.

About this task

Note: During an Emergency Recovery, the vProxy gets associated with the ESXi host and is unavailable for other operations on the vCenter server. Wait until the recovery completes before initiating any other operations on the vProxy.

To complete the Recovery wizard with the Emergency Recovery method, perform the following:

Procedure

1. In the **Select the Virtual Machine Recovery Method** page:

   a. Select **Emergency Recovery**.

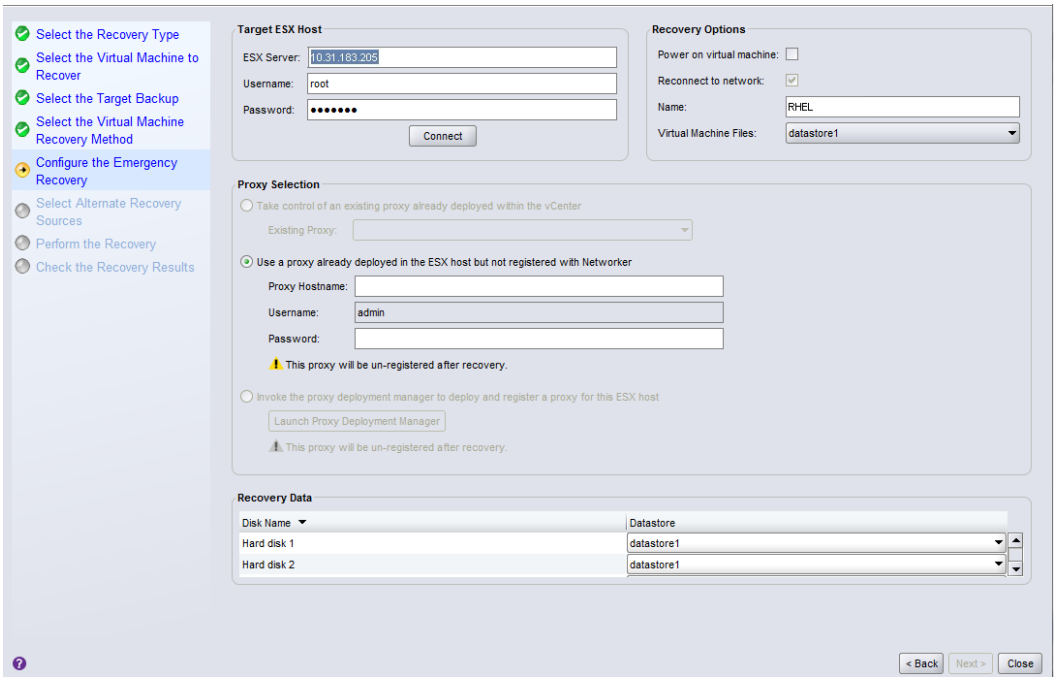
   b. Click **Next**.

2. In the **Configure the Emergency Recovery** page:

   a. Specify the target ESXi server in the vCenter environment.

   b. Click **Connect**.

Figure 45 Configure the Emergency Recovery



The **Proxy Selection** and **Recovery Data** panes get populated with the ESXi server details.

3. In the **Proxy Selection** pane, if a proxy is not discovered, add a new proxy which is deployed in vCenter but not added to NetWorker.
4. For the disks in the **Recovery Data** pane:
   a. Select a datastore.
   b. Optionally, select the **Power on virtual machine** and **Reconnect to network** options.
   c. Click **Next**.
5. In the **Select Alternate Recovery Sources** page:
   a. Select the original disk backup, or a clone copy if one is available.
   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the staging pool.
6. In the **Perform the Recovery** page:
   a. Specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct.
   b. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display a progress bar with the duration of the recovery, and a log file entry when the Emergency Recovery is complete.

Note: The progress bar may not update correctly when you perform an Emergency Recovery directly to the ESXi host.

File Level recovery (Admin mode only)

The final virtual machine recovery option available in the NMC Recovery wizard is File Level recovery. With file level recovery, you can recover individual files from backups

of virtual machines or VMDKs to a primary or secondary vCenter server, and for application-consistent backups, you can also restore the transaction log from Data Domain to the SQL database.

Before you begin

NetWorker only supports file level recovery operations from a primary or cloned backup if the save set is on a Data Domain device. If a cloned backup does not exist on the Data Domain device, you must manually clone a save set from the tape device to Data Domain before launching the **Recovery** wizard.

For the Data Domain resource, ensure that you provide the management credentials and, if required, type the export path appropriately. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only) provides detailed steps.

Additionally, if recovering to a virtual machine on a secondary vCenter, ensure that a vProxy appliance has been deployed on the secondary vCenter server and configured with the NetWorker server.

About this task

File level recovery in the NMC **Recovery** wizard can only be performed by an administrator.

Note: For file-level recovery of high-density file systems (more than few hundred files/folders), it is recommended to use either the **NetWorker Management Web UI** or the **Dell EMC Data Protection Restore Client** (User or Admin mode, as applicable) instead of the NMC **Recovery** wizard.

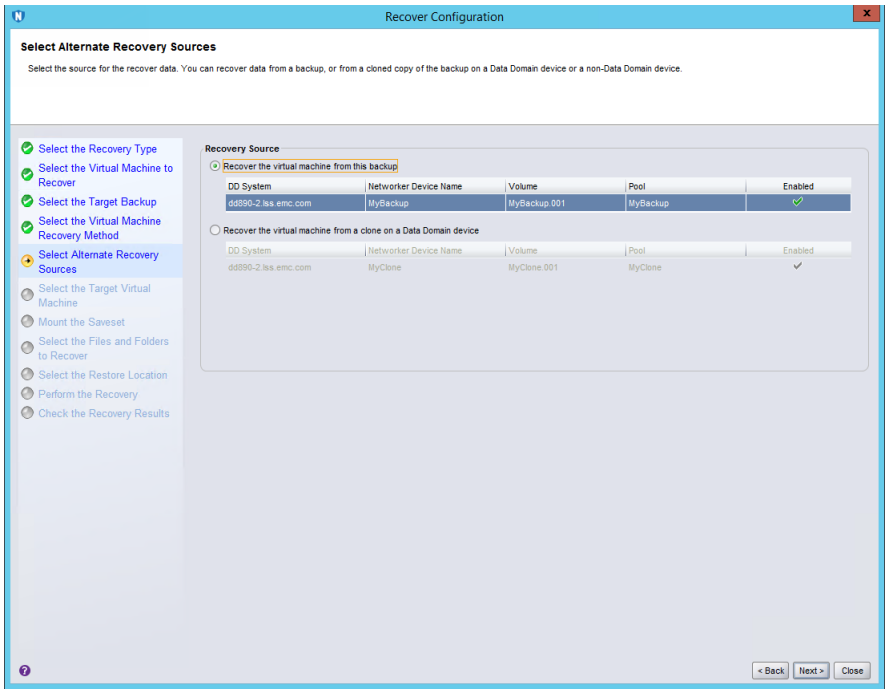
To complete the Recovery wizard with the file level recovery method, perform the following:

Procedure

1. In the **Select the Virtual Machine Recovery Method** page:
   a. Select **File Level recovery**.
   b. Click **Next**.
2. In the **Select Alternate Recovery Sources** page:
   a. Select the primary backup to recover from, or select the **Recover the Virtual machine from a clone on a Data Domain device** option.
   b. Select the clone copy that you want to recover files from.
   c. Click **Next**.

   Note: If selecting a clone from **Select Alternate Recovery Sources**, additionally review the section "Selecting alternate recovery sources".

Figure 46 Select Alternate Recovery Sources for file level recovery



3. In the **Select the target Virtual Machine** page:

   a. Select the virtual machine that you want to recover the files to.

      By default, the virtual machine that you selected for recovery in the **Select the Virtual Machine to Recover** page is displayed.

   b. To recover to another virtual machine in the vCenter, or recover to a virtual machine on a secondary vCenter, select **Browse the vCenter server to select a Virtual Machine to recover to**, and choose a vCenter from the drop-down to browse that vCenter's tree and select a different virtual machine.

   c. Click **Next**.

   Note: Cross-platform recovery, for example from a Windows to a Linux virtual machine, is not supported.

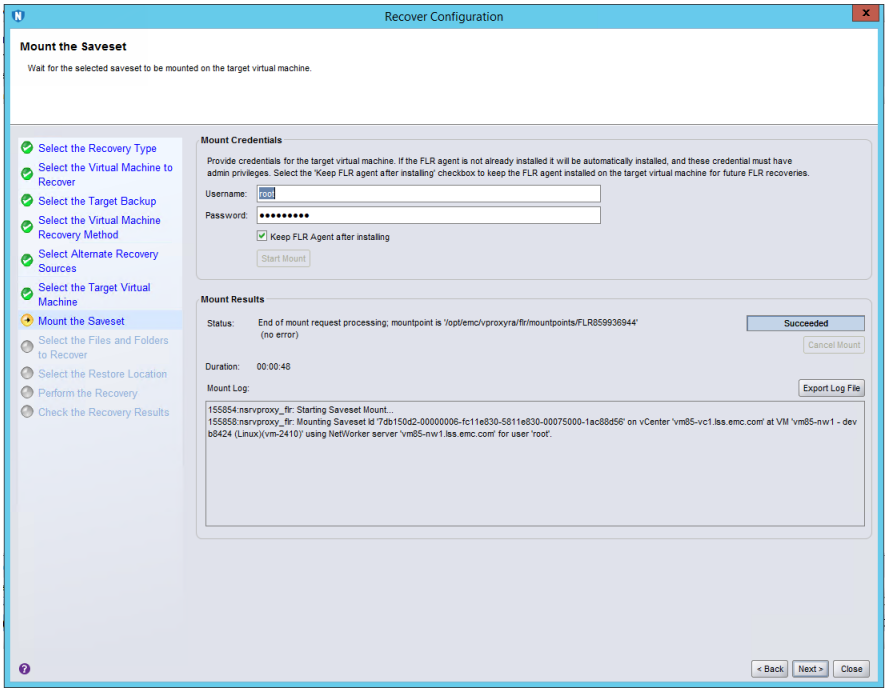
4. In the **Mount The Saveset** page:

   a. Provide the username and password of the virtual machine where the files will be restored to.

   b. Click **Start Mount**.

   c. If performing file level recovery as a domain user, provide the AD user details—no operating system or local account is required if you have configured the AD/domain user.

Figure 47 Mount the save set for file level recovery

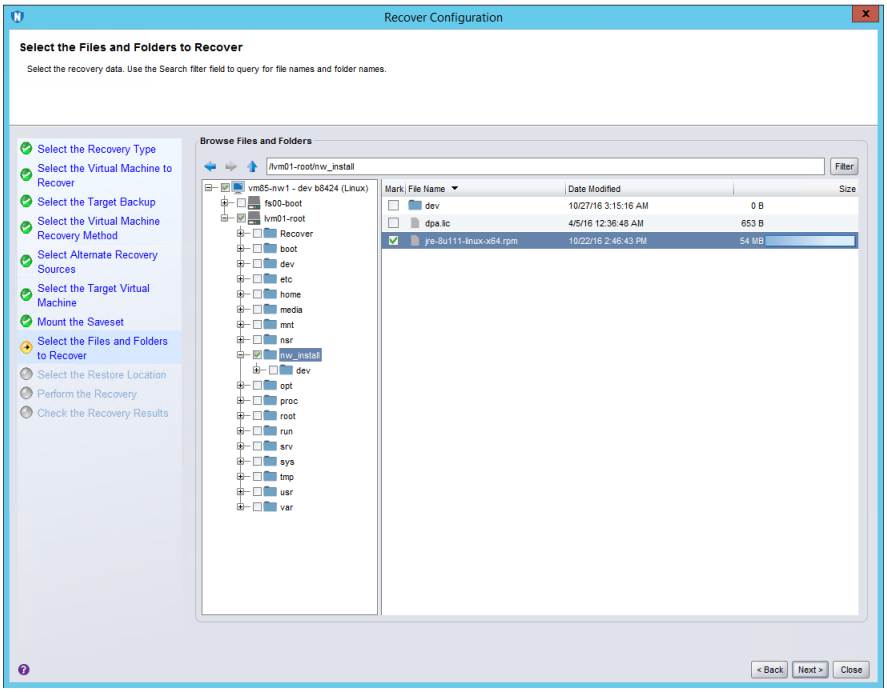


When the **Mount Results** pane shows that the mount has succeeded, click **Next**.

Note: This user should have privileges to install the **FLR Agent**, which is required to perform file level recovery. For Linux virtual machines, this requires the root user account or an equivalent sudo local user account, as described in the section "FLR Agent installation on Linux platforms" of the *NetWorker VMware Integration Guide*.

5. In the **Select the Files and Folders to Recover** page:
   a. Browse through the folder structure to select the files you want to recover.
   b. Click **Next**.

Figure 48 Select the files and folders to recover



6. In the **Select the Restore Location** page:
   a. Select the folder that you want to recover the files to, or create a folder.
   b. Click **Next**.

   Note: NetWorker does not currently support creating folders with spaces in the folder name.

7. In the **Perform the Recovery** page:
   a. Specify a name for the recovery.
   b. To ensure all the details are correct, check the summary at the bottom of the page
   c. Click **Run Recovery**.

Results

The **Check the Recovery Results** page displays the duration of the recovery, and a log file entry when the file level recovery is complete.

Selecting alternate recovery sources in the NMC Recovery wizard

The NMC Recovery wizard contains a step for each virtual machine recovery method where you can select an alternate source to recover from, for example, a clone copy on a Data Domain or non-Data Domain device. If the primary source is present, it is recommended that you recover from the primary source. However, if both the primary source and clone copies are present and enabled and you want to recover from a clone copy, perform the following.

Procedure

1. In the **Select Alternative Recovery Sources** page, select the clone you want to recover from, either a clone on a Data Domain device or non-Data Domain device.

Additionally, make note of the name indicated in the **Volume** column for all of the volumes you do not want to recover from, as you will require this information in steps 5 and 6.

2. Click **Close** to display the **Save Progress** dialog, and then specify a name for the recover and click **Save** to save your progress.
3. In the NMC **Administration** window, click **Devices** to display the **Devices** window.
4. In the left navigation pane, select **Devices**. The list of devices displays in the right pane.
5. For each volume you do not want to recover from that you made note of in step 1, locate the corresponding device, and make note of that device name.
6. For each device you identify as corresponding with those volumes, right-click the device and select **Unmount** from the drop-down, and then also select **Disable** from the drop-down.

   Note: Ensure that no backups are currently running to these devices prior to unmounting.

7. In the NMC **Administration** window, click **Recover** to display the **Recover** window, and locate the saved recovery
8. Right-click the saved recovery and select Open Recover.

   The Recovery wizard re-opens on the **Select Alternative Recovery Sources** page.
9. In the **Recovery Source** pane of the **Select Alternative Recovery Sources** page, select either **Recover the virtual machine from a clone on a Data Domain device**, or **Recover the virtual machine from a clone on a non-Data Domain device**. Click **Next**.

   Note: If you want to recover from a clone on a non-Data Domain device, manually change the staging pool to a different pool, and ensure that your selected pool does not already contain copies for this backup. If the primary source is present and you select a clone to recover from using the same staging pool that contains the existing copy, the recovery may become unresponsive.

10. In the **Perform the Recovery** page, specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct. Click **Run Recovery**.

    The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the recovery is complete.
11. In the NMC **Administration** window, click **Devices** to return to the **Devices** window, and in the left navigation pane, select **Devices** to display the list of devices in the right pane.
12. For each device that you unmounted and disabled in step 6, right-click the device and select **Enable** from the drop-down, and then select **Mount** from the drop-down.

Monitoring and verifying Virtual Machine recoveries

After selecting Run Recovery to complete the Recovery wizard, there are multiple ways you can monitor the progress of the virtual machine recovery, and then verify when the recovery is complete.

NMC Recover and Monitoring windows

To monitor the progress of the virtual machine recovery, use the **Recover sessions** pane in the **Monitoring** window, or the **Currently Running** pane of the **Recover** window.

To verify that the virtual machine recovery is complete, use the **Configured Recovers** pane in the **Recover** window.

Check the Recovery results in the NMC Recovery wizard

The final step of the **Recovery** wizard also allows you to check the recovery results. Upon completion of the virtual machine recovery, an entry for the log file appears in the **Recovery log** pane. Click **Export log** to save and view the log file.

Recovery configuration information storage

When you create a recover configuration by using the Recovery wizard, NetWorker saves the configuration information in an NSR recover resource in the resource database of the NetWorker server. NetWorker uses the information in the NSR recover resource to perform the recover job operation.

When a recover job operation starts, NetWorker stores:

- Details about the job in the nsrjobsd database.
- Output sent to stderr and stdout in a recover log file. NetWorker creates one log file for each recover job.

  NOTICE NetWorker removes the recover log file and the job information from the job database based on value of the *Jobsdb retention in hours* attribute in the properties of the NetWorker server resource. The default jobsdb retention is 72 hours.

vProxy recovery in the NetWorker Management Web UI

The NetWorker Management Web UI contains the same vProxy recovery functionality that is available in the **NetWorker Management Console** through the **Recovery** wizard, including support for all image-level recovery types and file-level recovery. Additionally, if you have legacy VMware Backup appliance backups from a previous NetWorker release, you can use vProxy to recover these backups within the NetWorker Management Web UI.

When logged in to the NetWorker Management Web UI, the landing page displays options for **Monitoring**, **Protection**, and **Recover** in the left pane. If not already selected, select **Recover**, and then select **VMware Recovery**.

In the **VMware Recovery** window's **Select vCenter** drop-down, choose the vCenter server that contains the virtual machines or objects that you want to recover. A list of virtual machines displays. When you select a virtual machine, the backup details display in a table within the **Backups and Clones** pane. You can choose to display hidden columns, such as the virtual machine UUID and type of backups, by clicking the blue filter icon in the lower left corner of the table. The backup type can be VBA, vProxy, or both.

From the **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down to choose from one of the image-level recovery types available, or file level recovery. Additionally, ensure that you specify the correct time range of the backup(s) that you want to recover.

Revert (or rollback) a virtual machine backup

Select **Revert** to rollback one or more virtual machine disks (VMDKs) as a virtual machine to the original virtual machine. Additionally, you can rollback the virtual machine configuration.

About this task

Note: You cannot use the **Revert** recovery type when the ESXi has been removed from the vCenter and then added back to the vCenter. In this case, use the **Virtual Machine recovery** method instead.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **Revert**.

   The **Recover** wizard launches.
3. In the **Configuration** page:
   a. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.
   b. Select **Power On** to power on the virtual machine after the recovery completes.

      Note: If the virtual machine is currently powered on, a dialog displays requesting confirmation to power off the virtual machine. Additionally, if a change has occurred in the virtual machine configuration since the backup, a warning message will display on the **Summary** page.

   c. Select **Revert VM configuration** to restore the virtual machine with the same configuration details used at the time of backup. Additionally, select the **Delete existing disk on config mismatch** option if you want to continue with the removal of the existing disk if the configuration details do not match. If you do not select **Revert VM configuration**, the recovery will revert only the virtual machine data without changing the virtual machine configuration.
   d. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.
   e. Click **Next**.

   The **Disk Selection** page displays
4. In the **Disk Selection** page, choose one or more of the available hard disks, and then click **Next**.

   Note: The entire VMDK will be rolled back unless you have CBT enabled, in which case only the changed blocks will be moved.

   The **Summary** page displays.

5. In the **Summary** page, review the recovery details and then click **Finish**.

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Recover to a new virtual machine

Select **New Virtual Machine** to recover a virtual machine backed up with the vProxy appliance to a new virtual machine.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **New Virtual Machine**.

   The **Recover** wizard launches.
3. In the **Configuration** page:
   a. From the **Destination vCenter** drop-down, select a different destination vCenter server if required, or leave the default selection of the same vCenter server.
   b. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.
   c. In the **Virtual Machine Name** field, specify the name of the new virtual machine.
   d. Select **Power On** to power on the virtual machine after the recovery completes.
   e. Select **Reconnect NIC** to reconnect the network interface card after the recovery completes.
   f. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.
   g. Click **Next**.

   The **Destination Location** page displays.
4. In the **Destination Location** page, select the location where you want to recover the virtual machine. If the target location contains a specific folder that you need to select, select the desired folder from the **VM Folder** drop-down. Click **Next**.

   The **Disk Selection** page displays.
5. In the **Disk Selection** page:
   a. Use the **VM Configuration Files** drop-down to select the datastore where the virtual machine configuration files will reside.
   b. Select **Use same datastore for all disks** to use the same datastore that you selected for the configuration files. This option is enabled by default. Clear this option to select one or more of the available hard disks, and select a **Destination Datastore** for each selected disk. The default **Destination Datastore** selected is the original datastore, however, you can select a different datastore for each disk you want to recover.

6. Click **Next**.

   The **Summary** page displays.

7. In the **Summary** page, review the recovery details and then click **Finish**.

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Instant Restore of a virtual machine

When you select **Instant Restore**, the virtual machine backup is read directly from the Data Domain device and the VMDKs will be restored directly on a Data Domain device. You can perform one instant recovery session at a time.

Before you begin

Before you begin, make note of the following:

- For the Data Domain resource, ensure that you provide the management credentials and, if required, enter the export path appropriately.
- Ensure that the free space on the Data Domain system is equal to or greater than the total disk size of the virtual machine being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target virtual machine fails.
- Ensure that you have at least one proxy that is not restricted to a specific datastore. For the vProxy, select **Properties** and then select **Configuration**, and verify that datastores is left blank.
- Do not perform an instant recovery of virtual machines in resource pools and other similar containers that are part of a currently running protection group.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **Instant Restore**.

   The **Recover** wizard launches.

3. In the **Configuration** page:
   a. From the **Destination vCenter** drop-down, select a different destination vCenter server if required, or leave the default selection of the same vCenter server.
   b. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.
   c. In the **Virtual Machine Name** field, specify the name of the new virtual machine.
   d. Select **Power On** to power on the virtual machine after the recovery completes.
   e. Select **Reconnect NIC** to reconnect the network interface card after the recovery completes.
   f. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

g. Click **Next**.

The **Destination Location** page displays.

4. In the **Destination Location** page, select the location in the vCenter server where you want to recover the virtual machine, and then click **Next**.

   The **Summary** page displays.

5. In the **Summary** page, review the recovery details and then click **Finish**.

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.
Note that the status might not update to "Completed" or "Succeeded" upon a successful instant recovery. If this occurs, cancel the corresponding NetWorker restore task in the **vSphere Client** and the status will update correctly in the NetWorker Management Web UI.

Note: To optimize use of NetWorker and Data Domain resources, it is strongly recommended that you stop the instant recovery session once you satisfy your recovery objectives.

Virtual Disk (VMDK) recovery

Select **Virtual Disk** to recover the disks from the virtual machine backup to an existing virtual machine.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **Virtual Disk**.

   The **Recover** wizard launches.

3. In the **Configuration** page:

   a. From the **Destination vCenter** drop-down, select a different destination vCenter server if required, or leave the default selection of the same vCenter server.

   b. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.

   c. Select **Power On** to power on the virtual machine after the recovery completes.

   d. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

   e. Click **Next**.

   The **Virtual Machine Selection** page displays.

4. In the **Virtual Machine Selection** page, select the location of the virtual machine in the vCenter server where you want to recover the virtual disk(s), and then click **Next**.

   Note: This location can be the original virtual machine, or another existing virtual machine.

The **Disk Selection** page displays.

5. In the **Disk Selection** page, choose one or more of the available hard disks, and select a **Destination Datastore** for each selected disk. The default **Destination Datastore** selected is the original datastore, however, you can select a different datastore for each disk you want to recover. Click **Next**.

   The **Summary** page displays.

6. In the **Summary** page, review the recovery details and then click **Finish**.

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Note: When you start a Virtual Disk recovery, the virtual machine will be powered off automatically without issuing a warning message.

Emergency Recovery

Select **Emergency** when you need to restore the virtual machine to an ESXi host.

Before you begin

Emergency recovery requires a vProxy set up on the ESXi host prior to running the recovery.

Additionally, ensure that you disconnect the ESXi host from the vCenter server.

About this task

Note: During an Emergency Recovery, the vProxy gets associated with the ESXi host and is unavailable for other operations on the vCenter server. Wait until the recovery completes before initiating any other operations on the vProxy.

To complete the Recovery wizard with the Emergency Recovery method, perform the following:

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **Emergency**.

   The **Recover** wizard launches.

3. In the **Configuration** page:
   a. From the **ESX Server** drop-down, select the IP of the ESX server in the vCenter environment where you want to restore the virtual machine backup.
   b. Specify the root **Username** and **Password** for the ESX Server.
   c. In the **Virtual Machine Name** field, specify the name of the new virtual machine.
   d. Select **Power On** to power on the virtual machine after the recovery completes.

      Note: If the virtual machine is currently powered on, a dialog displays requesting confirmation to power off the virtual machine. Additionally, if a change has occurred in the virtual machine configuration since the backup, a warning message displays.

e. Select **Reconnect NIC** to reconnect the network interface card after the recovery completes.

f. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

g. Click **Next**.

The **VMware Proxy Configuration** page displays.

4. In the **VMware Proxy Configuration** page:

a. For **Proxy Selection Type**, if the desired proxy has been discovered, select an existing vProxy for the recovery. Alternatively, you can use a new vProxy that is deployed in the vCenter but not yet added in NetWorker by selecting **Register a new VMware Proxy**.

b. From the **Select Proxy** drop-down, select one of the registered vProxies.

c. Click **Next**.

The **Disk Selection** page displays.

5. In the **Disk Selection** page:

a. Use the **VM Configuration Files** drop-down to select the datastore where the virtual machine configuration files will reside.

b. Select **Use same datastore for all disks** to use the same datastore that you selected for the configuration files. This option is enabled by default. Clear this option to select one or more of the available hard disks, and select a **Destination Datastore** for each selected disk. The default **Destination Datastore** selected is the original datastore, however, you can select a different datastore for each disk you want to recover.

6. Click **Next**.

The **Summary** page displays.

7. In the **Summary** page, review the recovery details and then click **Finish**.

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Note: The progress bar may not update correctly when you perform an Emergency Recovery directly to the ESXi host.

File Level recovery

Select **File Level** to recover individual files from backups of virtual machines or VMDKs to a primary or secondary vCenter server.

Before you begin

NetWorker only supports file level recovery operations from a primary or cloned backup if the save set is on a Data Domain device. If a cloned backup does not exist on the Data Domain device, you must manually clone this save set to Data Domain before launching the **Recovery** wizard.

For the Data Domain resource, ensure that you provide the management credentials and, if required, type the export path appropriately. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only) provides detailed steps.

Additionally, if recovering to a virtual machine on a secondary vCenter, ensure that a vProxy appliance has been deployed on the secondary vCenter server and configured with the NetWorker server.

About this task

Note: File level recovery in the NetWorker Management Web UI can only be performed by an administrator. Note, however, that a user who is a member of the Administrators group can perform the recovery when the **Run with Elevated Privileges** option is enabled in the **Mount Configuration** page of the **Recover** wizard.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. Select **File Level**.

   The **Recover** wizard launches.
3. In the **Configuration** page:
   a. From the **Destination vCenter** drop-down, select a different destination vCenter server if required, or leave the default selection of the same vCenter server.
   b. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.
   c. Select **Overwrite** to overwrite files in the destination location that have the same name as files being recovered.
   d. Select **Terminate mount session** to release the disk mount after the recovery completes.
   e. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.
   f. Click **Next**.

   The **Destination Virtual Machine** page displays.
4. In the **Destination Virtual Machine** page, the location of the original virtual machine backup displays by default in blue. If you do not want to recover to the original location, navigate to the desired virtual machine in the vCenter server where you want to recover the objects, and click **Next**.

   The **Mount Configuration** page displays.
5. In the **Mount Configuration** page:
   a. Type the user credentials to access the virtual machine that you want to recover objects to in order to initiate the disk mount. This user should have privileges to install the **FLR Agent**, which is required to perform file level recovery. For Linux virtual machines, this requires the root user account or an equivalent sudo local user account, as described in the section "FLR Agent installation on Linux platforms" of FLR Agent requirements.
   b. Optionally, select **Keep FLR agent after installation** if you do not want to remove the **FLR Agent** from the virtual machine upon recovery completion.
   c. Select **Run with Elevated Privileges** to allow a user who is a member of the Administrators group to perform the recovery.

> **Note:** This feature is not supported for vProxy versions earlier than NetWorker 18.2, even though the option is not greyed out.

d. Click **Mount**.

The disk mount initializes and a progress bar displays.

> **Note:** You cannot browse the contents of the virtual machine backup until the mounting of the destination virtual machine completes successfully.

6. When the mount completes successfully, click **Next**.

   The **Source Data** page displays.

7. In the **Source Data** page, select individual folders to browse the contents of the backup, and select the objects you want to recover. You can select all objects in a folder by clicking the checkbox to the left of the **Name** field in the **Contents** pane.

   When any objects in a folder are selected, that folder is highlighted in blue in the **Folders** pane. After selecting the objects that you want to recover, click **Next**.

   The **Destination Location** page displays.

8. In the **Destination Location** page, browse the folder structure of the destination virtual machine to select the folder where you want to recover the objects. Click **Next**.

   The **Summary** page displays.

9. In the **Summary** page, review the recovery details and then click **Finish**.

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Monitor recovery operations in the NetWorker Management Web UI

After initiating a recovery operation in the NetWorker Management Web UI, select **Monitoring** in the left pane to view the status and progress of the recovery in the right pane.

In addition to the progress and completion status of individual recovery operations, a column displays the recovery type. You can choose to display hidden columns by clicking the blue icon in the lower left corner of the table.

If you need to troubleshoot recovery operations, you can view the vProxy logs by clicking the menu in the first column and selecting **View Messages** from the drop-down.

To stop a recover operation that is in progress, click the menu in the first column and select **STOP** from the drop-down. When prompted to confirm, click **STOP**. This option is available only for VMware image level recovery and file-level restore.

vProxy restore from legacy VMware Backup appliance backups

If you have VMware Backup appliance (VBA) backups from previous Networker releases, you can recover those backups from the **NetWorker Management Web UI**

by using the vProxy. Running VBA backups in NetWorker 18.2 and later is not supported.

