

# Dell EMC NetWorker 19.8 VMware Integration Guide

Dell Inc.

## Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

<b>Figures.....</b>	<b>7</b>
<b>Tables.....</b>	<b>10</b>
Preface.....	11
<b>Chapter 1: Introduction to NetWorker VMware Protection with the vProxy appliance.....</b>	<b>15</b>
Introduction to NetWorker VMware Protection with vProxy appliance.....	15
Components in the NetWorker VMware Protection Solution with vProxy appliance.....	16
System requirements.....	16
Compatibility information.....	18
Port requirements.....	18
NetWorker VMware Protection Solution best practices with the vProxy appliance.....	20
Performance and scalability.....	22
Configuration checklist.....	25
Basic configuration.....	25
Data Domain system configuration.....	25
NetWorker configuration.....	25
Virtual machine configuration.....	25
vProxy FLR Limitations.....	26
vProxy limitations and unsupported features.....	26
Accessing Knowledge Base Articles.....	31
IPv6 Considerations.....	31
Remote Authentication Support for FLR and HTML 5 vCenter plug-in .....	31
<b>Chapter 2: Deploy the vProxy appliance and configure the NetWorker datazone.....</b>	<b>33</b>
Deploying the vProxy appliance.....	33
Deploy the vProxy OVA on a vCenter server.....	33
Deploy the vProxy OVA on an ESXi host.....	36
VMware vCenter server management.....	37
Add the vCenter server using NMC's VMware View.....	37
Add the vCenter server using the NetWorker Management Web UI.....	38
Configuring and registering the vProxy appliance.....	39
Configure and register the vProxy in NMC.....	39
Add and configure the vProxy in the NetWorker Management Web UI.....	41
Installing the vCenter plug-in.....	42
Install the vCenter plug-in using VMware View in NMC.....	42
Install the vCenter plug-in using the NetWorker Management Web UI.....	43
Updating the vCenter plug-in.....	44
Accessing the HTML 5 based vCenter plug-in as a non-administrator Active Directory user.....	44
Creating a dedicated vCenter user account and VM Backup and Recovery role.....	45
Create vCenter user account.....	45
Create a customized role.....	46
vSphere Client user accounts.....	47
Migrating policies from VMware Backup appliance to vProxy appliance.....	49
Migration pre-requisites.....	49

Policy migration to vProxy by using NMC.....	49
Policy migration to vProxy by using the command line.....	50
Renaming a NetWorker server with legacy VMware Backup appliance.....	51
Resetting the admin account password .....	51
Upgrading the vProxy appliance.....	51
Limitations.....	53
Troubleshooting Redeployment Failures.....	53
<b>Chapter 3: Protecting virtual machines.....</b>	<b>54</b>
Overview of protection policies.....	54
Preparing the NetWorker data zone.....	55
Configure the Data Domain System.....	55
VMware backups in the NetWorker Management Web UI.....	56
Policies, workflows, and actions in NetWorker Management Web UI.....	56
Create a policy using the NetWorker Management Web UI.....	56
Create a workflow using the NetWorker Management Web UI.....	57
Create an action using the NetWorker Management Web UI.....	59
Create a save set group using the NetWorker Management Web UI.....	66
Create a VMware group using the NetWorker Management Web UI.....	67
Create a rule using the NetWorker Management Web UI.....	68
vProxy backups in NMC.....	69
Default data protection policies in NMC's NetWorker Administration window.....	70
Create a VMware policy in NetWorker Administration.....	70
Create a workflow for a new policy in NetWorker Administration.....	71
Create a workflow for an existing policy in NetWorker Administration.....	73
Create or edit a VMware group in NetWorker Administration.....	74
Enabling a VMware group with Dynamic Association and applying rules.....	76
Create a VMware backup action.....	79
Create a clone action in NetWorker Administration.....	84
Creating an action for Microsoft SQL Server application-consistent protection.....	86
Starting, stopping, and restarting policies.....	86
Visual representation of VMware policy and associated actions.....	87
VMware View in NMC.....	87
Enabling vProxy Health Monitoring.....	92
vProxy backup workflows in the vSphere Client's Dell EMC NetWorker interface.....	93
Connect to the NetWorker server in the vSphere Client.....	93
Start a vProxy policy in the vSphere Client Dell EMC NetWorker interface.....	94
Add virtual machines to a vProxy policy in the vSphere Client Dell EMC NetWorker interface.....	95
Additional vProxy backup configuration options.....	97
Configure a backup to support VMware encryption.....	97
Configure a backup to support vSAN encryption.....	98
Enabling or disabling Changed Block Tracking.....	98
Enable the Microsoft VM App Agent for SQL Server application-consistent protection.....	99
Updating the Microsoft VM App Agent and FLR Agent software.....	103
Troubleshooting Data Protection Policies.....	103
Backup operations.....	103
Managing command execution for vProxy Agent operations on Linux.....	106
vProxy backup log files.....	106
vProxy Log Bundle collection using NMC.....	107
vProxy Log Aggregation Management Tool.....	107



Adding vProxy for Log aggregation.....	108
Removing vProxy from Log aggregation.....	108
Viewing vProxy Information.....	108
Running Log Aggregation.....	108
Logs for SQL application-consistent data protection.....	109
<b>Chapter 4: Recover virtual machines and data.....</b>	<b>110</b>
Preparing the NetWorker datazone for recovery.....	110
Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only).....	110
File-level restore as an Active Directory user.....	111
Active Directory user access to the vCenter plug-in and NMC.....	113
vProxy recovery in NMC.....	114
Recovering a virtual machine using the NMC Recovery wizard.....	114
vProxy recovery in the NetWorker Management Web UI.....	127
Revert (or rollback) a virtual machine backup.....	127
Recover to a new virtual machine.....	128
Instant Restore of a virtual machine.....	129
Virtual Disk (VMDK) recovery.....	129
Emergency Recovery.....	130
File Level recovery.....	131
Recover jobs.....	133
vProxy file-level restore and SQL restore in the Dell EMC Data Protection Restore Client.....	133
Pre-requisites for file-level restore and SQL restore.....	133
File-level restore and SQL restore limitations.....	138
Using the Dell EMC Data Protection Restore Client for file-level restore and SQL restore.....	140
vProxy recovery in the vSphere Client's Dell EMC NetWorker interface.....	150
Connect to the NetWorker server in the vSphere Client.....	150
Recovery to the original virtual machine.....	151
vCenter HTML5 UI Staging Pool Selection to recover from non-Boost Devices.....	153
Recovery to a new virtual machine.....	153
Virtual disk recovery (restore to an existing virtual machine).....	155
Instant recovery of a virtual machine.....	157
vProxy recovery log files.....	158
vProxy backups and restores using Direct Fiber channel.....	159
Configuring Direct Fibre Channel (DFC) for vProxy.....	159
vProxy DFC limitations .....	160
<b>Appendix A: Backing up and recovering a vCenter server.....</b>	<b>161</b>
vCenter deployments overview.....	161
Best practices for vCenter server backup and restore.....	161
Protecting an embedded PSC.....	162
Restore an embedded PSC with Emergency Recovery.....	162
Protecting external deployment models.....	164
vCenter server appliance with one external PSC where PSC fails.....	164
vCenter server appliance is lost but the PSC remains.....	165
vCenter server appliance with multiple PSCs where one PSC is lost but one remains.....	165
vCenter server appliance remains but all PSCs fail.....	165
vCenter server appliance remains but multiple PSCs fail.....	166
vCenter server appliance fails.....	166

vCenter server restore workflow.....	167
Platform Services Controller restore workflow.....	168
Additional considerations.....	168
Command reference.....	169
<b>Appendix B: NetWorker VMware Protection in VMware Cloud on Amazon Web Services.....</b>	<b>170</b>
Introduction to NetWorker VMware Protection in VMware Cloud on AWS.....	170
Prerequisites.....	170
Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS.....	172
NetWorker VMware Protection for VMware Cloud on AWS best practices.....	173
Unsupported NetWorker operations.....	174
Limitations.....	174
<b>Appendix C: NetWorker VMware Protection for Azure VMware Solution.....</b>	<b>176</b>
Introduction to NetWorker VMware Protection for Azure VMware Solution.....	176
Deploy the vProxy OVA on a vCenter server running in Azure VMware Solution.....	176
Prerequisites.....	177
Best practices for NetWorker VMware protection running on Azure VMware Solution.....	178
Limitations.....	180
Unsupported NetWorker operations.....	180
<b>Appendix D: Regular expressions for NetWorker vProxy dynamic policies rule definitions.....</b>	<b>181</b>
Regular expression syntax accepted by dynamic policy rule definition.....	181

1	Components in a NetWorker VMware Protection Solution.....	16
2	Port requirements for NetWorker VMware Protection with the vProxy appliance.....	19
3	Install vCenter Plugin in NMC.....	42
4	vCenter plug-in for Dell EMC NetWorker in the vSphere Client.....	43
5	vCenter plug-in for Dell EMC NetWorker in the vSphere Client.....	44
6	Hosts and Clusters in the vSphere Web Client.....	48
7	Migrating a VMware Backup appliance policy to vProxy in NMC.....	50
8	Migrate Operation Results dialog.....	50
9	Data Protection Policy.....	55
10	Platinum policy configuration.....	70
11	Changing the Backup Optimization mode in the vProxy protection group.....	76
12	Create a new rule to apply to a VMware group.....	78
13	Specify the vProxy and Application Protection Options page.....	81
14	VMware protection policy in the Protection window.....	87
15	VMware protection policy save sets in Media window.....	87
16	Add a vCenter server to VMware View in NMC.....	88
17	Map view of VMware environment in NMC.....	89
18	Cluster with child elements in VMware View.....	90
19	Filtering results in VMware View.....	90
20	VMware table view.....	91
21	Add group in VMware View.....	92
22	Accessing Dell EMC NetWorker in the vSphere Client.....	93
23	NetWorker connection information in the vSphere Client.....	94
24	Dell EMC NetWorker Basic Tasks pane.....	94
25	Policies pane with available vProxy policies.....	95
26	Policy backup options.....	95
27	Recent Tasks pane.....	95
28	Policies pane with available vProxy policies.....	96
29	Edit a vProxy policy.....	96
30	Backup sources in the Editing backup policy dialog.....	97
31	NSR Data Domain Properties.....	111
32	Virtual machine recovery in the NMC Recovery wizard.....	114
33	Select the Virtual Machine to Recover.....	115
34	Select the Target Backup (individual virtual machine).....	115
35	Select the Target Backup (multiple virtual machines).....	116
36	Select the Virtual Machine Recovery method.....	116
37	Choose Disks to Revert.....	117
38	Select Alternate Recovery Sources.....	118
39	Configure the Instant Recovery.....	119
40	Configure the virtual machine recovery.....	120

41	Configure the Virtual Disk Recovery.....	121
42	Configure the Emergency Recovery.....	122
43	Select Alternate Recovery Sources for file level recovery.....	123
44	Mount the save set for file level recovery.....	124
45	Select the files and folders to recover.....	125
46	Deploy FLR Agent if not found.....	133
47	Manage Authentication service users.....	137
48	Application Administrators user group properties.....	137
49	VMware FLR Users user group properties.....	138
50	Select backups to restore from.....	141
51	Select restore location.....	141
52	Select items to restore.....	142
53	Restore Monitoring.....	142
54	Select the backup(s) to restore from.....	143
55	Select restore location.....	144
56	Select items to restore.....	144
57	Total items available for recovery.....	145
58	Restore Monitoring.....	145
59	Select App Backups page.....	147
60	Restore Target page.....	148
61	Restore Options page.....	149
62	Restore Monitoring.....	149
63	Accessing Dell EMC NetWorker in the vSphere Client.....	150
64	NetWorker connection information in the vSphere Client.....	151
65	Dell EMC NetWorker Basic Tasks pane.....	151
66	Restore pane with available virtual machine backups.....	152
67	Select Restore from the Action drop-down.....	152
68	Restore to original location.....	152
69	Staging Pool Selection.....	153
70	Restore pane with available virtual machine backups.....	154
71	Select Restore from the Action drop-down.....	154
72	Restore to new virtual machine.....	154
73	Restore pane with available virtual machine backups.....	155
74	Select Restore from the Action drop-down.....	156
75	Restore virtual disks to existing virtual machine.....	156
76	Restore pane with available virtual machine backups.....	157
77	Select Restore from the Action drop-down.....	157
78	Instant Restore.....	158
79	Proxy selection.....	163
80	Proxy selection.....	163
81	vCenter server restore workflow.....	167
82	PSC restore workflow.....	168
83	Enable internet access for Forwarders.....	172

84	Add a vCenter Server to VMware View with Deployed in Cloud enabled.....	173
85	NSR VMware Proxy Properties.....	174
86	Enable internet access for Forwarders.....	178
87	Add a vCenter Server to VMware View with Deployed in Cloud enabled.....	179
88	NSR VMware Proxy Properties.....	179

1	Revision history.....	11
2	Style conventions.....	13
3	NetWorker VMware Protection with vProxy appliance requirements.....	17
4	Incoming port requirements.....	18
5	Outgoing port requirements.....	19
6	Performance and scalability factors.....	22
7	Minimum required vCenter user account privileges.....	46
8	Location of the vProxy redeployment log files.....	53
9	Schedule icons.....	80
10	Schedule icons.....	84
11	MSVMAPPAGENT binaries called by vProxy.....	100
12	Supported characters in SQL database names.....	102
13	SQL Skipped Database Cases and Descriptions.....	105
14	Backup log files.....	107
15	FLR privilege requirements.....	135
16	Recovery log files.....	158

# Preface

As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

**NOTE:** This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website <https://www.dell.com/support>.

## 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
01	December, 2022	First release of this document for NetWorker 19.8.

## 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.dell.com/eln/elhome>.
- *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 Update 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.
- *NetWorker Snapshot 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 documentation](#)  
Contains the NetWorker APIs and includes tutorials to guide you in their use.
- *CloudBoost 19.8 Integration Guide*  
Describes the integration of NetWorker with CloudBoost.
- *CloudBoost 19.8 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.

## Typographical conventions

The following type style conventions are used in this document:



**Table 2. Style conventions**

<b>Formatting</b>	<b>Description</b>
<b>Bold</b>	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
<i>Italic</i>	Used for full titles of publications that are referenced in text.
Monospace	Used for: <ul style="list-style-type: none"><li>• System code</li><li>• System output, such as an error message or script</li><li>• Pathnames, file names, file name extensions, prompts, and syntax</li><li>• Commands and options</li></ul>
<i>Monospace italic</i>	Used for variables.
<b>Monospace bold</b>	Used for user input.
[ ]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

## Where to find product documentation

- <https://www.dell.com/support>
- <https://www.dell.com/community>

## Where to get support

The Support website <https://www.dell.com/support> provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to <https://www.dell.com/support>.
2. In the search box, type a product name, and then from the list that appears, select the product.

## Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

## Live chat

To participate in a live interactive chat with a support agent:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

## Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.

**i** **NOTE:** To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To find the details of a service request, in the `Service Request Number` field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

## Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network <https://www.dell.com/community>. Interactively engage with customers, partners, and certified professionals online.

## How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. Perform one of the following steps to provide feedback:

- Go to <https://contentfeedback.dell.com/s>, and submit a ticket.
- Send feedback to [DPADDocFeedback@dell.com](mailto:DPADDocFeedback@dell.com).

# Introduction to NetWorker VMware Protection with the vProxy appliance

This chapter contains the following topics:

## Topics:

- [Introduction to NetWorker VMware Protection with vProxy appliance](#)
- [Components in the NetWorker VMware Protection Solution with vProxy appliance](#)
- [System requirements](#)
- [Compatibility information](#)
- [Port requirements](#)
- [NetWorker VMware Protection Solution best practices with the vProxy appliance](#)
- [Performance and scalability](#)
- [Configuration checklist](#)
- [vProxy limitations and unsupported features](#)
- [Accessing Knowledge Base Articles](#)
- [IPv6 Considerations](#)
- [Remote Authentication Support for FLR and HTML 5 vCenter plug-in](#)


## 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.

NetWorker vProxy appliance leverages VMware vSphere Storage APIs - Data Protection (formerly known as vStorage APIs for Data Protection or VADP) to perform image backup or image restore using supported transport modes.

NVP features the following:

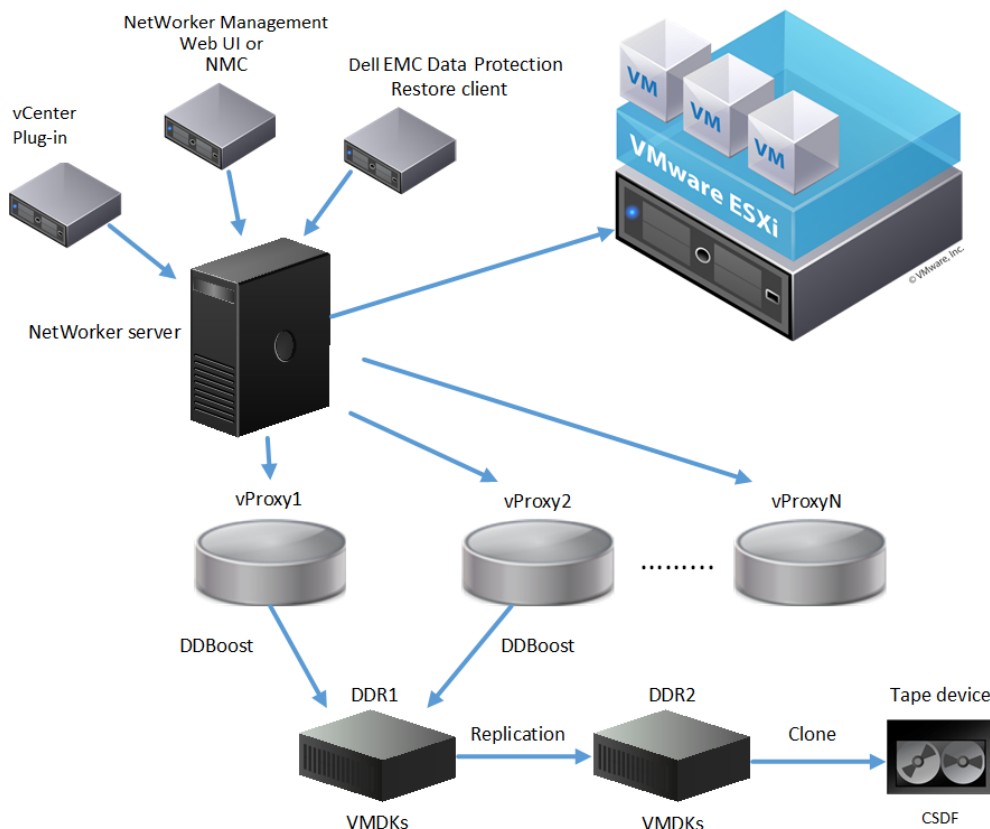
- Uses standalone data-mover proxy appliances, or vProxy appliances, to backup and restore virtual machines that run in a virtualized infrastructure, with the ability to offload the data mover from NetWorker and run the backup as a virtual workload.
- NetWorker directly manages the vProxy appliances 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.

 **NOTE:** Any references to the Data Domain systems and the Data Domain devices in the document indicate PowerProtect DD appliances.

# 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.
- 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 that are supported, see the NetWorker compatibility matrix at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.

**Table 3. NetWorker VMware Protection with vProxy appliance requirements**

Component	Requirements
NetWorker	<ul style="list-style-type: none"> <li>NetWorker 19.8 server software with NMC The NetWorker storage node should be the same version as the NetWorker server.</li> </ul>
vProxy Appliance	<p>Version 4.x. System requirements for the vProxy include:</p> <ul style="list-style-type: none"> <li>CPU: 4 * 2 GHz (4 virtual sockets, 1 core for each socket)</li> <li>Memory: 8 GB</li> <li>Disks: 2 disks (59 GB and 98 GB)</li> <li>Internet Protocol: IPv4 only or IPv6 only; dual stack not supported</li> <li>SCSI controller: Maximum 4</li> <li>NIC: One vmxnet3 NIC with one port</li> </ul>
vCenter server	<ul style="list-style-type: none"> <li>6.5, 6.5U1, 6.5U2, 6.5U3, 6.7, 6.7U1, 6.7U2, 6.7U3, 7.0</li> <li>Version 6.5 and later is required to perform Microsoft SQL Server application-consistent protection.</li> <li>Linux or Windows platform, or VC appliance</li> </ul> <p><b>i NOTE:</b> The NetWorker compatibility matrix at <a href="https://elabnavigator.emc.com/eln/modernHomeDataProtection">https://elabnavigator.emc.com/eln/modernHomeDataProtection</a> provides detailed information about NetWorker and vCenter/vSphere version compatibility.</p>
ESX/ESXi server	<ul style="list-style-type: none"> <li>6.5, 6.5U1, 6.5U2, 6.5U3, 6.7,6.7U1, 6.7U2, 6.7U3, 7.0</li> <li>Version 6.5 and later is required to perform Microsoft SQL Server application-consistent protection.</li> <li>Automatically enables Changed Block Tracking (CBT) on each virtual machine.</li> </ul> <p><b>i NOTE:</b> The NetWorker compatibility matrix at <a href="https://elabnavigator.emc.com/eln/modernHomeDataProtection">https://elabnavigator.emc.com/eln/modernHomeDataProtection</a> provides detailed information about NetWorker and vCenter/vSphere version compatibility.</p>
VMC on AWS	vProxy is compatible with SDDC version 1.6, 1.7, 1.8, 1.9 and 1.10, 1.18
VMware Tools	<ul style="list-style-type: none"> <li>VMware Tools version 10 or later VMware Tools version 10.1 or later is required to perform Microsoft SQL Server application-consistent protection.</li> <li>Open VM Tools, version support as outlined in the VMware Software Compatibility Guide.</li> </ul>
Data Domain	<ul style="list-style-type: none"> <li>A minimum of one configured DD Boost device is required. Also, you must specify one pool that contains the DD Boost device.</li> <li>Data Domain system operating system at DDOS version 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x.</li> <li>A Data Domain user account with administrator privileges, which you use to manage file-level restore and instant access restore.</li> <li>NFS v3 is enabled and running. This is required for the file-level restore and instant recovery operations.</li> </ul> <p><b>i NOTE:</b></p> <ul style="list-style-type: none"> <li>The NetWorker compatibility. matrix at <a href="https://elabnavigator.emc.com/eln/modernHomeDataProtection">https://elabnavigator.emc.com/eln/modernHomeDataProtection</a> provides detailed information about NetWorker and DD Boost version compatibility</li> <li>Ensure that the NFS "default-export-version" is set to 3 on the Data Domain by running the following command on Data Domain console:</li> </ul> <pre style="background-color: #f0f0f0; padding: 10px;">sysadmin@XXXXXXXXX# nfs option set default-export-version 3</pre>

**Table 3. NetWorker VMware Protection with vProxy appliance requirements (continued)**

Component	Requirements
	<p>You can check the default-export-version value by running the following CLI command on the Data Domain console</p> <pre>sysadmin@XXXXXXXXXX# nfs option show all</pre>
JRE	The minimum Java requirement is Java 8 build 211.