About this task

Note:

- You can only perform image-level recoveries of legacy VBA backups (the **Revert** or **New Virtual Machine** recovery types). Other types or recovery are not supported using the **NetWorker Management Web UI**. You can, however, use the **EMC Backup and Recovery** plug-in within the **vSphere Web Client** for other types of VBA recovery, provided that you still have an active VBA instance.
- For the recovery of VBA backups, the staging pool must be a clone pool of type Data Domain.

Procedure

1. In the **NetWorker Management Web UI**, go to **Recover** > **VMware Recovery**

   The **VMware Recovery** window appears
2. From the **Select vCenter** drop-down, select a vCenter server.

   A list of virtual machines in the vCenter displays.
3. Select the desired virtual machine, and then select one of the duration options from the **Showing results for** drop-down in the **Backups and Clones** pane.

   A list of primary and clone backups of the virtual machine performed within that duration appear in a table within the **Backups and Clones** pane. The table contains a column that allows you to identify which backups are legacy VBA backups.
4. Click the filter icon in the lower left corner of the **Backups and Clones** pane, and select **VBA Backups** and click **OK**.

   A column appears in the table that allows you to identify which backups are legacy VBA backups.
5. Select one of the available primary or cloned backups that indicates VBA, and then click the **Recovery** drop-down.
6. From the drop-down, select **Image Level**, and then select the **Revert** or **New Virtual Machine** recovery type. Note that these are the only supported types for recoveries of VBA backups.

   The **Recover** wizard launches.
7. Complete the **Recover** wizard according to the type you selected.

   Note: When you select the staging pool for recovery, ensure that at least one volume does not contain a copy of the selected save set. Alternatively, if a save set is already recovered, then you can select the recovered save set for further recoveries of the same virtual machine.

Results

When the recovery is initiated, the Networker performs resurrection on a staging pool to convert the VBA backups to a vProxy-readable format, and then restores the virtual machine. Note that the staging pool should reside on a Data Domain system.

vProxy file-level restore and SQL restore in the Dell EMC Data Protection Restore Client

You can also use the **Dell EMC Data Protection Restore Client** to perform granular recovery from a primary or cloned vProxy backup on a Data Domain device. The **Dell EMC Data Protection Restore Client** allows you to restore specific files and folders from virtual machines in **User** and **Admin** modes, and also restore individual SQL databases from SQL server application-aware backups. The **Dell EMC Data Protection Restore Client** is part of the NetWorker client installation.

Note: Before you start a file-level restore, review the prerequisites in the section File-level restore prerequisites, as well as File-level restore and SQL restore limitations to ensure that you can perform file-level restores in your configuration.

Pre-requisites for file-level restore and SQL restore

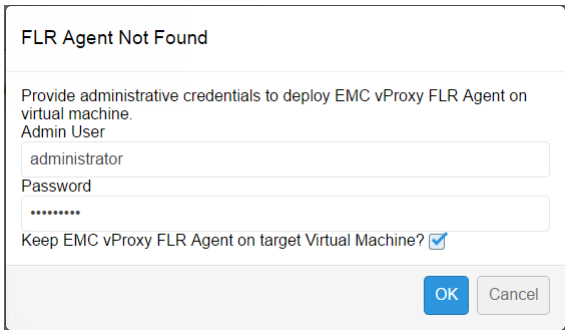
Review the following information before performing a file-level restore or SQL restore in the **Dell EMC Data Protection Restore Client**.

FLR Agent requirements

The **FLR Agent** is required for file-level restore operations, and gets installed automatically on the target virtual machine when you initiate a file-level restore and provide the virtual machine credentials.

If the request to install the FLR Agent was not successful and you initiate a file-level restore, the following message appears.

Figure 49 Deploy FLR Agent if not found



This message provides an option to deploy the FLR Agent by providing the appropriate credentials. Review the user requirements in the following sections for Linux and Windows platforms to determine which users are supported.

FLR Agent installation on Linux platforms

The **FLR Agent** installation on Linux virtual machines requires that you use the root account, or be a user in the operating system's local sudousers list. If credentials for any other user are provided for the target virtual machine, the **FLR Agent** installation fails, even if this user has privileges similar to a root user.

To allow a non-root user/group to perform the **FLR Agent** installation, provide sudo access to the following files at a minimum:

- rpm command (SLES, RHEL, CentOS) and dpkg command (Debian/Ubuntu)

- /opt/emc/vproxyra/bin/postinstall.sh
- /opt/emc/vproxyra/bin/preremove.sh

Note the following additional requirements:

- Using the local sudouser for the **FLR Agent** installation requires NetWorker 18.2 and later and vProxy 3.0.1-1 or later. Any earlier versions will require you to use the root account for the **FLR Agent** installation
- The sudo user/group must be configured for no password prompt
- The sudo user/group must be provided with the no `requiretty` option.
- To browse files for a file-level restore when you have user elevation enabled, you must have appropriate authority in the guest virtual machine operating system, for example, being allowed to run `vflrbrowse` via sudo without prompting for a password.
- To perform a file-level restore when you have user elevation enabled, you must have appropriate authority, for example, being allowed to run `vflrcopy` via sudo without prompting for a password.

Once you complete the **FLR Agent** installation on the target virtual machine using the root user account or a sudouser with the minimum file access requirements, you can perform file-level restore operations as a non-root user on supported Linux platforms. File-level restore on Linux is only supported on Red Hat Enterprise Linux versions 6 and 7, and SuSE Linux Enterprise Server versions 11 and 12.

FLR Agent installation on Windows

FLR Agent installation on Windows virtual machines requires that you use administrative privileges. If the provided credentials for the target virtual machine do not have administrative privileges, the**FLR Agent** installation fails. Once you complete the **FLR Agent** installation on the target virtual machine using administrative privileges, you can perform file-level restore using a non-administrator user.

FLR Agent installation on Windows for UAC-enabled Windows virtual machines

FLR Agent installation on a User Account Control (UAC) enabled Windows virtual machine requires you to perform one of the following:

- Provide the credentials of the administrator user.
- Disable UAC during the **FLR Agent** installation, and then re-enable on completion.

On Windows versions 7, 8, and 10, the administrator account is disabled by default. To enable the account, complete the following steps:

1. To activate the account, open a command prompt in administrative mode, and then type `net user administrator /active: yes`.
2. To set a password for the administrator account, go to **Control Panel** > **User Accounts** and select the **Advanced** tab. Initially, the account password is blank.
3. In the **User Accounts** pane, right-click the user and select **Properties**, and then clear the **Account is disabled** option.

To disable UAC during the **FLR Agent** installation and then re-enable on completion of the installation, complete the following steps:

1. Log in to the **Dell EMC Data Protection Restore Client** as an administrator user to initiate a request to launch the **FLR Agent installation** window.
2. In the **FLR Agent installation** window, select the **Keep vProxy FLR on target virtual machine** option.

3. Open **regedit** and change the EnableLUA registry key value at `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` to **`0x00000000`**. By default, this is set to 1.
4. Proceed with the FLR Agent installation.
5. Open **regedit** and reset the EnableLUA registry key to the previous value to re-enable UAC.

File-level restore and SQL database/instance level restore only supported from primary or clone backup on a Data Domain device

NetWorker only supports file-level restore and SQL database/instance level restore operations from a primary or cloned backup when the save set is on a Data Domain device.

If a cloned backup does not exist on the Data Domain device, you must manually clone a save set from the tape device to Data Domain before launching the **Dell EMC Data Protection Restore Client**.

If backups reside on a non-Data Domain Device such as Cloud Boost, tape, Cloud Tier, or AFTD, the backups do not display in the **Dell EMC Data Protection Restore Client**. In this case, use NMC to identify and clone the save sets back to the Data Domain device.

Supported browser versions

Use of the **Dell EMC Data Protection Restore Client** may require upgrading your browser to the latest version.

For example, the **Dell EMC Data Protection Restore Client** does not work on Mozilla FireFox unless you install a minimum version of 43.0.3.

If you notice an error when logging in to the **Dell EMC Data Protection Restore Client** or are unable to login, ensure your browser is up-to-date and then retry the login.

Support for Debian or Ubuntu operating system

vProxy file-level restore is supported on the Debian/Ubuntu operating system. To configure the Debian or Ubuntu guest operating system for file-level restore, perform the following steps.

About this task

Note: File-level restore is not supported on Debian/Ubuntu ext4 file systems.

Procedure

1. Log in to the system console as a non-root user.
2. Run the `sudo passwd root` command.

   Enter the new password twice to set a password for the root account.
3. Run the `sudo passwd -u root` command to unlock the root account.
4. Specify the root user credentials in the **Dell EMC Data Protection Restore Client** and proceed to complete the file-level restore operation at least once.

   While performing the file-level restore operation for the first time, remember to select **`Keep FLR agent`**.
5. After performing the above steps at least once, you can revert the root account to the locked state and use non-root account for future file-level restore

requests. Non-root user can lock the root account with the `sudo passwd -l root` command.

NetWorker privileges required by File-level restore and SQL database/instance level restore users

A new user group, **VMware FLR Users**, requires NetWorker privileges for User and Admin logins to perform file-level restore and SQL database/instance level restore operations in the **Dell EMC Data Protection Restore Client**.

Specify the following privileges for the VMware FLR Users group by using the NMC **NetWorker Administration** window or `nsradmin`.

Table 14 FLR privilege requirements

User	Admin
Remote Access All Clients	Remote Access All Clients
Operate NetWorker	Operate NetWorker
Monitor NetWorker	Monitor NetWorker
Operate Devices and Jukeboxes	Operate Devices and Jukeboxes
Recover Local Data	Recover Local Data
Backup Local Data	Backup Local Data
	View Security Settings

Operating system utilities required for file-level restore

On Linux and Windows, the installed operating system must include several standard utilities in order to use file-level restore. Depending on the target operating system for restore and the types of disks or file systems in use, some of these standard utilities, however, may not be included.

The following utilities and programs may be required for performing file-level restore.

On Windows:

- msiexec.exe
- diskpart.exe
- cmd.exe

On Linux:

- blkid
- udevadm
- readlink
- rpm
- bash

Note: On Linux LVM, LVM2 rpm version 2.02.117 or later is required. Also, additional binaries required on Linux LVM include dmsetup, lvm, and vgimportclone.

Create a user in the NetWorker authentication service (User mode file-level restore only)

When performing file-level restore in User Mode, you must create a user in the Networker Management Console (NMC) using the **Manage Authentication Service**

Users option, and make note of the password as you will require this information when logging in to the **Dell EMC Data Protection Restore Client**.

Before you begin

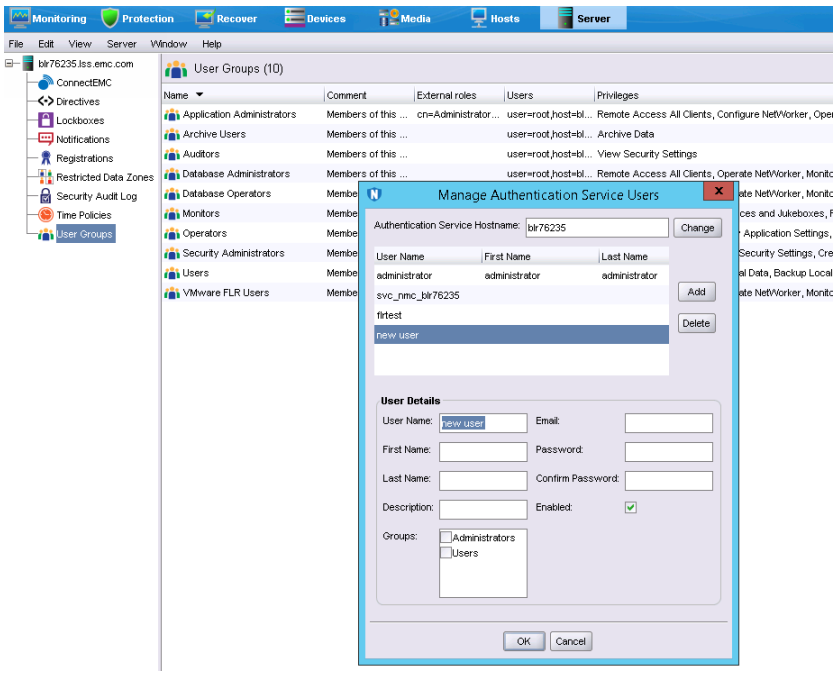
For file-level restores on Linux virtual machines, the root account or an equivalent sudo local user account credentials is required for the target virtual machine in order to install the **FLR Agent**. The section "FLR Agent installation on Linux platforms" of FLR Agent requirements provides more details.

For file-level restores on Windows virtual machines, if the provided credentials for the target virtual machine do not have administrative privileges, the**FLR Agent** installation fails. To perform a file-level restore using a non-administrator user, ensure that the **FLR Agent** is already installed on the target machine using administrative privileges.

Procedure

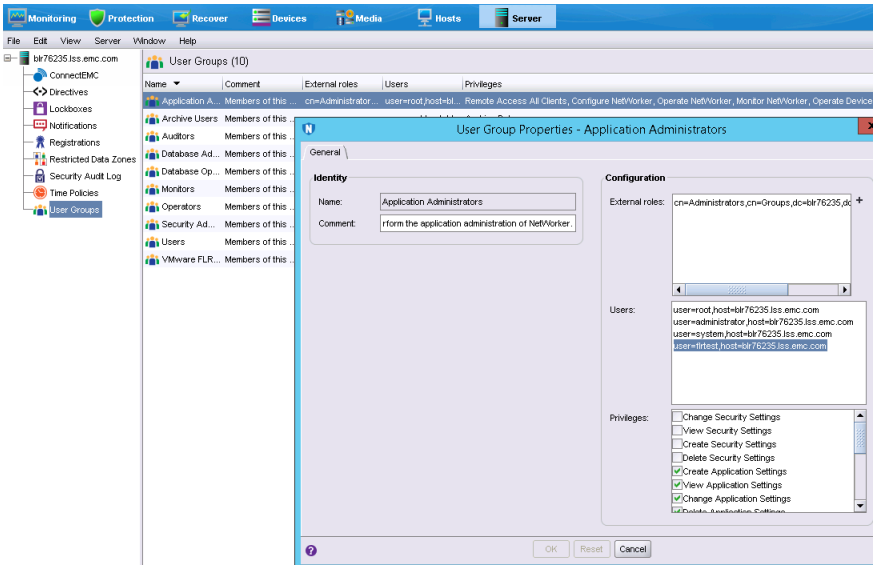
1. In the NMC **NetWorker Administration** window, click **Server** to open the **Server** window.
2. In the left navigation pane, highlight **User Groups**, and then right-click and select **Manage Authentication Service Users**.

   Figure 50 Manage Authentication service users



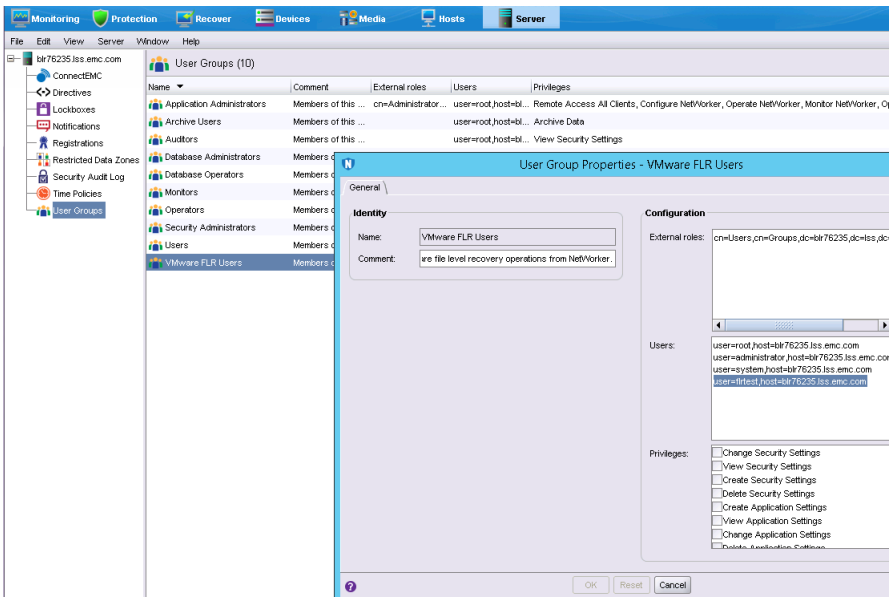
3. In the **Manage Authentication Service Users** dialog box, click **Add**.
4. For the new user **user1**, provide a username, password and other details, and then select the checkbox next to **Users** in the **Group** field and click **OK**.
5. Right-click **Application Administrators** and select **Properties**. In the **User Group Properties**, create an entry for the user created in step 4 (for example, **user1**), in the format `user=user1,host=NW server FQDN`.

Figure 51 Application Administrators user group properties



6. Right click **VMware FLR Users** and select **Properties**. In the **User** field, create an entry for the user created in step 4 (for example, **user1**), in the format `user=user1,host=NW server FQDN`.

Figure 52 VMware FLR Users user group properties



Results

You can now use this new user to log into the **Dell EMC Data Protection Restore Client**.

File-level restore and SQL restore limitations

This section provides a list of limitations that apply to file-level restore and individual SQL database and instance restore.

Compatibility requirements and unsupported configurations

Review the following limitations related to file-level restore compatibility requirements and unsupported configurations.

- File-level restore and SQL instance restore in the **Dell EMC Data Protection Restore Client** is only supported on the platforms and versions identified in the online compatibility guide, available at https://elabnavigator.emc.com/eln/modernHomeDataProtection.
- In order to perform a file-level restore as a domain user in the NMC **NetWorker Administration** window's **Recovery** wizard or the **Dell EMC Data Protection Restore Client**, you need to register a tenant user and provide the FLR Domain user required permissions, as described in the section File-level restore as a domain user.
- Update your web browser to the latest version. It is recommended that you use the Chrome or Mozilla browser for file-level restore operations.
- Install VMware Tools version 10 or later. For best results, ensure that all virtual machines run the latest available version of VMware Tools. Older versions are known to cause failures when you perform browse actions during file-level restore or SQL restore operations. For Linux operating systems, ensure that you install a supported Open VM Tools package, as outlined in the VMware Software Compatibility Guide.
- You can perform file-level restore across vCenters as long as the vCenters are configured in the same NetWorker server, and the source and target virtual machine have the same guest operating system. For example, Linux to Linux, or Windows to Windows.
- File-level restore from a Data Domain Cloud Tier device is not supported. To perform file-level restores of data that resides only on this device, first clone the data to a Data Domain device, and then recover the data from the Data Domain device.
- File-level restore does not support the following virtual disk configurations:
  - LVM thin provisioning
  - Unformatted disks
  - FAT16 file systems
  - FAT32 file systems
  - Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)
  - Two or more virtual disks mapped to single partition
  - Encrypted partitions
  - Compressed partitions

Platform-specific limitations

Review the following limitations specific to Linux and Windows operating systems.

- You can only restore files and/or folders from a Windows backup to a Windows machine, or from a Linux backup to a Linux machine.

- When you enable Admin Approval Mode (AAM) on the operating system for a virtual machine (for example, by setting `Registry/FilterAdministratorToken` to `1`), the administrator user cannot perform a file-level restore to the end user's profile, and an error displays indicating "Unable to browse destination." For any user account control (UAC) interactions, the administrator must wait for the mount operation to complete, and then access the backup folders located at `C:\Program Files (x86)\EMC\vProxy FLR Agent\flr\mountpoints` by logging into the guest virtual machine using Windows Explorer or a command prompt.
- The **FLR Agent** installation on Linux virtual machines requires you to use the root account, or be a local sudouser with the minimum required file access, as described in the section FLR Agent requirements. Note that using the sudouser for the **FLR Agent** installation requires NetWorker 18.2 or later and vProxy 3.0.1-1 or later. Any earlier versions will require you to use the root account for the **FLR Agent** installation. Once the **FLR Agent** installation is completed by a root user, you can perform file-level restore operations as a non-root user.
- Mounting a Linux virtual machine for file-level restore requires a local Linux account with permissions to the file system files.
- When you perform file-level restore on Ubuntu/Debian platforms, you must enable the root account in the operating system. By default, the root account will be in locked state.
- File-level restore is not supported on Ubuntu/Debian ext4 file systems.
- When running the NetWorker server on Windows platforms, file-level restore session logs are not kept.
- For file-level restores on Windows 2012 R2 virtual machines, the volumes listed under the virtual machine display as "unknown." File-restore operations are not impacted by this issue.
- File-level restore of virtual machines with Windows dynamic disks is supported with the following limitations:
  - The restore can only be performed when recovering to a virtual machine different from the original. Also, this virtual machine cannot be a clone of the original.
  - The restore can only be performed by virtual machine administrator users.
  - If Windows virtual machines were created by cloning or deploying the same template, then all of these Windows virtual machines may end up using the same GUID on their dynamic volumes.
- File-level restore of Windows 8, Windows Server 2012 and Windows Server 2016 virtual machines is not supported on the following file systems:
  - Deduplicated NTFS
  - Resilient File System (ReFS)
  - EFI bootloader

Restore operations and performance limitations

Review the following limitations related to file-level restore operations and performance considerations.

- When a file-level restore or SQL restore operation is in progress on a virtual machine, no other backup or recovery operation can be performed on this virtual

machine. Wait until the file-level restore session completes before starting any other operation on the virtual machine.

- When the backup chain for an SQL instance restore contains 30 or more transaction log backups, a message indicating the required permissions to complete this action does not display in the **Dell EMC Data Protection Restore Client**. Check the `flr-server` log for an error message similar to the following to determine what additional privileges are required:
  ```
  ERROR c.e.f.u.ProcessRestores - Failed restore attempt:
  Recover request failed: Permission denied, user does not
  have 'Create Application Settings' or 'Configure NetWorker'
  privilege to create this resource - NSR recover.
  ```
- SQL instance restore fails in the **Dell EMC Data Protection Restore Client** when the backup chain contains more than 75 transaction log backups. In such scenarios, ensure that you perform a SQL database restore for each database in the SQL instance one at a time.
- When you switch between different Data Domain devices for backup and clone operations, the SQL transaction log backup does not get promoted to FULL on the primary backup device. As a result, the transaction log backup fails with the error `Previous backup path must be specified for Transaction Log backup`. Note that this issue does not occur when the same Data Domain device is used for the backup and clone.
  If relabelling of the primary device has occurred, or you added a new Data Domain device, unselect the **Tlog backup** option for the Backup Action, and then run the SQL application-consistent workflow. After the FULL backup and clone completion, re-select the **Tlog backup** option for the Backup Action and run the SQL application-consistent workflow again. Subsequent transaction log backups and clones will complete successfully.
- For file-level restore of high-density file systems (more than few hundred files/folders), it is recommended to use either the **NetWorker Management Web UI** or the **Dell EMC Data Protection Restore Client** (User or Admin mode, as applicable) instead of the **Recovery** wizard in the NMC **NetWorker Administration** window.
- A restore of individual SQL Server databases or instances in the **Dell EMC Data Protection Restore Client** will overwrite the existing database, even if your NetWorker version provides an option where you can unselect **Overwrite the existing DB**.
- A SQL database restore to alternate is only supported for restoring from a lower SQL version to a higher SQL version.
- The **Dell EMC Data Protection Restore Client** incorrectly allows you to select a VMware Backup appliance as a destination client for file-level restore.
- After migrating from the VMware Backup appliance to the vProxy appliance, the **Dell EMC Data Protection Restore Client** may continue to display VMware Backup appliance backups along with the new vProxy backups for virtual machines. Note, however, that you will only be able to perform file-level restore from the new vProxy backups.
- After migrating from the VMware Backup appliance to the vProxy appliance, new vProxy backups of virtual machines that were previously backed up with the VMware Backup appliance will not be visible in the **Dell EMC Data Protection Restore Client** in Admin mode. You must log in using User mode to view and recover from these backups.
- You cannot use clone volumes for file-level restore when the primary backup volume is unmounted or unavailable. The restore will fail looking for backup

volumes. If this occurs, dynamic staging allows you to use the secondary copy by staging the requested virtual machine backups from the clone to an available backup volume and then recovering the virtual machine.

- Browsing a large number of files at once may cause Internet Explorer to become slow or unresponsive. The Chrome and Mozilla browsers issue a warning when encountering a difficulty handling many files, but Internet Explorer does not.
- In a large environment where many virtual machines appear in the **Dell EMC Data Protection Restore Client**, the navigation buttons (**Back**, **Next**, **Finish**) may appear very small, requiring you to zoom in to see the options. It is recommended that you use the latest versions of the Chrome or Firefox browsers to avoid the issue.
- File-level restore supports direct restore from a cloned backup only if the clone copy is on a Data Domain device.
- File-level restore does not restore or browse symbolic links.
- When you create partitions, fill the lower ordered indices first. For example, you cannot create a single partition and place it in the partition index 2, 3, or 4. You must place the single partition in partition index 1.

Using the Dell EMC Data Protection Restore Client for file-level restore and SQL restore

The **Dell EMC Data Protection Restore Client**, which you access through a web browser, allows you to select specific virtual machine backups as file systems, and then browse the file system to locate the directories and files you want to restore. The browser also allows you to restore individual SQL databases and instances.

The login page of the **Dell EMC Data Protection Restore Client** features two tabs—an **FLR** tab for virtual machine file and folder restore, and an **App** tab for SQL database and instance restore.

Additionally, the **Dell EMC Data Protection Restore Client** operates in one of two user modes:

- User—For file-level restore, a user account that can restore folders or files to the original virtual machine, as described in the section Restoring specific folders or files to the original virtual machine in User mode.
  For SQL restore, a user account that can restore individual SQL databases and instances to the original machine from the virtual machine you are logged into. This user can be an Authentication Service user, as described in the section Restore of SQL Server application-consistent backups.
- Admin—For file-level restore, a NetWorker administrator account or Authentication Service user that can restore folders or files from a different virtual machine to any available destination client, as described in the section Restoring specific folders or files from different virtual machines in Admin mode.
  For SQL restore, a NetWorker administrator account or Authentication Service user that can restore individual SQL databases and instances to the original machine from any virtual machine you have access to that contains an SQL Server application-consistent backup, or restore to a different virtual machine, as described in the section Restore of SQL Server application-consistent backups.

Note: When a file-level restore operation is in progress on a virtual machine, no other backup or recovery operation can be performed on this virtual machine. Wait until the file-level restore session completes before starting any other operation on the virtual machine.

Restoring specific folders or files to the original virtual machine in User mode

To restore specific folders and files to the original virtual machine on Windows and Linux virtual machines, select the **User** tab in the **Dell EMC Data Protection Restore Client** login page. In this mode, you connect to the **Dell EMC Data Protection Restore Client** from a virtual machine that has been backed up by the vProxy Appliance.

Before you begin

For the Data Domain resource, ensure that you provide the management credentials and, if required, enter the export path appropriately. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only)provides detailed steps.

Additionally, you must create a user in the NetWorker Authentication Service by using the NetWorker Management Console (NMC), as described in the section Create a user in the NetWorker authentication service (User mode file-level restore only).

Procedure

1. Open a browser from the virtual machine that the restored files will be recovered to, and enter a URL that points to the NetWorker server host and indicates file-level restore. For example:

   `https://NetWorker server:9090/flr`

   Note: For User recoveries, you must connect to the NetWorker server from a web browser on the virtual machine that will receive file-level restore data.

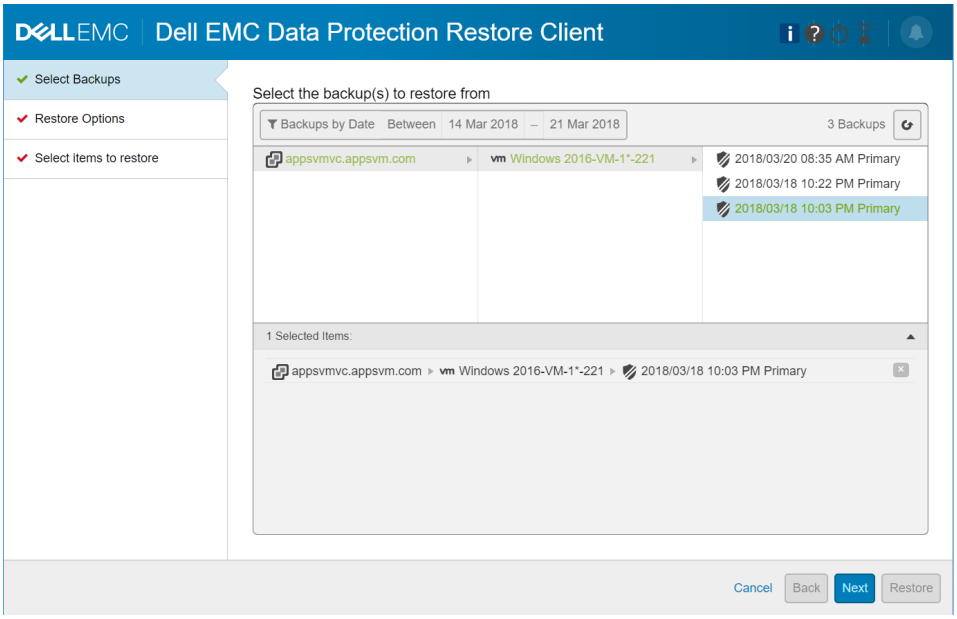
   The **Dell EMC Data Protection Restore Client** login window appears.

2. Select the **User** tab and the **FLR** tab, and then log in to the **Dell EMC Data Protection Restore Client** with the user credentials of the virtual machine to which you are logged in. This user account should also belong to the NetWorker user group "VMware FLR Users" in order to be authorized to perform file-level restore. The section NetWorker privileges required by File-level restore users provides more information.

   When you log in, the **Select Backups** page displays with a list of backups for the local virtual machine.

3. On the **Select Backups** page, use the drop-down list to view the available backups. You can set the backup filter to view backups on a specific day or within a specific date range. Highlight a backup and double-click or drag and drop to move the backup to the **Selected Items** pane. Click **Next**.