## 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 that are 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.

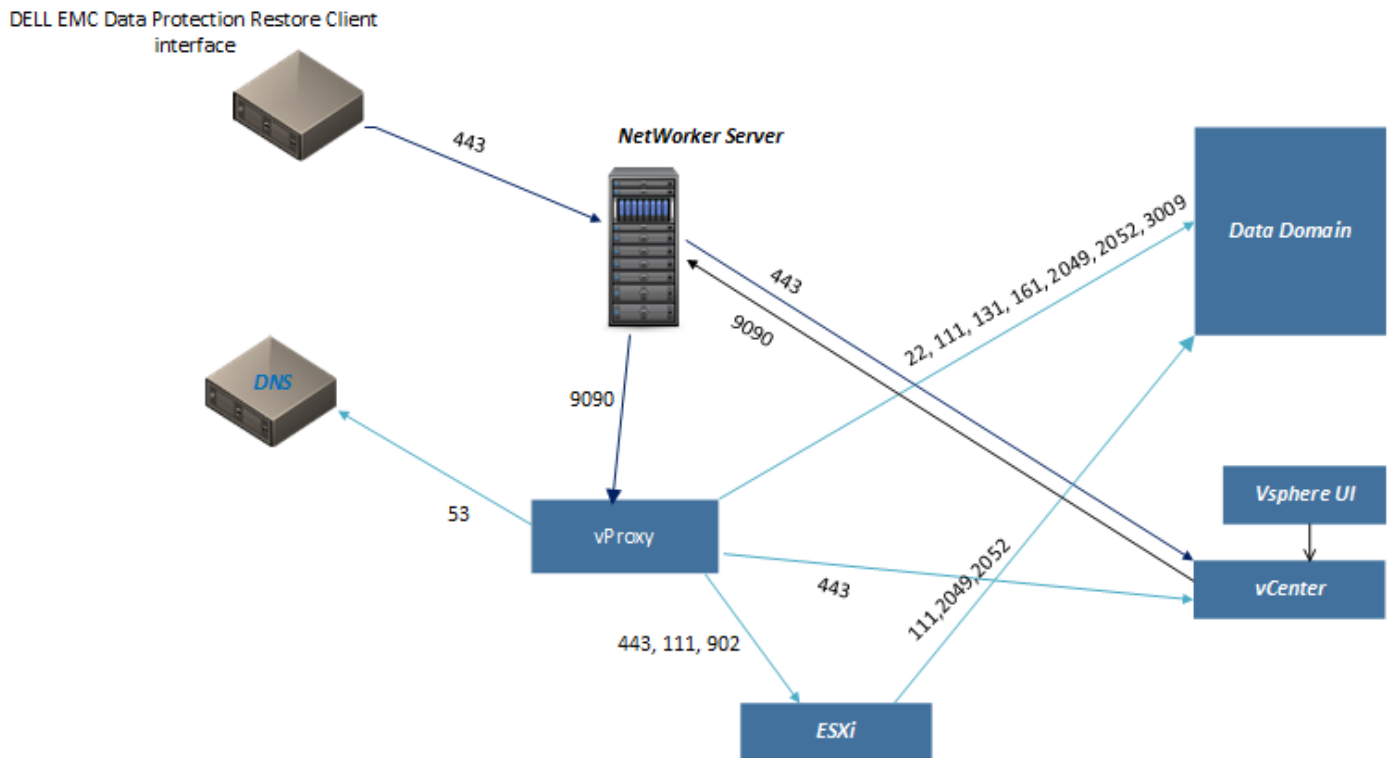
**Table 4. Incoming port requirements**

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	<b>VMware View</b> in NMC <b>NetWorker Administration</b>
NetWorker server	ESXi server	443	Emergency restore, vProxy redeployment
vCenter server	NetWorker server	9090	vSphere Client's <b>Dell EMC NetWorker</b> plug-in
Dell EMC Data Protection Restore Client interface	NetWorker server	9090	File-level recovery in the <b>Dell EMC Data Protection Restore Client</b>
ESXi servers	Data Domain	111, 2049, 2052	File-level recovery and instant recovery
Virtual machines	Data Domain	111, 2049	SQL application-consistent backup

**Table 5. Outgoing port requirements**

From	To	Port	Purpose
vProxy Appliance	DNS	53	Name resolution
vProxy Appliance	Data Domain	22, 111, 131, 161, 2049, 2052, 3009	Data Domain management <b>i</b> <b>NOTE:</b> Data Domain Management port 3009 is required by the vProxy with DDOS 7.0 or newer to perform FLR/IA.
vProxy Appliance	ESXi server	443, 902	Backup and recovery operations
vProxy Appliance	vCenter server	443	vProxy registration, backup, and recovery operations <b>i</b> <b>NOTE:</b> Using a non-default vCenter port for HTTPS is not supported.
vProxy Appliance	Target Virtual Machine	9613	vProxy FLR operations <b>i</b> <b>NOTE:</b> Port 9613 is used for FLR operations only when available. If port is not available, then it will fallback to older method through VIX API.

NetWorker VMware Protection with vProxy Appliance Firewall Ports



**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.
- Install **VMware Tools** on each virtual machine by using the **vSphere Web Client**. VMware Tools add 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 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 `vpzd.cfg` file does not contain the **enableHttpDatastoreAccess** entry or that it is set to **True**. For further details, see 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 millisecond 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 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:
  - 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 recovers the vRDM disk as a regular thick eager zeroed VMDK disk to the datastore selected during the restore.
- Instant Restore of Virtual Machine recovers all the disks in a VM with vRDM disk as regular thick eager zeroed VMDK disks.
- 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.
- If all the disks and vRDM disk are restored to the same datastore, then Recover to New Virtual Machine will recover all the disks in a VM with vRDM disk as regular thick eager zeroed VMDK disks.
- vProxy backs up only the independent persistent disk configuration without any data. That is, independent persistent disk is restored as raw unformatted disk in the guest operating system without any data. On restoration, the independent persistent disk will have the original size and will be a part of the virtual machine configuration with the same disk number. When you select a VM that has independent persistent disks for image restore, then you are notified about the presence of independent persistent disks.
- You should initiate independent persistent disk restore operation from NWUI, and the warnings are displayed in NWUI only.
- The vProxy Appliance uses Changed Block Tracking (CBT) by default. If CBT is disabled on the virtual machine, then it enables 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 about disabling CBT, see 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, five vProxy appliances with backup and clone operations 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. 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 I/O may stop responding 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 that is 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 one or more target virtual disks 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 many virtual machines that do not support hotadd requirements, NBD transport mode is 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 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.
- During a backup operation, when NBD sessions are not available in any of the vProxies, the backup of VMs with IDE disks is not guaranteed. Enabling fallback to NBD mode will ensure that the backups fallback to NBD mode for VMs with IDE disks, even when HotAdd sessions are only available in any vProxy. Restore is not supported with this feature. If you try to perform a restore, it might fail with an error VDDK Error: 13: You do not have access rights to this file.
- If the VMs that are being backed up are residing on VMware Virtual Volume (VVol) datastores, then ensure that you use NBD or NBDSSL transport modes for all your vProxies residing in VVol datastores. You can do this by setting the NBD to a nonzero value and HOTADD to zero. This is performed to overcome a limitation in VMware that makes the VM unresponsive during snapshot removal phase of the backup and, when the VM and hotadd-capable vProxy are running on different ESXi hosts.

## vSphere Cluster Services (vCLS) support recommendations

- The VM will not be application-consistent quiescing when using vProxy backup in NetWorker.
- The vSphere Replication will run on non-quiescent mode.
- Backup of vCLS will fail since locking of vCLS VM are not allowed.

## 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 about these scalability factors and maximum recommendations, besides 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 6. 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	48 (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 about vCenter NFC session connection limits.
Virtual machines concurrent backups per vCenter server	See the Note below	100	Can be achieved with a combination of the number of proxies that are multiplied by the number of configured hotadd sessions per vProxy.
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.

**Table 6. Performance and scalability factors (continued)**

Component	Maximum limit	Recommended count	Notes
			<p>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.</p> <p>However, ensure that you do not exceed 100 connections per vCenter at any time during the backup window.</p>
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		<p>You can perform up to 32 parallel instant recovery sessions using <code>nsrvproxy_recover</code>, provided that you satisfy the following prerequisites:</p> <ul style="list-style-type: none"> <li>For the backups being restored, you must select <b>Performance</b> backup optimization mode during VMware type group creation in NMC.</li> <li>If you are using DDoperating system version 6.0.x, then minimum Data Domain OS version 6.0.0.30 is required.</li> <li>Data Domain platforms that are supported include DD6300 (EOS-T2), DD6800 (EOS-T3), DD9300 (EOS-T4), and DD9800.</li> <li>The ESXi host requires the following default values to be updated to the maximum supported: <ul style="list-style-type: none"> <li>Under NFS, update <b>NFS.MaxVolumes</b>.</li> <li>Under Net, update <b>Net.TcpipHeapSize</b>.</li> <li>Under Net, update <b>Net.TcpipHeapMax</b>.</li> </ul> </li> </ul> <p>The VMware knowledgebase article at <a href="https://kb.vmware.com/kb/2239">https://kb.vmware.com/kb/2239</a> provides more information. Also, see the VMware Documentation for concurrent virtual machine migration limits.</p>
Total number of virtual machines in a single NetWorker policy	2000	1000	<p>You can run multiple vProxy policies concurrently as long as the total number of concurrent backup streams does not exceed the vCenter limits that are indicated in this table.</p> <p>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.</p>
Backup Optimization modes			During creation of a VMware type group in NMC, you can select a backup optimization mode of either <b>Capacity</b> or <b>Performance</b> . <b>Performance</b> mode results in additional space use on the Data Domain

**Table 6. Performance and scalability factors (continued)**

Component	Maximum limit	Recommended count	Notes
			device (around 20%) but significantly improves random I/O performance for instant access restores.
Number of vProxies per NetWorker server	70	20	More than 20 vProxies per NetWorker server requires NetWorker server of large configuration. See the NetWorker Performance Optimization Planning Guide for more information about sizing for large configuration. If more than 8 proxies are required per vCenter, configure the hotadd limits on the proxies to ensure that not more than 100 proxy streams run concurrently against any given vCenter. If you are planning to exceed more than 100 proxy streams per vCenter, see the following note.
Number of properties or conditions inside a rule definition	75	10	<p>Ensure that you do not exceed more than 10 properties or conditions inside a rule definition.</p> <p><b>i NOTE:</b> There is no limit on the number of rules that can be created in a given NetWorker server, the mentioned limit here applies only to the number of properties or conditions in a single rule definition.</p> <p>Ensure that you do not combine multiple vCenters into same rule, that is, using one single rule for all the vCenters in your environment is not recommended. We recommend you to have a separate rule created for each vCenter in your environment.</p>

**i NOTE:** Maximum limit of the virtual machine's concurrent backups per vCenter server depends on the following factors:

- Type of transport mode
- Backing disks for the virtual machines to be backed up
- Network throughput between vProxy uplink and Data Domain appliance
- Number of concurrent sessions per vProxy
- Backup retry option setting in the backup action associated with the vCenter
- Resource availability for the vProxy appliances in the given vCenter server
- Data Domain limit of concurrent streams for write for the given physical model of Data Domain or DDVE

As a general recommendation, a maximum limit of 300 backups per vCenter server is supported only if all the below factors are in place in the customer environment.

- Only hotadd transport mode is set, and NBD/NBDSSL is set to zero in all vProxies.
- The virtual machines to be backed up are placed in high-performance data stores consisted of solid-state drives (SSD) hard disks.
- Network throughput of 10 GbE exists between vProxy data path uplink and Data Domain appliance.
- Maximum of 13 concurrent hotadd sessions are set for each vProxy.
- Backup retry must be set to 1 retry and 360 s retry delay in every backup action that is associated with the vCenter.
- Ensure that the minimum resources of four cores of 2.66 GHz and 8 GB RAM is available for each vProxy. Do not over commit on CPU and memory if you plan to go beyond 100 concurrent backups.
- If all 300 backups are being written to the same Data Domain, then the Data Domain model must support at least 400 concurrent write streams. If not, you must plan according to concurrent stream capacity of each Data Domain model .

If one or more of the above factors are not in place, do not exceed 100 backups per vCenter server.

# 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.

## Data Domain Smart Scale

- All Data Domain Smart Scale systems must be upgraded to the DDOS 7.8.0.0 version for the NetWorker VMware Protection solution.
- For the Data domain Smart Scale retention lock feature, the DDOS version must be 7.8 and later. The minimum DDOS version is 7.8.0.0.
- Ensure that the Data Domain Smart Scale system does not reach the MTree limit and max-streams limit. The *NetWorker Data Domain Boost Integration Guide* provides more information on the maximum MTree limit.
- Check the NFS settings and ensure that NFS v3 is enabled and running. If NFS v4 is enabled, ensure that NFS v3 is also set to enabled in order to avoid issues with file-level restore operations or instant recovery operations.
- Transaction log restores for virtual machines within application-consistent data protection policy is not supported.

## 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 FLR Limitations

File-level restore does not support the following virtual disk configurations:

- LVM (Logical Volume Management) thin provisioning
- LVM having any PV (Physical Volume) not allocated to a VG (Volume Group)
- FAT16 file systems
- FAT32 file systems
- Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)
- Two or more virtual disks that are mapped to single partition
- Encrypted partitions
- Compressed partitions
- BTRFS subvolumes
- Raw disks without any file system
- RAID configured Linux Operating System

### NOTE:

- FLR is supported only for non-system files or folders, that is, user created files/folders. Restoring operating system or system files or folders should be done using image restore functionality only.
- FLR recovery for Windows Virtual Machine when multi-level nested mounted virtual disks are attached to the Virtual Machine is not supported.

## vProxy limitations and unsupported features

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

<b>vCenter server using nondefault HTTPS port is not supported.</b>	The vProxy appliance does not support the use of a nondefault vCenter HTTPS port. To perform data protection operations using the vProxy appliance, ensure that your vCenter server uses the default 443 HTTPS port.
<b>VMware limitations by vSphere version</b>	VMware limitations for vSphere 6.0 and later versions are available at <a href="https://configmax.vmware.com/home">https://configmax.vmware.com/home</a> .
<b>SQL Server application consistent data protection.</b>	Review the SQL Server application-consistent protection support limitations in the section <a href="#">Enable the Microsoft VM App Agent for SQL Server application-consistent protection</a> .
<b>Network configuration settings do not get restored with virtual machine after recovery of a vApp backup.</b>	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.
<b>vCenter version that is not updated in RAP database after upgrade.</b>	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 <b>VMware View</b> in NMC's <b>Administration</b> window for the vCenter version to update.
<b>Concurrent vProxy workflow on the same virtual machine is not supported when not using a vCenter server.</b>	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.

<b>Data Domain system requires REPLICATION license when clone of VMware backup. that is performed to same system as the backup</b>	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.
<b>No new policies can be created or run with VMware Backup appliance.</b>	After upgrading to a NetWorker 19.3 and later 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.
<b>Virtual machine. alert "VM MAC conflict" is displayed after successful recovery of virtual machine</b>	After performing a successful recovery of a virtual machine through vCenter version 6, an alert may appear to indicate 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. This alert can be triggered even when the MAC address conflict is resolved. The VMware release notes at <a href="http://pubs.vmware.com/Release_Notes/en/vsphere/60/vsphere-vcenter-server-60u2-release-notes.html">http://pubs.vmware.com/Release_Notes/en/vsphere/60/vsphere-vcenter-server-60u2-release-notes.html</a> provide more information.
<b>Emergency recovery cannot be performed until vProxy registration event successful with NetWorker.</b>	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 appears in the logs and in NMC.
<b>Datastore names cannot contain special characters.</b>	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.
<b>Backups fail for resource pools that are re-created with the same name as deleted pool</b>	When you delete a resource pool in vCenter and then re-create a resource pool with the same name, backups fail. Reconfigure the protection group with the newly created resource pool.
<b>Data Domain SMT not supported</b>	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.
<b>Only hotadd, NBD, and NBDSSL transport modes are supported.</b>	The NetWorker VMware Protection Solution supports only the hotadd and NBD/NBDSSL transport modes. The hotadd mode is the default transport mode. If you want to use both modes, the <i>maximum sessions</i> value for each must be set to the same nonzero 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. <b>i</b> <b>NOTE:</b> If upgrading to NetWorker 18.1 and later from a previous release where the hotadd and nbd transport modes were configured with different nonzero values for <i>maximum sessions</i> , ensure that you change these settings to the same nonzero value. Setting different nonzero values for both transport modes is not supported in NetWorker 18.1 and later.
<b>Specify NBD for datastores if proxies should use NBD mode only.</b>	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.
<b>Backup of individual folders</b>	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.

**within a Virtual Machine is not supported.**

**The Inactivity Timeout option for VMware backup action is not supported.**

The **Inactivity Timeout** option that appears during creation of a VMware backup action in the **NetWorker Management Web UI** and **NMC** is not supported. You can ignore this option 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, delete 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 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 recovers the vRDM disk as a regular thick eager zeroed VMDK disk to the datastore selected during the restore.
- Instant Restore of Virtual Machine recovers all the disks in a VM with vRDM disk as regular thick eager zeroed VMDK disks.
- 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.
- If all the disks and vRDM disk are restored to the same datastore, then Recover to New Virtual Machine will recover all the disks in a VM with vRDM disk as regular thick eager zeroed VMDK disks.

**Datastore cluster does not display in the Datastore**

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



**selection drop-down of NMC Recovery wizard for Virtual Machine Recovery or Virtual Disk Recovery types.**

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 network adapter vProxy is supported only if VMkernel port is connected to backup subnet/VLAN.**

To use Instant Access restore, emergency restore, and file-level restore with vProxy having dual network adapter or multiple isolated VLANs configured, the destination ESXi requires a VMkernel port that is 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.

**vProxy DFC limitations**

The following features are unavailable for virtual machines that are configured with DirectPath:

- Hot adding and removal of virtual devices
- Suspend and resume.
- Record and replay
- Fault tolerance
- High availability
- DRS (limited availability. The virtual machine can be part of a cluster, but cannot migrate across hosts)
- Snapshots

Taking above limitations into consideration, configure your vProxy for VMDirect capability.

**Recovered virtual machine fails to turn on if the source virtual machine is attached to a dvportgroup which no longer exists.**

A recovered virtual machine fails to turn on if the source virtual machine is attached to a dvportgroup which no longer exists. This issue affects the following types of restore operations:

- Instant access recovery
- Virtual machine recovery
- Emergency recovery

To avoid this issue, manually edit the virtual machine settings and assign the required network connection before powering on the recovered virtual machine.


**Restore of VM with active directory does not update the GenerationID.**

When a VM with Active Directory role is restored using a backup, it retains the same vm GenerationID as that of Source VM. This could lead to a potential data loss (USN rollback) scenario. You can restore by performing the following steps:

1. Perform Restore as New of the Active Directory VM and do not choose the option to turn on automatically.
2. After restore completes take a snapshot when it is in powered off state.
3. Perform a revert to the snapshot, and delete the snapshot.
4. Power on the VM and the generationID will be updated.

**When the vCenter is renamed to a different hostname, NetWorker**

Perform the following steps to rename the vCenter to a different hostname:

1. Create a hypervisor resource in NetWorker server pointing to the new hostname of the vCenter.  
 **NOTE:** If you need the old backups, then retain both vCenter resources in NetWorker until savesets of older vCenter expires.
2. Configure new vCenter groups and workflows and map to the required VMs in the new vCenter.

- server treats the vCenter server as a new resource.**
3. Reconfigure the existing vProxy resources in NetWorker to point to the new vCenter.
  4. Use NWUI H5 interface to restore any of the older vCenter backups.
- i** **NOTE:** Restore of vCenter backup using vCenter plug-in is not supported.

**Installing vCenter plugin when Authentication server is remote.**

If the Authentication server is remote, then you cannot install vCenter plug-in using NMC . Instead, use NWUI to install the vCenter plug-in.

**vProxy might become unresponsive for a few seconds in case of large number of level0 backups or if number of concurrent backup operations is high.**

During backups of large number of level0 backups or if number of concurrent backup operations is high, the vProxy might become unresponsive for a few seconds. The error message NMI watchdog: BUG: soft lockup - CPU#X stuck for XXs! appears on the vProxy console. These are kernel messages that inform that vCPU did not get execution for N seconds. This occurs due to the overhead when dealing with snapshot mount and unmount during hotadd mode for large number of level0 backups or high number of concurrent backups. This message can be safely ignored and must not lead to issues on the vProxy appliance if timeout is within acceptable timeout range. If backups are getting impacted due to this behavior, use backup retry set to 1 retry and 360 seconds retry interval in every NetWorker backup action that is associated with the vCenter.

**Renaming the vCenter to a different hostname makes NetWorker server treat the vCenter server as a new resource.**

If you are renaming the vCenter to a different hostname, then ensure that the following steps are done in NetWorker:

- Create another Hypervisor resource in NetWorker server pointing to the new hostname of the vCenter.
- If restores of old backups are required, then you must retain both vCenter resources in NetWorker until the savesets of older vCenter expires.
- Configure new vCenter groups and workflows to map to the required VMs in the new vCenter.
- Reconfigure the existing vProxy resources in NetWorker to point to the new vCenter.
- Use the NetWorker Web UI HTML5 interface to restore any of the older vCenter backups.

**i** **NOTE:** Use of vCenter plug-in to restore older vCenter's backups is not supported. Instead, use NetWorker Web UI HTML5 interface.

**Successive reverts of the same VM fails when revert is performed without any new backups in between the revert attempts.**

Revert VM operation resets the CBT. Since the corresponding CBT signature is invalid, using the same backup copy again for next set of revert will perform a full recover. This results in Revert VM failure. Hence, you should perform a Backup operation in between successive Revert operation and use the next set of backup copy to perform revert operation instead of performing revert using the same backup copy repeatedly.