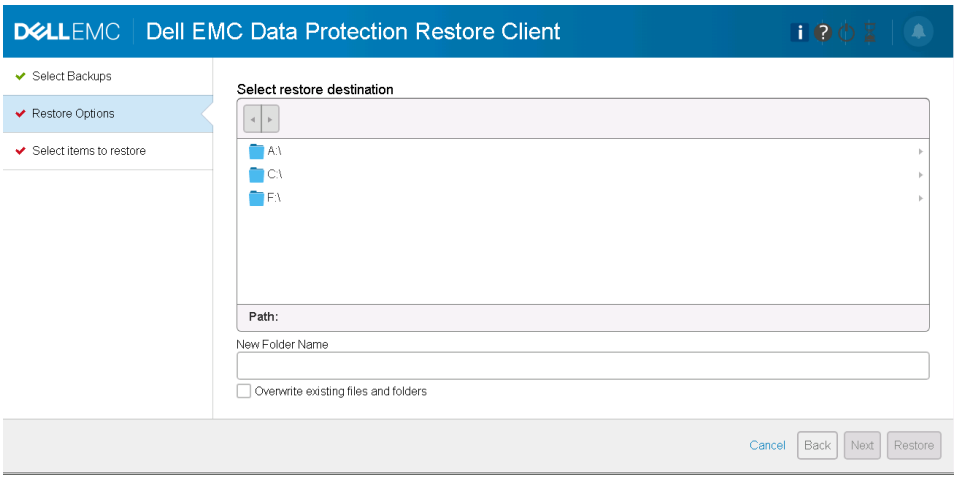
Figure 53 Select backups to restore from



Note: When you click **Next**, if a folder hierarchy does not appear, the **Dell EMC Data Protection Restore Client** may not support the file system in use on the virtual machine. The section File-level restore limitations provides more information.

4. On the **Restore Options** page, navigate to the file system drive where you want to restore the items and select an existing folder, or specify a new folder name in the restore destination, and then click **Next**.

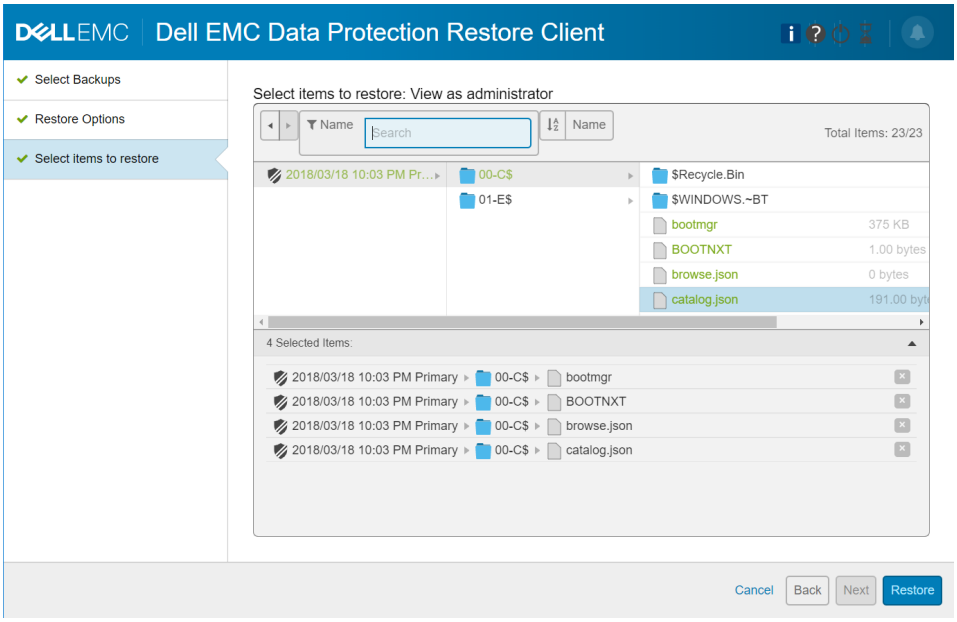
Figure 54 Select restore location



Note: Additionally, you can select the **Overwrite existing files and folders** option if you want to replace the existing files with the recovered files.

5. On the **Select items to restore** page, browse and select the files and folders available for recovery. Note that you can sort items by Name, File size, or Date, and you can also search for a specific file or folder name. To mark an item for recovery, double-click the item, or drag and drop the item into the **Selected Items** pane.

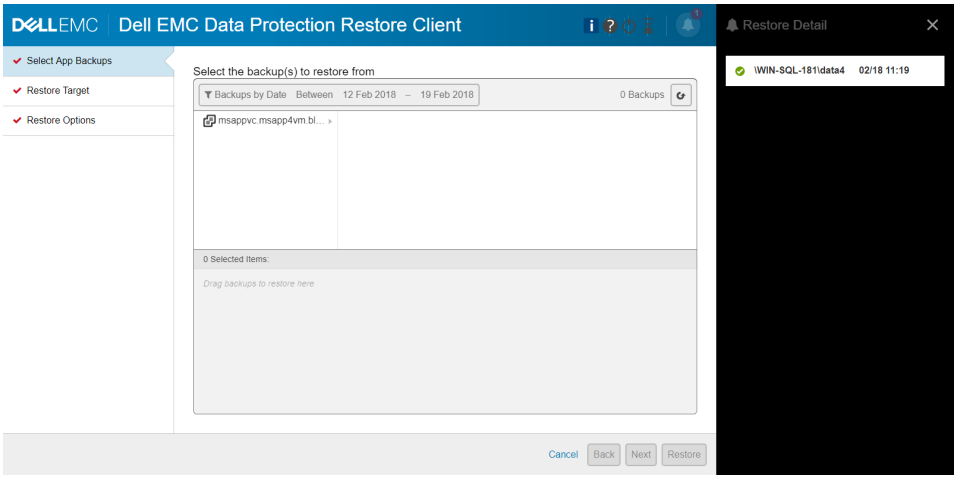
Figure 55 Select items to restore



6. When finished selecting items, click **Finish**.
7. Click **Yes** when you are prompted to continue the restore.
8. To enable the polling feature so that you can monitor the status of the restore, click the hourglass icon located in the upper right-hand corner of the window and set to **ON**. By default, the polling feature is set to **OFF** due to the memory consumption that occurs when the server is queried every few seconds for the restore status.
9. Once the polling feature is enabled, you can monitor the status of the restore by clicking the icon located in the upper right-hand corner of the window.

   When you click the icon, the **Restore Detail** pane slides into view on the right side of the window, displaying the ongoing restore operations. Clicking the entry displays the progress of the restore and a recovery logs download option.

Figure 56 Restore Monitoring



Restoring specific folders or files from different virtual machines in Admin mode

To restore specific folders or files from a different virtual machine, select the **Admin** tab in the **Dell EMC Data Protection Restore Client** login page. Once connected, you can browse, select, and restore files and folders from any virtual machine that you backed up with the vProxy Appliance. You can then restore items to the virtual machine on which you are currently logged in, or to any available destination virtual machine.

Procedure

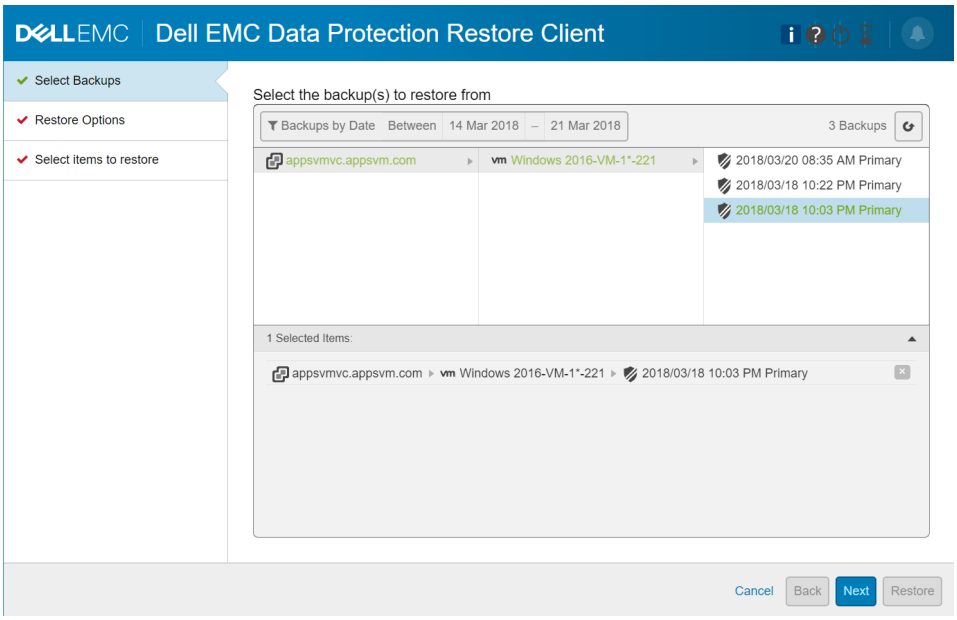
1. Open a browser and specify a URL that points to the NetWorker server and indicates FLR, as in the following example:

   `https://NetWorker server:9090/flr`
   The **Dell EMC Data Protection Restore Client** login window appears.

2. Click the **Admin** tab and the **FLR** tab, and then log in to the **Dell EMC Data Protection Restore Client** with the NetWorker Authentication Service User credentials.

   Note: When using **Admin** mode, ensure that the user you specify for the NetWorker server login has the correct privileges to use this option.

   When you log in, the **Select Backups** page appears with a list of all the virtual machines that were backed up by using the vProxy Appliance. The available backups appear under each virtual machine, as shown in the following.
   Figure 57 Select the backup(s) to restore from



   Note: After migrating from the VMware Backup appliance to the vProxy appliance, new vProxy backups of virtual machines that were previously backed up with the VMware Backup appliance will not be visible in the **Dell EMC Data Protection Restore Client** in Admin mode. You must log in using User mode to view and recover these backups.

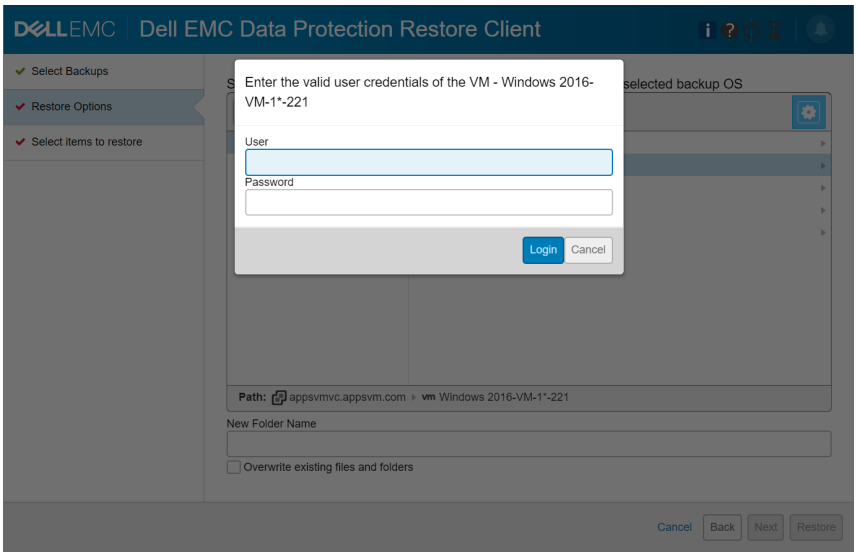
3. On the **Select Backups** page, use the arrows to the right of the entry to view the available backups. You can set the backup filter to view backups on a

specific day or within a specific date range. Highlight a backup and double-click or drag and drop to move the backup to the **Selected Items** pane. Click **Next**.

4. On the **Restore Options** page, select a destination virtual machine.

   A login dialog box similar to the following figure appears for the restore destination.

   Figure 58 Select restore location

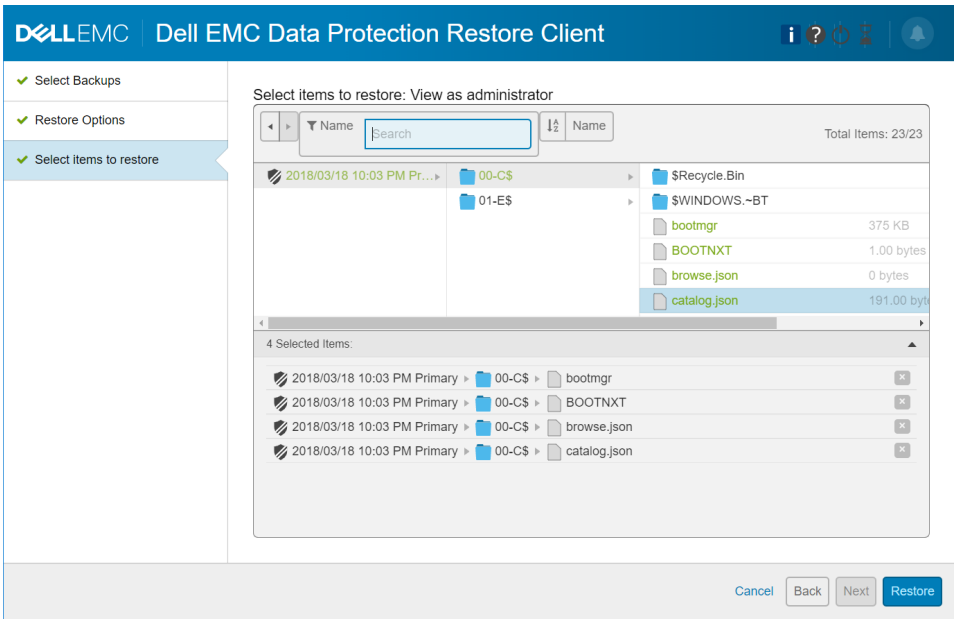


5. Log in to the destination virtual machine to initiate the mounting of the backup.
6. After you successfully log in, select the restore location. If desired, specify a new folder name in this location. Click **Next**.

   Note: Additionally, you can select the **Overwrite existing files and folders** option if you want to replace the existing files with the recovered files.

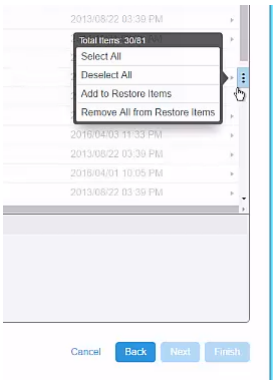
7. On the **Select items to restore** page, browse and select the files and folders available for recovery. Note that you can sort items by Name, File size, or Date, and you can also search for a specific file or folder name. To mark an item for recovery, double-click the item, or drag and drop the item into the **Selected Items** pane.

Figure 59 Select items to restore



Within this window, you can also discover and select the total number of items available for recovery by scrolling to the far right of the directory structure and right-clicking the icon located on the vertical scroll bar, as shown in the following figure.

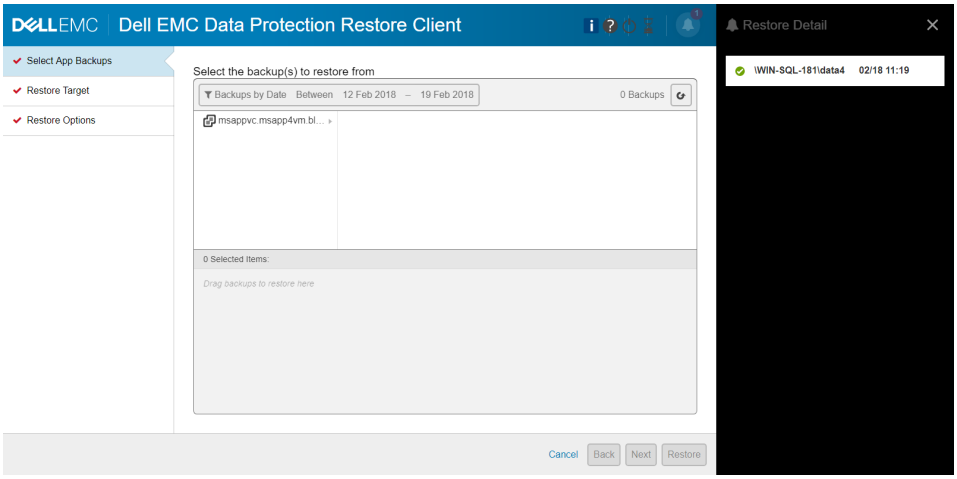
Figure 60 Total items available for recovery



8. When finished selecting items, click **Finish**.
9. Click **Yes** when you are prompted to continue with the restore.
10. To enable the polling feature so that you can monitor the status of the restore, click the hourglass icon located in the upper right-hand corner of the window and set to **ON**. By default, the polling feature is set to **OFF** due to the memory consumption that occurs when the server is queried every few seconds for the restore status.
11. Once the polling feature is enabled, you can monitor the status of the restore by clicking the icon located in the upper right-hand corner of the window.

    When you click the icon, the **Restore Detail** pane slides into view on the right side of the window, displaying the ongoing restore operations. Clicking the entry displays the progress of the restore and a recovery logs download option.

Figure 61 Restore Monitoring



Restoring SQL Server application-consistent backups (Windows platforms only)

NetWorker 18.x allows you to restore an individual SQL database or an entire SQL instance for a virtual machine that was backed up as part of a SQL Server application-consistent protection policy. You can perform this restore to a running virtual machine, providing you with operational recovery of SQL databases and disaster recovery of SQL instances. Additionally, alternate restore allows you to restore to a database copy. Once you restore SQL database FULL backups, you can also apply SQL database transaction log backups to those databases. The individual database or instance restore target location can be the original location, or a new location on either the original virtual machine or a different virtual machine, with the ability to select the SQL instance where the database will be restored, the option to change the database name, and the option to select specific folder locations for file and log placement. Note that the ability to select a different virtual machine is only possible for individual SQL database restore. When performing SQL instance restore, you are restricted to selecting the original virtual machine and original instance.

SQL restore functionality is provided in the **Dell EMC Data Protection Restore Client** by using the **App** mode button on the login page. In **App** restore mode, the display of virtual machines and their primary backups is limited to virtual machines that have application consistent backups. Once a primary backup is selected, an additional index is loaded that allows you to browse and select the SQL instances, databases, and the database backup versions.

The **Backup Versions** pane displays the database backup versions on the original virtual machine, with a cumulative history of FULL and transaction log backups for that database for one cycle of the backup policy. The **Backup Versions** pane refreshes with each full backup, and each subsequent transaction log backup adds the transaction log backup versions. The cumulative backup history allows you to select a database and associated backup regardless of the primary backup that is selected. When you select a SQL instance or SQL database to restore and do not select a specific backup version, the most recent backup version of the selected primary backup will be restored automatically.

The **Dell EMC Data Protection Restore Client** requires the virtual machine administrative credentials during mounting of the primary FULL backup on the original virtual machine. During the mount, NetWorker also installs or upgrades the FLR Agent and Microsoft VM App Agent, if required, on the selected virtual machine

The **Dell EMC Data Protection Restore Client** will discover and display the SQL instance on the target virtual machine once the mount completes. If the target virtual

machine does not have any running SQL Instances, an error will be displayed. You may select the SQL instance from this where you want to restore the database. The ability to select a different SQL Instance is only possible for individual database restore, and when performing SQL Instance restore you are restricted to selecting the original SQL Instance.

NetWorker automates the complete restore of SQL databases, restoring the database FULL and any transaction log backups as a single operation according to the following sequence:

- The primary FULL database backup is identified, mounted on the original virtual machine, and the SQL database files from the FULL backup are restored to the original database.
- If a transaction log backup was selected, the series of transaction logs that occurred after the FULL backup to the selected transaction log are restored in sequence.

NetWorker automates the complete restore of SQL instances according to the following sequence:

- The **master** database is restored first, then **msdn**, then **model**. During this restore, the SQL instance restarts in single-user mode as required by the Microsoft SQL Server to restore the master database. When the restore completes, the SQL services restart in multi-user mode.
- Each remaining database is restored individually, and includes the backup versions present in the currently selected backup.

The **Dell EMC Data Protection Restore Client** provides the ability to monitor the restore operations while in progress by enabling the Polling feature, which is disabled by default. Once enabled, when you click the icon, the **Restore Detail** pane slides into view on the right side of the window, displaying the ongoing restore operations. Clicking the entry displays the progress of the restore and a recovery logs download option.

Restore specific SQL databases and instances to a running virtual machine (Windows platforms only)

To restore specific SQL instances and databases to a running virtual machine in the **Dell EMC Data Protection Restore Client**, select the **App** button, and then select **User** or **Admin**. In **User** mode, you can log in and connect to the virtual machine that was backed up as part of a SQL Server application-consistent protection policy to restore to the original virtual machine. In **Admin** mode, you can browse, select, and restore from any virtual machine that you backed up as part of a SQL Server application-consistent protection policy. In both modes, you can restore the virtual machine's SQL instance(s) to the original SQL instance, or an alternate SQL instance.

Before you begin

When planning to restore to an alternate instance between virtual machines in different domains, ensure that DNS is resolved.

For the Data Domain resource, ensure that you provide the management credentials and, if required, enter the export path appropriately. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only)provides detailed steps.

Additionally, if not using the NMC Administrator account to log in, you must create a user in the NetWorker Authentication Service by using the NetWorker Management Console (NMC), as described in the section Create a user in the NetWorker authentication service (User mode file-level restore only), and you must configure

Microsoft SQL Server instances in the original virtual machine to allow SYSTEM account login and membership in the SQL sysadmin role.

Procedure

1. Open a browser from the virtual machine that the SQL databases or instances will be recovered to, and enter a URL that points to the NetWorker server host and indicates file-level restore. For example:

   `https://NetWorker server IP:9090/flr`

   The **Dell EMC Data Protection Restore Client** login window appears.

2. Select the **User** or **Admin** tab, and then select the **App** tab.

   Note: For **User** mode recoveries, you must connect to the NetWorker server from a web browser on the virtual machine that the SQL database or instance will be restored to.

3. Type the user credentials, and then click **Login**.

   - For **User** mode, type the NetWorker credentials. These can be your NMC credentials, or the user account credentials specified for the NetWorker user group **VMware FLR Users**. This user must belong to the **VMware FLR Users** group in order to be authorized to perform SQL database or instance restore. The section NetWorker privileges required by File-level restore users provides more information.
   - For **Admin** mode, type the NetWorker credentials. When using this mode, ensure that the user you specify for the NetWorker server login has the correct privileges to use this option.

   When you log in, the **Select App Backups** page displays with a list of virtual machines that were backed up by the SQL Server application-consistent protection policy. The available backups (primary backups) appear under each virtual machine, and include the virtual machine FULL and transaction log backups, depending on the application-consistent policy settings. For **User** mode, this will be limited to a list of backups for the local virtual machine.

   Note: The polling feature, which enables monitoring of in-progress restore operations, is turned off by default. To turn on the polling feature, click the hourglass icon located in the upper right-hand corner of the window and set to **ON**.

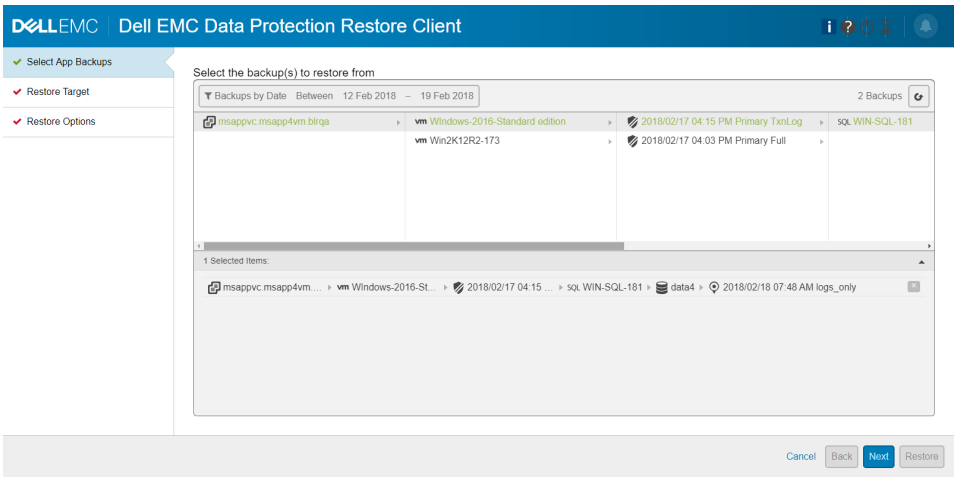
4. On the **Select App Backups** page, use the arrows to the right of the entry to browse and select from the available SQL Server application-consistent backups, including all SQL instances, databases, and backup versions.

   To select a backup version, expand the SQL instance and database to display the backup versions pane, and then click the backup version item once or drag and drop the item to move the backup to the **Selected Items** pane. You may be required to scroll right to view the backup versions.

   To select a SQL database or instance, drag and drop the entry to move the item to the **Selected Items** pane. Note that you cannot drag and drop the SQL database or instance when the entry has been expanded to view its children. If you expanded the entry, reselect the virtual machine, and then select the SQL database or instance to enable drag-and-drop.

   Note: The backup filter is set to the last seven days by default. You can expand the date range further back if desired.

Figure 62 Select App Backups page

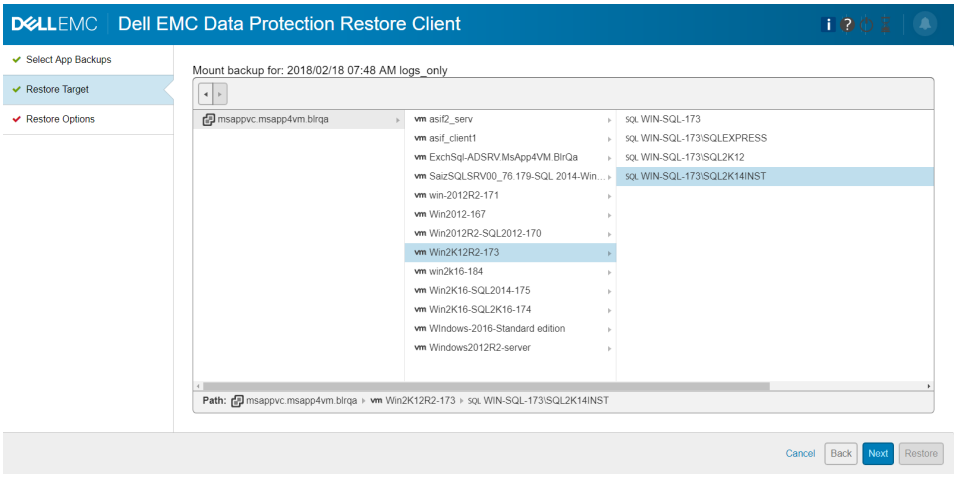


When finished, click **Next**. The **Restore Target** page displays.

5. On the **Restore Target** page, select the running virtual machine to which you want to restore the items. For an individual SQL database restore in **User** mode, you can only select the original virtual machine as the restore target. For an individual SQL database restore in **Admin** mode, you can select the original virtual machine or a different virtual machine as the restore target. For SQL instance restore, you must select the original virtual machine as the restore target.

   The **Dell EMC Data Protection Restore Client** prompts you to provide the system administrative credentials of the target virtual machine to initiate the mount of the backup and to verify that the vProxy FLR Agent and Microsoft VM App Agent are installed on this virtual machine.

   Figure 63 Restore Target page



When the mount completes, all SQL instances running on the selected virtual machine display in this window.

Note: If the SQL Server is not installed, or there are no SQL instances running, an error displays. If this occurs, log out of the **Dell EMC Data Protection Restore Client** to cancel the mount.

6. Select the SQL instance where you want to restore the database, and then click **Next**.

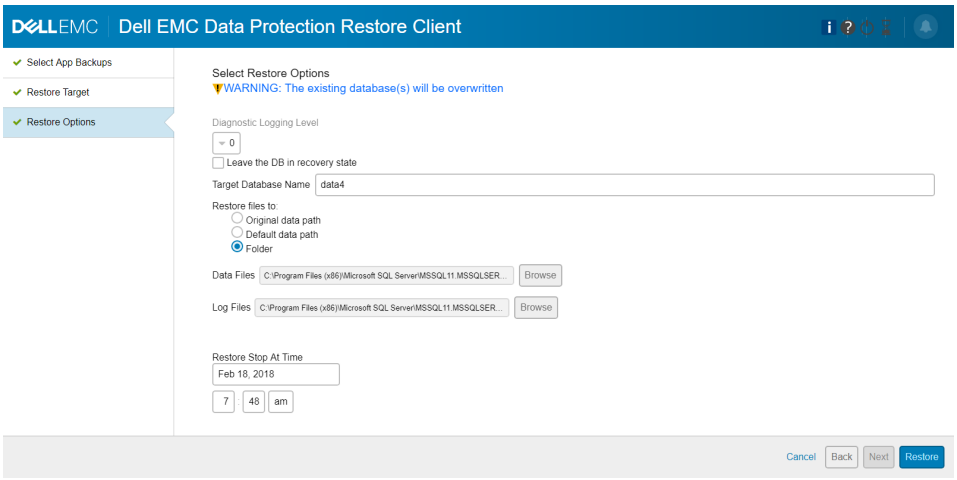
   The **Restore Options** page displays.

7. On the **Restore Options** page, set the **Diagnostic logging level**, if required. The default level is 0.
8. Select **Leave the DB in recovery state** if you want to activate the SQL Server NORECOVERY database restore option, which places the database in a recovering state upon completion of the restore and is useful for special situations such as restoring transaction log backups taken by third-party applications. Note that this option is not available for SQL instance restore. This option also overwrites the database and then leaves the database in restoring state.
9. In the **Target Database Name** field, you can type a new name if you want to change the name of the database, or leave the current name. By default, this field displays the name of the database at the time of backup.

   Note: If you change the database name, the new name must comply with the Microsoft SQL Server rules for database naming. Also, if you change the name and another database with the same name already exists on the target virtual machine and SQL instance, a warning displays that this database will be overwritten if you proceed.