**Backup of VMware Fault Tolerant virtual machines is not supported.**

When you enable Fault Tolerance for a VM, the backup fails. This is an expected behavior. NetWorker vProxy does not support backing up VMs with Fault Tolerance as enabled.

**FLR in Windows VMs requires disks to be attached to the target VM, beginning from SCSI Controller 0**

In order to match the Backup Virtual Disks that are attached among all the Physical Drives present in the virtual machine, in windows environment, FLR relies on the standard order of adding disks beginning "SCSI Controller 0" to the target virtual machine. A virtual machine with zero virtual disks attached to "SCSI Controller 0" might result in FLR not being able to match the requisite devices during mount operation and subsequently FLR mount operation fails.

**Backup of VMware Fault Tolerant virtual machines is not supported.**

When you enable Fault Tolerance for a VM, the backup fails. This is an expected behavior; NetWorker vProxy does not support backing up of VMs with Fault Tolerance enabled.

**FLR mount is not supported for VM with NVMe controller.**

If the destination VM has a NVMe controller, then FLR mount is not supported. Instead, specify the destination VM with SCSI controller.

**Independent persistent disks support limitation**

- This feature is available in NWUI only. Its not supported in NMC and vCenter UI.
- This feature is supported for all the backups taken in NetWorker 19.4 and later. The backups taken in NetWorker 19.3 and earlier are not supported.
- Only Virtual Machine recovery (recover to new) and emergency recovery types are supported.
- Restoring independent persistent disks from backups of individual VMDKs instead of the entire virtual machine is not supported.
- The feature is not supported when older vProxy running NetWorker 19.4 is used.

**Registering the vProxy using the separate private IP which belong to data domain network is not supported.**

In multi-NIC environment, registering the vProxy using the separate private IP which belong to the data domain network is not supported. Ensure that vProxy production network IP, or hostname is used for vProxy registration.

**Backup of VMware fault tolerant virtual machines is not supported**

When you enable fault tolerance for a VM, the backup fails. This is expected behavior; NetWorker vProxy does not support backing up VMs with fault tolerance enabled.

## 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**.

## IPv6 Considerations

In IPv6 enabled VMware environment, the following components should not have any unreachable IPv4 entries in the DNS server:

- NetWorker server FQDN
- vProxy appliance FQDN
- Data Domain FQDN
- vCenter FQDN
- ESXi FQDN

The FQDNs listed above should return only AAAA records from the DNS and should not have any unreachable IPv4 records in the DNS.

## Remote Authentication Support for FLR and HTML 5 vCenter plug-in

The Remote Authentication support for FLR and HTML 5 vCenter plug-in for vProxy is introduced in NetWorker 19.3.

The proposed feature enables end users to use a Remote AuthC server and support the operations with vProxy.

- You can login to FLR WebUI using remote Authc and perform FLR.
- You can login to vCenter plug-in H5 using remote Authc and perform backups and restores using the plug-in.

**NOTE:**

- To use the remote authentication, you should select the advanced option in the login screen and enter the remote Authentication hostname and port number.

- If the Authentication server is remote, then you cannot install vCenter plug-in using NMC . To install vCenter plug-in, use NWUI.
- NetWorker 19.3 and later, does not support Flash plug-in. You cannot use remote Authentication with vCenter Flash plug-in. Instead, use HTML5 plug-in.

# Deploy the vProxy appliance and configure the NetWorker datazone

This chapter contains the following topics:

## Topics:

- Deploying the vProxy appliance
- VMware vCenter server management
- Configuring and registering the vProxy appliance
- Installing the vCenter plug-in
- Accessing the HTML 5 based vCenter plug-in as a non-administrator Active Directory user
- Creating a dedicated vCenter user account and VM Backup and Recovery role
- Migrating policies from VMware Backup appliance to vProxy appliance
- Resetting the admin account password
- Upgrading the vProxy appliance

## Deploying the vProxy appliance

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

- The vCenter server.
- The ESXi host.

For vProxy appliance, you can add multiple NTP servers (2 to 4), and also configure *Remote Logging Server* functionality through syslog (UDP or TCP) during vProxy deployment.

Registration and configuration of the vProxy appliance must then be completed in the NMC **NetWorker Administration** 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.

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](https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2145066).

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 deploy the OVA and select **Deploy OVF template**.
4. On the **Source** window, type a URL path to the OVA package or click **Browse**, select 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. In case of multiple networks, vProxy registration in NetWorker server, should be done using only the “vProxy Production network” IP address or FQDN. Otherwise, ensure that you assign the networks according to the following considerations:

- If the 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 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 system, as indicated in the description when the network is selected.

11. Select **IPv4** or **IPv6** 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 or IPV6 address for the vProxy appliance.
- In the **Default gateway** field, specify the IPV4 or IPV6 address of the gateway host.
- In the **Network Netmask/Prefix** field, specify the netmask for an IPv4 Network IP address, or the prefix length for an IPv6 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:

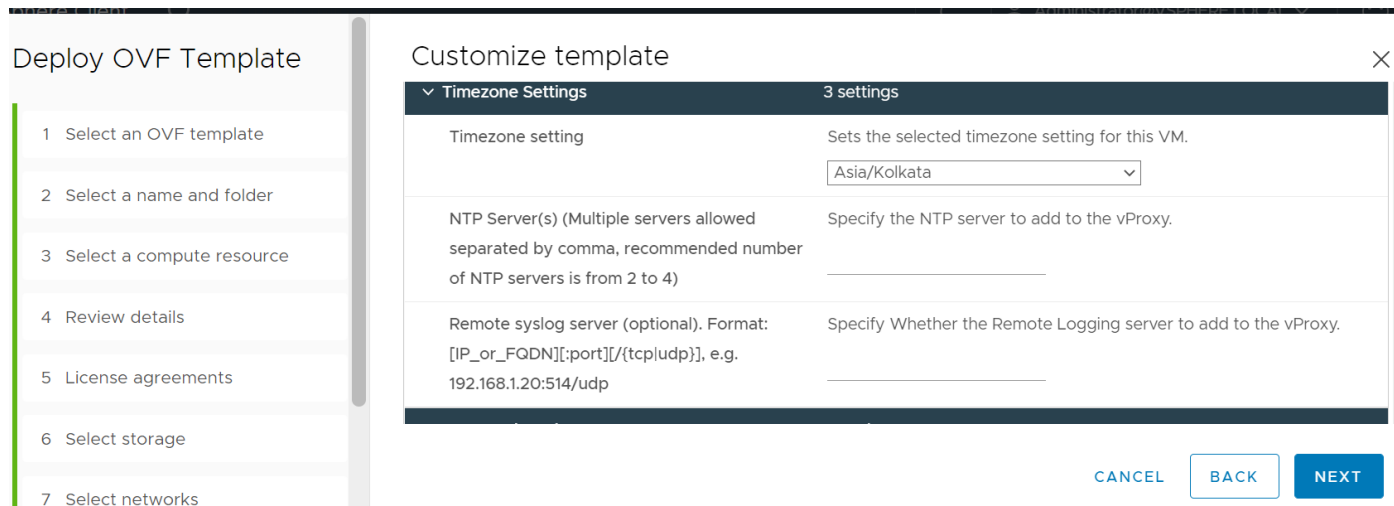
- In the **Timezone setting** field, select the timezone.

**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. You can also manually add multiple NTP servers IP addresses (2-4), and the details are updated in `/etc/ntp.conf` in required format. If you do not specify the NTP server addresses, then the vProxy will time sync with the ESXi host.

d. (Optional) In the **Remote syslog server** field, specify the remote logging server to add to the vProxy.

- Provide the remote server IP address or FQDN during vProxy deployment, and the same will reflect in `/opt/emc/vproxy/conf/rsyslog.conf` file.
- Specify TCP or UDP protocol along with the remote server address and port number in format: `[IP_or_FQDN][:port][/{tcp|udp}]` during vProxy deployment (for example: `192.168.1.20:514/udp`). The same will reflect in `/opt/emc/vproxy/conf/rsyslog.conf` file. In case you have not specified port numbers, default port number for each protocol will be used.



In case you forget to configure Remote syslog server during the vProxy deployment, perform the following to do it manually in vProxy:

Make the following changes in vProxy:

- Go to the path "`cd /opt/emc/vproxy/conf/`", and create the file `rsyslog.conf`
- vi **rsyslog.conf**
  - Provide the remote server IP address or `fqdn`. For example: `10.XXX.XXX.XXX:<port>/<tcp or udp> OR FQDN:<port>/<tcp OR udp> .`
- Reboot the vProxy

Make the following changes in the Remote syslog server:

- i. Run the below configuration on the remote server side:

```
# Provides UDP syslog reception
#$ModLoad imudp (Remove the # to uncomment this line if you are using UDP)
#$UDPServerRun 514 (Remove the # to uncomment this line if you are using UDP)
```

```
# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

- ii. Stop and start the `rsyslog.service`.

```
[root@blrv076c188 ~]# systemctl restart rsyslog.service
```

- e. 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 do not have an option to set the vProxy password during deployment. You must change the default passwords from the console window of the vProxy appliance or use the default passwords to configure vProxy 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.

Download the vProxy OVA package specific to your platform from the NetWorker downloads page at <https://www.dell.com/support/home/en-in/product-support/product/networker/>.

### NOTE:

- If adding standalone ESXi host to NetWorker server as hypervisor, you should set the `deployed in cloud` option.
- Instant Restore, File level Restore, Dynamic rule based backups and SQL app-aware are not supported when standalone ESXi is configured to the NetWorker server as hypervisor.

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**, select 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.
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 do not have an option to set the vProxy password during deployment. You must change the default passwords from the console window of the vProxy appliance or use the default passwords to configure vProxy 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.

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 ethx fqdn IP address netmask/prefix gateway`

where:



- *fqdn* is the Fully Qualified Domain Name of the appliance.
- *IP address* is the IPv4 or IPV6 address of the appliance.
- Specify the *netmask* for an IPv4 Network IP address, or the prefix length for an IPv6 Network IP address.
- *gateway* is the name or address of IPV4 or IPV6 address of the gateway host.

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.

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.

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.

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 disabled 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 unselected, select the **Deployed in Cloud** checkbox.

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

6. Click **OK**.

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

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

Backup policy fails when a virtual machine is configured as a static item in the workflow and later removed from the inventory of the vCenter. A message with the UUID and virtual machine name is logged and the total number of such virtual machines is displayed under the "VMs not in inventory" in the final summary of the action log file.

**i** **NOTE:** There should be at least one successful backup of the virtual machines that has been removed from the inventory of the vCenter.

## 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.

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.

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 is 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.

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

9. Use the **Snapshot Free Space Warning Threshold** spin boxes to set a warning threshold percentage value. If the Snapshot Free Space Warning Threshold value is greater than the percentage of free space available in the datastore, the backup proceeds with warnings in the log. The minimum and default value is 0% and the maximum value is 100%.

10. Use the **Snapshot Free Space Failure Threshold** spin boxes to set a failure threshold percentage value. If the Snapshot Free Space Failure Threshold value is greater than the percentage of free space available in the datastore, the backup job is terminated and an error is reported in the log. The minimum and default value is 0% and the maximum value is 100%.

The threshold values apply to all the datastores that belong to the vCenter. For example if vCenter has three datastores, datastoreA, datastoreB and, datastoreC of 1 TB, 2 TB and, 3 TB respectively. If the warning threshold for the datastores is set to 30, then warnings are logged when 30 percent of the disk space remains, that is, when datastoreA, datastoreB and, datastoreC reaches 700 GB, 1.4 TB and, 2.1 TB.

By default, the threshold value for both warning and failure threshold is set to 0. This disables the threshold check feature for the vCenter server. If the failure threshold values are set to 100, then the NetWorker server will check for the threshold value. For example, if the warning is set to 0 and failure is set to 100, then the backups of all the virtual machines that belong to the vCenter fails.

You must ensure that the threshold values are properly set. For example, if the Snapshot free space warning threshold is set to 30 and the failure threshold is set to 20, then the virtual machine backup succeeds with a warning message in the backup action log of that particular virtual machine. If the vSphere datastore where the virtual machine resides has 30 percent or

lesser free space, then the virtual machine backup fails without creating a snapshot when the vSphere datastore reaches 20 percent or lesser free space.

11. Click **Save**.

An entry for the added vCenter server appears 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.

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. You can choose to display hidden columns such as Snapshot Free Space Warning Threshold and Snapshot Free Space Failure Threshold by clicking the blue icon in the lower left corner of the table.

## 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.

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. Use the **Snapshot Free Space Warning Threshold** spin boxes to set a warning threshold percentage value. If the Snapshot Free Space Warning Threshold value is greater than the percentage of free space available in the datastore, the backup proceeds with warnings in the log. The minimum and default value is 0% and the maximum value is 100%.

7. Use the **Snapshot Free Space Failure Threshold** spin boxes to set a failure threshold percentage value. If the Snapshot Free Space Failure Threshold value is greater than the percentage of free space available in the datastore, the backup job is terminated and an error is reported in the log. The minimum and default value is 0% and the maximum value is 100%.

8. Click **Save**.

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.


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

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** 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**.

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**.

 **NOTE:** You can receive notifications when the vProxy goes to unavailable state by configuring the NSR notification resource "vProxy is unavailable" to send an email notification or an snmp trap. The "vProxy is unavailable" notification can be configured using NMC, NWUI and CLI.


## 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**.

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.
- e. Setting **Fallback to NBD for IDE disks** to Yes. It checks whether the VM has an IDE disk. If IDE disk is present then the backup fallback to NBD mode when only HotAdd sessions are available in the vProxy.

 **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 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](#).

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.

- e. Set **Fallback to NBD for IDE disks** to Yes. It checks whether the VM has an IDE disk. If an IDE disk is present, then the backup falls back to NBD mode, if HotAdd sessions are available in the vProxy.
6. Click **Finish**.

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 the HTML5 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 the HTML5 based vCenter plug-in to enable virtual machine backup and recovery in the **vSphere Client** or **vSphere Web Client**.

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

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.

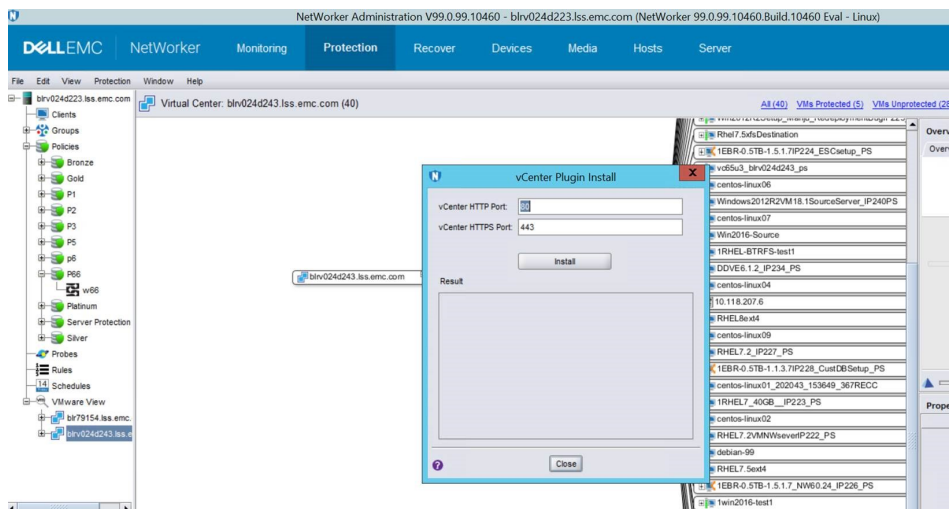


Figure 3. Install vCenter Plugin in NMC

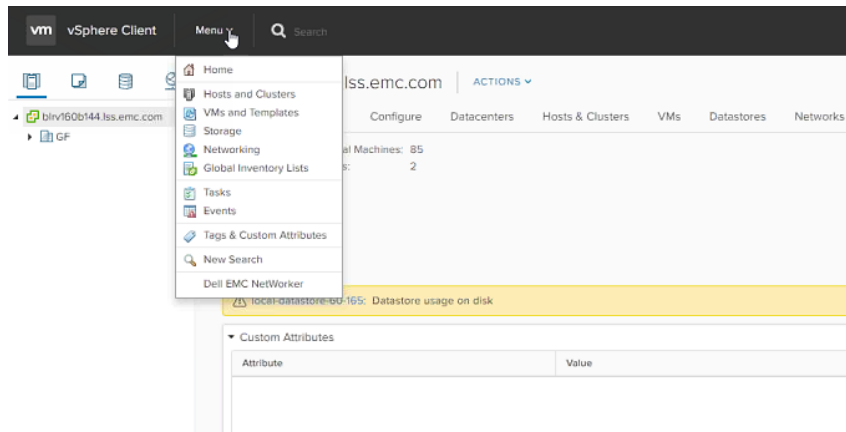
4. If a security warning appears, click **Continue** to dismiss the warning.
5. In the **vCenter Plugin Install** dialog, enter the required HTTP port configured for the vCenter server. Retain the default value of 443 for the HTTPS port.

**NOTE:** For HTTPS, vProxy appliance supports the port 443 only.

6. Click **Install**.

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, an entry for **Dell EMC NetWorker** 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.

## 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 want to remove the HTML5-based plug-in and then reinstall the plug-in, perform the following steps.

1. Stop the **vSphere Client** services.
2. Log in to 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-ui/vc-packages/vsphere-client-serenity` on Linux, and `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` on Windows.
10. Restart the **vSphere UI** services.
11. Perform the steps in the section [Install the vCenter plug-in for the vSphere UI](#) to reinstall the HTML5-based plug-in, and verify that the **Dell EMC NetWorker** interface appears in the **vSphere Client**.

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

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

- 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 short name alias for the vCenter server when adding it to NetWorker is not supported for the vCenter plug-in.
  - The HTML5 based vCenter plug-in requires the NetWorker server and NetWorker Authentication service to be installed on the same machine.
1. Select **Protection > VMware vCenters** in the left pane.
  2. In the **Protection** window's **VMware vCenters** pane, click the **Install** icon.

**NOTE:** From NetWorker 19.3 and later, flash plug-in installation is not supported

The **Install vCenter Plugin** dialog displays.

3. Provide the required HTTP port configured for the vCenter server, and retain the default value of 443 for the HTTPS port.

**NOTE:** For HTTPS, vProxy appliance supports the port 443 only.

4. Type the username and password for the NetWorker administrator user.

5. Click **Install**.

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, an entry for **Dell EMC NetWorker** 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**.

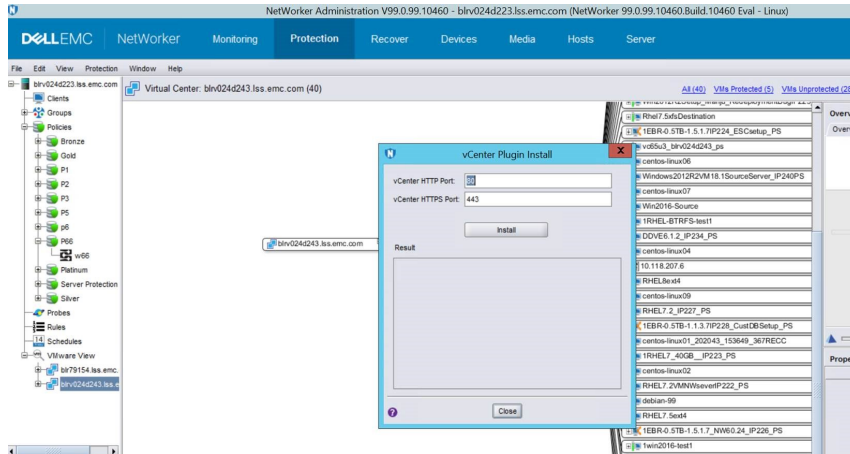


Figure 5. vCenter plug-in for Dell EMC NetWorker in the vSphere Client

**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.

## Updating the vCenter plug-in

When you upgrade the NetWorker server to NetWorker 19.8, you must also upgrade the HTML-5 based vCenter plug-in to the latest version for NetWorker 19.8.

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 based vCenter plug-in as a non-administrator Active Directory user

You can only access the HTML-5 based vCenter plug-in if you are a 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.

Install the vCenter plug-in. The section [Installing the vCenter plug-in](#) provides instructions.

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**

The Active Directory user that you create using these steps will only have access to the HTML-5 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 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.

 **NOTE:** If you are using a stand-alone ESXi, then only root privileges are supported.

### Create vCenter user account

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

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 7. Minimum required vCenter user account privileges**

Setting	vCenter required privileges
Alarms	<ul style="list-style-type: none"> <li>• Create alarm</li> <li>• Modify alarm</li> </ul>
Datastore	<ul style="list-style-type: none"> <li>• Allocate space</li> <li>• Browse datastore</li> <li>• Configure datastore</li> <li>• Low level file operations</li> <li>• Move datastore</li> <li>• Remove datastore</li> <li>• Remove file</li> <li>• Rename datastore</li> </ul>
Extension	<ul style="list-style-type: none"> <li>• Register extension</li> <li>• Unregister extension</li> <li>• Update extension</li> </ul>
Folder	<ul style="list-style-type: none"> <li>• Create folder</li> </ul>
Global	<ul style="list-style-type: none"> <li>• Cancel task</li> <li>• Disable methods</li> <li>• Enable methods</li> <li>• Licenses</li> <li>• Log event</li> <li>• Manage custom attributes</li> <li>• Settings</li> <li>• Set custom attribute</li> </ul>
Host	<ul style="list-style-type: none"> <li>• Configuration &gt; Storage partition configuration</li> </ul>
Network	<ul style="list-style-type: none"> <li>• Assign network</li> <li>• Configure</li> </ul>
Resource	<ul style="list-style-type: none"> <li>• Assign virtual machine to resource pool</li> <li>• Migrate powered off virtual machine</li> <li>• Migrate powered on virtual machine</li> </ul>
Sessions	<ul style="list-style-type: none"> <li>• Validate session</li> </ul>
Tasks	<ul style="list-style-type: none"> <li>• Create task</li> <li>• Update task</li> </ul>
vApp	<ul style="list-style-type: none"> <li>• Export</li> <li>• Import</li> <li>• vApp application configuration</li> </ul>
Virtual Machine	
Configuration	<ul style="list-style-type: none"> <li>• Add existing disk</li> <li>• Add new disk</li> <li>• Add or remove device</li> <li>• Advanced</li> </ul>

**Table 7. Minimum required vCenter user account privileges (continued)**

Setting	vCenter required privileges
	<ul style="list-style-type: none"> <li>● Change CPU count</li> <li>● Change resource</li> <li>● Configure managed by</li> <li>● Disk change tracking</li> <li>● Disk Lease</li> <li>● Extend virtual disk</li> <li>● Host USB device</li> <li>● Memory</li> <li>● Modify device settings</li> <li>● Raw device</li> <li>● Reload from path</li> <li>● Remove disk</li> <li>● Rename</li> <li>● Reset guest information</li> <li>● Set annotation</li> <li>● Settings</li> <li>● Swapfile placement</li> <li>● Upgrade virtual machine compatibility</li> </ul>
Guest Operations	<ul style="list-style-type: none"> <li>● Guest operation modifications</li> <li>● Guest operation program execution</li> <li>● Guest operation queries</li> </ul>
Interactions	<ul style="list-style-type: none"> <li>● Configure CD media</li> <li>● Console interaction</li> <li>● Device Connection</li> <li>● Guest operating system management by VIX API</li> <li>● Power off</li> <li>● Power on</li> <li>● Reset</li> <li>● VMware Tools install</li> </ul>
Inventory	<ul style="list-style-type: none"> <li>● Create new</li> <li>● Register</li> <li>● Remove</li> <li>● Unregister</li> </ul>
Provisioning	<ul style="list-style-type: none"> <li>● Allow disk access</li> <li>● Allow read-only disk access</li> <li>● Allow virtual machine download</li> <li>● Mark as Template</li> </ul>
Snapshot Management	<ul style="list-style-type: none"> <li>● Create snapshot</li> <li>● Remove Snapshot</li> <li>● Revert to snapshot</li> </ul>

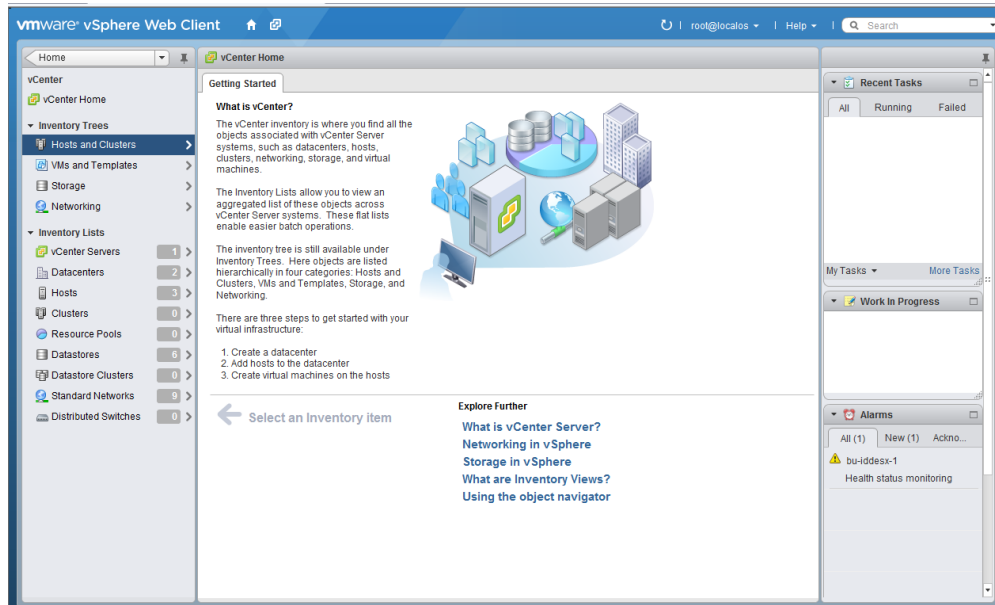
## vSphere Client user accounts

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.

**i NOTE:** In high-security environments, you can restrict the vCenter user account permissions required to configure and administer the vProxy appliance. [Minimum required vCenter user account privileges](#) on page 46 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**.

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 cursor 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:

- Starting with NetWorker 19.7, support for restores from VBA is deprecated.
- 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:

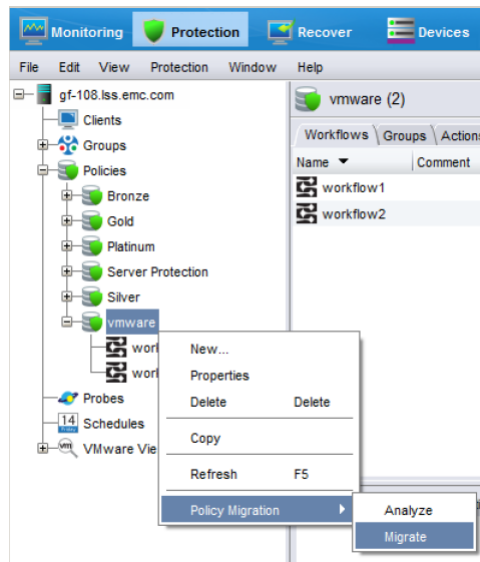
- The NetWorker version must be 19.6 or earlier for you to migrate VBA policies to vProxy.
- The Data Domain OS (DD-OS) is DDOS version 6.0.0.30, 6.0.1-10, or 6.1.x and later DDOS versions. Note that use of the DD Retention Lock feature on vProxy backup and clone actions requires DDOS 6.1.x and later.
- 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 19.3, this is version 4.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.

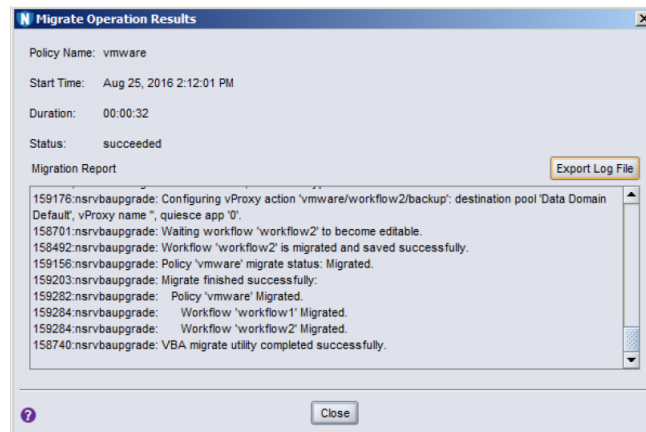
1. In the NMC **Administration** window, click **Protection**.
2. In the left pane, expand **Policies** to view the VMware policy.
3. (Optional) Right-click the **vmware** policy and select **Policy Migration > Analyze** from the drop-down if you want to perform a compatibility pre-check before migration.
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.

A **Migrate Operation Results** dialog box opens which provides a real-time report of the analysis and the migration until the process completes. You can then choose to export a log of the analysis 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.

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.

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.

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

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 and NetWorker Web UI. Starting with NetWorker 19.7, you can redeploy a vProxy from an OVA file located in the Content Library of vCenter 7.0 U3 and later using CLI.

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.

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.

vProxy redeployment retains disk provisioning type of previous vProxy during redeployment. After redeployment, vProxy disk provisioning type is:

- Set to thin if both vProxy disks are thin
- Set to thin if one of the vProxy disk is thick and the other is thin

- Set to thick if both vProxy disks are thick
- Set to thick provision lazy zeroed, if one is thick provision lazy zeroed and the other is thick provision eager zeroed

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

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	<p>For a single vProxy deployment, open a command prompt on the NetWorker Server, and then run the <code>nsrvproxy_mgmt</code> command in the following format:</p> <pre><b>nsrvproxy_mgmt redeploy -h vProxy-host-name -z vProxy-root-password [-x] [-f] [-u comments] [-t timeout in minutes] [-D debug-level]</b></pre>