10. For the restore location, select from one of the following options under **Restore files to**:
    - **Original Location**—Select this option to restore the database files to the original, or current, location. This option is only available if the original virtual machine and SQL instance were selected as the restore target. By default, the files are restored to the database location as it was at the time of backup. Note, however, that if the database file locations were changed after the backup, the files will be restored to the changed location.
    - **Default data path**—Select this option to restore the database files to the default data path for the target SQL Server instance. Each SQL Server instance has a configuration variable for the default database data path and log file path. When you select this option, all SQL data files will be restored to the default data path, and all log files will be restored to the default log path.
    - **Folder** —Allows you to specify the folders where you want to restore the database and log files. With this option, you can specify two folder locations on the target virtual machine; one folder to store all the data files for the database, and another folder to store all the log files for the database. Click **Browse** to navigate the file system on the target virtual machine and select the desired folders. By default, both folder locations are populated with the SQL default data paths for the target SQL Server instance. Note that you can only select an existing folder and cannot create a new folder using the **Dell EMC Data Protection Restore Client**.

Figure 64 Restore Options page



11. Select **Restore Stop At Time** if you want to restore transaction logs from the backup version that occurred before the specified restore date and time. This option is only available when you select a specific transaction log backup.
12. Click **Restore**.

    Note: A restore of individual SQL Server databases or instances in the **Dell EMC Data Protection Restore Client** will overwrite the existing database.

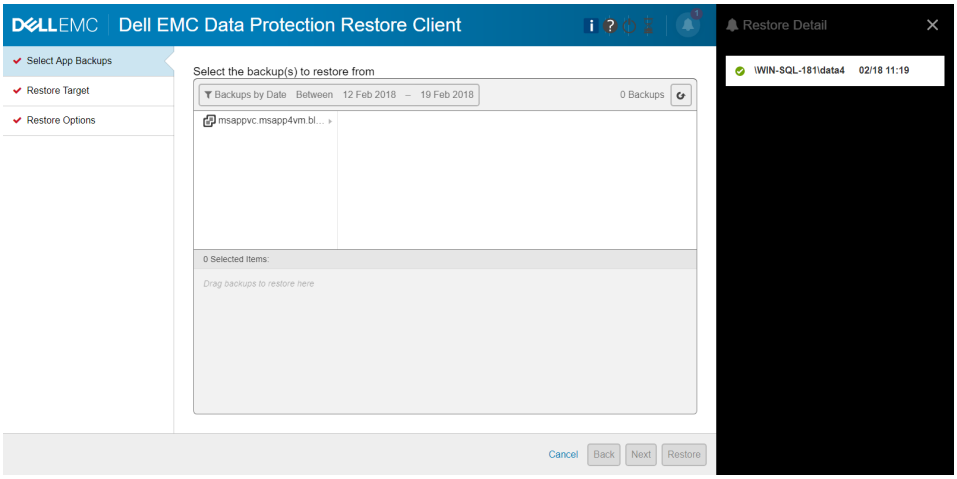
13. In the **Restore Confirmation** dialog, click **Yes** to continue the restore and overwrite the existing database, or **No** to exit the restore.

    If you changed the name of the database and another database with the same name already exists on the target virtual machine and SQL instance, an additional warning displays that this database will be overwritten if you proceed. If you changed the name of the database and the name does not match any available databases on the target virtual machine and SQL instance, an additional warning displays indicating that a new database will be created.

14. To enable the polling feature so that you can monitor the status of the restore, click the hourglass icon located in the upper right-hand corner of the window and set to **ON**. By default, the polling feature is set to **OFF** due to the memory consumption that occurs when the server is queried every few seconds for the restore status.
15. Once the polling feature is enabled, you can monitor the status of the restore by clicking the icon located in the upper right-hand corner of the window.

    When you click the icon, the **Restore Detail** pane slides into view on the right side of the window, displaying the ongoing restore operations. Clicking the entry displays the progress of the restore and a recovery logs download option. For SQL database restore, a single line displays. For SQL instance restore, one line per database displays. In both cases, the **Target** field indicates the database associated with the progress line.

Figure 65 Restore Monitoring



vProxy recovery in the vSphere Client's Dell EMC NetWorker interface

You can also perform virtual machine image-level recoveries of vProxy backups by using the **vSphere Client** HTML-5 based **Dell EMC NetWorker** interface. Recoveries can be performed to the original virtual machine or to a new virtual machine.

Dell EMC NetWorker appears in the left navigation pane of the **vSphere Client** after you install the vCenter plug-in. The section Installing the vCenter plug-in provides instructions.

Note: Backup and recovery operations in the **vSphere Client Dell EMC NetWorker** interface are not supported for SQL Server advanced application-consistent protection policies. Perform these operations from the NMC **NetWorker Administration** window or the **Dell EMC Data Protection Restore Client**.

Connect to the NetWorker server in the vSphere Client

You must establish a connection to the NetWorker server before performing any vProxy backup and recovery operations in the **vSphere Client**.

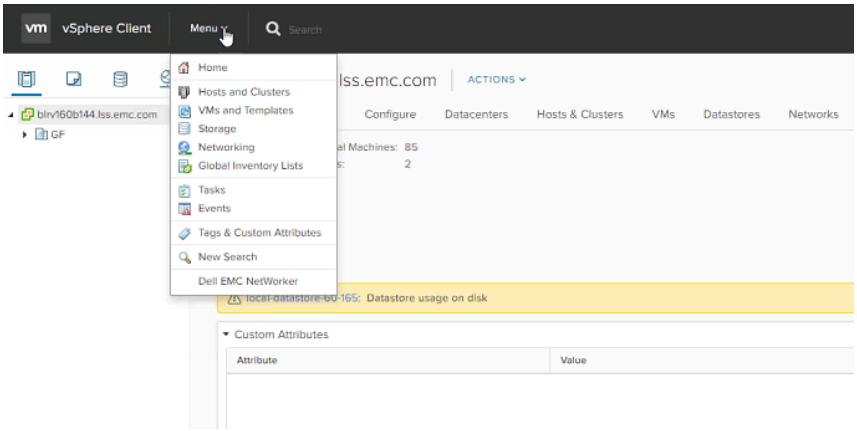
Before you begin

Dell EMC NetWorker only appears in the **vSphere Client** after you install the vCenter plug-in. The section Installing the vCenter plug-in provides instructions.

Procedure

1. Login to the **vSphere Client** as an administrator, or as a non-administrator Active Directory user that you created using the steps in the section Accessing the HTML-5 or flash-based vCenter plug-in as a non-administrator Active Directory user.
2. In the **vSphere Client**, select **Menu** > **Dell EMC NetWorker**, or select **Dell EMC NetWorker** in the left pane.

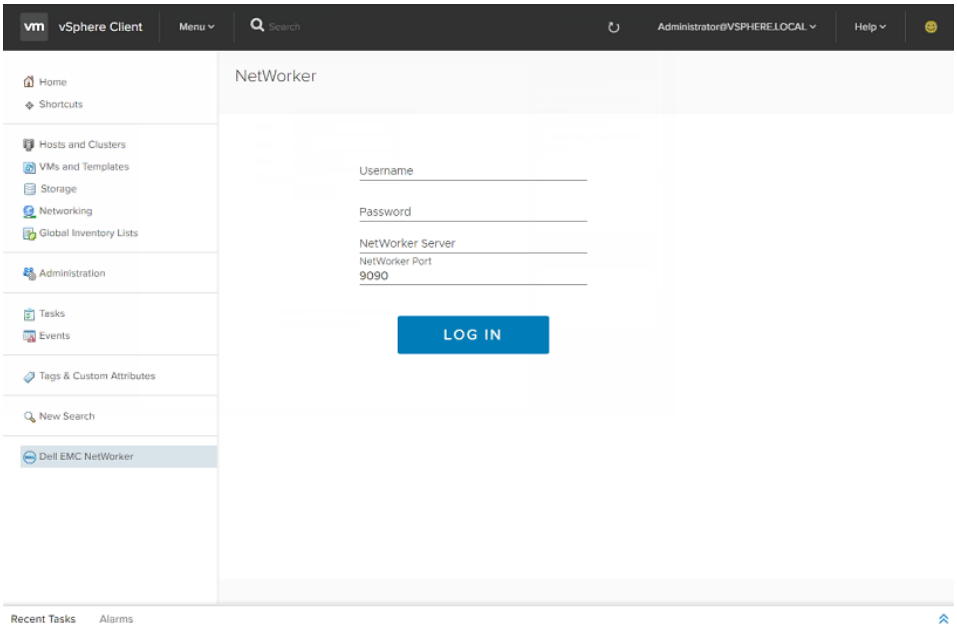
Figure 66 Accessing Dell EMC NetWorker in the vSphere Client



A prompt displays in the right pane with fields required to connect to the NetWorker server.

3. For the NetWorker server, type the following information:
   a. In the **Username** field, type the NetWorker administrator username.
   b. In the **Password** field, type the NetWorker administrator password.
   c. In the **NetWorker Server** field, type the IP address of the NetWorker server.
   d. In the **Port** field, type **9090**.

Figure 67 NetWorker connection information in the vSphere Client



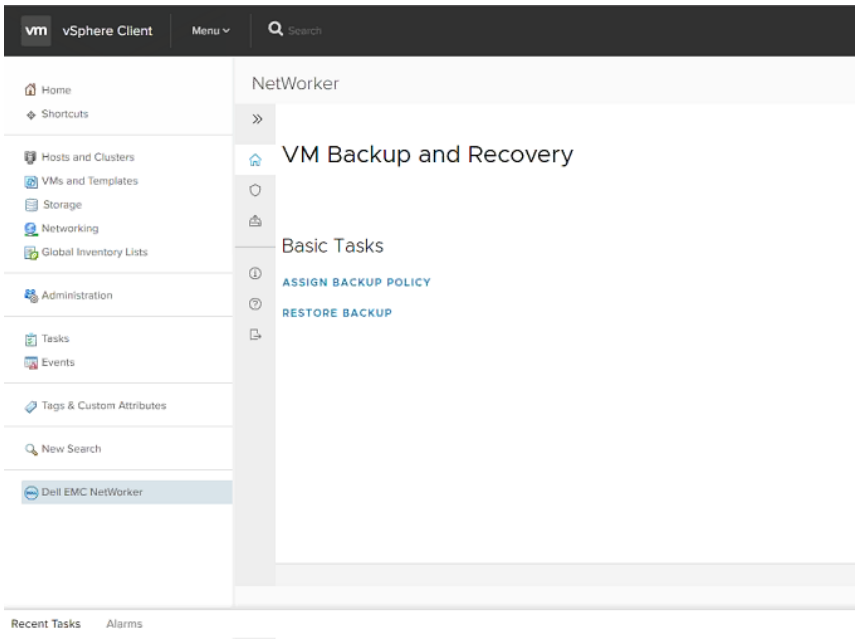
Note: The vCenter plug-in (HTML5 or flash-based) requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.

4. Click **Log in**.

Results

When a connection to the NetWorker server is established, the **Basic Tasks** pane appears, as shown in the following.

Figure 68 Dell EMC NetWorker Basic Tasks pane



Recovery to the original virtual machine

To start a vProxy image-level recovery to the original virtual machine by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

Before you begin

Ensure that the virtual machine you want to restore to is in powered OFF state.

Procedure

1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

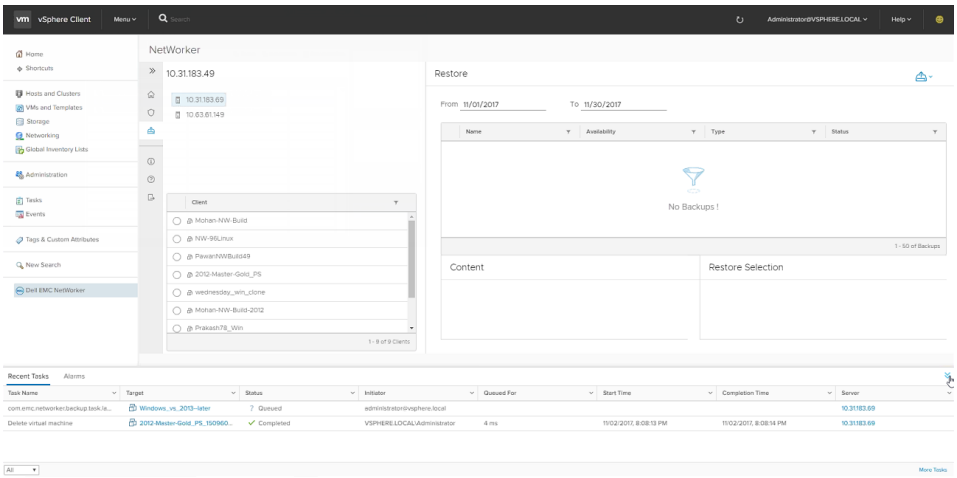
   When a connection to the NetWorker server is established, links to **Basic Tasks** appear in the right pane.

2. From the **Basic Tasks** pane, click **Restore Backup**, or click the Restore icon

   in the vertical navigation bar.

   A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.

Figure 69 Restore pane with available virtual machine backups



Note: If this list does not contain a virtual machine that was recently backed up, refresh the window.

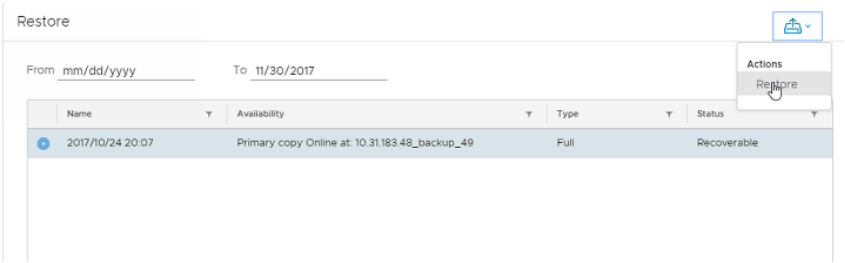
3. From the **Client** pane, click the radio button next to the virtual machine that you want to recover.

   A list of available restore points for that virtual machine displays in the right pane. You can also specify a date range to view only the virtual machine backups that were performed within that range.

4. Within the **Restore** pane, click the radio button next to the desired restore point.

5. In the top-right of the **Restore** pane, click the **Action** icon and select **Restore** from the drop-down.

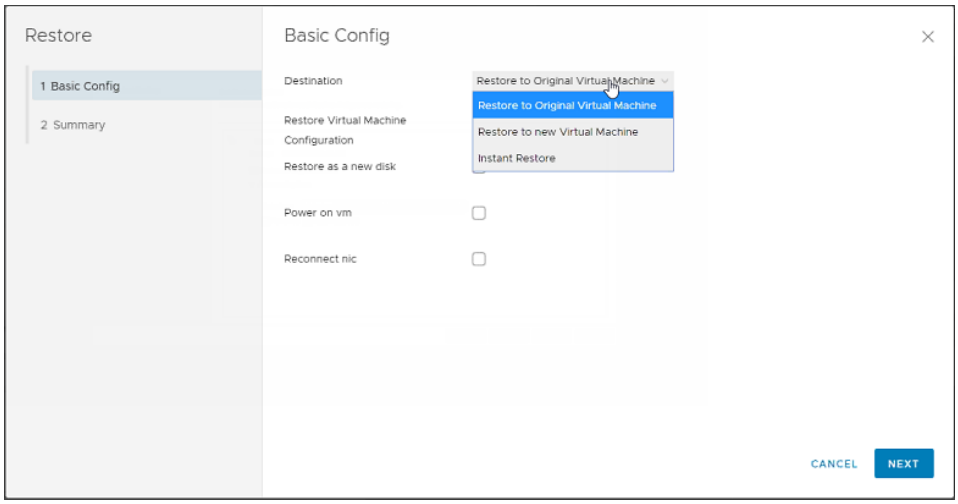
   Figure 70 Select Restore from the Action drop-down



   The **Restore** wizard opens on the **Basic Config** page.

6. From the **Destination** drop-down, leave the default **Restore to original location** selected.

Figure 71 Restore to original location



7. (Optional) Select from the following options:
   a. **Power on vm**—Select this checkbox to automatically power on the virtual machine after the restore completes.
   b. **Reconnect nic**—Select this checkbox to automatically reconnect the network interface card after the restore completes.
8. Click **Next**.
9. In the **Summary** page, review the information and then click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Recovery to a new virtual machine

To start a vProxy image-level recovery to a new virtual machine by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

Procedure

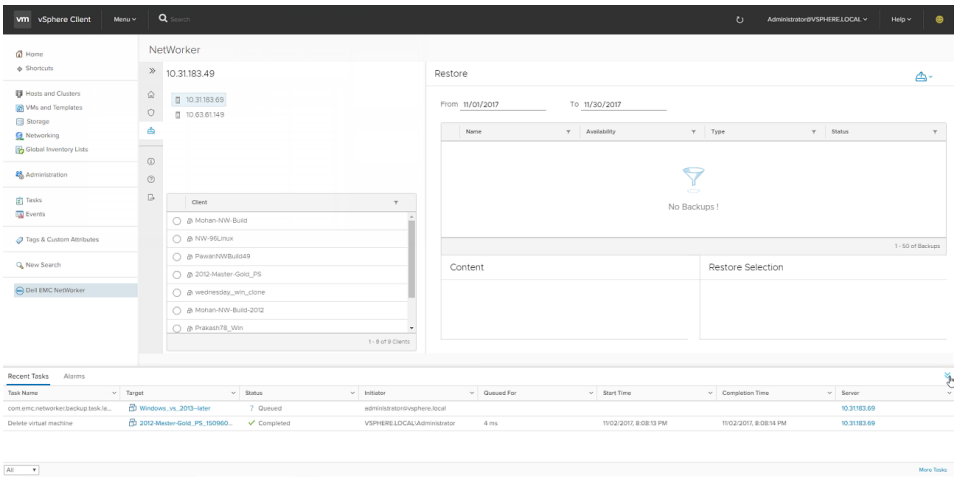
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

   When a connection to the NetWorker server is established, links to **Basic Tasks** appear in the right pane.
2. From the **Basic Tasks** pane, click **Restore Backup**, or click the Restore icon

   in the vertical navigation bar.

   A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.

Figure 72 Restore pane with available virtual machine backups



Note: If this list does not contain a virtual machine that was recently backed up, refresh the window.

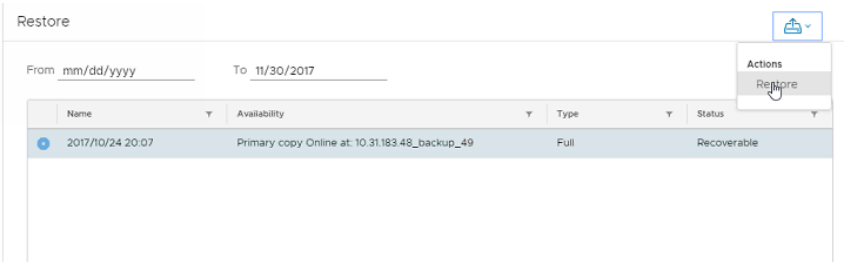
3. From the **Client** pane, click the radio button next to the virtual machine that you want to recover.

   A list of available restore points for that virtual machine display in the right pane. You can also specify a date range to view only the virtual machine backups that were performed within that range.

4. Within the **Restore** pane, click the radio button next to the desired restore point.

5. In the top-right of the **Restore** pane, click the **Action** icon and select **Restore** from the drop-down.

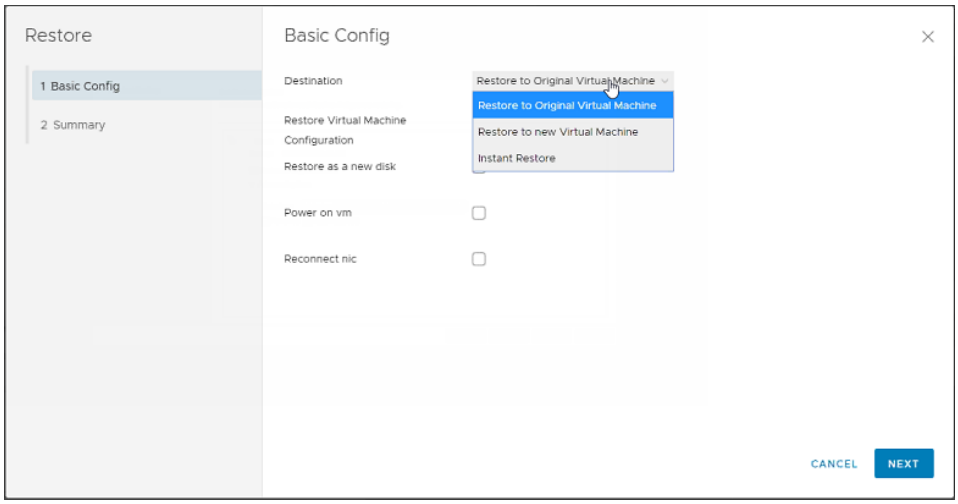
   Figure 73 Select Restore from the Action drop-down



   The **Restore** wizard opens on the **Basic Config** page.

6. From the **Destination** drop-down, select **Restore to new Virtual Machine**.

Figure 74 Restore to new virtual machine



7. (Optional) Select from the following options:
   a. **Restore Virtual Machine Configuration**—Select this checkbox to restore this virtual machine with the existing configuration settings.
   b. **Power on vm**—Select this checkbox to automatically power on the virtual machine after the restore completes.
   c. **Reconnect nic**—Select this checkbox to automatically reconnect the network interface card after the restore completes.
8. Click **Next**.

   The **Advanced Config** page displays.
9. From the **vCenter** drop-down, select the destination vCenter server, and then specify a name for the new virtual machine. Click **Next**.

   The **Location** page displays.
10. Expand the vCenter server tree and select a destination for recovery within the vCenter server, and then click **Next**.

    The **Host/Cluster** page displays.
11. Select a host within the destination datacenter, and then click **Next**.

    The **Resource Pool** page displays.
12. Select a resource pool, and then click **Next**.

    The **Datastore** page displays.
13. From the **Destination Datastore** drop-down, select a datastore that is compatible with the virtual machine, and then click **Next**.
14. In the **Summary** page, review the information and then click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Virtual disk recovery (restore to an existing virtual machine)

To start a VMDK recovery to an existing virtual machine by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

About this task

Procedure

1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

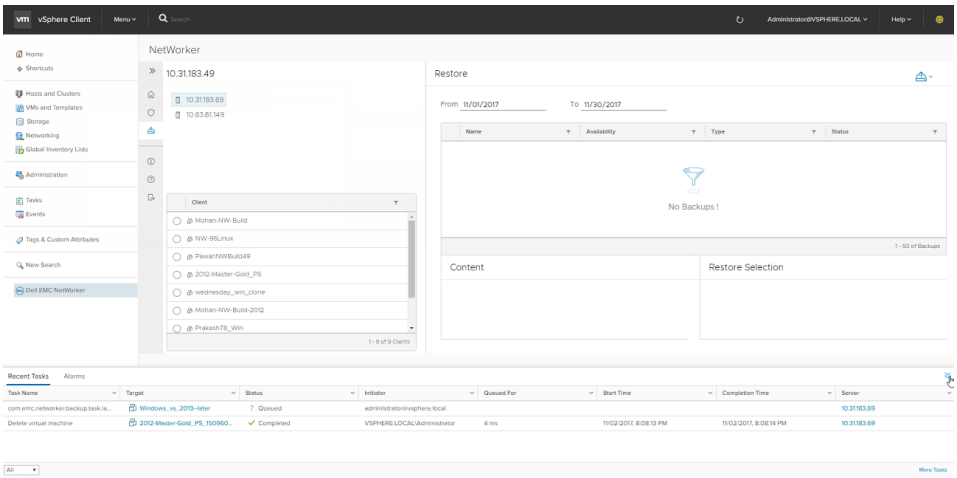
   When a connection to the NetWorker server is established, links to **Basic Tasks** appear in the right pane.

2. From the **Basic Tasks** pane, click **Restore Backup**, or click the Restore icon

   in the vertical navigation bar.

   A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.

   Figure 75 Restore pane with available virtual machine backups

   Note: If this list does not contain a virtual machine that was recently backed up, refresh the window.

3. From the **Client** pane, click the radio button next to the virtual machine that you want to recover.

   A list of available restore points for that virtual machine displays in the right pane. You can also specify a date range to view only the virtual machine backups that were performed within that range.

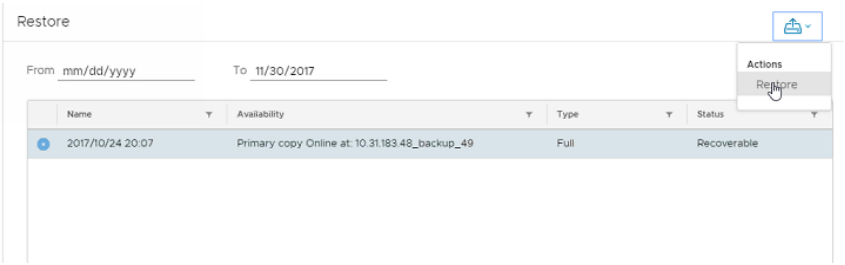
4. Within the **Restore** pane, click the radio button next to the desired restore point.

   The **Content** pane displays the virtual disks available for recovery.

5. Select the checkbox next to the disk(s) in the **Content** pane that you want to recover. When selected, the disk will appear in the **Restore Selection** pane.

6. Click the **Action** icon and select **Restore** from the drop-down.

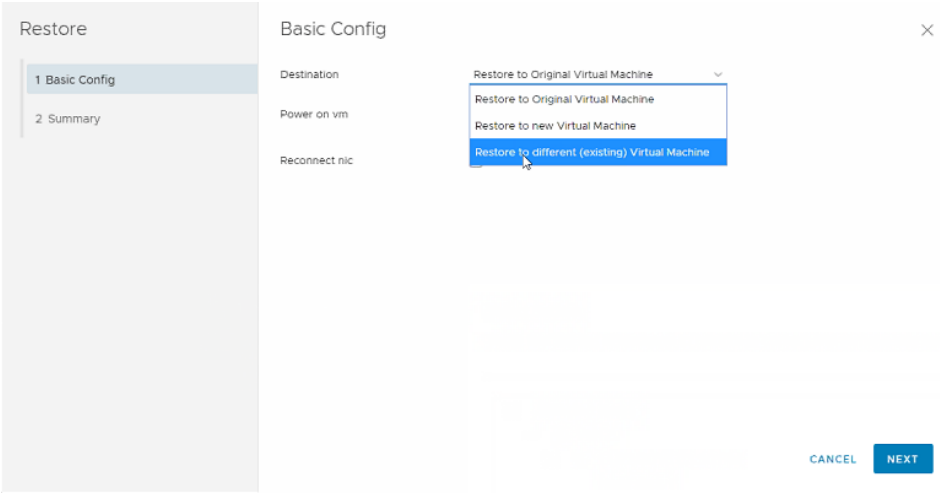
Figure 76 Select Restore from the Action drop-down



The **Restore** wizard opens on the **Basic Config** page.

7. From the **Destination** drop-down, select **Restore to different (existing) virtual machine**.

Figure 77 Restore virtual disks to existing virtual machine



8. (Optional) Select from the following options:
   a. **Reconnect nic**—Select this checkbox to automatically reconnect the network interface card after the restore completes.
   b. **Power on vm**—Select this checkbox to automatically power on the virtual machine after the restore completes.
9. Click **Next**.

   The **Advanced Config** page displays.
10. In the **Host/Cluster** pane, select the location in the datacenter of the existing virtual machine(s). A list of virtual machines for this location displays in the **Virtual Machines** pane. You can click the + icon next to a virtual machine to view more details.
11. Click **Next**.

    The **Datastore** page displays.
12. For each virtual disk listed in the **Datastore** pane, select a **Destination Datastore** from the drop-down, and then click **Next**.
13. In the **Summary** page, review the information and then click **Finish** to start the recovery.

WARNING When you start a VMDK recovery, the virtual machine will be powered off automatically without issuing a warning message.

Results

You can monitor the progress of the recovery in the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Instant recovery of a virtual machine

To start an instant recovery to a new virtual machine by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

Before you begin

Note the following before performing an instant recovery in the **Dell EMC NetWorker** interface:

- Ensure that you provide the management credentials for the Data Domain resource before you initiate the recovery. If you do not configure the management credentials in NMC prior to the recovery, the recovery will fail silent without an error message. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only) provides instructions.
- Ensure that you do not perform an instant recovery of virtual machines in resource pools and other similar containers that are part of a currently running protection group.
- Ensure that the free space on the Data Domain system is equal to or greater than the total disk size of the virtual machine being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target virtual machine fails.

Procedure

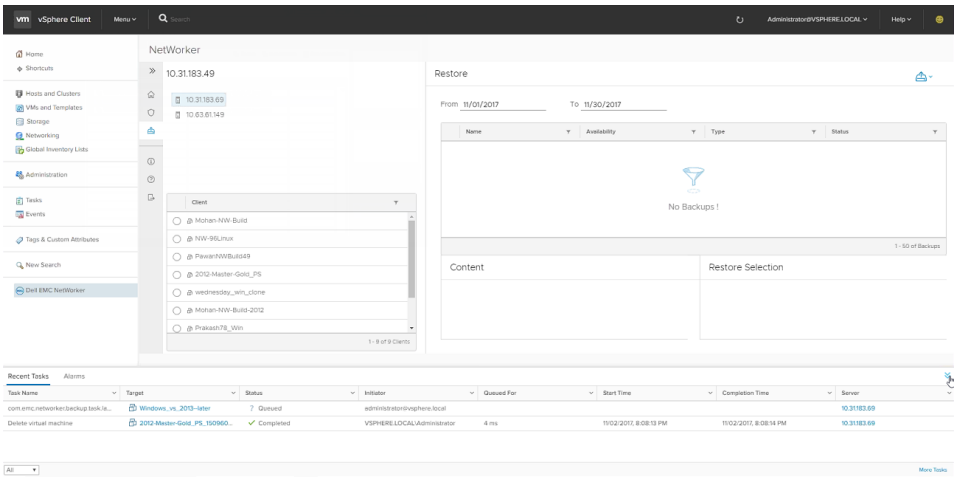
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

   When a connection to the NetWorker server is established, links to **Basic Tasks** appear in the right pane.

2. From the **Basic Tasks** pane, click **Restore Backup**, or click the Restore icon in the vertical navigation bar.

   A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.

Figure 78 Restore pane with available virtual machine backups



Note: If this list does not contain a virtual machine that was recently backed up, refresh the window.

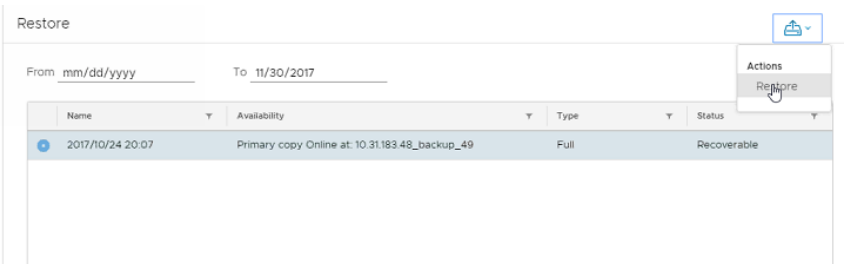
3. From the **Client** pane, click the radio button next to the virtual machine that you want to recover.

   A list of available restore points for that virtual machine display in the right pane. You can also specify a date range to view only the virtual machine backups that were performed within that range.

4. Within the **Restore** pane, click the radio button next to the desired restore point.

5. Click the **Action** icon and select **Restore** from the drop-down.

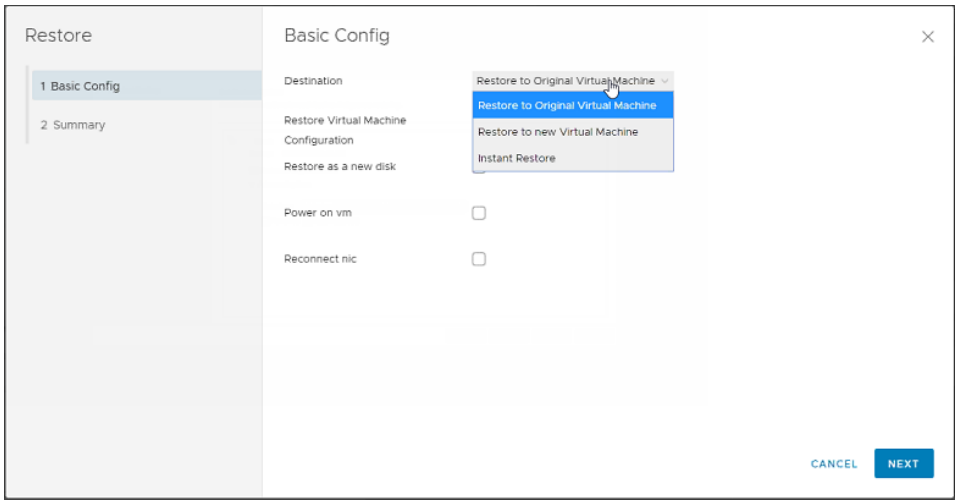
   Figure 79 Select Restore from the Action drop-down



   The **Restore** wizard opens on the **Basic Config** page.

6. From the **Destination** drop-down, select **Instant Restore**.

Figure 80 Instant Restore



7. Click **Next**.

   The **Advanced Config** page displays.

8. Specify a name for the new virtual machine, and then click **Next**.

   The **Location** page displays.

9. Expand the vCenter server tree and select a destination for recovery within the vCenter server, and then click **Next**.

   The **Host/Cluster** page displays.

10. Select a host within the destination datacenter, and then click **Next**.

    The **Resource Pool** page displays.

11. Select a resource pool, and then click **Next**.

12. In the **Summary** page, review the information and then click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Recent Tasks** pane. Once the instant restore completes, use storage vMotion to save the virtual machine, and then cancel the vSphere **NetWorker Recovery** task to delete the datastore. Power ON the virtual machine to validate the recovery.

vProxy recovery in the vSphere Web Client's VM Backup and Recovery interface

If using a vSphere version prior to 6.5, you can still use the vSphere Web Client's flash-based **VM Backup and Recovery** interface to perform image-level recoveries to the original virtual machine or to a new virtual machine.

In the **vSphere Web Client**, click **VM Backup and Recovery** in the left navigation pane. Once you establish a connection to the required NetWorker server, click the **Restore** tab to open the **Restore** pane.

Connect to the NetWorker server in the vSphere Web Client

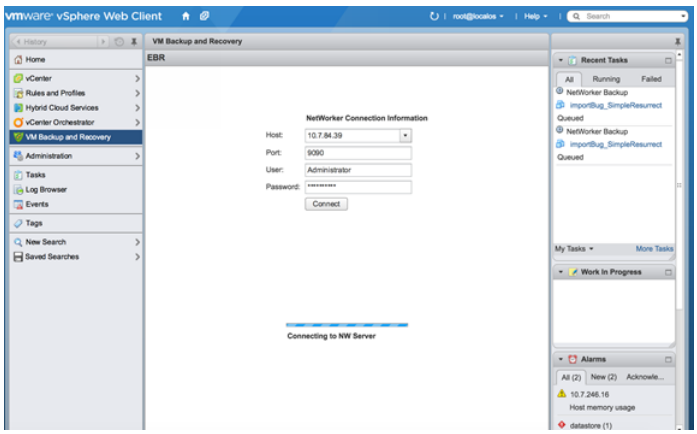
After installing the vCenter plug-in, you must establish a connection to the NetWorker server before performing any vProxy operations in the vSphere Web Client.

Procedure

1. Log in to the **vSphere Web Client** as an administrator, or as a non-administrator Active Directory user that you created using the steps in the section Accessing the HTML-5 or flash-based vCenter plug-in as a non-administrator Active Directory user.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   The required NetWorker connection information appears in the right pane.

   Figure 81 NetWorker connection information in the vSphere Web Client

3. Enter the following information for the NetWorker server:
   a. In the **Host** field, type the IP address of the NetWorker server.
   b. In the **Port** field, type **9090**.
   c. In the **User** field, type the NetWorker administrator username.
   d. In the **Password** field, type the NetWorker administrator password.

   Note: The vCenter plug-in (HTML5 or flash-based) requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.

4. Click **Connect**.

Results

When a connection to the NetWorker server is established, the **Getting Started** pane appears.

Recovery to the original virtual machine

In the vSphere Web Client's **VM Backup and Recovery** interface, use the following procedure to perform an image-level recovery to the original virtual machine.

Before you begin

Ensure that the virtual machine you want to restore to is in powered OFF state.

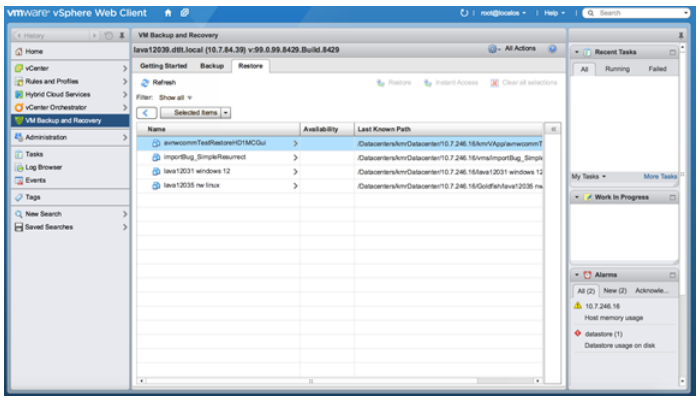
Procedure

1. Login to the **vSphere Web Client** as an administrator.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   When a connection to the NetWorker server is established, the **Getting Started** pane appears.
3. Click **Restore** to open the **Restore** pane.

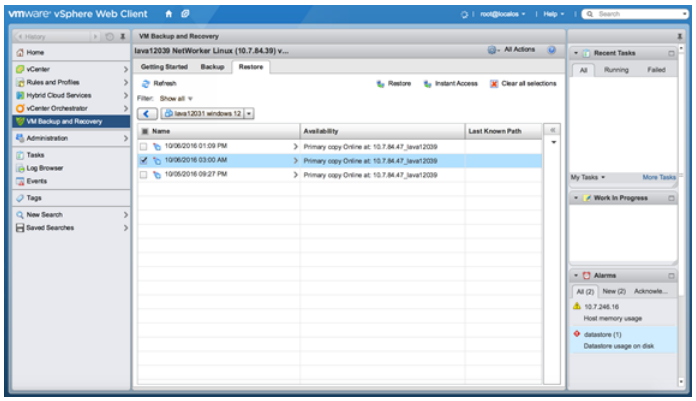
   A list of virtual machines available for recovery displays.

   Figure 82 Virtual machines for recovery in the Restore pane

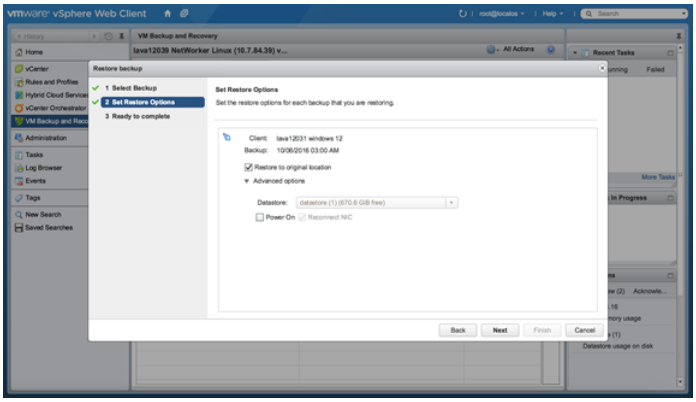
   If you do not see the virtual machine backup listed, refresh the window.
4. Browse the list of virtual machines and select the virtual machine backup you want to recover. You can expand the virtual machine backup to view a list of restore points from which to select.

   Figure 83 Select a restore point

   
5. Select one of the restore points by clicking the checkbox next to the backup time, and then click **Restore**.

   The **Restore Backup** wizard launches.
6. In the **Set Restore Options** page of the **Restore Backup** wizard, leave the default **Restore to original location** selected and click **Next**.

Figure 84 Restore to original location



7. In the **Ready to Complete** page, click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Running** tab of the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Recovery to a new virtual machine

In the vSphere Web Client's **VM Backup and Recovery** interface, use the following procedure to perform an image-level recovery to a new virtual machine.

Procedure

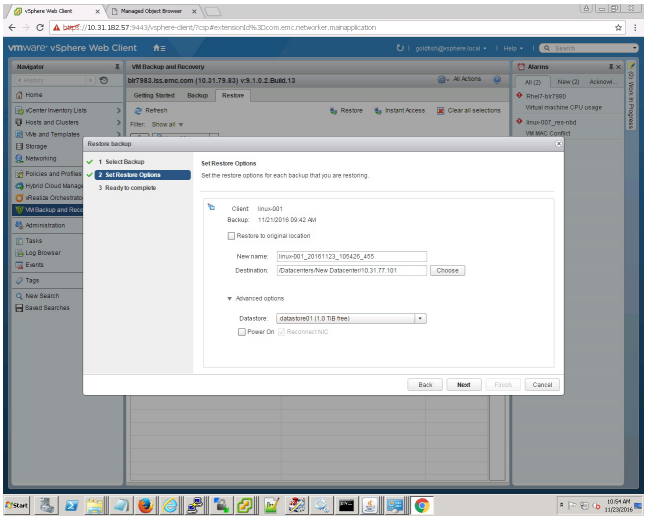
1. Login to the **vSphere Web Client** as an administrator.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   When a connection to the NetWorker server is established, the **Getting Started** pane appears.
3. Click the **Restore** tab to open the **Restore** pane.

   If you do not see the virtual machine backup listed, refresh the window.
4. Browse the list of virtual machines and select the virtual machine backup you want to recover. You can expand the virtual machine backup to view a list of restore points from which to select.
5. Select one of the restore points by clicking the checkbox next to the backup time, and then click **Restore**.

   The **Restore Backup** wizard launches.
6. In the **Set Restore Options** page of the **Restore Backup** wizard, uncheck the default **Restore to original location**.
7. Specify a name for the new virtual machine, and select a destination for recovery in the vCenter server. You are not required to select the **Choose** button and can ignore the text New or Existing.

Figure 85 Restore options for the new virtual machine recovery



8. Specify a datastore for the virtual machine, and then click **Next**.
9. In the **Ready to Complete** page, click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Running** tab of the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Virtual disk recovery

In the vSphere Web Client's **VM Backup and Recovery** interface, use the following procedure to perform a VMDK recovery to an existing virtual machine.

About this task

Procedure

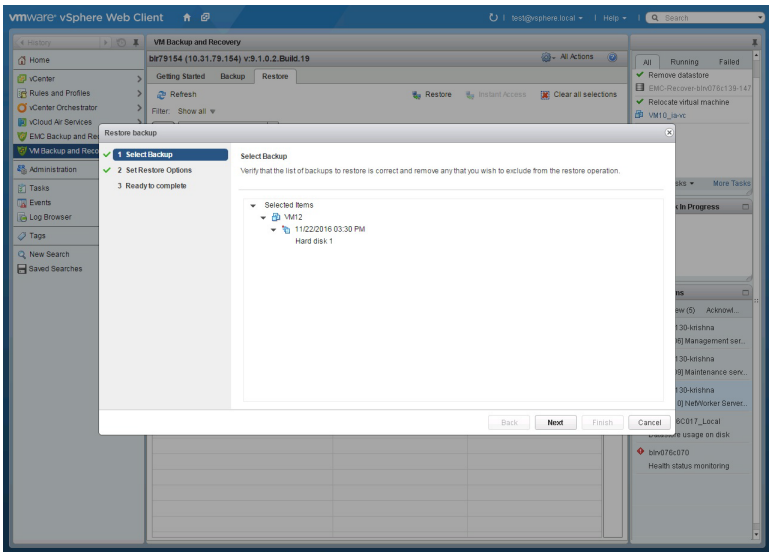
1. Log in to the **vSphere Web Client** as an administrator.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   When a connection to the NetWorker server is established, the **Getting Started** pane displays.
3. Click the **Restore** tab to open the **Restore** pane.

   If you do not see the virtual machine backup listed, refresh the window.
4. Browse the list of virtual machines and select the virtual machine backup that contains the VMDK you want to recover. You can expand the virtual machine backup to view a list of restore points from which to select.
5. Double-click one of the restore points to view the list of available VMDKs for the virtual machine.
6. Select the VMDK you want to restore by selecting the checkbox next to the VMDK, and then click **Restore**.

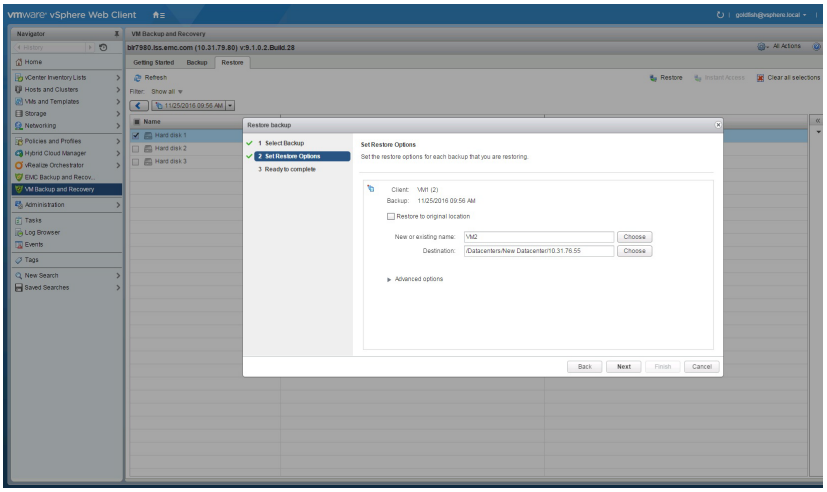
   The **Restore Backup** wizard launches.

Figure 86 Select VMDK backup to restore



7. In the **Select Backup** page, verify that the correct VMDK is selected and click **Next**.
8. In the **Set Restore Options** page, uncheck the default **Restore to original location** and then click **Next**.
9. Click **Choose** to browse the existing virtual machine where the VMDK needs to be restored in the vCenter.

Figure 87 Set Restore Options for VMDK recovery



10. Specify a datastore for the VMDK, and then click **Next**.
11. In the **Ready to Complete** page, click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Running** tab of the **Recent Tasks** pane.

Note: When you start a VMDK recovery, the virtual machine will be powered off automatically without issuing a warning message.

Instant recovery of a virtual machine

In the vSphere Web Client's **VM Backup and Recovery** interface, use the following procedure to perform an instant access recovery to a new virtual machine.

Before you begin

Note the following before performing an instant access recovery in the **VM Backup and Recovery** plug-in:

- Ensure that you provide the management credentials for the Data Domain resource before you initiate the recovery. If you do not configure the management credentials in NMC prior to the recovery, the recovery will fail silent without an error message. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only) provides instructions.
- Ensure that you do not perform an instant recovery of virtual machines in resource pools and other similar containers that are part of a currently running protection group.
- Ensure that the free space on the Data Domain system is equal to or greater than the total disk size of the virtual machine being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target virtual machine fails.

Procedure

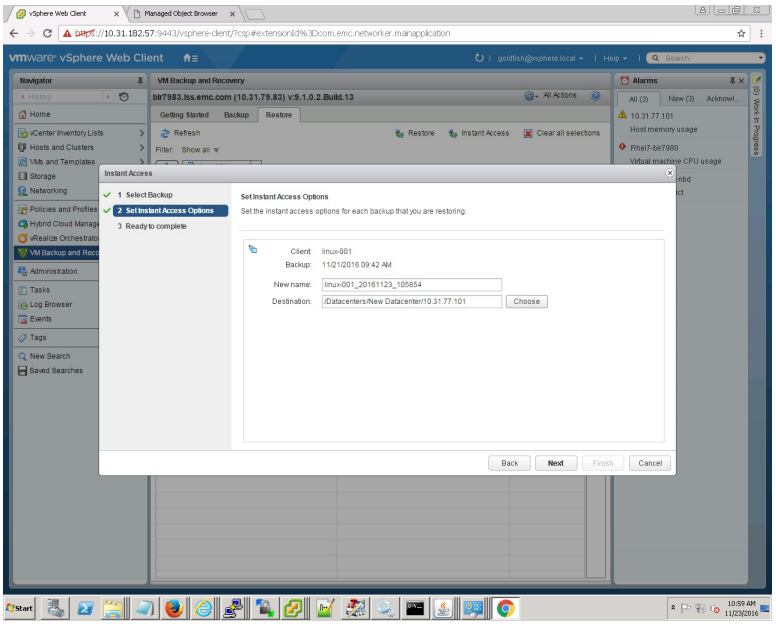
1. Log in to the **vSphere Web Client** as an administrator.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   When a connection to the NetWorker server is established, the **Getting Started** pane displays.
3. Click the **Restore** tab to open the **Restore** pane.

   If you do not see the virtual machine backup listed, refresh the window.
4. Browse the list of virtual machines and select the virtual machine backup you want to recover. You can expand the virtual machine backup to view a list of restore points from which to select.
5. Select one of the restore points by selecting the checkbox next to the backup time, and then click **Instant Access**.

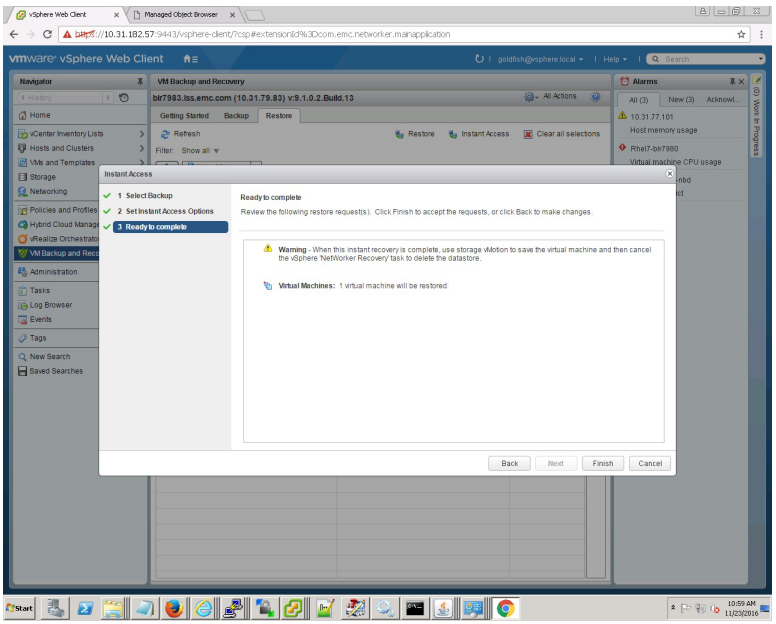
   The **Restore Backup** wizard launches.
6. In the **Set Instant Access Options** page, specify a name for the new virtual machine, and select a destination for recovery in the vCenter server, and then click **Next**. You can ignore the text New or Existing.

Figure 88 Set Instant Access restore options



7. In the **Ready to Complete** page, click **Finish** to start the recovery.

Figure 89 Finish Instant Access recovery



Results

You can monitor the progress of the recovery in the **Running** tab of the **Recent Tasks** pane. Once the instant access recovery completes, use storage vMotion to save the virtual machine, and cancel the vSphere **NetWorker Recovery** task to delete the datastore. Power ON the virtual machine to validate the recovery.

vProxy recovery log files

The vProxy appliance contains log files, which you can configure to display debug information.

The following table provides information about the vProxy recovery log files and how to enable debugging.

Table 15 Recovery log files

Log file	Log location and name	Logging levels
Primary recovery log	For image level recoveries, `/opt/emc/vrproxy/runtime/logs/vrecoverd/vrecoverd-engine.log`. For file-level recoveries or SQL application-consistent recoveries, `/opt/emc/vrproxy/runtime/logs/vflrd/vflrd-engine.log`.	To modify the logging level: 1. Edit the `/usr/lib/systemd/system/vrecoverd.service` file. 2. Search for the for the *ExecStart=* string. 3. Edit the *--program-log-level=* argument with one of the following values: • warn • info • trace • debug 4. Reload the unit config file into systemd: **`systemctl daemon-reload`** 5. Restart the recovery engine: **`systemctl restart vrecoverd.service`**
DD Boost recovery log	For image level recoveries, `/opt/emc/vrproxy/runtime/logs/vrecoverd/vrecoverd-boost.log`. For file-level recoveries or SQL application-consistent recoveries, `/opt/emc/vrproxy/runtime/logs/vflrd/vflrd-boost.log`.	To modify the logging level: 1. Edit the `/usr/lib/systemd/system/vrecoverd.service` file. 2. Search for the for the *ExecStart=* string. 3. Edit the *--boost-log-level=* argument with one of the following values: • none • error • warn • info • trace • debug • all 4. Reload the unit config file into systemd: **`systemctl daemon-reload`** 5. Restart the recovery engine: **`systemctl restart vrecoverd.service`**

Table 15 Recovery log files (continued)

Log file	Log location and name	Logging levels
VDDK recovery log	`/opt/emc/vrproxy/runtime/logs/vrecoverd/vrecoverd-vddk.log`	To modify the logging level: 1. Edit the `/opt/emc/vproxy/conf/VixDiskLib.config` file. 2. Edit the *vixDiskLib.transport.LogLevel =* to specify one of the following values: • 0—No logging • 1—Errors only • 2—Warnings and Errors • 3—Important information messages, errors and warnings • 4 —All messages, including debug messages. 3. Restart the recovery engine: **`systemctl restart vrecoverd.service`**

CHAPTER 5

VADP Recovery (legacy)

Note: NetWorker 18.x releases do not feature a new version of the VADP proxy. For VADP, NetWorker 18.x only supports recoveries that were configured in a previous release. The NetWorker Online Compatibility Guide available on the Dell EMC Online Support site at https://support.emc.com/products/1095_NetWorker provides the most up-to-date compatibility information.

This chapter contains the following topics:

- Software and hardware requirements 218
- Limitations and unsupported features 218
- Transport modes 219
- Independent persistent disks cannot be recovered 220
- Configuring the VADP proxy host and Hypervisor resource 220
- Creating a VADP User role in vCenter 223
- Recovering VADP Backups 226
- VADP Planning and Best Practices 232

Software and hardware requirements

The software and hardware requirements for VADP include the following.

- One or more VADP proxy systems running any of the following 64-bit operating systems (English versions only):
  - Windows 2008 R2
  - Windows 2012
- One or more vCenter servers running vSphere 6.0 with ESX 6.0 and vCenter 6.0.
- Perform the following prerequisites on the NetWorker server/proxy machine in order to run vSphere version 6.0:
  1. Since the registry key for SSL verification is not set by default, add the following keypath in the registry:

     ```
     'HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/VMware, Inc./VMware
     Virtual Disk Development Kit'
     ```

     Add a DWORD VerifySSLCertificates and set it to zero ('VerifySSLCertificates=0'). This will disable SSL verification for all VDDK Hotadd operations.
  2. Install .NET framework 3.5.1 or later on the proxy. In Windows 2008 R2, even though the .NET framework is bundled with the operating system, ensure that you enable the framework under **Server Manager-** > **features**.
  3. Install VC++ runtime 9.0 (VC++2008 SP1) on the proxy. The following link provides more details: http://www.microsoft.com/en-us/download/details.aspx?id=2092
- Network connectivity must be available between the VADP proxy server and the vCenter Server managing the ESX server cluster. It also requires connection to the ESX server system.
- To connect to a Fibre Channel (FC) SAN, the VADP proxy requires a FC host bus adapter (HBA).
- You must install the NetWorker 9.0.x client software on the VADP Proxy host.
- The NetWorker server requires NetWorker 18.x software.
- The VADP proxy host must have access to the LUNs required for supported virtual machines. Considerations vary depending on the environment, for example, physical and virtual Compatibility RDMs are not supported and therefore do not require proxy access. The section VADP proxy access to LUNs on page 239 provides more information.

Limitations and unsupported features

The following limitations apply to the VADP solution with NetWorker:

- NetWorker supports the recovery of non-English versions of guest operating systems for virtual machines. However, if using non-English versions of the Windows operating system for the vCenter or VADP proxy host, note the limitations in the sections Limitations to vCenter on non-English versions of Windows on page 219 and Limitation for VADP proxy host on non-English versions of Windows on page 219.

- Global directives (both encryption and compression directives) are not supported by NetWorker for VADP recovery.
- Image-level recovery from a CBT-based incremental backup is not supported.

Limitations to vCenter on non-English versions of Windows

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

- The following names should always contain only English characters:
  - Backup VM display name in the left pane of vCenter
  - Backup VM hostname/FQDN
  - vCenter Datacenter name
  - vCenter Resource pool name
  - ESX datastore names containing the VM configuration files and virtual disks.
- You can only restore VMs to the same language OS vCenter that you perform the backup from. For example, you cannot recover a VM backed up from a Japanese OS vCenter onto an English OS vCenter.
- You can only perform VADP recovery using the NetWorker User program. A command line recovery of the entire image will not work for backups from a non-English vCenter.

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

The following limitation applies to non-English versions of the Windows operating system for the VADP proxy host:

On the machine where you launch the VADP recovery, install the NetWorker package in English only without any language packages. You must unselect all the other language packages explicitly during the NetWorker installation.

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

Transport modes

The VADP proxy host supports advanced transport modes for image-level recovery. You can set the configured network transport mode to the following values during recovery:

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

  SAN mode requires a physical proxy with SAN access, and the VMs need to be hosted on either Fibre Channel or iSCSI-based storage. The corresponding VMFS volumes must be visible in the Microsoft Windows Disk Management snap-in of the VADP proxy host.
- Hotadd—In this mode, the I/O happens internally through the ESX I/O stack using SCSI hot-add technology. This provides better I/O rates than NBD/NBDSSL. However, selecting this mode places CPU, memory and I/O load on the ESX hosting the VADP proxy.

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

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

- NBD (Network Block Device): in this mode, the CPU, memory and I/O load gets directly placed on the ESX hosting the production VMs, because the data has to move through the same ESX and reach the proxy over the network. NBD mode can be used either for physical or virtual proxy, and also supports all storage types.
- NBDSSL (Network Block Device with SSL): NBDSSL transport mode is the same as NBD except that the data transferred over the network is encrypted. Data transfer in NBDSSL mode can therefore be slower and use more CPU due to the additional load on the VADP host from SLL encryption/decryption.

You can set multiple transport modes to be used by the VADP proxy host using the pipe symbol "|" (for example, san|nbd|nbdssl).

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

More information on configuring transport modes is provided in Configuring the VADP proxy host and Hypervisor resource. The transport modes are outlined in the table Table 16 on page 221.

Independent persistent disks cannot be recovered

VADP does not support the recovery of independent persistent disks. If NetWorker detects these disks, they are skipped and a message is logged that indicates the disks were skipped. If using independent persistent disks, you must use traditional NetWorker recovery.

Configuring the VADP proxy host and Hypervisor resource

A NetWorker client must be created for the VADP proxy host when configuring the virtual clients for recovery. The VADP proxy NetWorker client will be referred to by VM clients during VADP recovery operations.

You can create a NetWorker client for the VADP proxy host manually by using the `nsradmin` command.

Note: If multiple client instances of the same VADP proxy host exist in the NetWorker server, ensure that all the instances have the same application information attributes related to VADP. Manually copy the application information attributes into all the VADP proxy client instances. Note, however, that when a virtual proxy is used, it cannot be created by copying the template of other VMs that are being protected.

If vCenter is configured in the environment, there must be a Hypervisor resource for the vCenter server hosting the VMs that use VADP. You may also need to create a

Hypervisor resource if you cannot use **VMware View** in the NMC **NetWorker Administration** window.

If vCenter is not configured in the environment, there must be a Hypervisor resource created for each server in the environment.

You must create the corresponding Hypervisor resource in the NetWorker server prior to starting the VADP recovery.