Sequential deployment	<p>For sequential redeployment, you must create a batch file or a shell script on the NetWorker Server. For example, to initiate three sequential deployments run the following batch file or shell script.</p> <ul style="list-style-type: none"> <li>• On a NetWorker server running on Windows platform, to initiate sequential redeployment you must create a batch file.</li> </ul> <pre>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</pre> <ul style="list-style-type: none"> <li>• On a NetWorker server running on Linux platform, to initiate sequential redeployment you must create a shell script.</li> </ul> <pre>[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</pre>

**NOTE:** You can upgrade the vProxy appliance using NetWorker Web UI. For more information, see the NWUI Online Help. From NWUI, a maximum of 5 concurrent redeployment is supported.

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 of existing vProxy .
- `-z` is used when specifying the vProxy root password of existing vProxy.
- `-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.

vProxy is successfully redeployed.

## Limitations

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

- Concurrent vProxy redeployment is not supported using CLI. However, you can sequentially redeploy multiple vProxies 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.
- During vProxy redeployment, the manual settings that were performed in vProxy are not retained.

## Troubleshooting Redeployment Failures

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

**Table 8. Location of the vProxy redeployment log files**

Log file	Location on NetWorker server	Description
<job-uuid>.log	<ul style="list-style-type: none"> <li>• Linux: /nsr/logs/adhoc/nsrvproxy_mgmt</li> <li>• Windows: C:\Program Files\EMC NetWorker\nsr\logs\adhoc\nsrvproxy_mgmt</li> </ul>	vProxy management job log file is created during the redeployment of the associated vProxy.
vproxy_upgrade_session_<vProxyidentifier>_<jobuid>	<ul style="list-style-type: none"> <li>• Linux: /nsr/logs/adhoc/nsrvproxy_mgmt</li> <li>• Windows: C:\Program Files\EMC NetWorker\nsr\logs\adhoc\nsrvproxy_mgmt</li> </ul>	Associated nsrvisd log file is created during redeployment of the vProxy.
nsrvisd-daemon.log	<ul style="list-style-type: none"> <li>• Linux: /opt/nsr/vproxy/logs/nsrvisd</li> <li>• Windows: C:\Program Files\EMC NetWorker\nsr\vproxy\logs\nsrvisd</li> </ul>	Associated nsrvisd detailed log file is created.
ProxySessions-<uid>.log	<ul style="list-style-type: none"> <li>• Linux: /nsr/logs/adhoc/nsrvproxy_mgmt</li> <li>• Windows: C:\Program Files\EMC NetWorker\nsr\logs\adhoc\nsrvproxy_mgmt</li> </ul>	Associated ProxySessions log file is created during redeployment of the vProxy.
Nsrvisd logs	<ul style="list-style-type: none"> <li>• Linux: /opt/nsr/vproxy/logs/nsrvisd</li> <li>• Windows: C:\Program Files\EMC NetWorker\nsr\vproxy\logs\nsrvisd</li> </ul>	Associated inventory sessions log file is created.

# Protecting virtual machines

This chapter contains the following topics:

## Topics:

- [Overview of protection policies](#)
- [Preparing the NetWorker data zone](#)
- [VMware backups in the NetWorker Management Web UI](#)
- [vProxy backups in NMC](#)
- [Enabling vProxy Health Monitoring](#)
- [vProxy backup workflows in the vSphere Client's Dell EMC NetWorker interface](#)
- [Additional vProxy backup configuration options](#)
- [Enable the Microsoft VM App Agent for SQL Server application-consistent protection](#)
- [Updating the Microsoft VM App Agent and FLR Agent software](#)
- [Troubleshooting Data Protection Policies](#)

## 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, browse and 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.

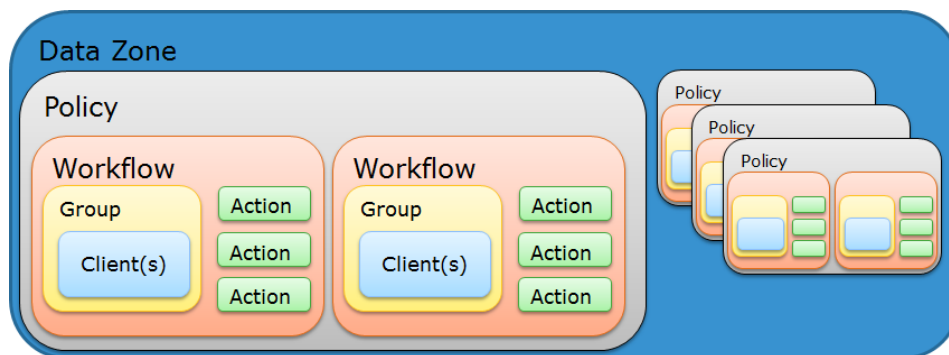


Figure 9. Data Protection Policy

## 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.

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

2. 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 a policy using the NetWorker Management Web UI

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

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 a restricted datazone (RDZ) from the **Restricted Data Zone** list to specify a RDZ for the directive.
6. Select **Enable Protection Period** to specify the protection period.
7. Enter the protection period value in minutes, hours, days, months, or years.
8. Click **NEXT**.
9. 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**.
10. 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.

#### 11. Click **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:


#### 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.

#### 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.

**NOTE:** If the interval attribute is set with less than 24 hours and the vProxy backup schedule is set to run, level Full from backup action, manual start of the workflow will run level Incremental instead of level Full. Level Full backup will be run during manual start of workflow only if the Interval is changed to 24 hours in the Workflow.

- 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.

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:

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.

Create the required policy and workflow.

To create an action:

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.

Create the required policy and workflow.

1. Select **Protection > Policies**.

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

2. Click an available policy to create a workflow or view existing workflows.

3. Click an existing workflow with the appropriate group association, or create a 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 that the virtual machines 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.
- Creating VMware backup action from NWUI with Transaction Log Backup enabled is always a full backup. It is recommended to use NMC for incremental level.

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 schedule. Click **ADD SCHEDULE** to create a schedule. The section "Create a schedule using the NetWorker Management Web UI" in NetWorker Administration Guide provides more information about 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 each day to specify the type of backup to perform.


The backup levels for NetWorker include 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 `smtmail` 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. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. The default value is 100.

26. 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**.

27. In the **Retries** field, specify the number of times that NetWorker should retry a failed backup action, before NetWorker considers the action as failed. When the Retries value is 0, NetWorker does not retry a failed backup action. The default value is 1. The number of retries can be set to a maximum of 24.

28. In the **Retry Delay** field, specify a delay in seconds to wait before retrying a failed backup action. When the Retry Delay value is 0, NetWorker retries the failed backup action immediately. The default value is 360. Retry delay can be set to a maximum of 3600 seconds.

 **NOTE:** If vProxy backup action is saved with retry delay set to 1, then retry delay will be automatically changed to 360.

29. 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.

30. 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.

31. Click **NEXT**.

The Action Configuration Summary appears.

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

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. To ensure that the savesets are cloned in chronological order (order in which the savesets were generated), enable the **Chronological Order** option. This option is disabled by default.
10. Click **NEXT**.
11. 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.
12. 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.
13. Specify the **Browse Period** value.

The browse period is less than or to equal to the retention period. The browse configuration is displayed only if it is following a traditional backup or if the clone is the first action within a workflow.

**NOTE:** To set a browse period that is different from the retention period, ensure that the group associated with the workflow does not include client types other than File System or NDMP.

14. 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.
15. If you want to have the same retention period as that of the backup action, select **Keep Retention Same as Backup**. However, if the clone action is the first action or if it is following a traditional backup, the option is **Keep Retention and Browse same as Backup**.
 

**NOTE:** A concurrent clone action always picks the save set (maximum) browse and retention time among all existing copies of (same) save set to be cloned. This maximum time is set as the retention period for newly generated clone copy, and not just the one which corresponds to the backup copy. Consistency of retention time for clone copies cannot be guaranteed in case multiple concurrent cloning actions are configured together.
16. Select **Apply Lock** under **DD Retention Lock** to enable retention lock for the virtual machines included in this clone action.
17. 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.
18. Click **NEXT**.
19. (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.

20. 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.

21. 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 in NetWorker Administration Guide provides more information on creating schedules.

 **NOTE:** For clone actions, you can only select or create an execute 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.
  - **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
- 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**.

22. 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.

23. Click **NEXT**.

24. 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**.

25. 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.

26. Click **NEXT**.

27. 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.

28. (Optional) Select **Concurrent** to enable concurrent operations for the action.

29. 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**.

30. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. The default value is 100.

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**.

(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:

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.

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. Select a restricted datazone (RDZ) from the **Restricted Data Zone** list to specify a RDZ for the directive.
6. From the **Type** list, select **Save Set**.
7. (Optional) From the **Policy** list, select a policy that you want to assign the group to.
8. (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.

9. 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 <b>Up To Now</b> . To specify a time period, select <b>Up to</b> .
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.

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. Select a restricted datazone (RDZ) from the **Restricted Data Zone** list to specify a RDZ for the directive.
6. From the **Type** list, select **VMware**.
7. (Optional) From the **Policy** list, select a policy that you want to assign the group to.
8. (Optional) From the **Workflow** list, select a workflow that you want to assign the group to.

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

9. Select a backup optimization mode.
  - **Capacity** - Use for variable segment sizing.
  - **Performance** - Use for fixed segment sizing.
10. (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.
11. Click **NEXT**.
12. 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.
13. 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.
14. 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.

**i** **NOTE:** When the VMware or Backup administrator removes or deletes the virtual machine from the vCenter, you can view the virtual machine name along with the failed UUID of a virtual machine in the **Monitoring > Workflows > Actions** page. You can click on the details icon beside the action name to view the **Failed Virtual Machines**. This is applicable for static selection of any virtual machine while creating protection groups for VMware workflows. If a virtual machine which is part of a static VMware group is deleted before a backup is performed, only the UUID is listed under the **Failed Virtual Machines** accordion.

15. Click **Preview** to view a list of the static and dynamic virtual machines and objects that have been added to the group.
16. Click **Finish**.

## Edit a group using the NetWorker Management Web UI

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

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.

**i** **NOTE:** You cannot change the name of the group.

3. Click **EDIT**, and make the required changes.

**i** **NOTE:** When editing client groups, the retired or decommissioned clients are not displayed.

4. Click **Save**.

**i** **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.

To create a rule, perform the following:

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. Select a restricted datazone (RDZ) from the **Restricted Data Zone** list to specify a RDZ for the directive.

7. 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

**i** **NOTE:** Rules with some special characters in category name and tag name may work during rule creation. However, it may lead to issues during editing or saving or fetching operations.

- Comma ,
- Double quotes "
- Single quotes '



- Backward slash \
- Forward slash /
- Colon :

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.

8. Click **Create**.

The Rule is successfully created.

9. 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:

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.

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**.

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

## Create a workflow for a new policy in NetWorker Administration

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.

 **NOTE:** If the interval attribute is set with less than 24 hours and the vProxy backup schedule is set to run, level Full from backup action, manual start of the workflow will run level Incremental instead of level Full. Level Full backup will be run during manual start of workflow only if the Interval is changed to 24 hours in the Workflow.

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

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.

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

**NOTE:** If the interval attribute is set with less than 24 hours and the vProxy backup schedule is set to run, level Full from backup action, manual start of the workflow will run level Incremental instead of level Full. Level Full backup will be run during manual start of workflow only if the Interval is changed to 24 hours in the Workflow.

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.

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.

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.

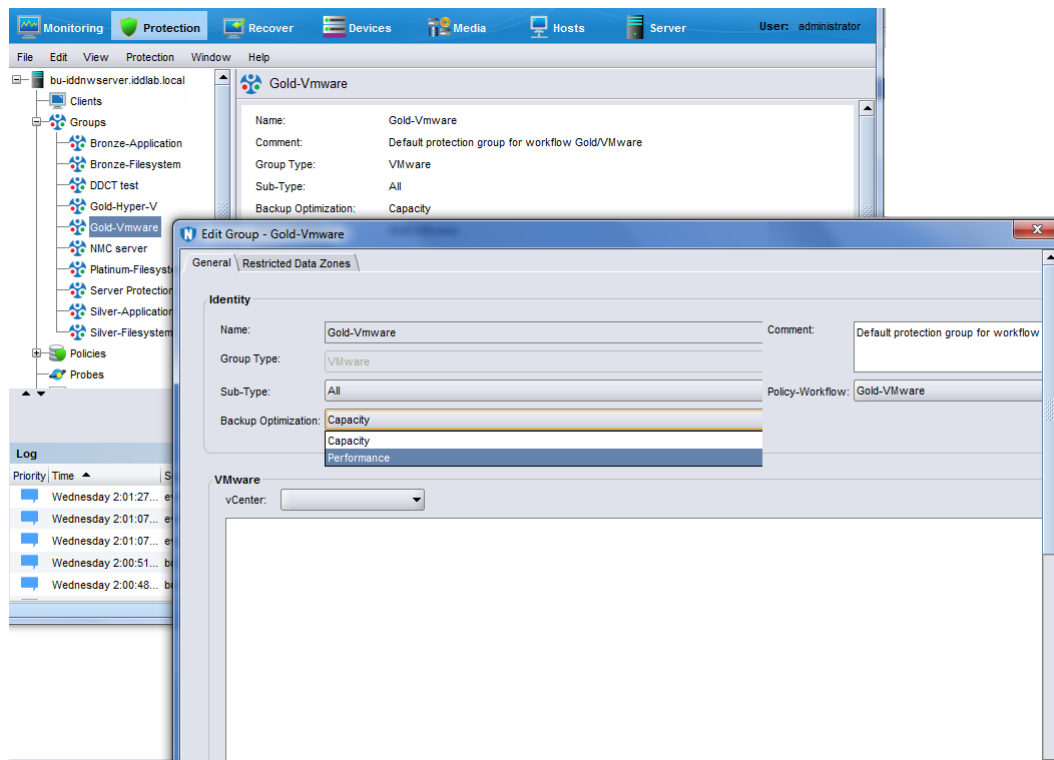


Figure 11. Changing the Backup Optimization mode in the vProxy protection group

## 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:Category1,Tag:Bronze1
- Category:Category2,Tag:Bronze2
- Category:Category3,Tag:Bronze3
- and so on up to Category:Category50,Tag:Bronze50

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 definitions](#) describes the acceptable rules, syntax, and grammar to use when writing such regular expressions.

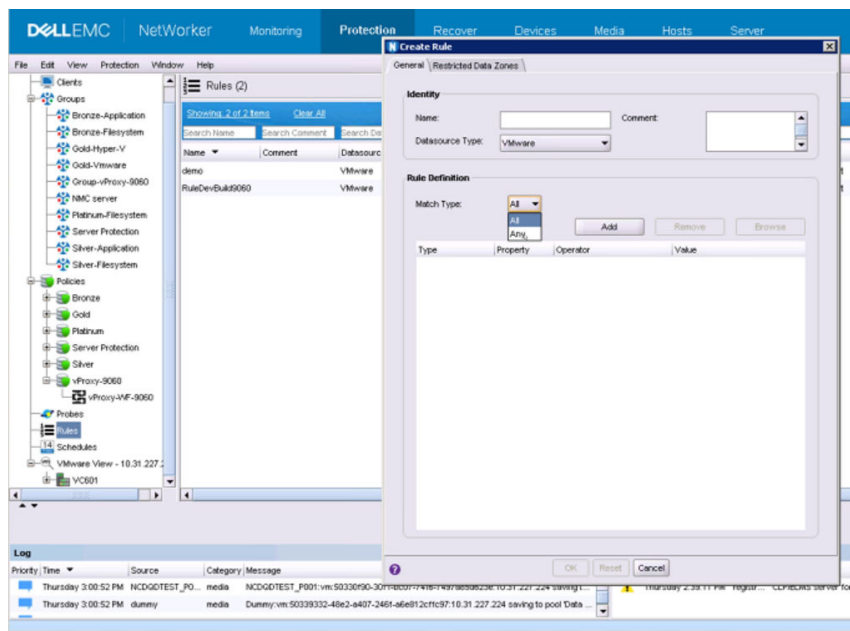
## Create a rule in NMC and associate the rule to a VMware group

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

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

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.

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.
- Rules with some special characters in category name and tag name may work during rule creation. However, it may lead to issues during editing or saving or fetching operations.
  - Comma ,
  - Double quotes "
  - Single quotes '
  - Backward slash \

- Forward slash /
- Colon :

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.

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

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 a vProxy policy and workflow. The *NetWorker Administration Guide* provides information about other action types.

Create the policy and workflow that will contain the action.

1. 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.

2. 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: / \ \* : ? [ ] ( ) \$ ! ^ ; ' " ~ ~ > < & | { }

3. In the **Comment** field, type a description for the action.

4. 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 occur after a disabled action do not start, even if the subsequent options are enabled.

5. From the **Action Type** list, select **Backup**.

6. From the secondary action list, select **VMware (vProxy)**.

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. 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.

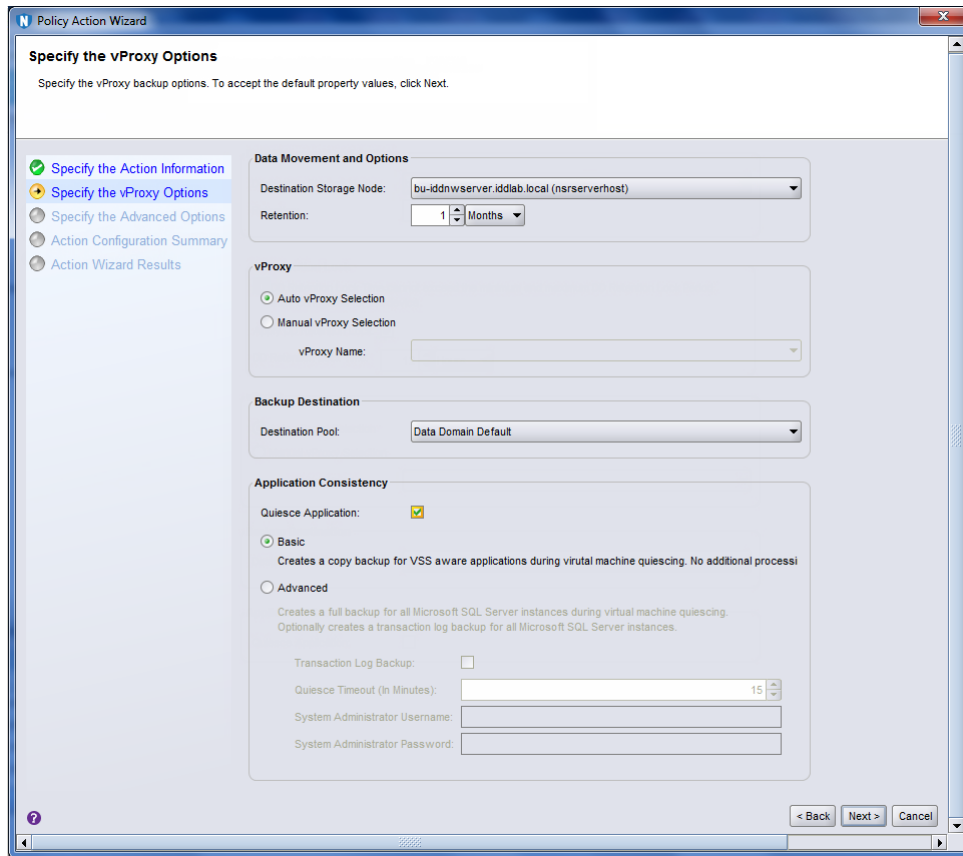
**Table 9. Schedule icons**

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.  <b>NOTE:</b> 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. If you want to perform the SQL Server backup separately from the VMware image-level FULL backup, you can set all days to **Skip**.

11. Click **Next**.  
The **Specify the vProxy and Application Protection Options** page displays.



**Figure 13. Specify the vProxy and Application Protection Options page**

12. In the **Data Movement and Options** pane:
  - a. From the **Destination Storage Node** box, select the storage node that contains the devices where you want to store the backup data. Note that 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`.
  - b. From the **Retention** spin boxes, specify the amount of time to retain the backup data. Note that after the retention period expires, the save set will be removed from the client file index and marked as recyclable in the media database during an expiration server maintenance task.
13. In the **DD Retention Lock** pane:,
  - a. 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. When you select **Apply DD Retention Lock**, the **DD Retention Lock Time** field displays.
  - b. 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.