Creating a Hypervisor resource from the NetWorker server

Procedure

1. Start the NetWorker administration program by running **nsradmin**. Use the **help** command for help, or the **visual** command to enter full-screen mode.
2. Type the following:

```
nsradmin> create type:NSR Hypervisor;name:vCenter_FQDN_or_IP
nsradmin> vi
Select type: NSR hypervisor;
name: esx3-vc1.lss.emc.com;
comment: ;
service: [VMware VirtualCenter];
endpoint: "https://esx3-vc1.lss.emc.com/sdk";
username: "ajayads\\nemo";  ======================> vCenter
info
password: *******;
command: nsrvim;
proxy: nemo220-3.lss.emc.com;  ============> NW Server
```

Creating a NetWorker client for the VADP Proxy host by using the Client properties windows

About this task

Table 16 Application information values

Attribute name	Description	Default value
VADP_HYPERVISOR This attribute is mandatory.	Specify the hostname of the VC server configured as part of the NSR Hypervisor resource. If there are multiple VC servers configured as part of the NSR hypervisor resource, specify their hostnames here. For example: *VADP_HYPERVISOR=any.vc* *VADP_HYPERVISOR=another.vc*	
VADP_TRANSPORT_MODE	Specify the transport mode to transfer data from a VMFS data store to a VADP proxy server. The following options are supported: • SAN – Virtual disk data is read directly off a shared storage device that the virtual disk resides on. This requires VMFS storage on SAN or iSCSI and the storage device has to	Blank. If left blank, the default values are selected in the order of the description list. You can specify multiple modes by inserting a pipe (|) symbol between each value as shown in the following example: *VADP_TRANSPORT_MODE=*

Table 16 Application information values (continued)

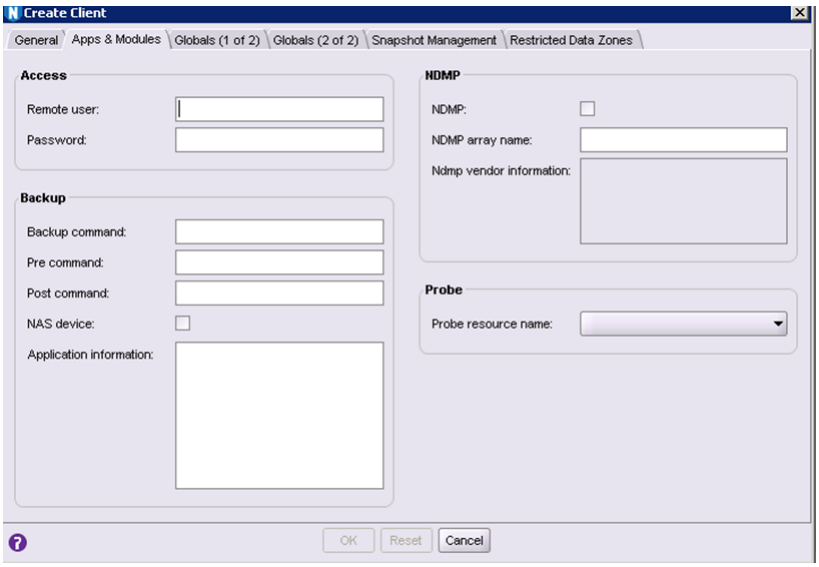
Attribute name	Description	Default value
	be accessible from both ESX and the VADP proxy. • Hotadd – This mode can be used when VADP is used in a virtual proxy. Because it uses the ESX I/O stack to move data, Hotadd is more efficient than the transport mode NBD. • NBDSSL – This mode is the same as nbd except that the data transferred over the network is encrypted. The data transfer in nbdssl mode can be slower and use more CPU than in the nbd transport mode. • NBD – VADP will use an over-the-network protocol to access the virtual disk. Data is read from the storage device by the ESX host and then sent across an unencrypted network channel to the VADP proxy. Please note that this mode does not provide the offload capabilities of the san mode (because data is still transferred from the ESX host across the network). However, nbd does not require shared storage and also enables VADP to be run inside a VM.	*san* / *Hotadd* / *nbdssl* / *nbd*. The order in which modes are specified dictate the priority in which they are attempted. In the above example, the san mode is attempted first; if that fails the Hotadd mode is attempted, and so on.

Procedure

1. In the NMC **NetWorker Administration Protection** window, right-click **Clients**, and select **New**.

   The **Create Client** dialog box displays.
2. Select the **General** tab.
3. In the **Name attribute** field, type the name of the proxy.
4. Select the **Apps and Modules** tab, shown in the following figure.

Figure 90 Apps and Modules tab in NMC



5. In the **Application Information** field, type the following:

```
VADP_HYPERVISOR=any.vc
VADP_HYPERVISOR=another.vc
VADP_BACKUPROOT=G:\mnt
VADP_TRANSPORT_MODE=Hotadd
```

6. Click **OK**.

Creating a VADP User role in vCenter

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

Creating a VADP Proxy role

About this task

The section Minimum vCenter permissions needed to recover using VADP on page 224 provides more information.

Procedure

1. Log in to the vCenter Server with Administrator privileges using vSphere Client.
2. From the vCenter Server, select **View** > **Administration** > **Roles**.
3. Click **Add Role**.
4. Name the role **VADP User**.
5. Assign the required permissions to the **VADP User** role and click **OK**.

Assigning the VADP User role to the user specified in the NetWorker Hypervisor resource

About this task

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

VMware documentation can be found at http://www.vmware.com/support/pubs/

Procedure

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

Minimum vCenter permissions needed to recover using VADP

It is recommended to create a single VADP User role with the recovery privileges specified in the following tables. You can then use the associated user for VADP recovery operations.

The following table provides VADP recovery privileges.

Table 17 VADP recovery privileges

Setting	Privileges
Global	• Cancel task • Licenses • Log Event • Settings
Resource	• Assign virtual machine to resource pool
Datastore	• Allocate space • Browse datastore • Low level file operations • Remove file • Update virtual machine files (only found in 4.1 and later)
Virtual machine > Inventory	• Create new • Register • Remove • Unregister

Table 17 VADP recovery privileges (continued)

Setting	Privileges
Virtual machine > Configuration	• Add existing disk • Add new disk • Add or Remove device • Advanced • Change CPU count • Change Resource • Disk change Tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility
Virtual machine > Interaction	• Power Off • Power On • Reset
Virtual machine > Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download
Virtual machine > State	• Create snapshot • Remove snapshot • Revert to snapshot
Network	• Assign network • Configure
Session	• Validate session
Tasks	• Create task

Table 17 VADP recovery privileges (continued)

Setting	Privileges
	• Update task

Recovering VADP Backups

This section covers these topics:

- File based recovery of a VM on page 226
- Image level (single step) recovery of a full VM on page 228

File based recovery of a VM

File-level recovery (FLR) is supported only on VMs that have a Windows operating system with the NTFS file system. FLR is not supported in the following configurations:

- Windows 8 and Windows Server 2012 VMs with Resilient File System (ReFS)
- VM operating system containing GPT or dynamic disks
- VM operating system containing uninitialized disks
- VM operating system containing unformatted partitions
- VM operating system containing partitions without drive letters
- VM configuration with Virtual IDE Disk Devices (only SCSI)
- VM configuration with independent disk mode

Performing a file based recovery on the local host

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

About this task

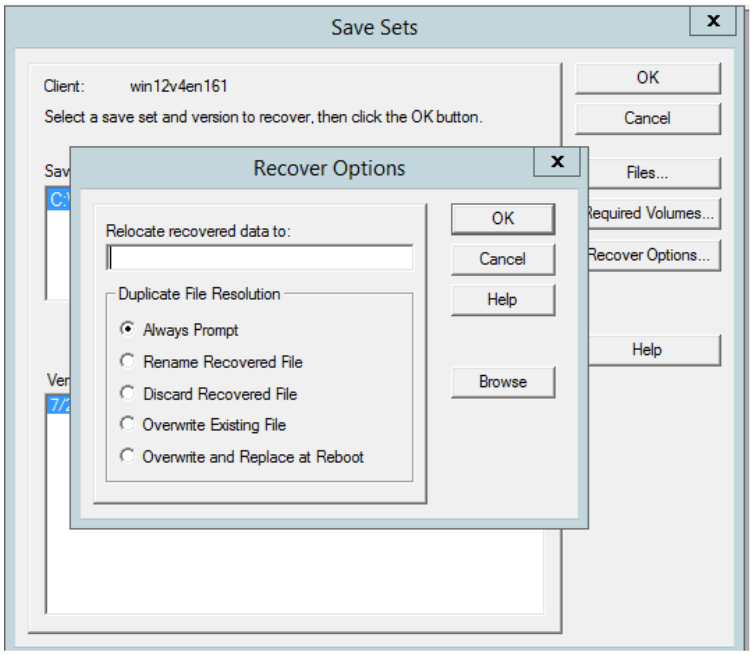
To perform a file based recovery on the local host:

Procedure

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

   If you click OK without specifying a restore path in the Recover Options dialog, a warning message displays, indicating that restoring data to the proxy storage node from the VM image can result in overwriting system files. To ensure overwriting of files does not occur, enter a restore path prior to clicking OK.

Figure 91 Recover Options dialog



Performing a file based recovery using CIFS share

Before you begin

Ensure that the remote access list of the VM client includes either user@server or user@proxy and that you add the proxies to the DD Boost access list. To add a client to the DDBoost access list, run the following command from the DDBoost command line:

```
 ddboost access add clients (- Add clients to a DD Boost access
list)
ddboost access add clients client-list
```

Procedure

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

Performing a file based recovery using directed recovery

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

About this task

Procedure

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

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

2. Select the VM client as the source client.
3. Select the target client as VM-client.
4. Select a destination folder.
5. Follow the procedure in the NetWorker Administration Guide's Recovery chapter to select files for recovery and perform the recovery.

Image level (single step) recovery of a full VM

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

- Performing an image level recovery from the NetWorker User program on page 229
- Performing an image level recovery from the command line on page 230

Recommendations and considerations

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

- For a remote VADP proxy client, image level recovery requires the members of the VADP proxy client's administrator group to be part of the remote access list of the VM clients or the member should have the "Remote access all clients" privilege.
- The user must have VMware privileges to register or create VMs.
- Recovery of the full VM is only supported using save set recovery.
- Only level FULL of FULLVM save sets are supported for VM image recovery.
- The VADP proxy system must be running one of the following:
  - Microsoft Windows 2008 R2
  - Microsoft Windows 2012
- If any hardware level changes such as a new disk partition, are made to the VM, you must perform a level full backup before you can perform an image level recovery of the full VM.
- The VM can recover to the same VMware ESX server or VMware vCenter (VC) taken at the time of backup or to a different ESX or VC. Recovery to different resource pools and different datastores are also supported. A different datastore can be specified for each disk and a configuration datastore can be specified to restore the configuration files.
- During the recovery of a full VM (FULLVM save set), the recovered VM will start in forceful powered off state because of a VADP snapshot limitation.
- For non-Windows VMs: If using traditional NetWorker client-based backups along with VADP image based backups for the same VM client, ensure that the browse policy for the client-based backups does not exceed the frequency of VADP image based backups. This practice is recommended because the indices of client-based backups may have to be removed prior to image-level recovery.
  For example, a Linux client has a schedule of daily level FULL client-based backups along with monthly VADP image based backups. In this case, it is recommended to set the browse policy of the client-based backups to a maximum of 1 month.
- If the image level backup of the VM being recovered was performed with the Encryption directive, the current Datazone pass phrase by default is automatically

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

Performing an image level recovery from the NetWorker User program

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

About this task

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

Procedure

1. Launch the **NetWorker User** program on the NetWorker client or VADP proxy.
2. From the **Operation** menu, select **Save Set Recover**.
3. In the **Source Client** dialog box, select the VM client from where the save set originated and click **OK**.
4. In the **Save Sets** dialog box, select the Save Set name for the full VM backup client (FULLVM) and select a level **FULL** backup. Click **OK**.

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

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

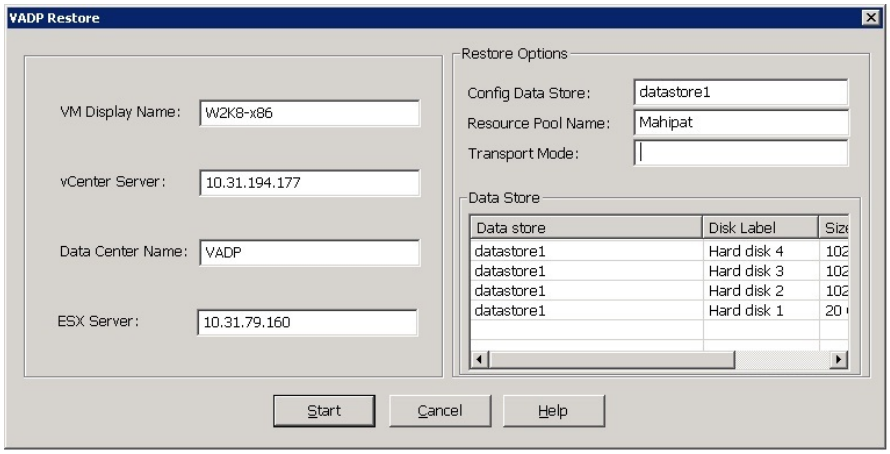
   Restore to VMware vCenter (VC):

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

Results

The following figure depicts a VADP Restore dialog box that is set up for a VMware vCenter restore.

Figure 92 VMware vCenter restore



Performing an image level recovery from the command line

The following describes how to perform a command line recover of a full VM to the VMware ESX server or VMware vCenter (VC) server.

About this task

Procedure

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

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

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

2. Recover the full VM using the **recover** command, for example:

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

   where

   - *ssid* is the save set identifier of the FULLVM.
   - *staging-location* is the staging location path to recover the FULLVM image to the proxy. This value is needed only for a recovery to staging location and applies only to backups taken before NetWorker 7.6 SP2.
   - *VC hostname* is the VMware VC name that is used to perform the restore.
   - *port* is the port used to log in to the web server of the VC host. If no value is entered, the default port number is used.
   - *transport mode* is the transport mode to use for recovery. For example,SAN.
   - *datacenter name* is the data center name where the VM is restored to.
   - r*esource pool name* is the resource pool that the restored VM is connected to.
   - *ESX hostname* is the VMware ESX server machine name where the VMware VM needs to be restored.

- *datastores* is the list of datastores that need to be associated with the configuration and the disks of the VM that is being restored. They are name / value pairs separated with hash (#) symbols. For example:

```
VADP:datastore=”config=stor1#disk1=stor2#disk2=stor3”
```

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

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

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

If your VMs have a mix of both VADP image level backups and traditional guest based (also known as client based) backups, you may have to use the following recovery procedure.

Unable to browse guest based backups on non NTFS file systems

Traditional guest based (client based) backups are not browsable in the recovery GUI for VMs that are running a non NTFS file system and that have a mix of VADP and guest based backups. This issue does not apply to Windows VMs that are using NTFS. Additionally, save set recoveries are not affected and can be performed in the usual way.

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

To find the backup time:

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

To perform the recovery:

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

Example

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

```
C:\mminfo -av -s jupiter -q "client=mars"
volume type client date time size ssid fl lvl name
kuma-1 Data Domain mars 5/24/2011 10:38:39 PM 281 MB 1658578527 cb
full /root
kuma-1.RO Data Domain mars 5/24/2011 10:38:39 PM 281 MB 1658578527 cb
full /root
kuma-6 Data Domain mars 5/24/2011 10:59:22 PM 5243 MB 1440475890 cb
```

```
full FULLVM
kuma-6.RO Data Domain mars 5/24/2011 10:59:22 PM 5243 MB 1440475890
cb full FULLVM
C:\recover -t "5/24/2011 10:38:39 PM" -s jupiter -c mars
```

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

Image level recovery to a different FARM or vCenter

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

Recovering a VM using SAN or Hotadd transport mode on Windows 2008

About this task

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

Procedure

1. Open a command prompt on the proxy host.
2. Run the following command:

   ```
   DISKPART
   ```

3. Enter **SAN** and check for the SAN policy.
4. If the policy indicates **offline**, enable the policy by entering the following:

   ```
   SAN POLICY=OnlineALL
   ```

   Note: After the recovery is successful, **SAN POLICY** can be changed back to the default value (SAN POLICY=offline or SAN POLICY=offlineshared).

5. Restart the proxy for the change to take effect.

Results

You can now initiate the VM recovery using SAN or Hotadd mode.

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

VADP Planning and Best Practices

This section covers topics related to best practices when using VADP.

Recommendations and considerations for VADP recovery

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

- Ensure that VC and ESX/ESXi are updated to the latest released update.
- VADP supports recovery via VMware VirtualCenter or vCenter. The section Software and hardware requirements on page 218 provides more information on supported vCenter versions.

  Note: Recovery directly to a standalone ESX/ESXi host is not supported. The ESX/ESXi must be connected to either VirtualCenter or vCenter.
- VADP does not support IPv6. Instructions for disabling IPv6 and using IPv4 are provided in the section Network and Firewall port requirements on page 235.
- It is recommended to keep the vCenter and VADP proxy as separate machines to avoid contention of CPU and memory resources.
- The vSphere Client does not need to be installed on the NetWorker server.
- Ensure the path specified in VixDisklib and VixMountAPI config files are enclosed in double quotes as below:

  ```
  tempDirectory="C:\Program Files\EMC NetWorker\nsr\plugins\VDDK
  \tmp"
  ```

  These files are stored in the following location by default:

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

  Note: Double quotes should be specified in the path even though the path is already present.
- It is recommended to use the VADP proxy host as the storage node. This provides the optimal configuration for any given transport mode as data transfer occurs directly from the ESX/ESXi datastore to the storage node.
- If reattaching RDM disks after recovery, make note of all LUNs that are zoned to the protected VMs.

Selection of physical vs. virtual proxy

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

Proxy node sizing and performance considerations

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

Note that there are no observed performance differences between physical and virtual proxies when running on similar hardware.

- The maximum number of concurrent sessions when using a physical proxy is higher than that of a virtual proxy. The section Recommendations and considerations for transport modes on page 237 provides more information on concurrent sessions for specific transport modes.

- Recommendations for a physical proxy is 4 CPU cores with 8GB of RAM. Recommendations for a virtual proxy is 4 vCPUs and 8GB vRAM per proxy, where each vCPU is equal to or greater than 2.66 GHz.
- Number of virtual proxies per ESX host depends only on the type of hardware on which the ESX has been installed.
- For lower-end ESX hosts, it is recommended not to mix I/O load on ESX (with the virtual proxy and VMs residing on a single ESX), but to have a separate ESX for the virtual proxy.
- For high-end ESX hosts, it is recommended to have a maximum of 5 virtual proxies concurrently running on a single ESX host.

Recommendations for Data Domain systems

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

- When using DD VTLs, SAN transport mode is required; as a result, the proxy host cannot be a virtual machine.
- For DD Boost enabled VADP backups:
  - The best CPU load and performance is observed with 4 concurrent backups per device. However, a NetWorker 8.x DD Boost library supports a greater number of concurrent backups (target sessions).
  - Setting a lower number of parallel sessions to a single device does not result in optimal performance.
  - Setting a higher number of parallel sessions to a single device increases the CPU load without any improvements to performance.
  - It is recommended to have at least 400MB to 500MB of RAM for each virtual machine being backed up if small to medium sized virtual machines are in use (virtual machines with less than 100GB virtual disks attached). If the largest virtual machine being backed up has more than 100GB of virtual disks attached, the RAM can be further increased.
- Better throughput is observed with DD Boost when there is less commonality between the virtual machines being backed up. As a best practice, it is recommended that virtual machines related to the same parent virtual machine template/clone should be part of different backup groups, and these backup groups should have different start times.
- In the case of both Hotadd and SAN modes, a 20-40% improvement is observed in the backup throughput for every additional proxy, provided the back-end storage where the virtual machines reside is not a bottleneck.
- If using Hotadd mode:
  - Refer to the section Recommendations and considerations for transport modes on page 237 for memory requirements. These requirements may increase depending on the size of the virtual machine's virtual disks, as described in the RAM recommendation above.
  - Virtual proxy parallelism should not be set to a value greater than 12. This limit can further be decreased if the virtual machines have more than one disk attached. More information related to best practices when using Hotadd mode is provided in the section Recommendations and considerations for transport modes on page 237.

- In the case of multiple virtual proxies, it is recommended to consolidate all virtual proxies under dedicated ESX/ESXi host(s) in the environment to minimize the impact on production VMs during the backup window. These ESX/ESXi hosts should not be running any other VMs.
- A maximum of 5 virtual proxies per one standalone ESX is recommended.
- A maximum of 3 virtual proxies per ESX is recommended in a DRS cluster for proxies.

Network and Firewall port requirements

Be aware of the following firewall and network requirements:

- If there is a firewall between the VADP proxy host and the servers that run VMs that you plan to back up from the VADP proxy host, ensure that bi-directional TCP/IP connections can be established on port 902 between the VADP proxy host and the servers.
- If the Virtual Center or vCenter server uses a port other than the default port of 443, specify the port in the endpoint attribute of NSRhypervisor field. Configuring the VADP proxy host and Hypervisor resource on page 220 provides more information.
- VADP does not support IPv6. If vCenter is installed in a Windows 2008 system with IPv6 enabled (IPv6 is enabled by default) and the same system is also used as the VADP proxy, VADP backups will hang.
  Ensure that IPv6 is disabled on the following:
  - vCenter
  - ESX/ESXi
  - VADP-Proxy

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

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

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

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

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

Support for tape drives in a virtual machine

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

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

The following section requires a working knowledge of VMware vSphere ESX/ESXi and virtual machine configuration.

VMDirectPath requirements and recommendations

The following requirements and recommendations apply when using VMDirectPath:

- VMDirectPath requires Intel Virtualization Technology for Directed I/O (VT-d) or AMD IP Virtualization Technology (IOMMU). You may need to enable this option in the BIOS of the ESX/ESXi system.
- The VM should be Hardware version 7. For example, vmx-07.
- The optimal VMDirectPath PCI/PCIe devices per ESX/ESXi host is 8.
- The optimal VMDirectPath PCI/PCIe devices per VM is 4.

VMDirectPath restrictions

The following restrictions apply during the configuration of VMDirectPath:

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

The VMware knowledge base article http://kb.vmware.com/kb/1010789 provides information on configuring VMDirectPath.

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

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

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

The following technical note provides additional information on VMDirectPath:

http://www.vmware.com/pdf/vsp_4_vmdirectpath_host.pdf

Considerations for VMDirectPath with NetWorker

The following are considerations apply when using VMDirectPath with NetWorker:

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

- If other VMs that reside on the same ESX/ESXi are sharing the underlying hardware (physical CPU), it may be required to add more vCPU and dedicating underlying hardware by using CPU affinity settings.
- To achieve optimal performance, it is recommended that the guest VM acting as the DSN has a minimum of 4 GB of memory available with 2 vCPUs allocated.
- If multiple target sessions are needed in each device and 4 or more vCPUs are assigned to the VM, ensure that there are enough devices available for backup operations. An insufficient amount of devices can result in less throughput due to CPU scheduling overhead of the Hypervisor.
- Ensure that the device drivers for the HBA are updated on the guest operating system.

Recommendations and considerations for transport modes

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

SAN transport mode considerations

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

- Prior to connecting the VADP proxy host to the SAN fabric, perform the steps in the section Diskpart utility for SAN and Hotadd transport modes on page 240.
- Memory usage per DD BOOST device should be approximately 500 MB.

Hotadd transport mode considerations

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

- Prior to running VADP backups using the virtual proxy host, perform the steps in the section Diskpart utility for SAN and Hotadd transport modes on page 240.
- A minimum of 4 vCPUs must be allocated per virtual proxy, with 8GB vRAM per proxy and each vCPU equal to or greater than 2.66 GHz.
- Memory usage per DD BOOST device should be approximately 300MB.
- The ESX server must be running ESX 3.5 update 4 or later.
- If there are multiple virtual proxies, it is recommended to host all the virtual proxies in a dedicated ESX/ESXi server. This would keep the virtual proxy resource consumption of CPU and memory isolated within that ESX/ESXi environment without impacting the production VMs.
- VMs having IDE virtual disks are not supported for Hotadd mode. Instead, nbd mode is recommended for these.
- The VM to restore and the VM where the restore is initiated must reside in the same VMware datacenter.
- The virtual proxy might fail to unmount Hotadd disks. In such cases, you must manually unmount the Hotadd disks from the virtual proxy. If any of the client VM disks are still attached to the virtual proxy, perform the following:

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

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

NBD/NBDSSL transport mode considerations

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

- You can only run a concurrent backup of 20 virtual disks against a given ESX/ESXi. The limit refers to the maximum number of virtual disks and is per ESX/ESXi host, irrespective of the number of proxies being used in the environment.
  Due to this limitation, it is recommended to apply the following best practices:
  - If the ESX is not part of a VMware cluster or is part of a DRS-disabled VMware cluster, then apply one of the following:
    - When using a single proxy to backup a given ESX via NBD/NBDSSL, set the client parallelism of the VADP proxy Client resource such that the limit of 20 concurrent disk connections per ESX host is not exceeded.
    - When using multiple proxies to backup a given ESX via NBD/NBDSSL, then the client parallelism on each VADP proxy should be calibrated such that the total concurrent disk connections per ESX host does not exceed 20.
  - If ESX is part of a DRS-enabled VMware cluster, then apply one of the following best practices:
    - When using a single proxy to backup via NBD/NBDSSL, set the client parallelism of the VADP proxy Client resource such that the limit of 20 concurrent disk connections per cluster is not exceeded.
    - When using multiple proxies to backup via NBD/NBDSSL, then the client parallelism on each VADP proxy should be calibrated such that the total concurrent disk connections per cluster does not exceed 20.

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

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

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

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

Use one of the following best practices:

- Set the client parallelism of the proxy to 8.
- Create a single backup group containing all 11 VMs from the given ESX and set the group parallelism to 8.

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

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

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

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

Use one of the following best practices:

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

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

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

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

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

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

Use one of the following best practices:

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

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

VADP proxy access to LUNs

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

SAN transport mode

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

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

Hotadd transport mode

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

NBD/NBDSSL transport modes

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

Diskpart utility for SAN and Hotadd transport modes

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

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

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

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

APPENDIX A

Backup and recovery of the vCenter server

This appendix describes how to protect the vCenter server Appliance (VCSA) and the Platform Services Controllers (PSC). It is intended for virtual administrators who utilize the distributed model of the vCenter server and require protection of the complete vCenter server infrastructure.

- vCenter deployments overview 242
- Best practices for backup and restore 242
- Protecting an embedded PSC 243
- Protecting external deployment models 244
- vCenter server restore workflow 248
- Platform Services Controller restore workfow 249
- Additional considerations 249
- Command reference 250
- Shutting Down VBA 250

vCenter deployments overview

You can protect vCenter 6.5 deployments with NetWorker by using the vProxy appliance. The instructions in this section assume that the vCenter server and the Platform Services Controller (PSC) are deployed as virtual machines.

For the restores to complete successfully:

- Ensure that these virtual machines use a fully qualified domain name (FQDN) with correct DNS resolution, or
- Ensure that the host name of the machine is configured as an IP address. Note that if the host name is configured as an IP address, the IP address cannot be changed.

There are mainly two types of vCenter deployments:

- vCenter server Appliance/Windows Virtual Machine with an embedded PSC.
- vCenter server (also multiple) Appliance/Windows virtual machine with an external PSC. This type has two sub categories:
  - vCenter server environment with a single external PSC.
  - vCenter server environment with multiple PSC instances: This environment contains multiple vCenter server instances registered with different external PSC instances that replicate their data.

Best practices for backup and restore

Review the following recommendations and best practices when planning a vCenter virtual machine or its component virtual machine(s) backup.

Note: Backups will not save Distributed switch configurations.

- It is recommended to schedule the backup of the vCenter server when the load on the vCenter server is low, such as during off-hours, to minimize the impact of vCenter virtual machine snapshot creation and snapshot commit processing overhead.
- Ensure that there are no underlying storage problems that might result in long stun times.
- Keep the vCenter virtual machine and all of its component virtual machines in one single isolated protection policy. The protection policy should not be shared with any other virtual machines. This is to ensure that the backup times of all vCenter Server component virtual machines are as close to each other as possible.
- Ensure that the backup start time of the vCenter Server does not overlap with any operations for other protected virtual machines being managed by this vCenter so that there is no impact on other protected virtual machines during snapshot creation and snapshot commit of the vCenter virtual machine.
- If the vCenter Server and Platform Services Controller instances fail at the same time, you must first restore the Platform Services Controller and then the vCenter Server instances.

Protecting an embedded PSC

The following section describes backup and recovery options for protecting an embedded PSC.

Backup

You can perform a backup of an embedded PSC by using the following guidelines.

1. Create a policy, and then add the vCenter virtual machine (VC VM) group to the policy.
2. Select the full virtual machine and not individual disks.
3. Run the scheduled or on-demand (ad-hoc) policy.

Recovery

Depending on the type of failure, you can perform the virtual machine recovery by using one of the following methods.

- Restore to original (Revert a virtual machine) — This method is valid only when the vCenter Server Appliance (VCSA) is intact and running, but corrupted.
- Recover as a new virtual machine to a managed ESXi server (Virtual Machine Recovery) — Use this method if you have completely lost your VCSA. Note that this vCenter must be registered with NetWorker.
- Emergency recovery to an ESXi server — Emergency recovery will be the main use case, and so the following steps describe how to perform the restore using the Emergency Recovery option.

Restore an embedded PSC with Emergency Recovery

Use the following steps to restore an embedded PSC using the Emergency Recovery option in the NetWorker Management Console.

Before you begin

Emergency Recovery requires you to set up a vProxy on the ESXi host prior to running the recovery. Ensure that there is one healthy ESXi host available for the emergency recovery, and that this host has a vProxy appliance registered to NetWorker.

Additionally, ensure that you disconnect the ESXi host from the vCenter server.

Note: There is no post-restore operation to be performed for embedded installs.

Procedure

1. In the NMC **NetWorker Administration Recover** window, select **Recover** > **New** from the main menu.

   The **Recover Configuration** wizard opens on the **Select the Recovery Type** page. **Virtual Machine Recovery** is the second option displayed in the **Recovery Type** pane.

2. In the **Select the Recovery Type** page, select **Virtual Machine Recovery**, and then select a vCenter server to recover from using the Source vCenter server drop-down. Click **Next**.
3. In the **Select the Virtual Machine to Recover** page, enter the name of the source virtual machine(s) to recover from, or perform a search for the virtual machine. Additionally, you can use the tabs on this page to choose a single virtual machine or multiple virtual machines from a selected backup, or browse

the source vCenter to determine the required virtual machine source. After selecting the desired virtual machine(s), click **Next**.