14. In the **vProxy** pane, 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.
15. In the **Backup Destination** pane, 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.
16. In the **Application Protection Options** pane, select the **Application Protection** checkbox to enable application-consistent protection as part of the policy backup action, which includes protection of the Microsoft SQL Server. If you do not want to enable **Application Protection**, skip to step 19.
17. (Optional) Choose one of the following options from the **Application Protection Type** drop-down:
  - Select **Separate Application Backups** to orchestrate and deploy the NetWorker Module for Microsoft (NMM) to perform an SQL Server backup separate from the VMware image-level FULL backup.

- Select **Part of VM Image Backup** to perform application-consistent protection as part of the VMware image-level FULL backup.

If you select the **Separate Application Backups** option, and then select the **Quiesce Application** checkbox, only **Basic** quiescing can be performed since NMM is used for the SQL server application-consistent backup with this option.


If you select the **Part of VM Image Backup** option, the **Quiesce Application** checkbox is selected and you can choose from the following quiesce methods:

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


18. Click **Next**.


The **Specify the Application Protection Configuration Options** page displays.

If you selected the **Separate Application Backups** option, complete the following additional fields:

- **System Administrator Username and Password**—Specify the virtual machine guest credentials for a user with administrative privileges.
- **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.
- **Period**—Select a schedule for NMM to run the backup action (Weekly by day or Monthly by day), and then set the backup level for specific day(s) if desired.
- **Promote to full backup**—Select this checkbox to always promote the SQL database backup to FULL to ensure the database gets backed up every time. This setting is particularly useful if you perform transaction log backups and are using more than one application for backups, which can cause interference with the log chain.
- **Exclude Databases**—If the VMware group is enabled with Dynamic Association, click the + sign if you want to create or assign a rule to this action that will exclude certain SQL databases from the backup. The section provides more information on creating and assigning rules.
- **Client Override Behavior**—As part of the default Orchestration behavior, some settings from the NMM Client Configuration wizard (if used) are applied to all SQL virtual machines. If you select **Client Can Override**, you can override some of those defaults in the client. This can be useful if you want the action to honor some settings, such as backup promotion or decision flags, from the NetWorker VMware backup policy instead of the NMM Client Configuration wizard.
- **Use System Admin credentials for App Admin**—Select this checkbox if you have a different user (an Application Administrator) that is responsible for performing **Separate Application Backups** using NMM, but this user has the same credentials as the System Administrator. When you select this checkbox, the **Application Administrator Username and Password** are grayed out.
- **Application Administrator Username and Password**—If the user performing the **Separate Application Backups** using NMM is different from the System Administrator, and this user has different log in credentials, specify the Application Administrator username and password in these fields.

If you selected the **Part of VM Image Backup** option with **Advanced** quiescing, complete the following additional fields:

- **System Administrator Username and Password**—Specify the virtual machine credentials for a user with administrative privileges.
- **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.

 **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.

19. Click **Next**.

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

20. Ignore the **Retries**, **Retry Delay**, and the **Inactivity Timeout** options. The VMware Backup action does not support these options.

21. In the **Parallelism** field, specify the maximum number of concurrent operations for the action.

22. 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.

23. 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.

24. (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.

25. 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**.

26. 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 Window, 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**.

The **Action Configuration Summary** page appears.




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

(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.



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 occur 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 10. 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**.

(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.

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.

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.

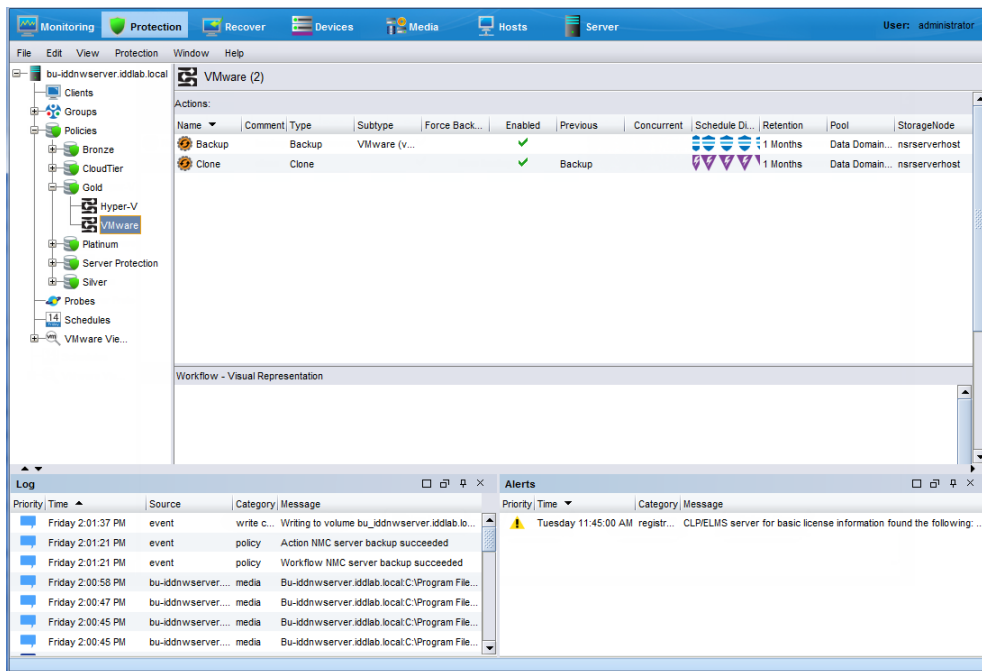


Figure 14. VMware protection policy in the Protection window

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.

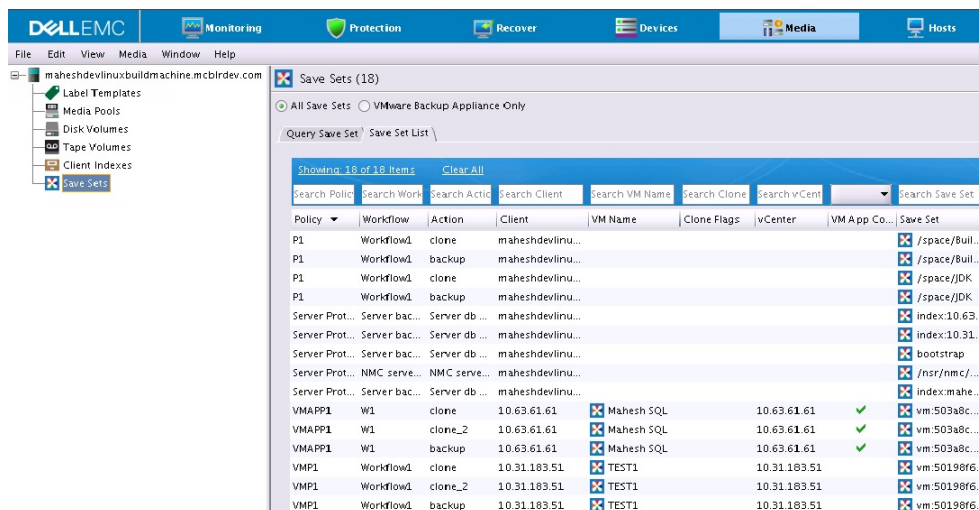
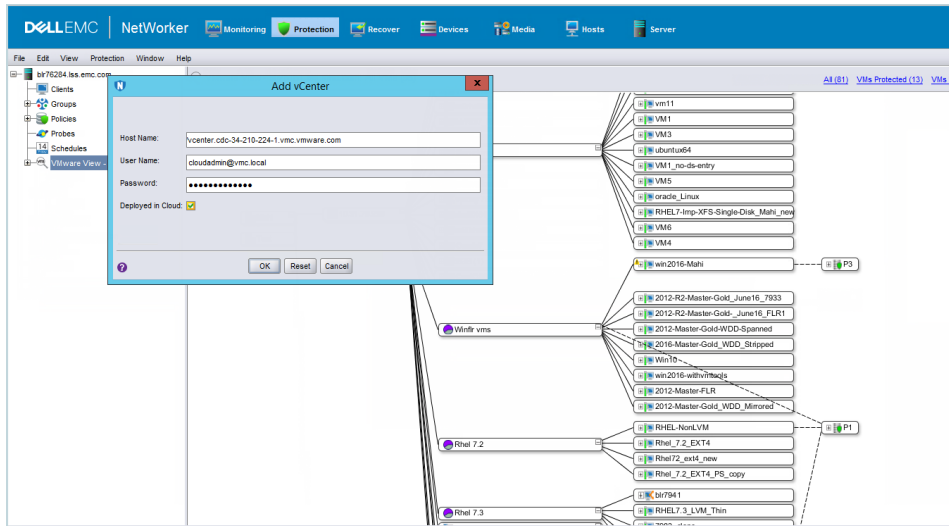


Figure 15. VMware protection policy save sets in Media window

## 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.

**NOTE:** Upon refresh of VMware View in NMC in a large VMware vCenter environment, the background process nsrvim consumes a high amount of memory on the NetWorker server. For example, nsrvim can consume up to 7 GB RAM in a site with 200 ESXi hosts and more than 4000 virtual machines in a single vCenter. This memory is used to load vCenter inventory data into local structures. If this occurs, depending on the scale of the VMware environment, allocate more RAM to the NetWorker server to reduce the impact of this memory consumption. As a best practice allocate at least 2GB of RAM per 1000 VMs on a given vCenter.

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

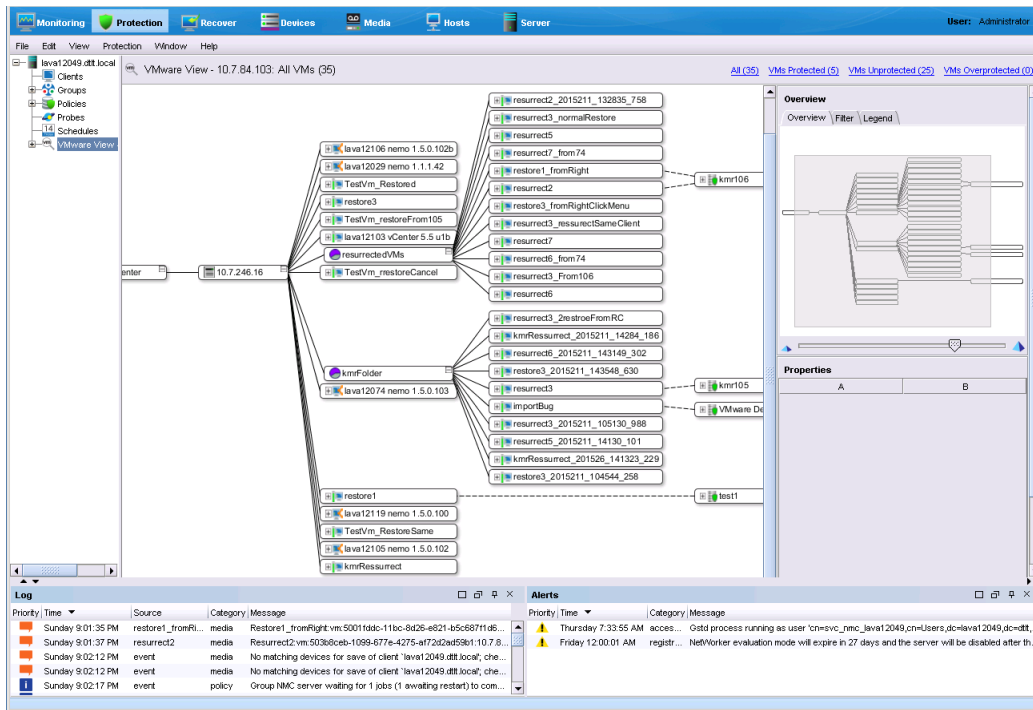
You can use several operations to navigate within the map view:

- 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.

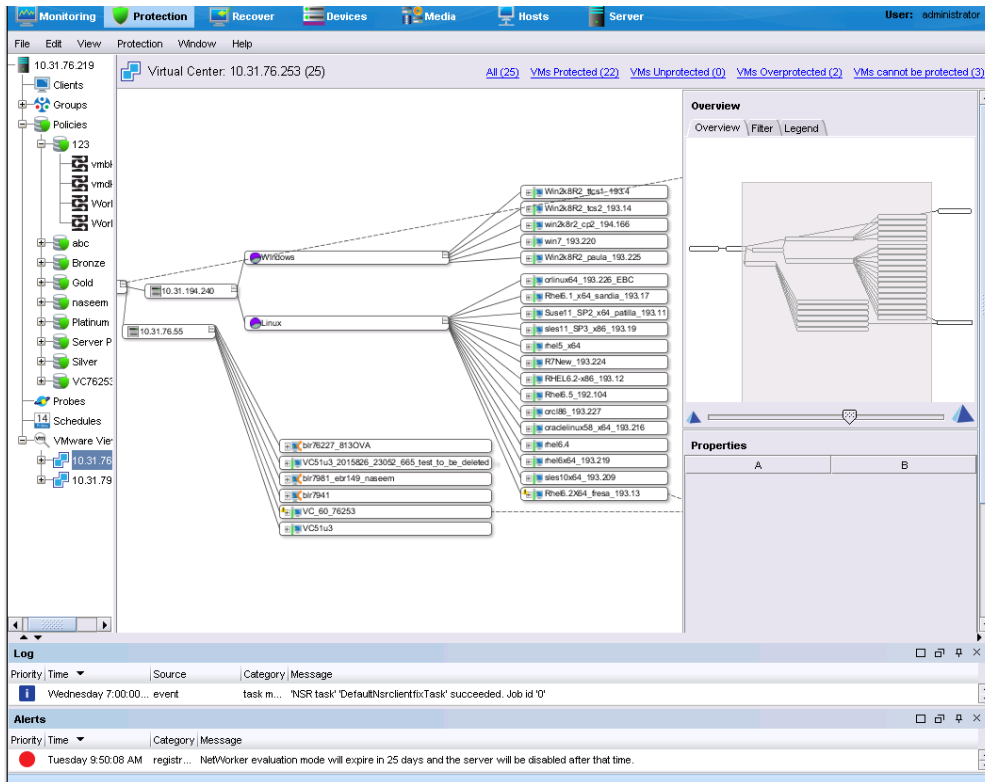


Figure 18. Cluster with child elements in VMware View

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.

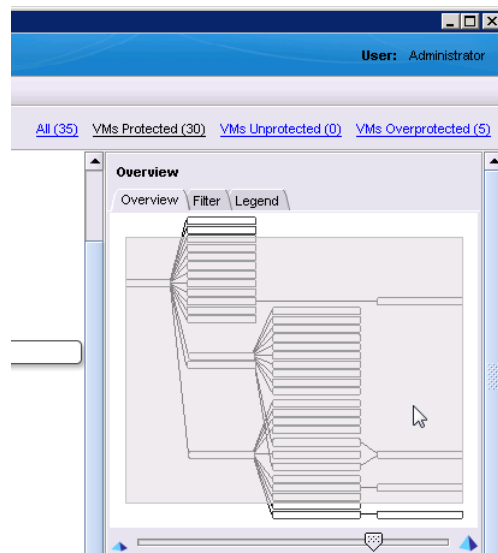


Figure 19. Filtering results in VMware View

## 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.

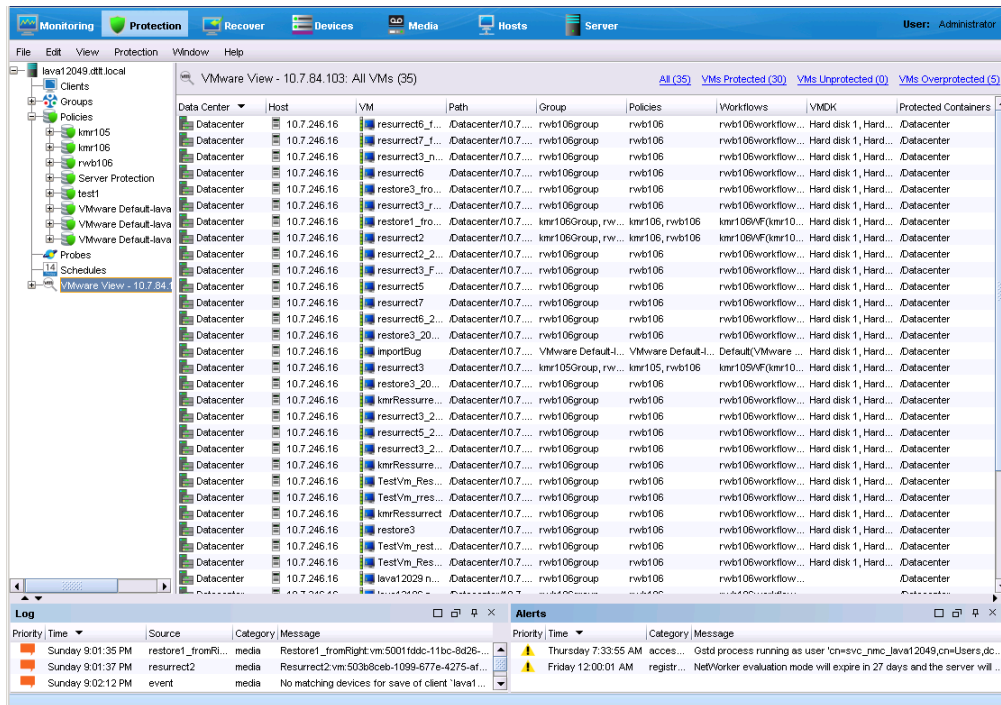


Figure 20. VMware table view

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**.

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.



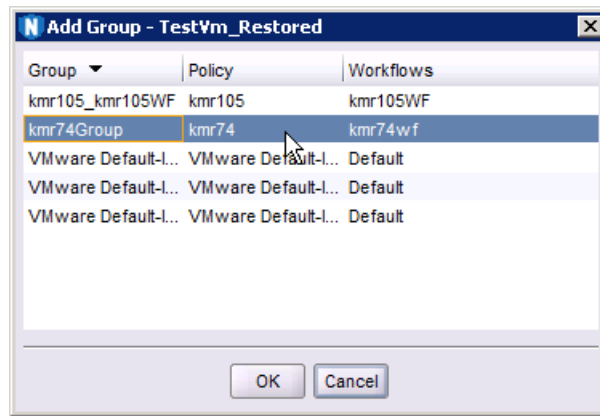


Figure 21. Add group in VMware View

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.

## Enabling vProxy Health Monitoring

You can receive notifications when the vProxy goes to unavailable state by configuring the NSR notification resource "vProxy is unavailable" to send an email notification or an snmp trap. The "vProxy is unavailable" notification can be configured using NMC, NWUI and CLI.

1. On the **NetWork Administration** window, click **Server**.
2. On the Server window, select **Notifications**, select **vProxy is Unavailable** and, then click **Edit**.
3. Specify the following command in the Action field to set SNMP trap notifications for Windows and Linux.
  - Windows: `C:\Program Files\EMC NetWorker\nsr\bin\nsrtrap.exe" <IP of Trap Receiver>`
  - Linux: `/usr/sbin/nsrtrap <IP of Trap Receiver>`
4. Configuring email notification.
  - Specify the following command in the Action field to set email notifications for Windows `smtplib -s subject -h mailserver recipient1@mailserver recipient2@mailserver...`
  - Perform the following steps to configure email notification in a Linux server:
    - a. Run the command `postfix stop`
    - b. Open `/etc/postfix/main.cf` in the vi/vim editor and set the relay host attribute value to `<Mail Server>`.
    - c. Run the command `postfix start`
    - d. Specify the command in the Action field: `/usr/bin/mail -r <sender_mail_address> -s "subject_name" <receiver_mail_address> <location of the file>`



# 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:**

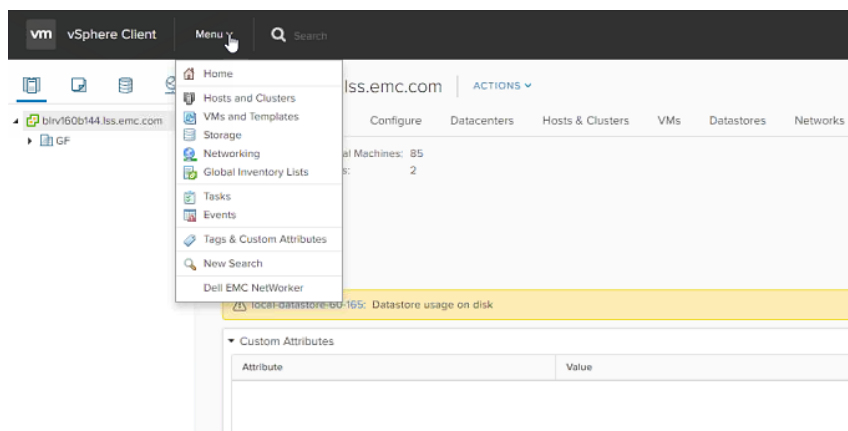
- Backup and recovery operations in the **vSphere Client Dell EMC NetWorker** interface are not supported for SQL Server advanced application-consistent protection policies. Perform these operations from the NMC **NetWorker Administration** window or the **Dell EMC Data Protection Restore Client**.
- Do not protect same virtual machine with NetWorker vProxy and any other backup, protection product or vSphere replication.

## 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**.

**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.

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 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**.

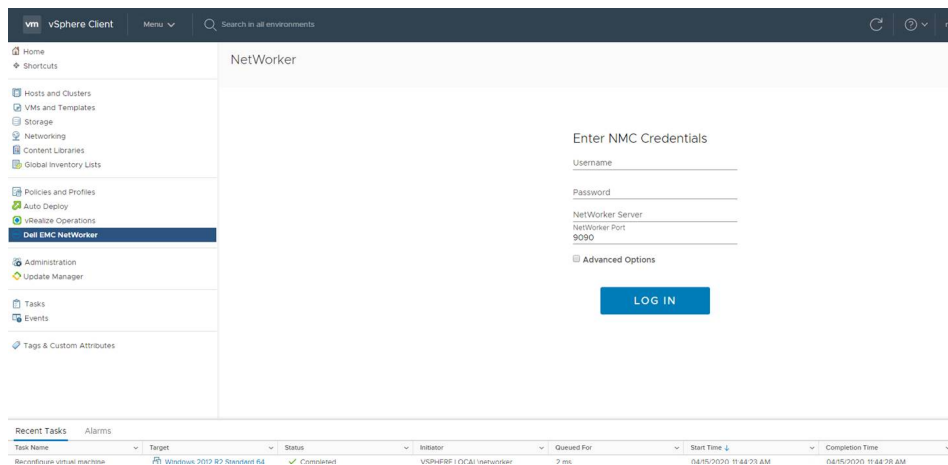


Figure 23. NetWorker connection information in the vSphere Client

#### 4. Click **Log in**.

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

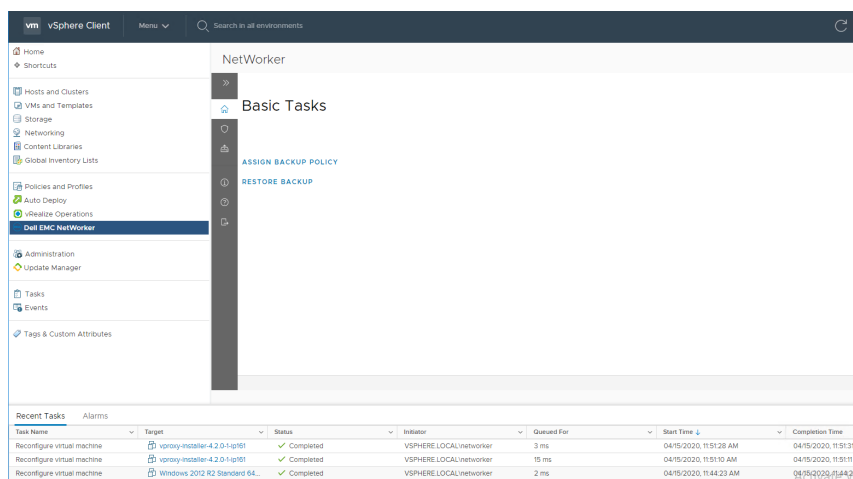

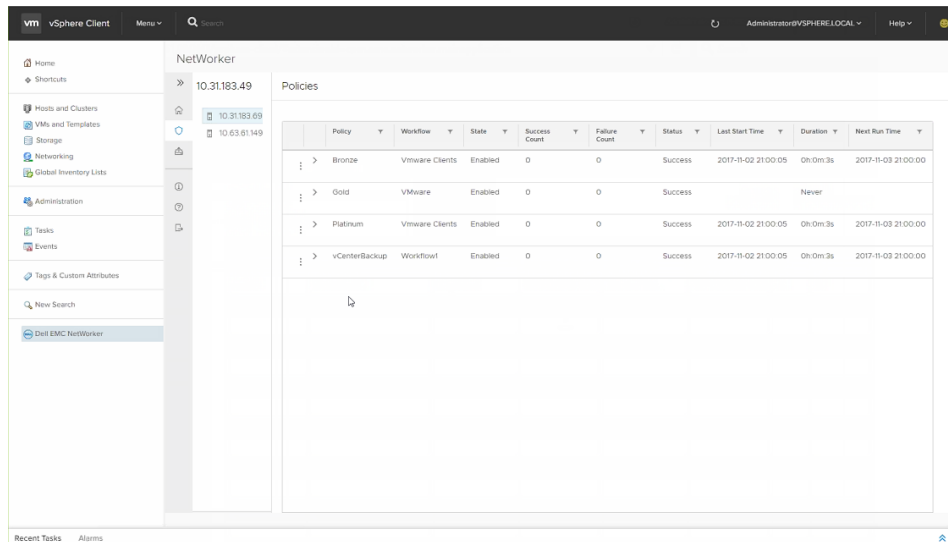


Figure 24. Dell EMC NetWorker Basic Tasks pane

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

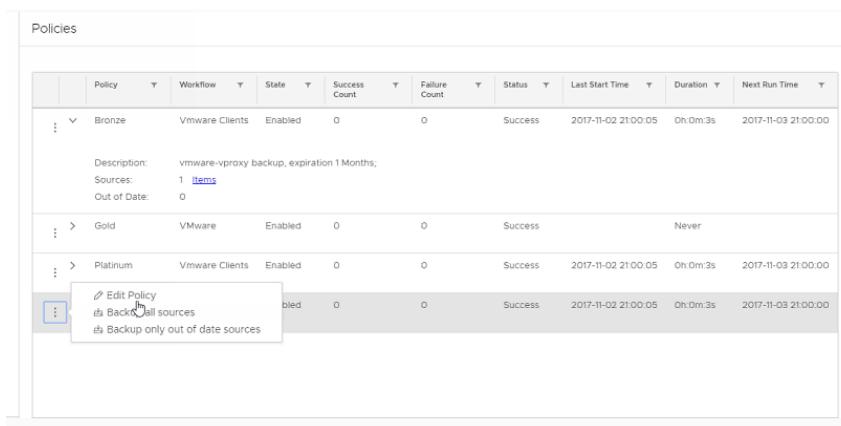
To start a vProxy backup policy by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

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.



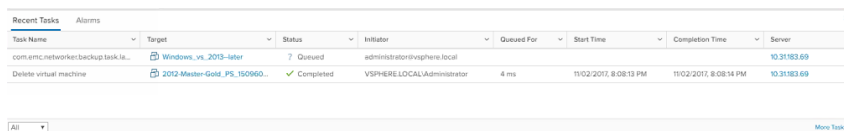
**Figure 25. Policies pane with available vProxy policies**

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**

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.



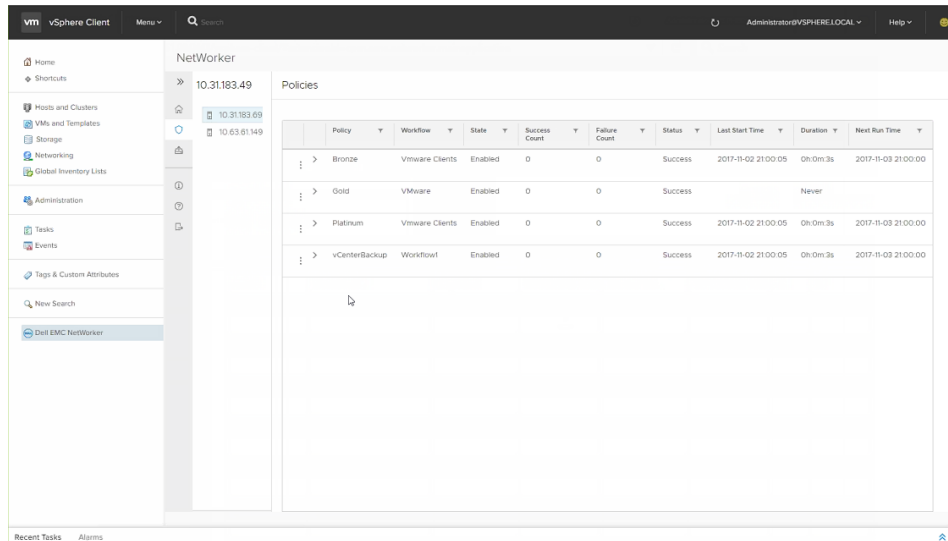
**Figure 27. Recent Tasks pane**

## 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**.

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**.

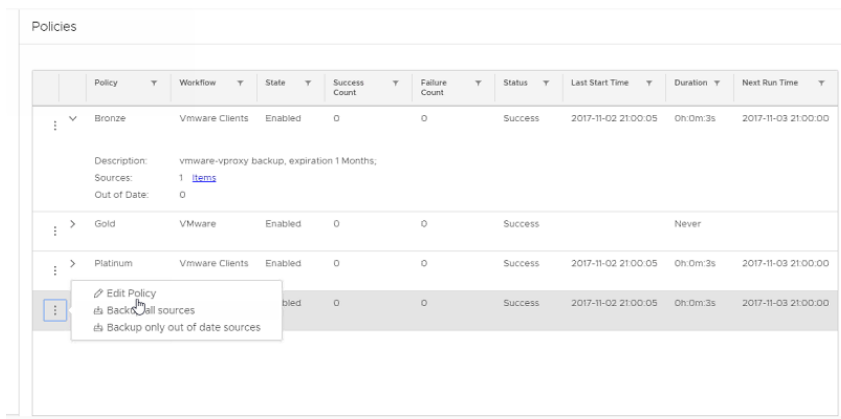
A list of available vProxy policies that were created in NMC displays in the right pane.



**Figure 28. Policies pane with available vProxy policies**

**NOTE:** The Backup tab in the vSphere Client's Dell EMC NetWorker user interface displays the last start time based on the start time of the backup for the virtual machines in the policy. Therefore, if the same virtual machine is contained within multiple policies, then the last start time displayed will be identical between the two policies.

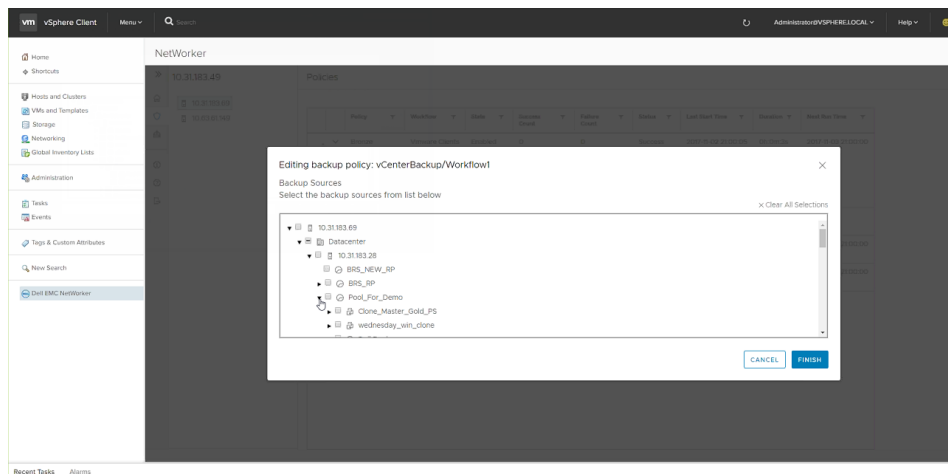
- Click the arrow to the left of a policy to expand and view the policy and workflow details. You can click the **Items** link under the Workflow to display the virtual machines protected by this workflow.
- To add virtual machines to the workflow, click the three dots next to the policy and select **Edit**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



**Figure 29. Edit a vProxy policy**

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

- 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**

**NOTE:** If you add a virtual machine that has already been backed up by an existing workflow to a new workflow within the Dell EMC NetWorker in the vSphere Client, the Last Start Time of the new workflow gets updated automatically in the Backup tab, even if the workflow has not yet been started.

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

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.

The *VMware vSphere Security Guide* provides more information about virtual machine encryption.

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.

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.

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 VM Proxy 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** in the **vSphere Client**. 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. Select 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.

## 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](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.

**i 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 11. MSVMAPPAGENT binaries called by vProxy**

Binary	Purpose	When called
<code>Msvmagent_discovery.exe</code>	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. <b>i NOTE:</b> If <code>Msvmagent_discovery.exe</code> 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.
<code>Msvmagentcatsnap.exe</code>	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.
<code>Msvmagent_appbackup.exe</code>	Performs transaction log backup.	Called by vProxy for transaction log backup workflows. The <code>Msvmagent_appbackup.exe</code> program will back up all SQL instances in the virtual machine. <code>Msvmagent_appbackup.exe</code> performs transaction log backup only, and does not create a virtual machine image backup.
<code>Msvmagent_snapshotrestore.exe</code>	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 <code>Msvmagent_snapshotrestore.exe</code> copies the VSS manifest documents



**Table 11. MSVMAPPAGENT binaries called by vProxy (continued)**

Binary	Purpose	When called
		<p>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 <code>msvmagent_snapshotrestore.exe</code> 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.</p>
<p><code>Msvmagent_apprestore.exe</code></p>	<p>Performs restore of individual SQL transaction log backup.</p>	<p>Called by vProxy during restore of the transaction log backup.</p> <p>For each transaction log restore, <code>Msvmagent_apprestore.exe</code> 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 option. The <code>msvmagent_apprestore.exe</code> 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.</p>

**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 12. Supported characters in SQL database names**

Special character	FULL and transaction log backup	FULL and transaction log restore
~ Tilde	Supported	Supported
- 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 <b>NOTE:</b> 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.

- 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, use the **Dell EMC Data Protection Restore Client**.
- The Backup and Restore of SQL App consistent VM with one or more independent persistent Disks is not supported for APPSVM.
- Multi NIC Networker server configuration is not supported for APPSVM

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.EnableUUID* 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 or when a previous backup 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 then select **Home > Inventory > Hosts and Clusters**.
2. Select the virtual machine, and then select the **Summary** tab.
3. Clear the value that appears in the **Dell VM Direct Engine 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.

## 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.

## Backup fails when names include special characters

When spaces or special characters are included in the virtual machine name, datastore, folder, or datacenter names, the `.vmtx` file is not included in the backup.

The vProxy appliance does not back up objects that include the following special characters (format: 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 is 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 13. 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 Engine, 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 vProxy Agent operations on Linux

The **vProxy 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 enables you to manage command execution through the **vProxy Agent**, is modeled on the corresponding `vmtoolsd` file. The settings in this file permit command execution by any user who is able to perform vProxy operations on the guest virtual machine. A system administrator can further modify this file to specify which users can perform **vProxy 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 14. 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 `vmbbackup` broker of `nsrd` is disabled by default. To turn on additional logging, you can touch an empty file at `<nsr>/tmp/vmbbackup_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.

## vProxy Log Bundle collection using NMC

To collect log bundle information for a particular vProxy, 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 configured vProxies.
3. Right-click the vProxy 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.
- NMC cannot collect the log bundle when accessed from a remote machine that cannot communicate with vProxy.

## vProxy Log Aggregation Management Tool

vProxy Log Aggregation Management tool is a CLI tool that helps you perform the following actions:

- Add or delete vProxies for log aggregation.
- Run the log aggregation for all the vProxies.
- View log aggregation status of all the vProxies.

NSR task schedules the periodic run of log aggregation for all the vProxies added for log aggregation. When you add a vProxy, log aggregation for this vProxy starts at the next scheduled time and vProxy logs are aggregated periodically in the directory path that you provided in NetWorker Server.

vProxy Log Aggregation Management tool (`nsrvproxy_log_mgmt`) is available as a binary bundled as a part of VISD component. The binaries are located in the following path:

- Windows: <NW install path>/nsr/vproxy/bin/
- Linux: /opt/nsr/vproxy/bin

vProxy Log Aggregation Management tool is operated by `nsrvproxy_log_mgmt.sh` or `nsrvproxy_log_mgmt.bat` scripts. This script sets the necessary environment variables to perform log aggregation and creates the directories for storing logs and state files. The location of the script is:

- Windows: `C:\Program Files\EMC NetWorker\nsr\bin`
- Linux: `/usr/sbin`

## Adding vProxy for Log aggregation

The vProxy log aggregation helps you to aggregate vProxy logs in NetWorker Server.

You can add the vProxy for log aggregation by running the command: `/nsrvproxy_log_mgmt.sh addvProxy -host=<host name/IP of vProxy> -port=<vProxy port number> -user=<vProxy user name> -password=<vProxy password> -logstoragelocation=<absolute path to store collected logs>`

Example,

```
./nsrvproxy_log_mgmt.sh addvProxy -host=10.x.x.4 -port=9090 -user=admin  
-password=emclegato -logstoragelocation=/root/logaggregation
```

## Removing vProxy from Log aggregation

You can remove the log aggregation by deleting the vProxy and unsetting the log aggregation environment variable.

You can remove the vProxy for log aggregation by running the command: `./nsrvproxy_log_mgmt.sh deletenvProxy -host=<host name/IP of vProxy>`

For example,

```
./nsrvproxy_log_mgmt.sh deletenvProxy -host=10.x.x.4
```

## Viewing vProxy Information

You can view the vProxy information by using `nsrvproxy_log_mgmt` command.

You can view the vProxy information by running the command: `./nsrvproxy_log_mgmt.sh show`


For example,

```
/nsrvproxy_log_mgmt.sh show  
  
Hostname/IP: 10.x.x.4  
Last Log Aggregation Status: ACTIVE  
Log Aggregation Location: /root/logaggregation  
Last Log Aggregation Time: 2019-10-17T01:58:08-04:00
```

## Running Log Aggregation

NSR task runs the `nsrvproxy_log_mgmt.sh` command to run the log aggregation of all the added vProxies.

To perform log aggregations of all the added vProxies, run the command: `/usr/sbin/nsrvproxy_log_mgmt.sh run`

 **NOTE:** For windows, run the `nsrvproxy_log_mgmt.bat` file.

NSR vProxy log aggregate RAP resource can be used for configuring the log aggregation task. For more information, see the Commands Reference Manual.



## Logs for SQL application-consistent data protection

The following section provides location information for all logs associated with SQL application-consistent data protection.

**i** **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/`.

# Recover virtual machines and data

This chapter contains the following topics:

## Topics:

- [Preparing the NetWorker datazone for recovery](#)
- [vProxy recovery in NMC](#)
- [vProxy recovery in the NetWorker Management Web UI](#)
- [vProxy file-level restore and SQL restore in the Dell EMC Data Protection Restore Client](#)
- [vProxy recovery in the vSphere Client's Dell EMC NetWorker interface](#)
- [vProxy backups and restores using Direct Fiber channel](#)

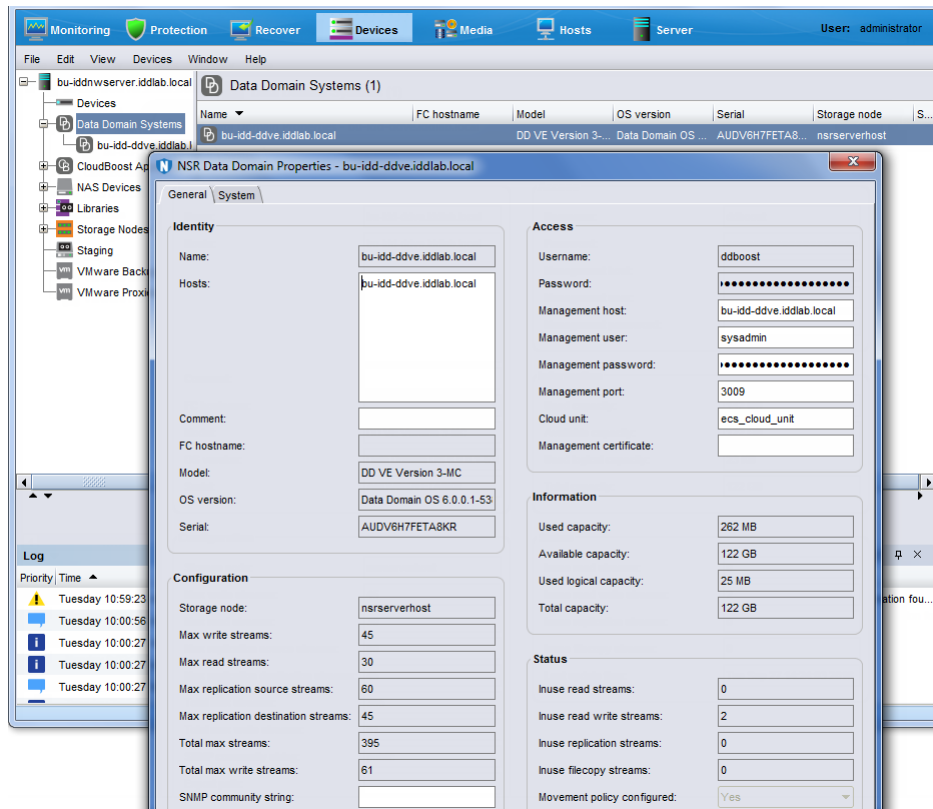
## Preparing the NetWorker datazone for recovery

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 Client**.

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 31. 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.

**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.

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/IPv6 address OU=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-objectclass=inetOrgPerson -D config-user-search-path=OU=user -D config-userid-attr=cn -D config-group-search-path=OU=user -D config-group-nameattr=cn -D config-group-object-class=group -D config-group-memberattr=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**.

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

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.

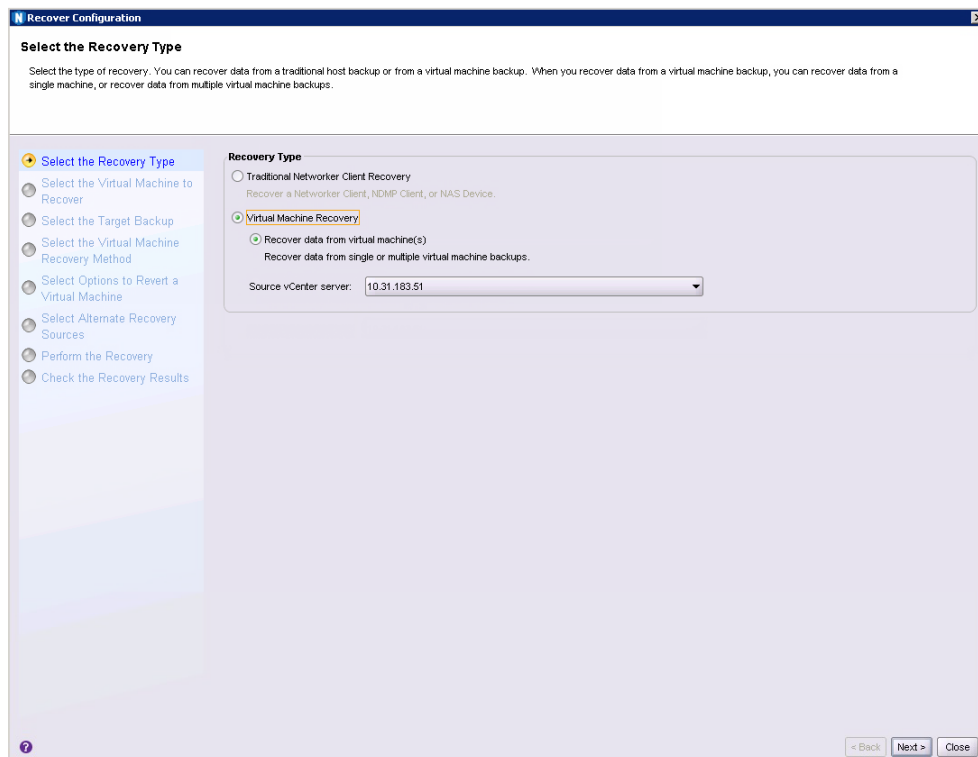


Figure 32. Virtual machine recovery in the NMC Recovery wizard

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.

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**.

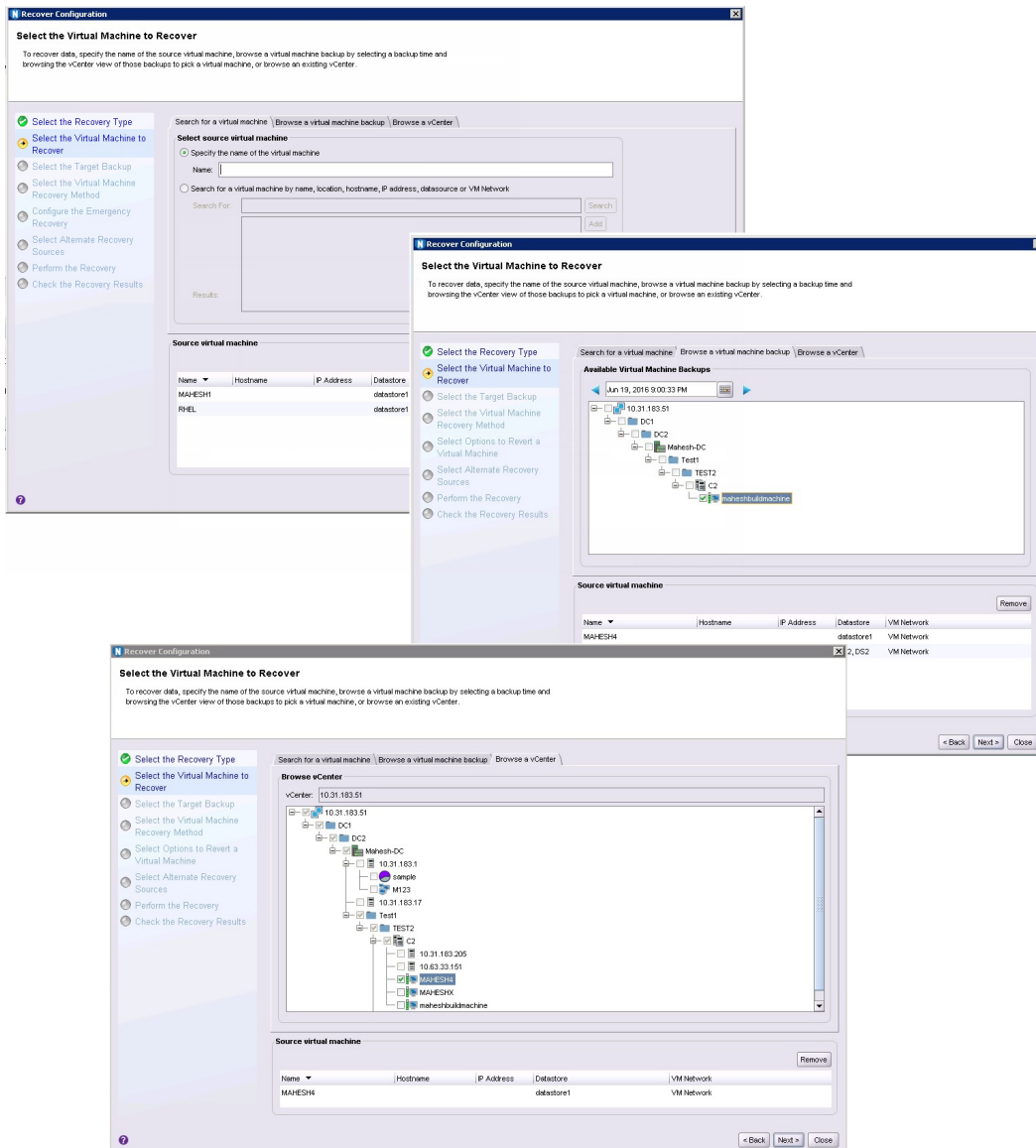


Figure 33. Select the Virtual Machine to Recover

- 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**.

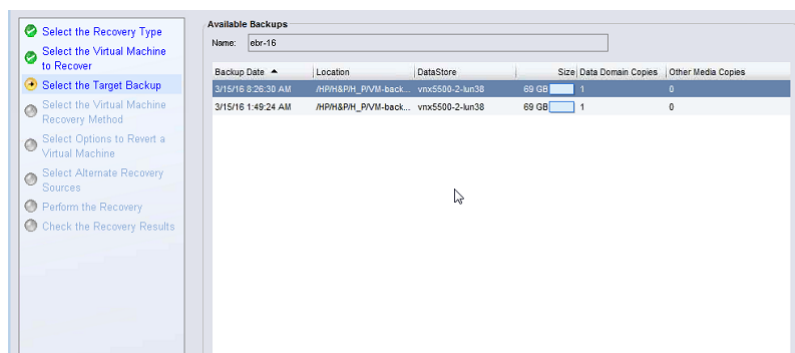


Figure 34. Select the Target Backup (individual virtual machine)

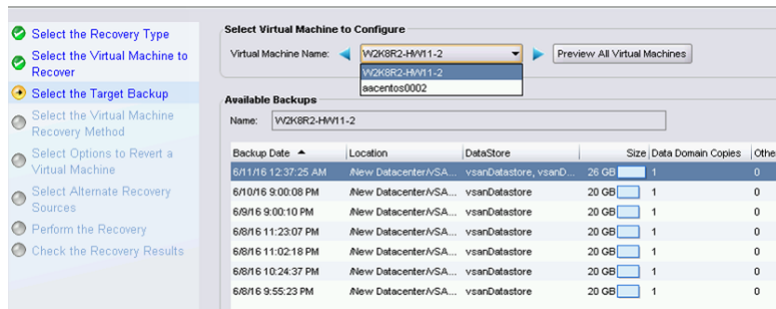


Figure 35. Select the Target Backup (multiple virtual machines)

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).

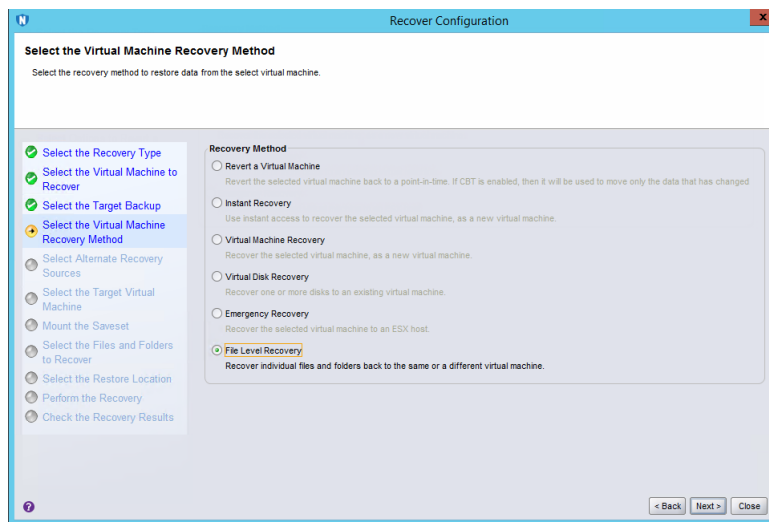


Figure 36. Select the Virtual Machine Recovery method

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.

**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.

1. In the **Select the Virtual Machine Recovery Method** page:
  - a. Select **Revert a Virtual Machine**.
  - b. Click **Next**.

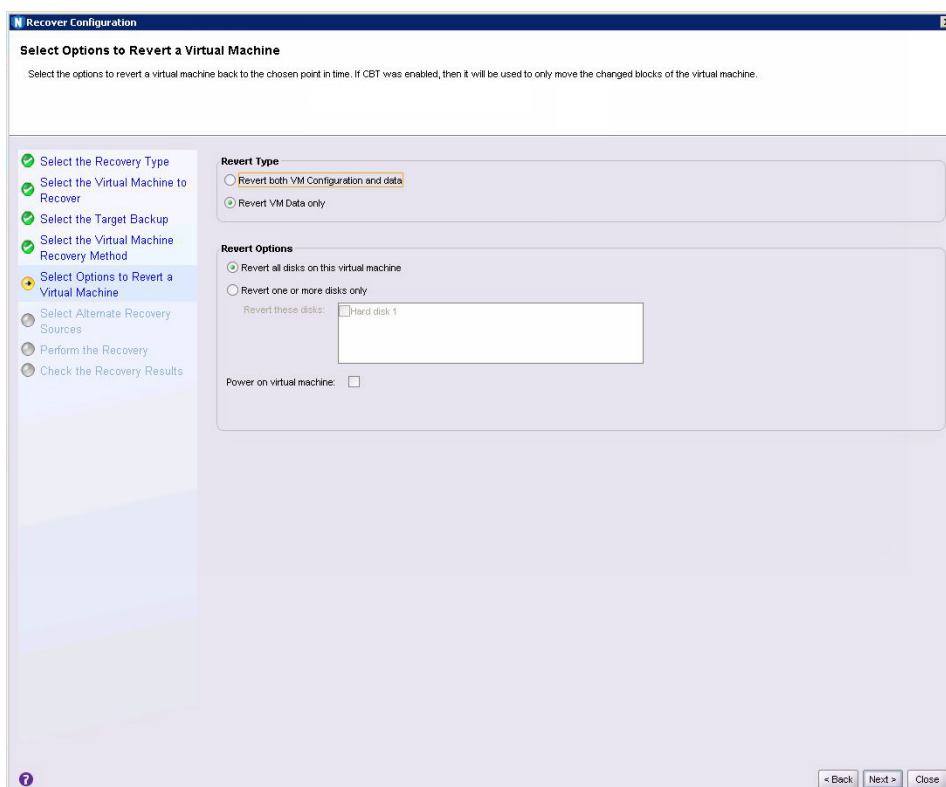
The **Select Options to Revert a Virtual Machine** page displays

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**.

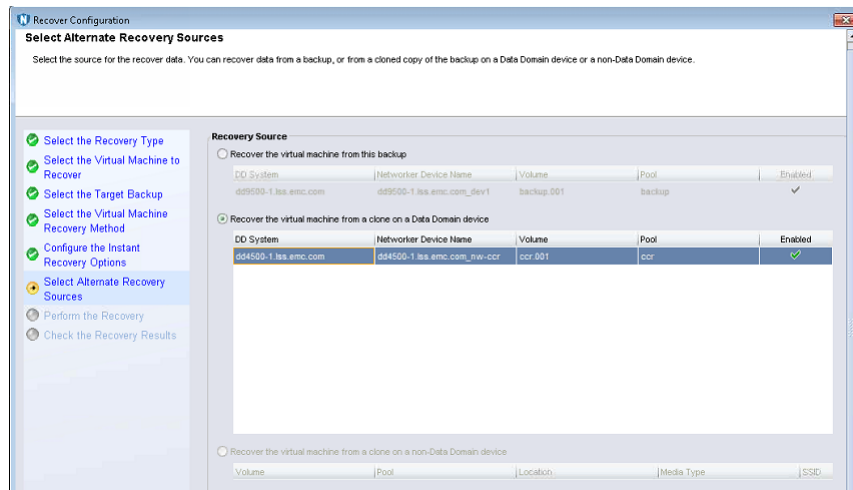
**NOTE:** If the virtual machine is currently powered on, a dialog displays requesting confirmation to power off the virtual machine. Additionally, if a change has occurred in the virtual machine configuration since the backup, a warning message displays.



**Figure 37. 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 38. 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**.

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

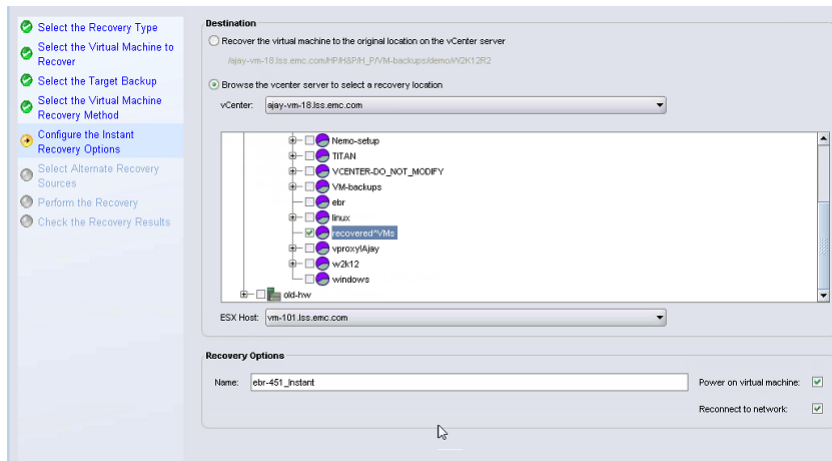
The next virtual machine recovery option available in the NMC Recovery wizard is instant recovery of a virtual machine backup. With instant recovery, the virtual machine backup is read directly from the Data Domain device and the VMDKs will be restored directly on a Data Domain device. You can perform one instant recovery session at a time.

Before you begin, 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.

To complete the Recovery wizard with the instant recovery method, perform the following steps:

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 39. 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**.

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.

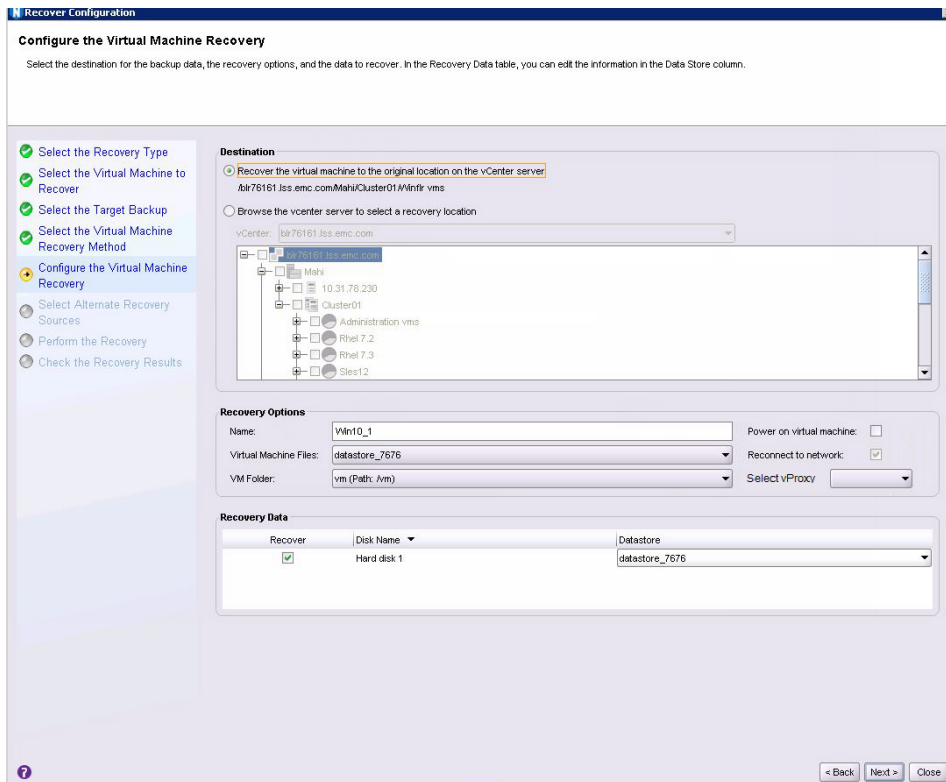
**NOTE:** To optimize use of NetWorker and Data Domain resources, it is strongly recommended that you stop the instant recovery session once you satisfy your recovery objectives.

## 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.

To complete the Recovery wizard with the virtual machine recovery method, perform the following.

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 40. 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:**

- Select the original virtual machine backup, or 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**.

**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:**

- 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 virtual machine recovery is complete.

## Virtual Disk Recovery

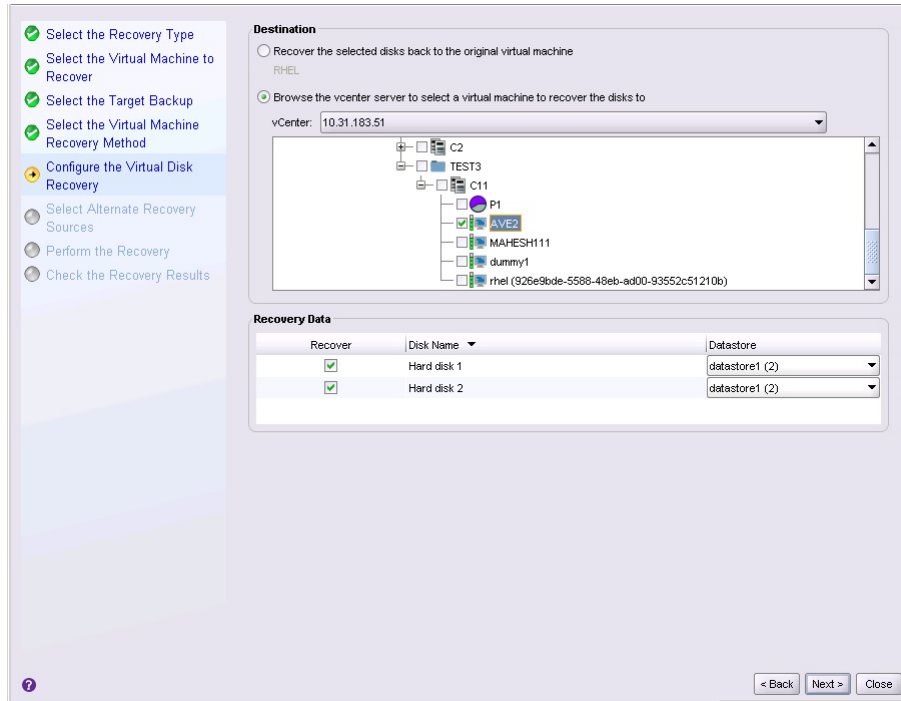
The next virtual machine recovery option available in the NMC Recovery wizard is to perform a virtual disk, or VMDK, recovery. With VMDK recovery, the disks from the virtual machine backup are recovered to an existing virtual machine.

To complete the Recovery wizard with the virtual disk recovery method, perform the following.

**1. In the **Select the Virtual Machine Recovery Method** page:**

- 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 41. 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**.

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.

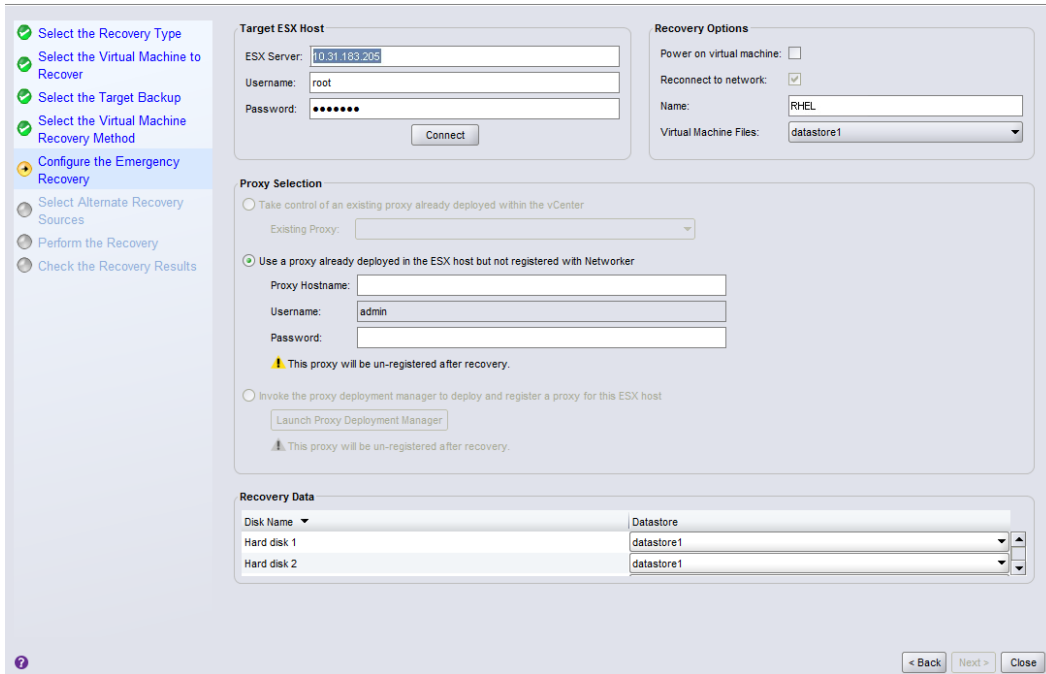
Emergency Recovery requires a vProxy set up on the ESXi host prior to running the recovery.

Additionally, ensure that you disconnect the ESXi host from the vCenter server.

**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:

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 42. 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**.

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

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.

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.

**NOTE:** vProxy FLR Agent creates and maintains a file on each discovered file system (volume) that has information about the volume's original path. The file name is in the form "DellEMC\_VolumeID\_path.info", where the path is in URL-encoded form of the last discovered path of the file system. These files are used during the FLR mount operation and are re-created again if they are found missing.

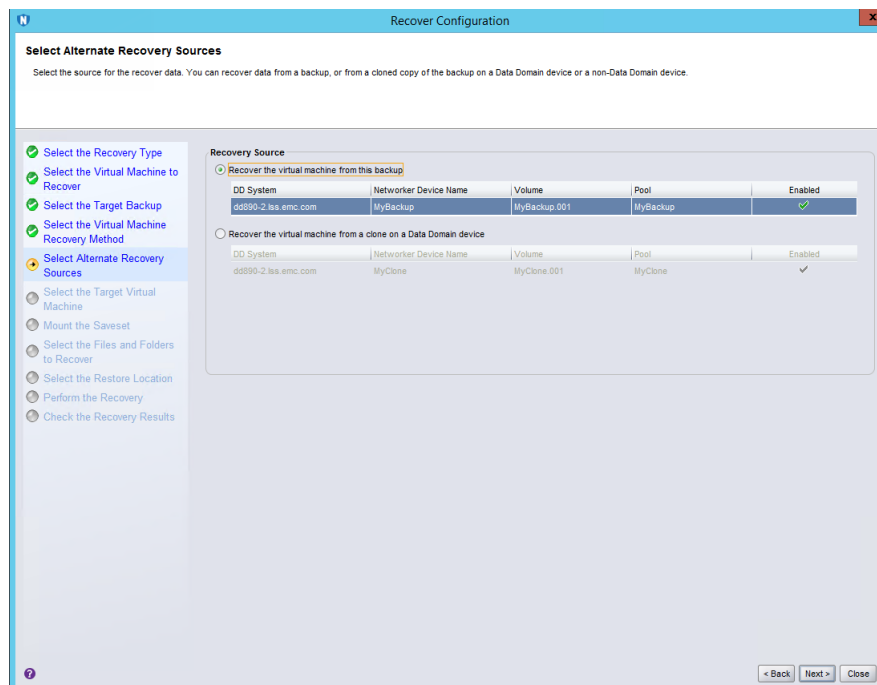
File level recovery in the NMC **Recovery** wizard can only be performed by an administrator.

**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:

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 43. 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.

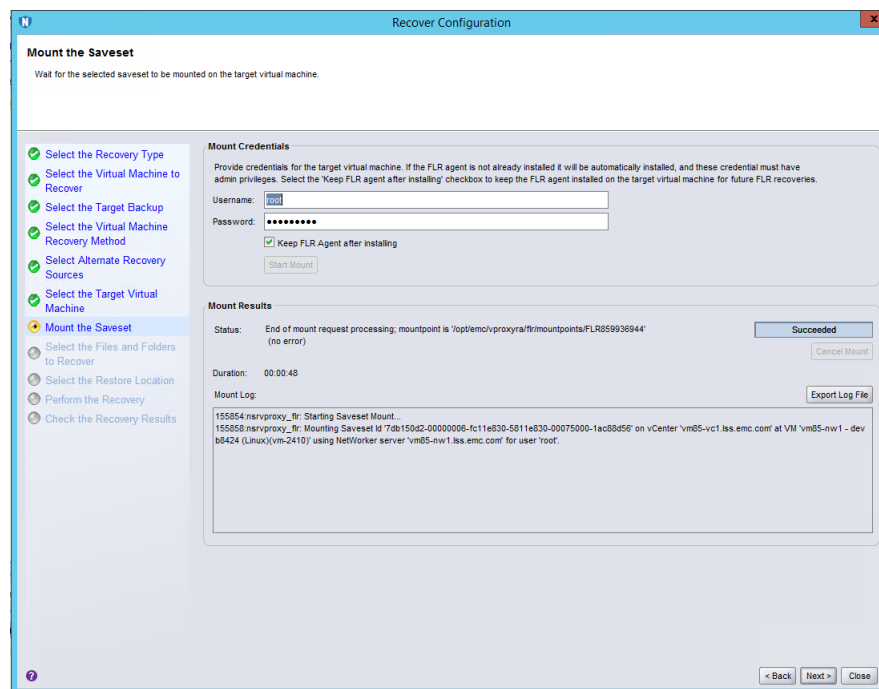


Figure 44. Mount the save set for file level recovery

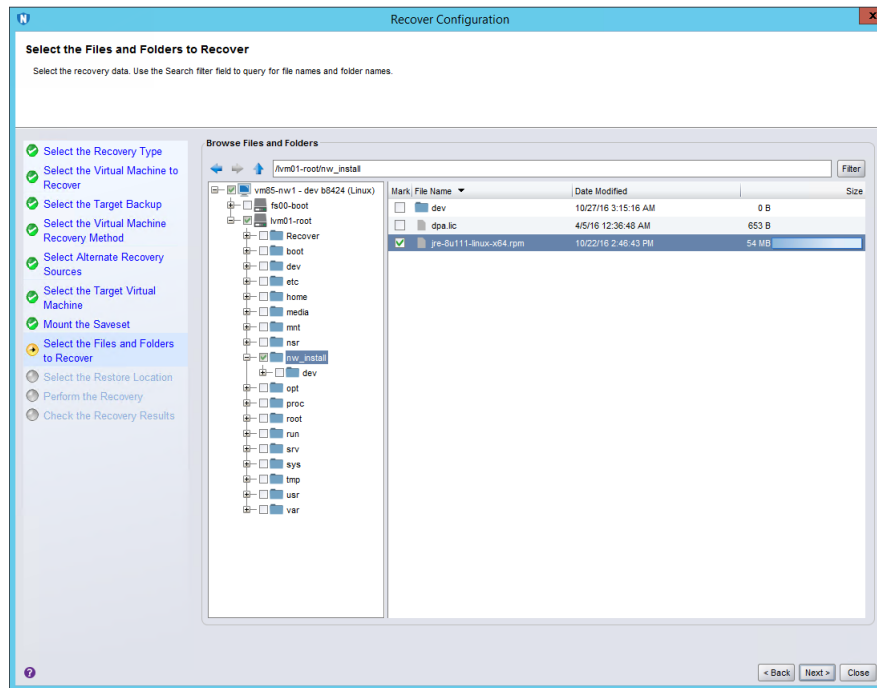
When the **Mount Results** pane shows that the mount has succeeded, click **Next**.

**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 45. 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**.

**NOTE:** vProxy FLR Agent creates and maintains a file on each discovered file system (volume) that has information about the volume's original path. The file name is in the form "DellEMC\_VolumeID\_path.info", where the path is in URL-encoded form of the last discovered path of the file system. These files are used during the FLR mount operation and are recreated again if they are found missing.

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.

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.
- NOTE:** 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.

When logged in to the NetWorker Management Web UI, the landing page displays options for **Monitoring**, **Protection**, **Recover and Savesets**, and so on, in the left pane. If not already selected, select **Recover and Savesets**, and apply the required filters, and click **SEARCH SAVESETS**.

- Time Range—Specify a time range for the backups that you want to recover. The default is Today.  
**i** **NOTE:** Save sets can be fetched only for a maximum period of one month.
- Clients—From the **Client Type** list, select **VMware**, from the **vCenter** list, select the vCenter server that contains the virtual machines or objects that you want to recover, and then select a virtual machine.
- Volumes—(Optional) Select a volume.

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, type of backups, and last used vProxy 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.

## 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.

**i** **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.

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.

**i** **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**.

**i** **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**.

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted.

Review the status of the request in the **Monitoring > Recover Jobs** window.

## 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.

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. Select **Parallelism** to perform parallel disks recovery based on available HotAdd or NBD sessions on selected vProxy for recovery.  
  
**NOTE:** The Max Parallelism attribute is 12 disks at a time. If no sufficient HotAdd or NBD sessions are available then the count will be exponentially decreased with power of two, it might be sequential if only one session is available.
  - g. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.