4. In the **Select the Target Backups** page, select the virtual machine backup(s) you want to restore from the **Available Backups** pane. This pane lists both primary backups and, if available, clone copies. If you selected recovery from multiple virtual machines, you can switch between virtual machines to browse each machine's available backups by using the Virtual Machine Name drop-down. Click **Next**.
5. In the **Select the Virtual Machine Recovery method** page, select **Emergency recovery**, and then click **Next**.
6. In the **Configure the Emergency Recovery** page, specify the target ESXi server in the vCenter environment, and then click **Connect**. The **Proxy Selection** and **Recovery Data** panes get populated with the ESXi server details
7. In the **Proxy Selection** pane, if a proxy is not discovered, add a new proxy which is deployed in vCenter but not added to NetWorker.
8. For the disks in the **Recovery Data** pane, select a datastore, and then optionally, select the **Power on virtual machine** and **Reconnect to network** options. Click **Next**.
9. In the **Select Alternate Recovery Sources** page, select the original disk backup or select a clone copy if one is available. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the staging pool. Click **Next**.
10. In the **Perform the Recovery** page, specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct, and then click **Run Recovery**.
11. After the recovery operation, wait until the virtual machine restarts, and then log into the vCenter Server Appliance shell as `root`
12. Verify that all PSC and vCenter services are running.
    - For an appliance, run the `service-control --status --all` command in the appliance shell.
    - For a vCenter installed on Windows, from the Windows Start menu, select **Control Panel** > **Administrative Tools** > **Services**.

After you finish

During an Emergency Recovery, the vProxy gets associated with the ESXi host and is unavailable for other operations on the vCenter server. Wait until the recovery completes before initiating any other operations on the vProxy.

Protecting external deployment models

Review the backup and recovery options for protecting external deployments.

Backup

You can perform a backup by using the following guidelines:

1. Create one lifecycle group and add the vCenter virtual machine and PSC virtual machine to the group. This will ensure that snapshots are taken at the same time.
2. Ensure that you select the full virtual machine and not individual disks.
3. Run the scheduled or on-demand (ad-hoc) policy.

Note: Ensure that you back up all vCenter server and PSC instances at the same time

Recovery

Depending on the failure, you can perform virtual machine recovery by using one of the following methods:

- Restore to original — This method is valid only when the VCSA is intact and running, but corrupted.
- Recover as a new virtual machine to a managed ESXi server: Use this method of you have completely lost your VCSA. Note that this vCenter must be registered with NetWorker.
- Emergency recovery to an ESXi server. For Emergency recovery, perform the steps specified in the section Restore an embedded PSC with Emergency Recovery.

Note: In the event of a complete environment failure, PSC should be restored first, followed by the vCenter server restore.

The following scenarios provide specific instructions based on the number of vCenter server appliances and external PSCs in the environment and the extent of the failure.

vCenter server appliance(s) with one external PSC where PSC fails

Procedure

1. Perform an image-level recovery of the PSC by using one of the methods indicated above, and then power ON the virtual machine.
2. Verify that all PSC services are running.
   - For a PSC deployed as an appliance, run the `service-control --status --all` command in the appliance shell.
   - For a PSC installed on Windows, from the Windows Start menu, select **Control Panel** > **Administrative Tools** > **Services**.
3. Log into the vCenter server appliance shell as `root`.
4. Verify that no vCenter services are running, or stop any vCenter services that are running by typing `service-control --stop`.
5. Run the vc-restore script to restore the vCenter virtual machines.
   - For a vCenter server appliance, type `vcenter-restore -u` ***`psc_administrator_username`*** `-p` ***`psc_administrator_password`***
   - For a vCenter Server installed on Windows, go to `C:\Program Files \VMware\vCenter Server\`, and then run `vcenter-restore -u` ***`psc_administrator_username`*** `-p` ***`psc_administrator_password`***

   where *psc_administrator_username* is the vCenter Single Sign-On administrator user name, which must be in UPN format.
6. Verify that all vCenter services are running and the vCenter Server is started, as specified in step two.
7. Perform a log in test to the vCenter Server.

   If the restore was successful, the login completes successfully.

vCenter server appliance is lost but the PSC remains

Procedure

1. Perform an image-level recovery of the lost vCenter server by using one of the following methods, and then power ON.
   - Restore to original — This method is valid only when the VCSA is intact and running, but corrupted.
   - Recover as a new virtual machine to a managed ESXi server — Use this method if you have completely lost your VCSA. Note that this vCenter must be registered with NetWorker.
   - Emergency recovery to an ESXi server.
2. After a successful boot, verify that all services are started.
3. Perform a log in test.

vCenter server appliance with multiple PSCs where one PSC is lost, one remains

Procedure

1. Repoint the vCenter instance (insert link) to one of the functional PSC in the same SSO domain.

   Note: Log in to all vCenter servers one by one to determine which vCenter log in fails. This will be the vCenter that requires the repoint steps.

2. Run the following command on the vCenter server appliance:

   ```
   cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
   ```

   Note: The square brackets enclose the command options.

3. Perform a log in test on the vCenter server.
4. Deploy the new PSC and join to an active node in the same SSO and site, replacing lost ones.
5. Repoint the vCenter server to the new PSC.

vCenter server appliance remains but all PSCs fail

About this task

Note: In this scenario, none of the vCenter logins (SSO user) have been successful.

Procedure

1. Restore the most recent PSC backup and wait for the vCenter services to start
2. Log in to the vCenter server appliance's shell as `root`.
3. Verify that no vCenter services are running, or stop vCenter services.
4. Run the `vc-restore` script to restore the VCSA (refer above for detailed steps).

> **Note:** If the login test to any vCenter server appliance fails, then the restored PSC is not the PSC that the vCenter server appliance is pointing to, in which case you may be required to perform a repoint, as described above.

5. Deploy the new PSC and join to an active node in the same SSO domain and site.
6. Repoint vCenter connections as required

vCenter server appliance remains but multiple PSCs fail

Procedure

1. Restore one PSC.
2. Test the vCenter server appliance login. If the login fails, repoint the vCenter server appliance to an active PSC.
3. Deploy the new PSC and join to an active node in the same SSO domain and site.

vCenter server appliance fails

About this task

> **Note:** If a total failure has occurred (all PSCs and all vCenter server appliances failed), restore one PSC first before restoring the vCenter server appliance.

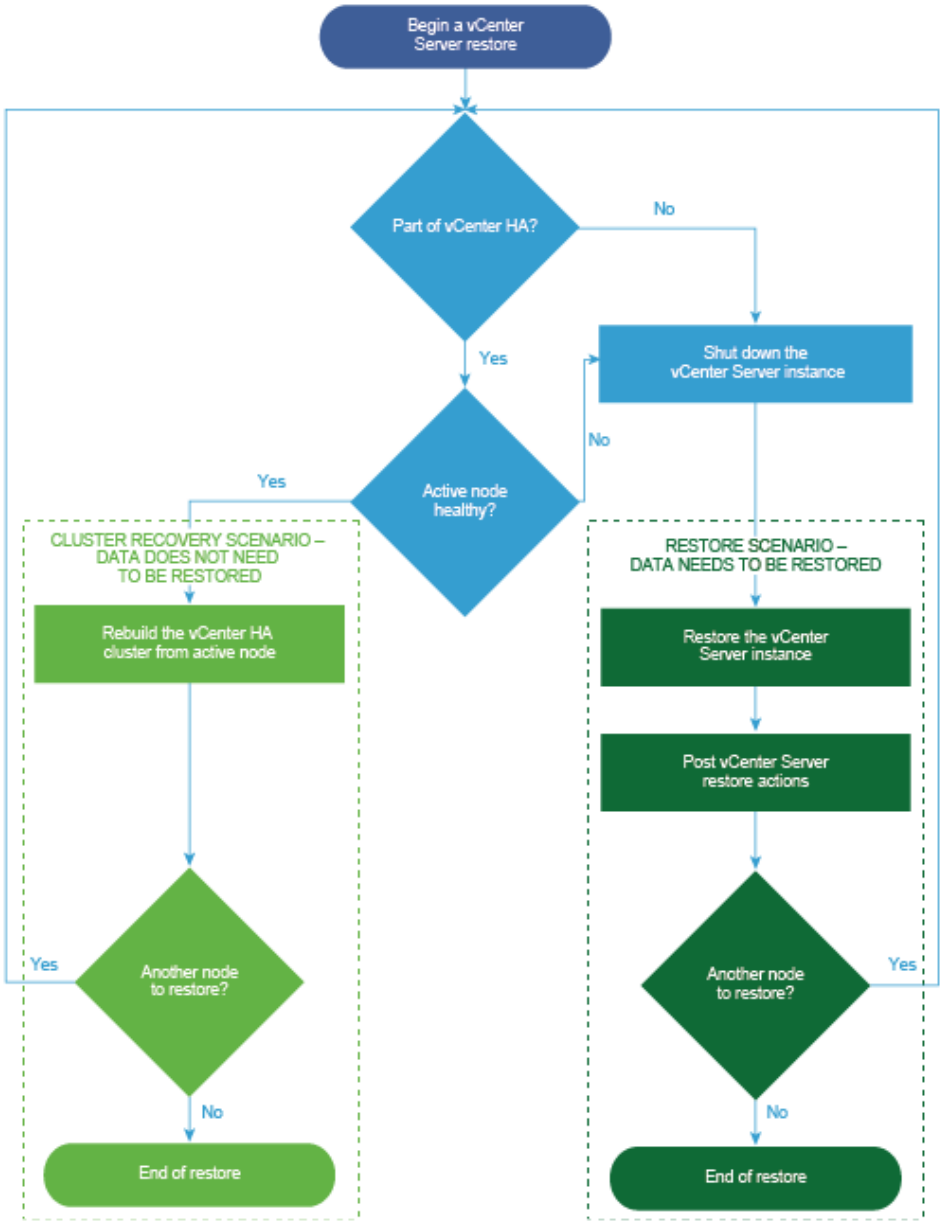
Procedure

1. Perform an image-level restore of the lost vCenter server by using one of the following methods, and then power ON the vCenter.
   - Restore to original — This method is valid only when the vCenter server appliance is intact and running, but corrupted.
   - Recover as a new virtual machine to a managed ESXi server — Use this method if you have completely lost your vCenter server appliance. Note that this vCenter must be registered with NetWorker.
   - Emergency recovery to an ESXi server.
2. After a successful boot, verify that all vCenter services have started.
3. Perform a log in test.
4. If the log in test fails, then this vCenter server appliance is pointing to an inactive PSC. Repoint to an active node.

vCenter server restore workflow

The following diagram shows the restore workflow for a vCenter server.

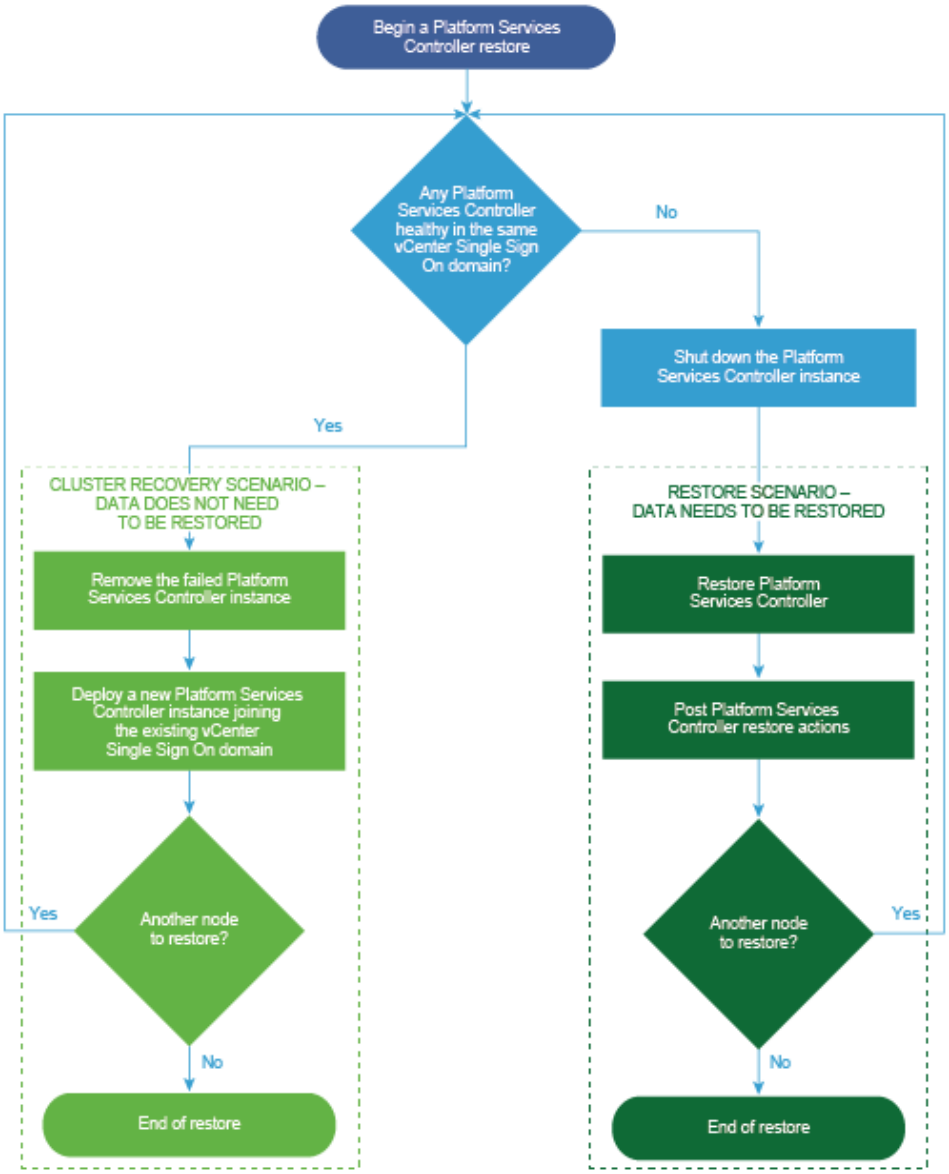
Figure 93 vCenter server restore workflow



Platform Services Controller restore workfow

The following diagram shows the restore workflow for a Platform Services Controller (PSC).

Figure 94 PSC restore workflow



Additional considerations

Review the following additional considerations when backing up and restoring the vCenter server and PSC.

- Backing up the vCenter server will not save the Distributed switch (vDS) configuration as it is stored on the hosts. As a best practice, back up the vDS configuration by using a script that can be used after restoring the virtual center.

- After restoring the PSC, verify that replication has been performed as designed by using the following commands to display the current replication status of a PSC and any of the replication partners of the PSC:
  - For VCSA, go to `/usr/lib/vmware-vmdir/bin` and type **`./vdcrepadmin -f showpartnerstatus -h localhost -u administrator -w Administrator_Password`**
  - For Windows, open a command prompt and type **`cd "%VMWARE_CIS_HOME%"\vmdird\`**
- For the vCenter server or PSC, do not select advanced quiesce-based backup options. Selecting these options will result in application quiescing on virtual machines, which impacts the overall environment due to stunning.

The VMware vCenter server documentation, available at https://docs.vmware.com/en/VMware-vSphere/index.html, provides more information about the vCenter server and PSC.

Command reference

Use the following command to start or stop services in the vCenter server/PSC, or obtain the status:

```
service-control -status/start/stop -all
```

You can use other Replication topology commands, as in the following example.

Example 1 Replication topology command

```
/usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h
localhost -u PSC_Administrator -w password
```

Note: You can replace **`localhost`** with another PSC FQDN to obtain all of the partnerships in the current vSphere domain.

Shutting Down VBA

VBA runs a number of services that manages memory data structures similar to a high transaction rate database. It is important that these data structures are flushed to a disk to ensure the data integrity. You should ensure that the VBA is healthy before the shutdown and also all the data is flushed to a disk.

Procedure

1. Log into the VBA Management page:https:// <VBA_HOSTNAME>:8543/ebr-configure/
2. Review the **Configuration** tab and check the status of the service.

   Note: Some of the services may be down when troubleshooting an existing issue

3. Review the **Rollback** tab and confirm that the latest validated checkpoint is less than 24 hours old.

Note: It is important that the checkpoint is validated, if the latest validated checkpoint is older than 24 hours, you should open a S1 service request with NetWorker support immediately.

4. Log into the VBA via SSH as user admin and take a manual checkpoint by running the command `mccli checkpoint create --override_maintenance_scheduler`
5. Use the `mccli` command to verify that you have successfully created a checkpoint by running: `mccli checkpoint show`

   An output similar to the following displays:

```
Tag Time Validated Deletable
---------------- ---------------------- ---------
---------
cp.20130206170045 2013-02-06 09:00:45 PST Validated Yes
```

6. Use the mccli command to validate the checkpoint: `mccli checkpoint validate --cptag=cp.20130206170045 --override_maintenance_scheduler`

   Note: Validation takes some time to complete. You should continue to check the status by running `mccli checkpoint show`.

7. Stop the services by running the command: `dpnctl stop`

   Alternatively, you can stop the services from VBA Management page, click on **Configuration** tab, and manually stop individual services.

8. You can shutdown the VBA by running the command:

   `root@VBA:~/>: shutdown -h now`

   The VBA may take 10-15 minutes to correctly shutdown. If there are issues during the reboot, a service request should be opened with NetWorker support.

APPENDIX B

NetWorker VMware Protection in VMware Cloud on Amazon Web Services

This appendix includes the following topics:

- Introduction to NetWorker VMware Protection in VMware Cloud on AWS 254
- Prerequisites 254
- Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS 256
- NetWorker VMware Protection for VMware Cloud on AWS best practices 258
- Unsupported NetWorker operations 259

Introduction to NetWorker VMware Protection in VMware Cloud on AWS

NetWorker 18.x supports NetWorker VMware Protection in VMware Cloud on Amazon Web Services (AWS).

Using NetWorker to protect virtual machines running in VMware Cloud on AWS is similar to how you protect the virtual machines in an on-premises datacenter. This appendix provides information on network configuration prerequisites, VMware Cloud on AWS best practices for NetWorker, and NetWorker operations that are currently unsupported for VMware Cloud on AWS

A NetWorker with CloudBoost environment can be useful for storing backups in Amazon S3 cloud object storage, including short term backups for operational recovery and long term retention backups for compliance. This capability is currently available with both in-guest filesystem agents as well as a broad range of application modules for NetWorker. NetWorker vProxy backups are currently not supported with CloudBoost, however cloning of vProxy backups to cloud object storage is supported via the CloudBoost appliance.

Additional information on NetWorker VMware Protection in VMware Cloud on AWS, including setup and configuration instructions, is provided in the whitepaper on https://support.emc.com/products/1095_NetWorker/Documentation/.

Prerequisites

Domain Name System (DNS) resolution is critical for NetWorker deployment and configuration. All infrastructure components should be resolvable through a fully qualified domain name (FQDN). This is especially important for the NetWorker Server, NetWorker vProxy, Data Domain appliance, and CloudBoost appliance. Resolvable means that components are accessible through both forward (A) and reverse (PTR) look-ups.

Review the following prerequisites prior to configuring NetWorker in a VMware Cloud on AWS. Also, ensure that you plan your firewall according to these prerequisites.

VMware Cloud on AWS web portal console

In the VMware Cloud on AWS web portal console, note the following requirements:

- If using NSX-T, configure the DNS to resolve to the internal IP address of the vCenter server. Navigate to **SDDC Management** > **Settings** > **vCenter FQDN** and select the **Private vCenter IP address** so that you can directly access the management network over the built-in firewall. Additionally, ensure that you open TCP port 443 of the vCenter server in both the management gateway and the compute gateway.
- By default, there is no external access to the vCenter Server system in your SDDC (Software Defined Data Center). You can open access to your vCenter Server system by configuring a firewall rule. Set the firewall rule in the compute gateway of VMware Cloud on AWS to enable communication to the vCenter public IP address from the desired logical network of your SDDC. The NetWorker server will not allow you to add the vCenter Server if this firewall rule is not configured in the SDDC.
- The default compute gateway firewall rules prevent all virtual machine traffic from reaching the internet. To allow your NetWorker Server virtual machine to connect

to the internet, you need to create a compute gateway firewall rule to allow outbound traffic on the logical network that your NetWorker Server virtual machine is connected to.

- Configure DNS to allow machines in your SDDC to resolve fully-qualified domain names (FQDNs) to IP addresses belonging to the internet. The NetWorker Server will not allow you to add the vCenter Server using the server's public FQDN or IP address if the DNS server is not configured in your SDDC.
- It is recommended that you deploy the Data Domain system as a virtual appliance in the Amazon VPC (Virtual Private Cloud) of your choice. During the SDDC creation, ensure that you connect your SDDC to an AWS account, and select a VPC and subnet within that account.
- The Data Domain system running in your Amazon VPC must be connected to your VMware SDDC by using the VMware Cloud Elastic Network Interfaces (ENIs), allowing your SDDC and services in the AWS VPC and subnet in your AWS account to communicate without requiring the routing of traffic through the internet gateway. The same ENI channel is recommended for access to Data Domain systems (for the vProxy solution) and access to cloud object storage (for the CloudBoost solution). Detailed steps on configuring ENI are provided by VMware at https://vmc.vmware.com/console/aws-link.
- Ensure that you configure the inbound and outbound firewall rules of your compute gateway for Data Domain connectivity if DDVE is running in your Amazon VPC.

Amazon AWS web portal

In the AWS web portal, note the following requirements:

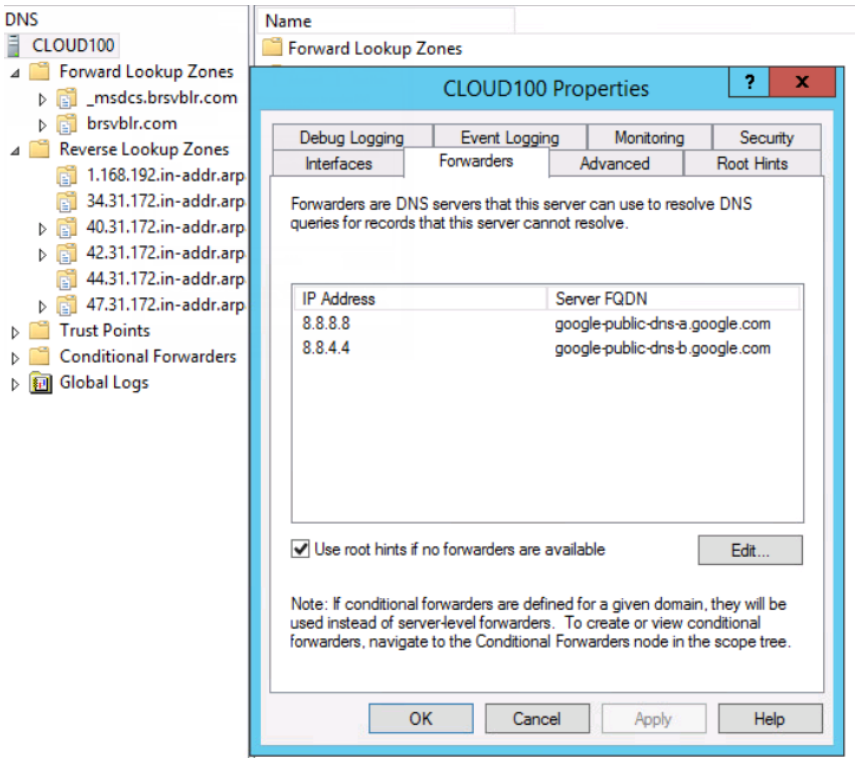
- Configure the inbound and outbound firewall rules of your Amazon VPC security group to provide connectivity between the VMware SDDC compute gateway and Data Domain connectivity if Data Domain is running in your Amazon VPC.
- If cloning from one Data Domain system to another, ensure that you configure the inbound rule for the security group in AWS to allow all traffic from the respective private IPs of Data Domain Virtual Editions running in your Amazon VPC.
- If you have more than one Data Domain running in AWS to perform cloning, then ensure that both Data Domain systems can ping each other using the FQDNs.

vCenter server inventory

In the vCenter Server inventory of your SDDC, note the following requirements:

- An internal DNS name lookup server must be running inside the vCenter inventory. This will be referenced by all the workloads running in the VMware SDDC.
- The internal DNS server must have Forwarders enabled to access the internet. This is required in order to resolve the vCenter Server's public FQDN

Figure 95 Enable internet access for Forwarders



Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS

Perform the following steps to deploy the OVA for the vProxy host from a vCenter server by using the HTML5 **vSphere Web Client**.

Before you begin

Review the Pre-requisites section.

Procedure

1. Log in to the HTML5 **vSphere Web Client** with the cloudadmin account credentials.
2. From the top-left of the window, select **Menu**, and then select **Hosts and Clusters** from the drop-down.
3. In the left inventory pane, expand the vCenter, and then expand the compute resource pool inside your SDDC cluster.
4. Right-click the resource pool where you want to deploy the OVA and select **Deploy OVF template**.
5. On the **Select an OVF template** window, type a URL path to the OVA package, or click **Choose Files** and navigate to the OVA package location, and then click **Next**.
6. On the **Select a name and folder** window, specify a name for the virtual appliance, and the inventory location (for example a virtual machine folder). Click **Next**.
7. On the **Select a compute resource** window, select the vApp or resource pool where you want to deploy the OVA, and then click **Next**.

8. On the **Review details** window, review the product details such as the product name, version, vendor, publisher, and download size, and then click **Next**.
9. On the **License agreements** window, review and accept the EULA, and then click **Next**.
10. On the **Select storage** window, select the disk format and the destination datastore where the virtual appliance files will be stored, and then click **Next**.

    It is recommended that you select **Thick Provision Lazy Zeroed** to ensure that amount of storage space allocated to the virtual appliance is available.
11. On the **Select networks** window, select the **Destination Network**. Provide the IP address in the text box and click **Next**.
12. On the **Customize template** window, expand **Networking properties**, and then specify the following attributes:
    a. In the **Network IP address** field, specify the IP address for the vProxy appliance.
    b. In the **Default gateway** field, specify the IP address of the gateway host.
    c. In the **Network Netmask/Prefix** field, specify the netmask for an IPv4 Network IP address.
    d. In the **DNS** field, specify the IP address of the DNS servers, separated by commas.
    e. In the **FQDN** field, specify the fully qualified domain name of the vProxy appliance.
13. Expand **Timezone settings**, and then perform the following tasks:
    a. in the **Timezone setting** field, select the time zone.
    b. SSH into the vProxy appliance using root credentials and run the following command: `/usr/bin/timedatectl set-timezone new-timezone`.

    Note: To set a time zone outside of the list supported by the vProxy appliance, you need to change the time zone manually.
14. Expand **Password settings**, and then perform the following tasks:
    a. In the **Root password** field, specify a new password for the root account.
    b. In the **Admin password** field, specify a new password for the admin account.

    Note: The passwords for the root and admin account should be between 8 and 20 characters in length. Specifying a new password is mandatory when deploying the vProxy using vCenter, otherwise the vProxy appliance fails to power on. Ensure that you change the default passwords of both the root and admin account during deployment.
15. Click **Next**.

    The **Ready to Complete** window displays.
16. On the **Ready to Complete** window, review the deployment configuration details, and then click **Finish**.

Results

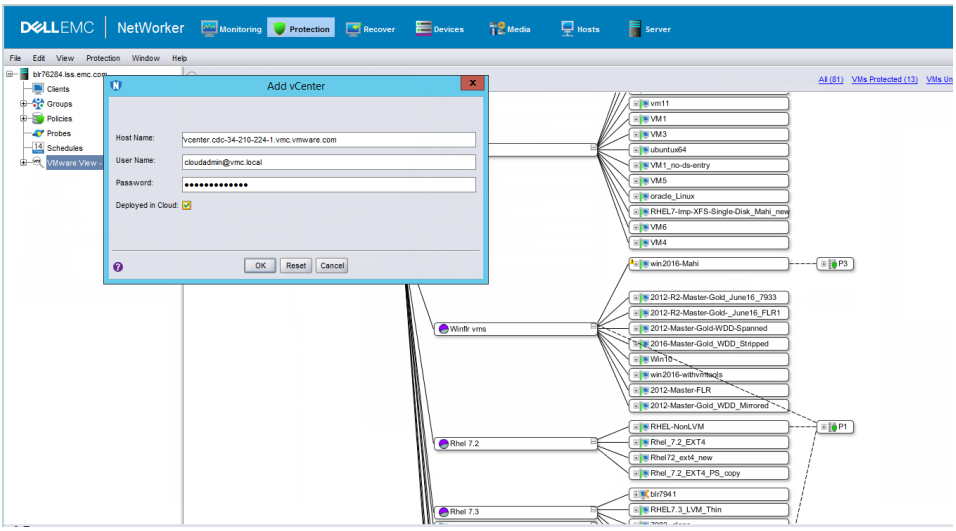
The **Deploying template** task appears in the vCenter and provides status information about the deployment.

NetWorker VMware Protection for VMware Cloud on AWS best practices

Observe the following best practices when using NetWorker to protect virtual machines running in VMware Cloud on AWS:

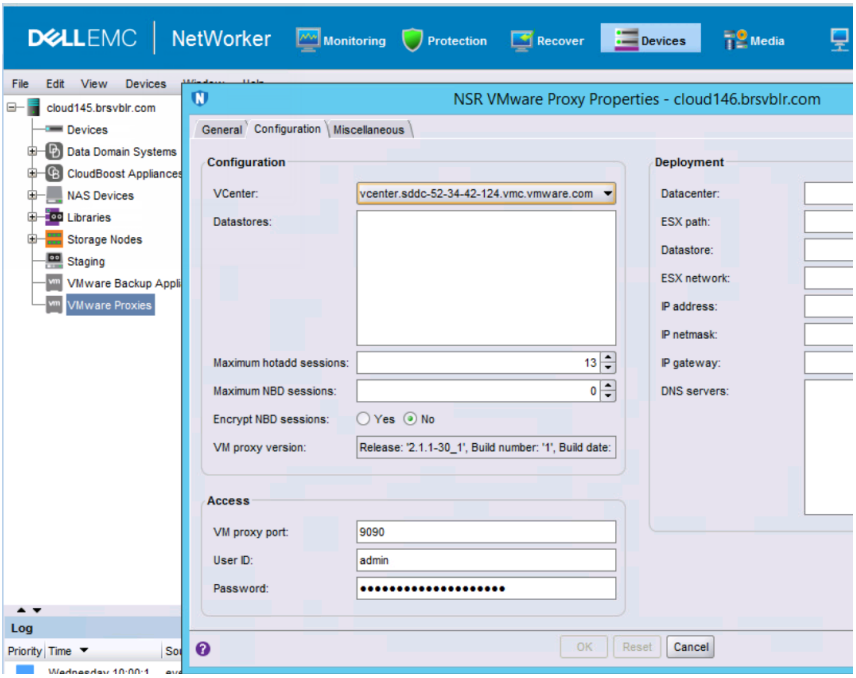
- When deploying or configuring the NetWorker Server or vProxy, ensure that you specify the DNS server IP that points to the internal DNS server running in the vCenter inventory.
- Ensure that both forward and reverse lookup entries in the internal DNS server are in place for all of the required components, such as the NetWorker Server, NetWorker vProxy appliance, Data Domain Virtual Edition (DDVE), and CloudBoost appliance.
- When adding the vCenter Server to NMC's **VMware View**, ensure that you select the **Deployed in Cloud** checkbox. Note that this setting is required for any vCenter Servers running in VMware Cloud on AWS, If you do not select this option, then some NetWorker operations will fail in the VMware Cloud on AWS.

Figure 96 Add a vCenter Server to VMware View with Deployed in Cloud enabled



- Add the vCenter Server to the NetWorker Server using either the public FQDN of the vCenter Server or the public IP address of the vCenter Server. It is recommended to use the FQDN.
- When adding the vCenter Server to the NetWorker Server, specify the login credentials for the cloudadmin user
- When configuring the vProxy in the NetWorker Server, set the **Maximum NBD sessions** for the vProxy to zero. VMware Cloud on AWS does not support NBD transport mode.

Figure 97 NSR VMware Proxy Properties



Unsupported NetWorker operations

NetWorker VMware Protection in VMware Cloud on AWS does not currently support the following operations:

- File-level restore from an image-level backup.
- Instant access recovery of an image-level backup.
- Emergency restore (image-level restore directly to an ESXi host, bypassing the vCenter).
- Image-level backups and restores using NBD or NBDSSL transport mode.
- Application-consistent data protection for MS-SQL with the vProxy appliance.
- If the datacenter is placed inside a folder in the SDDC, image backup and restore is not supported

APPENDIX C

Regular expressions for NetWorker vProxy dynamic policies rule definitions

This appendix includes the following topic:

- Regular expression syntax accepted by dynamic policy rule definition 262

Regular expression syntax accepted by dynamic policy rule definition

Rule definitions for NetWorker vProxy policies with dynamic association enabled can contain regular expressions.

The following tables list the acceptable rules, syntax, and grammar to use when writing such regular expressions.

Types of single-character expressions	Examples
Any character, possibly including newline (s=true)	.
character class	[xyz]
negated character class	[^xyz]
Perl character class	\d
negated Perl character class	\D
ASCII character class	[[:alpha:]]
negated ASCII character class	[[:^alpha:]]
Unicode character class (one-letter name)	\pN
Unicode character class	\p{Greek}
negated Unicode character class (one-letter name)	\PN
negated Unicode character class	\P{Greek}

Composites	
xy	x followed by y
x|y	x or y (prefer x)

Repetitions	
x*	zero or more x, prefer more
x+	one or more x, prefer more
x?	zero or one x, prefer one
x{n,m}	n or n+1 or ... or m x, prefer more
x{n,}	n or more x, prefer more
x{n}	exactly n x
x*?	zero or more x, prefer fewer
x+?	one or more x, prefer fewer
x??	zero or one x, prefer zero
x{n,m}?	n or n+1 or ... or m x, prefer fewer
x{n,}?	n or more x, prefer fewer

Repetitions	
x{n}?	exactly n x

Note: The counting forms x{n,m}, x{n,}, and x{n} reject forms that create a minimum or maximum repetition count above 1000. Unlimited repetitions are not subject to this restriction.

Grouping	
(re)	numbered capturing group (submatch)
(?P<name>re)	named & numbered capturing group (submatch)
(?:re)	non-capturing group
(?flags)	set flags within current group; non-capturing
(?flags:re)	set flags during re; non-capturing

Flags	
i	case-insensitive (default false)
m	multi-line mode: ^ and $ match begin/end line in addition to begin/end text (default false)
s	let . match \n (default false)
U	ungreedy: swap meaning of x* and x*? , x+ and x+? , etc (default false)

Flag syntax is xyz (set) or -xyz (clear) or xy-z (set xy , clear z).

Empty strings	
^	at beginning of text or line (m =true)
$	at end of text (like \z not \Z) or line (m =true)
\A	at beginning of text
\b	at ASCII word boundary (\w on one side and \W , \A , or \z on the other)
\B	not at ASCII word boundary
\z	at end of text

Escape sequences	
\a	bell (≡ \007)
\f	form feed (≡ \014)
\t	horizontal tab (≡ \011)
\n	newline (≡ \012)
\r	carriage return (≡ \015)
\v	vertical tab character (≡ \013)

Escape sequences	
*	literal * , for any punctuation character *
\123	octal character code (up to three digits)
\x7F	hex character code (exactly two digits)
\x{10FFFF}	hex character code
\C	match a single byte even in UTF-8 mode
\Q...\E	literal text ... even if ... has punctuation

Character class elements	
x	single character
A-Z	character range (inclusive)
\d	Perl character class
[:foo:]	ASCII character class foo
\p{Foo}	Unicode character class Foo
\pF	Unicode character class F (one-letter name)

Named character classes as character class elements	
[\d]	digits (≡ \d)
[^\d]	not digits (≡ \D)
[\D]	not digits (≡ \D)
[^\D]	not not digits (≡ \d)
[[:name:]]	named ASCII class inside character class (≡ [:name:])
[^[:name:]]	named ASCII class inside negated character class (≡ [:^name:])
[\p{Name}]	named Unicode property inside character class (≡ \p{Name})
[^\p{Name}]	named Unicode property inside negated character class (≡ \P{Name})

Perl character classes (all ASCII-only)	
\d	digits (≡ [0-9])
\D	not digits (≡ [^0-9])
\s	whitespace (≡ [\t\n\f\r])
\S	not whitespace (≡ [^\t\n\f\r])
\w	word characters (≡ [0-9A-Za-z_])
\W	not word characters (≡ [^0-9A-Za-z_])

ASCII character classes	
[[:alnum:]]	alphanumeric (≡ [0-9A-Za-z])
[[:alpha:]]	alphabetic (≡ [A-Za-z])
[[:ascii:]]	ASCII (≡ [\x00-\x7F])
[[:blank:]]	blank (≡ [\t])
[[:cntrl:]]	control (≡ [\x00-\x1F\x7F])
[[:digit:]]	digits (≡ [0-9])
[[:graph:]]	graphical (≡ [!-~] ≡ [A-Za-z0-9!"#$%&'()* +,\-./:;<=>?@[\\\]^_`{|}~])
[[:lower:]]	lower case (≡ [a-z])
[[:print:]]	printable (≡ [-~] ≡ [[:graph:]])
[[:punct:]]	punctuation (≡ [!-/:-@[-`{-~])
[[:space:]]	whitespace (≡ [\t\n\v\f\r])
[[:upper:]]	upper case (≡ [A-Z])
[[:word:]]	word characters (≡ [0-9A-Za-z_])
[[:xdigit:]]	hex digit (≡ [0-9A-Fa-f])

Unicode character class names--general category	
C	other
Cc	control
Cf	format
Co	private use
Cs	surrogate
L	letter
Ll	lowercase letter
Lm	modifier letter
Lo	other letter
Lt	titlecase letter
Lu	uppercase letter
M	mark
Mc	spacing mark
Me	enclosing mark
Mn	non-spacing mark
N	number
Nd	decimal number
Nl	letter number

Unicode character class names--general category	
No	other number
P	punctuation
Pc	connector punctuation
Pd	dash punctuation
Pe	close punctuation
Pf	final punctuation
Pi	initial punctuation
Po	other punctuation
Ps	open punctuation
S	symbol
Sc	currency symbol
Sk	modifier symbol
Sm	math symbol
So	other symbol
Z	separator
Zl	line separator
Zp	paragraph separator
Zs	space separator

Vim character classes	
\d	digits (≡ [0-9]) VIM
\D	not \d VIM
\w	word character VIM
\W	not \w VIM

APPENDIX D

EMC Backup and Recovery plug-in for Vmware Backup appliance restores

NetWorker 19.1 does not support the VMware Backup appliance (VBA) solution. If you have VBA backups from previous Networker releases, you can recover those backups from the **NetWorker Management Web UI** by using the vProxy, however, the recovery types available in this UI are limited to a **Revert** or **New Virtual Machine** restore. For other recovery types, such as VMDK-level, you can continue to use the **vSphere Web Client EMC Backup and Recovery** user interface.

This appendix includes the following topics:

- FULLVM (Image-level) Restore 268

FULLVM (Image-level) Restore

You can perform an image-level restore of full virtual machines by selecting either of the following options in the **vSphere Web Client EMC Backup and Recovery** user interface:

- Click **Restore Backup** on the **Getting Started** tab.
- Select the **Restore** tab.

When you select the **Restore** tab, available virtual machines for the selected appliance display. Additionally, you can select a different appliance from the **Restore points from** drop-down. For every clone, a backup appears under the restore point.

Figure 98 Restore tab in EMC Backup and Recovery user interface

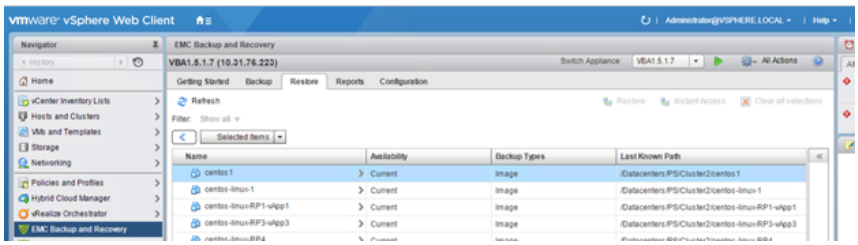


Image-level restore with resurrection

Restores from devices will be slow if resurrection is required. Resurrection is a type of recovery in which the primary backup (or snapup) in the VMware Backup Appliance is no longer available. Resurrection is not supported for VMDK-level backups, and you can only perform resurrection when you associate a client with the policy.

For Data Domain devices, resurrection only occurs when restoring a cloned backup. For AFTD and tape devices, resurrection requires a local Data Domain device on the NetWorker server. For a Cloud Boost device, a resurrection restore can take more than an hour depending on the virtual machine size, during which time the only progress that displays is message within ebrserver.log showing a save set copy is in progress.

Note: If there is no staging pool available when resurrecting from an AFTD, the restore does not fail automatically after timing out. You must manually cancel the restore operation.

Performing a FULLVM restore

About this task

Procedure

1. If restoring the VM to its original location, power off each virtual machine that you want to restore.

   Note: Power off is not required if restoring the VM to a new location.

2. In **EMC Backup and Recovery**, on the **Restore** tab, use the **Restore points from** drop-down to select the appliance from which you want to restore.

   EMC Backup and Recovery displays the virtual machines that are available to restore.

3. Click the virtual machine that you want to restore to expand its backups.

Use the **Filter** drop-down to display a specific VM and related items. You can also click a backup to display the VMDK level and select a single VMDK for restore, if you only want to restore that disk.

4. Select a backup, and then click **Restore**.

   The **Restore Backup** wizard launches.

5. On the **Select Backup** page, verify that the list of backups is correct. Remove any backup that you want to exclude, and click **Next**.
6. On the**Set Restore Options** page, perform one of the following tasks:
   - Select the **Restore to original location** option to restore the backup to its original location. If the VMDK file still exists at the original location, the restore process overwrites the file.
   - Unselect the **Restore to original location** option, and specify a new name and destination where the virtual machine or VMDK will be restored.
7. Optionally, select **Advanced options** to set the VM to **Power On** and **Reconnect NIC** after the restore process completes.

   Note: **Reconnect NIC** is enabled by default and greyed out. Only when you select **Power On** are you given the option to clear the **Reconnect NIC** option.

8. Click **Next**.
9. On the **Ready to complete** page, verify the selections. The wizard displays a summary of the number of machines that will be replaced (restore to the original location) and the number of machines that will be created (restore to a new location).
10. To change any of the settings for your restore request, either use the **Back** button to return to the appropriate screen, or click the appropriate numbered step title to the left of the wizard. If the settings are correct, then click **Finish**.

    The **Restore Backup** wizard displays a message that the restore process initiated successfully.

11. Click **OK**.

    You can monitor the restore progress by using the **Recent Tasks** pane.

    Note: If you selected **Reconnect NIC** during the restore process, then confirm the network configuration for the newly-created virtual machine. Once the restore completes, the new virtual machine NIC might use the same IP address as the original virtual machine, which will cause conflicts.

Results

When the recovery starts, a recovery session also displays in NMC. Any activities that occur on the vCenter side are visible on the NMC side.

Canceling a FULLVM restore

To cancel a restore at any time during setup, click the circular **x** symbol associated with the restore job in the **Recent Tasks** pane.

About this task

Instant Access restore (for Data Domain systems only)

If your primary backup is located on a Data Domain system, clicking the **Instant Access** button on the **Restore** tab allows you to perform a quick restore of these

backups, the same as you would perform a typical FULLVM restore. No further configuration is required to use this feature.

About this task

The Instant Access restore operation has the following limitations:

- The free space on the Data Domain system must be equal to or greater than the total disk size of the VM being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target VM fails.
- You cannot use the **Instant Access** button when you select more than one different Data Domain system backup for multiple VMs.
- You can perform only one Instant Access restore at a time. Ensure that you `vMotion` the VM to a different datastore and that you unmount the datastore before performing another instant access restore for the Data Domain system.
- You cannot recover multiple save sets concurrently using Instant Access restore.

Procedure

1. In the **EMC Backup and Recovery** user interface, select the **Restore** tab.

   EMC Backup and Recovery displays the virtual machines that are available to restore.

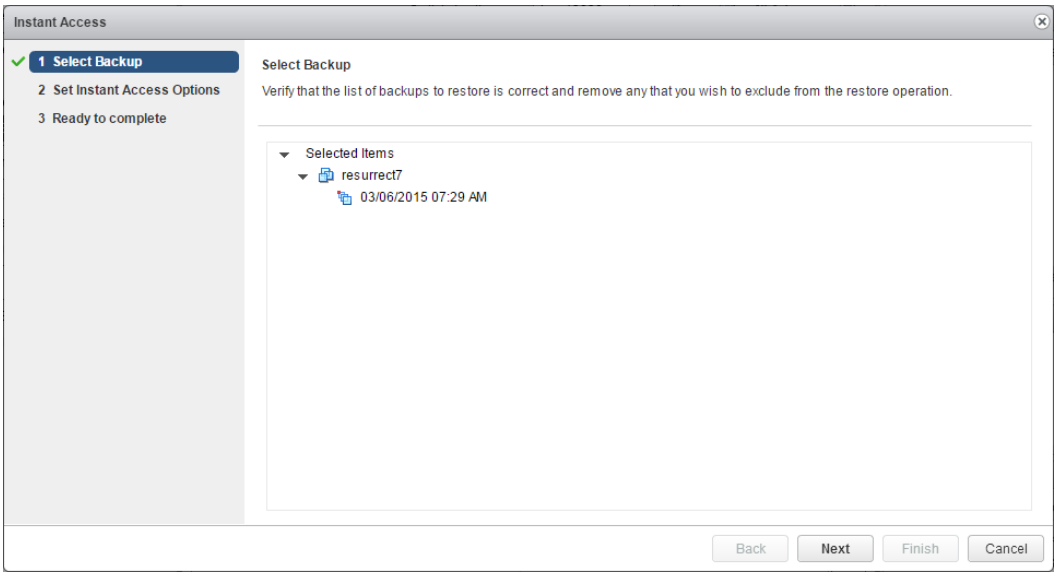
2. Click a virtual machine to expand the list of available backups, from which to restore.

   Note: You cannot browse and select backup data at the disk level.

3. Select the backup that you want to restore, and click **Instant Access**.

   The **Instant Access** wizard opens to the **Select Backup** page.

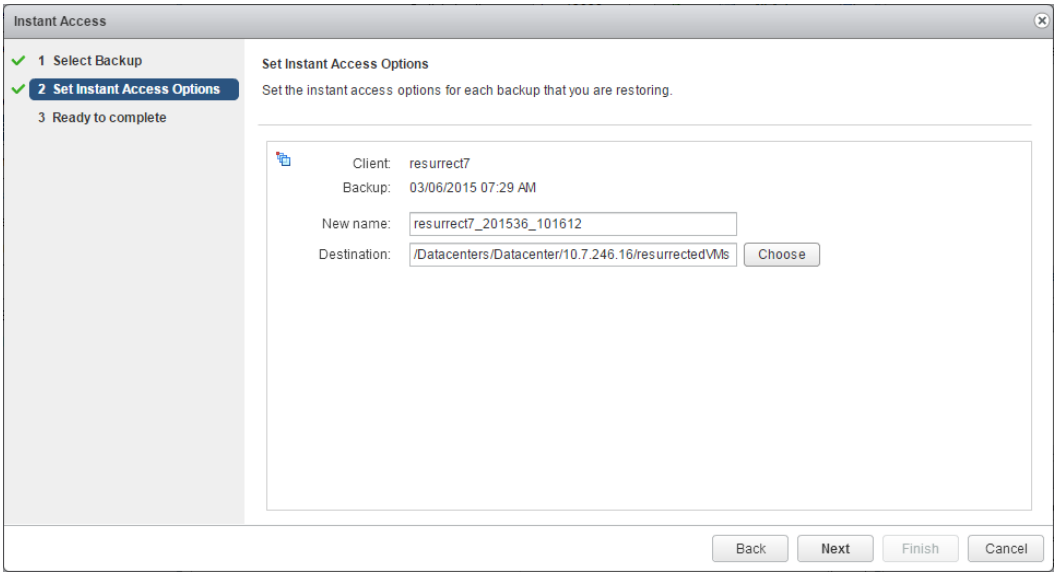
   Figure 99 Select a backup



4. Verify that the list of backups is correct, remove any backups that you want to exclude from the restore, and click **Next**.

   The **Set Instant Access Options** page displays.

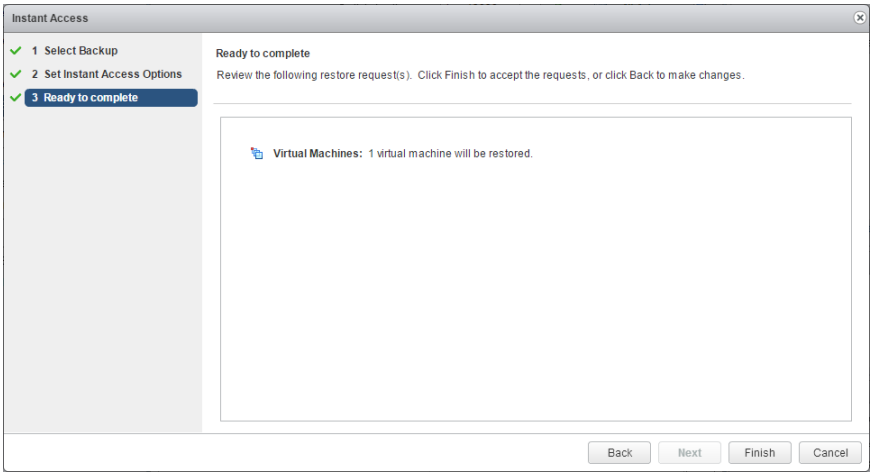
Figure 100 Set instant access options



5. Specify a new name and destination for the restore, and click **Next**.

   The **Ready to complete** page displays.

   Figure 101 Ready to complete



6. Review the restore request, and click **Finish**.

   You should see a message that indicates that the instant access operation was successfully completed.

Restore from last backup

The vSphere Web Client also provides an option to perform a VMware Backup Appliance restore from the last successful backup. This option is available when you right-click the VM and select **All EBR actions** > **Restore from last backup**.

About this task

Note: Before you use this option, make sure that you establish a connection to the VMware Backup Appliance by selecting the EMC Backup and Recovery user interface in the vSphere Web Client.

Direct to host recovery

You can recover image-level backups directly to an ESX host without requiring a vCenter server by using the **Emergency Restore** tab **EMC Backup and Recovery Configure** window. Direct to host recovery is available only for VMs that you back up to a VMware Backup appliance.

About this task

Before performing an emergency restore, ensure that you meet the following requirements:

- The VM you want to restore must have a VMware Hardware version that is supported by the ESX host running the VMware Backup Appliance (VMware Hardware version 7 or later).
- A vSphere host that is currently managed by the vCenter Server must be temporarily disassociated from the vCenter Server to perform the emergency restore. To disassociate the vCenter Server, use the vSphere Client (not the vSphere Web Client) connected directly to the vSphere host.
- You must have adequate free space in the target datastore to accommodate the entire VM. The target VMFS datastore to which the VM is being restored must support the VMDK file size.
- Network connectivity must be available for the restored VMs from the ESX host running the VMware Backup Appliance.
- You must have at least one local account with administrator privileges on the ESX host running the VMware Backup Appliance.

Note: You can only perform an emergency restore from a primary backup; you cannot use a cloned backup.

Procedure

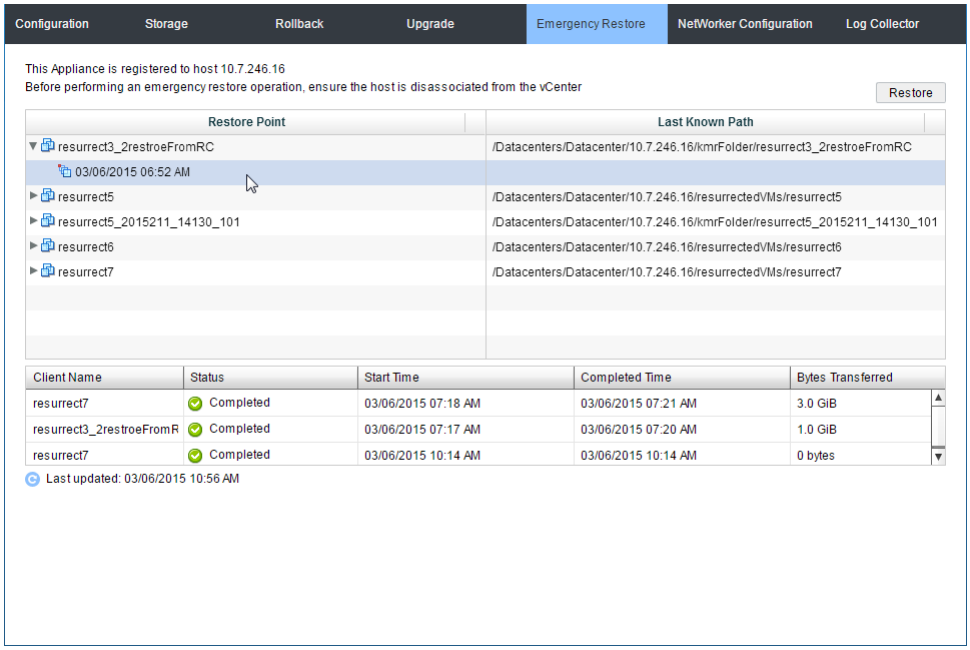
1. Log in to the **EMC Backup and Recovery Configure** window at the following URL using the EMC Backup and Recovery username and password credentials that you defined during configuration:

   `http://VMware_Backup_appliance_IP:8580/ebr-configure`

2. Select the **Emergency Restore** tab.
3. Click **Refresh** to view the most recent available VM backups.
4. Click the arrow beside a restore point to display its backups.
5. Select the backup that you want to restore, and then click **Restore**.

   The following figure provides an example of the **Emergency Restore** window.

Figure 102 Emergency Restore window



GLOSSARY

This glossary contains terms related to disk storage subsystems. Many of these terms are used in this manual.

B

backup

1. Duplicate of database or application data, or an entire computer system, stored separately from the original, which can be used to recover the original if it is lost or damaged.
2. Operation that saves data to a volume for use as a backup.

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

C

changed block tracking A VMkernel feature that keeps track of the storage blocks of virtual machines as they change over time. The VMkernel keeps track of block changes on virtual machines, which enhances the backup process for applications that have been developed to take advantage of VMware's vStorage APIs.

checkpoint A system-wide backup, taken only after 24 hours (and at the time of the checkpoint after that first 24 hours have elapsed), that is initiated within the vSphere Web Client and captures a point in time snapshot of the EMC Backup and Recovery appliance for disaster recovery purposes.

client Host on a network, such as a computer, workstation, or application server whose data can be backed up and restored with the backup server software.

client file index Database maintained by the NetWorker server that tracks every database object, file, or file system backed up. The NetWorker server maintains a single index file for each client computer. The tracking information is purged from the index after the browse time of each backup expires.

Console server **See** NetWorker Management Console (NMC).

D

datastore A virtual representation of a combination of underlying physical storage resources in the datacenter. A datastore is the storage location (for example, a physical disk, a RAID, or a SAN) for virtual machine files.

E

EMC Backup and Recovery Appliance The EMC Backup and Recovery appliance (or VMware Backup Appliance) is an appliance that, when deployed, enables VMware backup and clone policy creation in NMC, and enables the EMC Backup and Recovery plug-in in the vSphere Web Client to assign VMs to those policies.

EMC Data Protection Restore Client A browser that allows for file-level restores, where specific folders and files are restored to the original virtual machine on Windows and Linux virtual machines.

F

file index See client file index.

file-level restore (FLR) Allows local administrators of protected virtual machines to browse and mount backups for the local machine. From these mounted backups, the administrator can then restore individual files. FLR is accomplished using the EMC Data Protection Restore Client. See “Using File Level Restore” on page 63 for additional information on FLR.

G

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

H

hotadd A transport mode where the backup related I/O happens internally through the ESX I/O stack using SCSI hot-add technology. This provides better backup I/O rates than NBD/NBDSSL.

I

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

inactivity timeout Time in minutes to wait before a client is considered to be unavailable for backup.

J

JAR (Java Archive) A file that contains compressed components needed for a Java applet or application.

L

label Electronic header on a volume used for identification by a backup application.

M

managed application Program that can be monitored or administered, or both from the Console server.

media database Database that contains indexed entries of storage volume location and the life cycle status of all data and volumes managed by the NetWorker server.

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

N

NBD A transport mode over LAN that is typically slower than hotadd mode. In NBD mode, the CPU, memory and I/O load gets directly placed on the ESX hosting the production VMs, since the backup data has to move through the same ESX and reach the proxy over the network. NBD mode can be used either for physical or virtual proxy, and also supports all storage types.

NBDSSL A transport mode that is the same as NBD except that the data transferred over the network is encrypted. Data transfer in NBDSSL mode can therefore be slower and use more CPU due to the additional load on the VADP host from SLL encryption/ decryption.

NetWorker administrator NetWorker server user who may add, change, or delete NetWorker server users.

NetWorker client **See** client.

NetWorker Management Console (NMC) Software program that is used to manage NetWorker servers and clients. The NMC server also provides reporting and monitoring capabilities for all NetWorker processes.

NetWorker server Computer on a network that runs the NetWorker server software, contains the online indexes, and provides backup and restore services to the clients and storage nodes on the same network.

NetWorker storage node **See** storage node.

O

online indexes Databases located on the NetWorker server that contain all the information pertaining to the client backups (client file index) and backup volumes (media index).

Open VM Tools Open VM Tools (open-vm-tools) is the open source implementation of VMware Tools for Linux guest operating systems.

R

recover To restore data files from backup storage to a client and apply transaction (redo) logs to the data to make it consistent with a given point-in-time.

S

SAN (storage area network) A transport mode that, when used, completely offloads the backup related CPU, memory or I/O load on the virtual infrastructure. The backup I/O is fully offloaded to the storage layer where the data is read directly from the SAN or iSCSI LUN. SAN mode requires a physical proxy.

save NetWorker command that backs up client files to backup media volumes and makes data entries in the online index.

save set
1. Group of tiles or a file system copied to storage media by a backup or snapshot rollover operation.
2. NetWorker media database record for a specific backup or rollover.

single step backup and recovery See image level backup and recovery.

storage node Computer that manages physically attached storage devices or libraries, whose backup operations are administered from the controlling NetWorker server. Typically a "remote" storage node that resides on a host other than the NetWorker server.

U

update enabler Code that updates software from a previous release. It expires after a fixed period of time.

V

VADP An acronym for vStorage APIs for Data Protection. VADP enables backup software to perform centralized virtual machine backups without the disruption and overhead of running backup tasks from inside each virtual machineVADP supersedes the VCB framework for VMware backups.

vCenter An infrastructure management tool that provides a central point for configuring, provisioning, and managing virtualized IT environments, and is part of the VMware Virtual Infrastructure package.

Virtual machine Software that creates a virtualized environment between the computer platform and its operating system, so that the end user can install and operate software on an abstract machine.

VM An acronym for virtual machine.

VMDK Virtual Machine Disk (VMDK) is a file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. These files are commonly called VMDK files because of the .vmdk extension that VMware adds to these files.

VMware Backup Appliance The VMware Backup Appliance (or EMC Backup and Recovery appliance) is an appliance that, when deployed, enables VMware backup and clone policy creation in NMC, and enables the EMC Backup and Recovery plug-in in the vSphere Web Client to assign VMs to those policies.

VMware Tools Installed inside each virtual machine, VMware Tools enhance virtual machine performance and add additional backup-related functionality.

VSS (Volume Shadow Copy Service) Microsoft technology that creates a point-in-time snapshot of a disk volume. NetWorker software backs up data from the snapshot. This allows applications to continue to write data during the backup operation, and ensures that open files are not omitted.

VSS component A subordinate unit of a writer. **See** writer.

W

writer Database, system service, or application code that works with VSS to provide metadata about what to back up and how to handle VSS components and applications during backup and restore. **See** VSS (Volume Shadow Copy Service).