  - h. 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.

### **NOTE:**

- If you have selected the **Use same datastore for all disks** option, and if the virtual machine includes independent persistent disks, a warning message with the independent persistent disk names appear stating that the independent disks will be provisioned without data recovery.
- If you have not selected the **Use same datastore for all disks** option, all the disk information is displayed. The Mode column is also added to display the disk mode. If you select an independent persistent disk, a warning message appears stating that the independent disks will be provisioned without data recovery.
- The datastore free space is displayed in terms of size and percentage.
- You should initiate independent persistent disk restore operation from NWUI and the warnings are displayed in NWUI only.

6. Click **Next**.  
The **Summary** page displays.
7. In the **Summary** page, review the recovery details and then click **Finish**.

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted.

Review the status of the request in the **Monitoring > Recover Jobs** window.

## 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, 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.
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**.

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted.

Review the status of the request in the **Monitoring > Recover Jobs** window.

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.

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. Select **Reconnect NIC** to reconnect the network interface card after the recovery completes.
- f. Select **Parallelism** to perform parallel disks recovery based on available HotAdd or NBD sessions on selected vProxy for recovery.

**NOTE:** The Max Parallelism attribute is 12 disks at a time. If no sufficient HotAdd or NBD sessions are available then the count will be exponentially decreased with power of two, it might be sequential if only one session is available.

- g. 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**.

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted.

**NOTE:** When you start a Virtual Disk recovery, the virtual machine will be powered off automatically without issuing a warning message.

Review the status of the request in the **Monitoring > Recover Jobs** window.

## Emergency Recovery

Select **Emergency** when you need to restore the virtual machine to an ESXi host.

**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.

**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:

- 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.

**NOTE:**

- If you have selected the **Use same datastore for all disks** option, and if the virtual machine includes independent persistent disks, a warning message with the independent persistent disk names appear stating that the independent disks will be provisioned without data recovery.
- If you have not selected the **Use same datastore for all disks** option, all the disk information is displayed. The Mode column is also added to display the disk mode. If you select an independent persistent disk, a warning message appears stating that the independent disks will be provisioned without data recovery.
- The datastore free space is displayed in terms of size and percentage.
- You should initiate independent persistent disk restore operation from NWUI and the warnings are displayed in NWUI only.

6. Click **Next**.

The **Summary** page displays.

7. In the **Summary** page, review the recovery details and then click **Finish**.

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted.

Review the status of the request in the **Monitoring > Recover Jobs** window.

**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.

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 the 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.

Also, 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.

**NOTE:**

- File level recovery in the NetWorker Management Web UI for a Windows virtual machine can only be performed by an administrator of the target virtual machine. 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.
- You can perform file level recovery operations on backups of Linux virtual machines having unformatted disks.

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, go 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 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, you require 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 disabled.

- 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 that 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 selected 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**.

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted.

Review the status of the request in the **Monitoring > Recover Jobs** window.

**NOTE:**

- File-level restore failures are not immediately reflected in the log files that are seen in NetWorker Management Console UI. Wait for at least 2-3 minutes for the log files to get reflected in the NetWorker Management Console UI.
- vProxy FLR Agent creates and maintains a file on each discovered file system (volume) that has information about the volume's original path. The file name is in the form "DellEMC\_VolumeID\_path.info", where the path is in URL-encoded form of the last discovered path of the file system. These files are used during the FLR mount operation and are recreated again if they are found missing.



## Recover jobs

After initiating a recovery operation in the NetWorker Management Web UI, select **Monitoring > Recover Jobs** to view the status and progress of the recovery operation.

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 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**. For vProxy recovery, the **STOP** option is available only for VMware image level recovery and file-level restore.

## 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.

### **i** 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.
- During snapshot removal process, thinly provisioned virtual disks inflates to a larger size. This is a known VMware issue with vCenter version 7.0U1 and below. For more information, see <https://kb.vmware.com/s/article/56608>

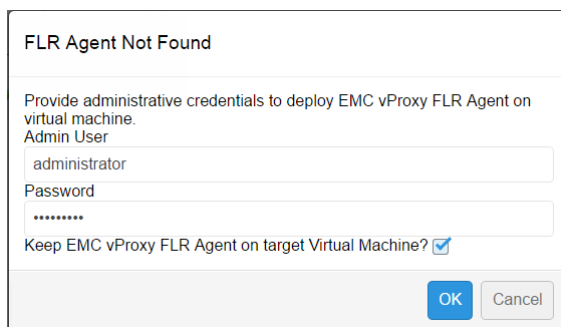
## Pre-requisites for file-level restore and SQL restore

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.



FLR Agent Not Found

Provide administrative credentials to deploy EMC vProxy FLR Agent on virtual machine.

Admin User  
administrator

Password  
\*\*\*\*\*

Keep EMC vProxy FLR Agent on target Virtual Machine?

OK Cancel

**Figure 46. 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 sudoers 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 sudoer 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 sudoer with the minimum file access requirements, you can perform file-level restore operations as a non-root user on supported Linux platforms. The E-Lab Navigator provides more information on the supported versions.

## 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.

 **NOTE:** File-level restore is not supported on Debian ext4 file systems.

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 15. 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

**Table 15. FLR privilege requirements (continued)**

User	Admin
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:

- msixec.exe
- diskpart.exe
- cmd.exe

On Linux:

- blkid
- udevadm
- readlink
- rpm
- bash

**i** **NOTE:** On Linux LVM, LVM2 rpm version 2.02.117 or later is required. To support the new features of LVM2.0, LVM2 version 2.03.15 is required. Additional binaries that are also required on Linux LVM include `dmsetup`, `lvm`, `vgimportclone`, `lvmconfig` and `lvmdevices`.

## 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 require this information when logging in to the **Dell EMC Data Protection Restore Client**.

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 nonadministrator user, ensure that the **FLR Agent** is already installed on the target machine using administrative privileges.

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**.

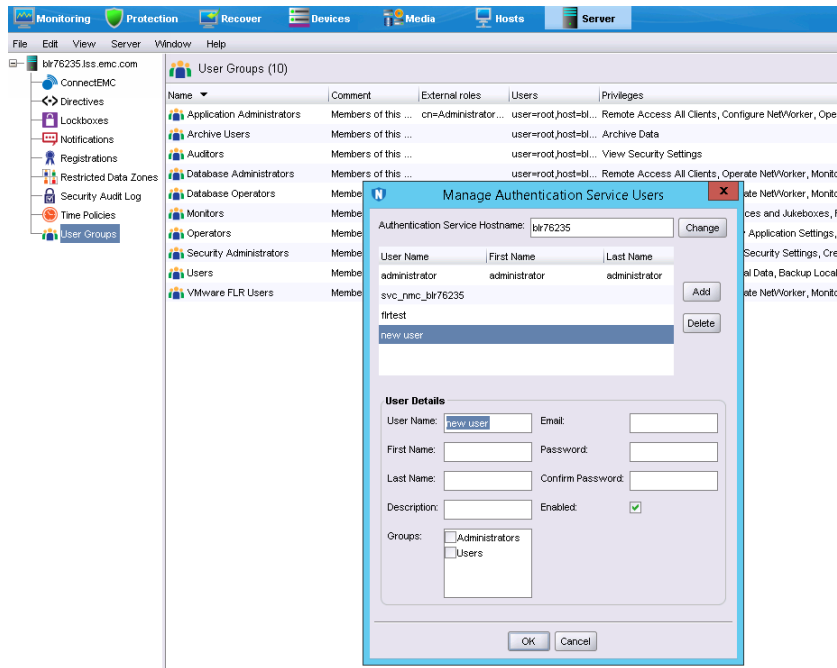


Figure 47. Manage Authentication service users

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 who is created in step 4 (for example, **user1**), in the format **user=user1,host=NW server FQDN**.

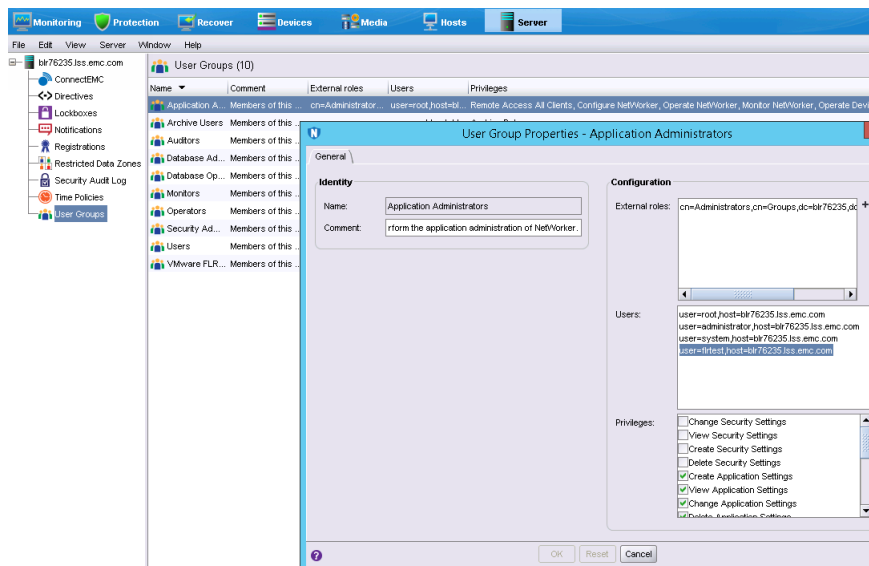


Figure 48. Application Administrators user group properties

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**.

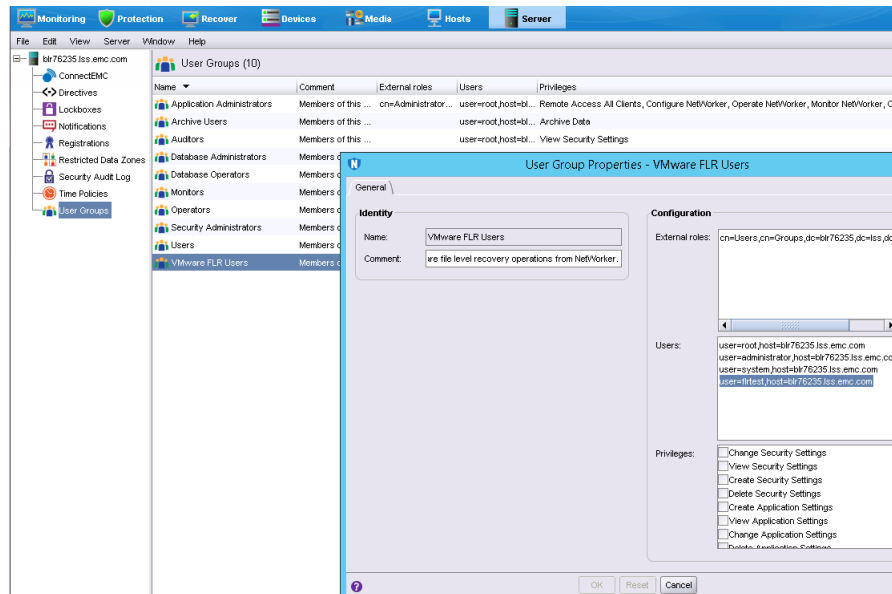


Figure 49. VMware FLR Users user group properties

- In **External roles** field, browse and add the new user created in step 4. The External role field gets populated by the new user details, in the format `cn=user1,cn=Users,dc=nwsrv081,dc=ridebl1r,dc=com`.

You can now use this new user to log in to 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 that are 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 must 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.

### 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 that are 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 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 nonroot 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.
- 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 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`. Notes that this issue does not occur when the same Data Domain device is used for the backup and clone.

If relabeling of the primary device has occurred, or you added a new Data Domain device, clear the **Tlog backup** option for the Backup Action, and then run the SQL application-consistent workflow. After the FULL backup and clone completion, reselect the **Tlog backup** option for the Backup Action and run the SQL application-consistent workflow again. Subsequent transaction log backups and clones 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 clear **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.

- Browsing many 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 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 indexes 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.

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 \(User mode file-level restore only\)](#).

1. Open a browser from the virtual machine that the restored files will be recovered to, and enter a URL that hovers over 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.

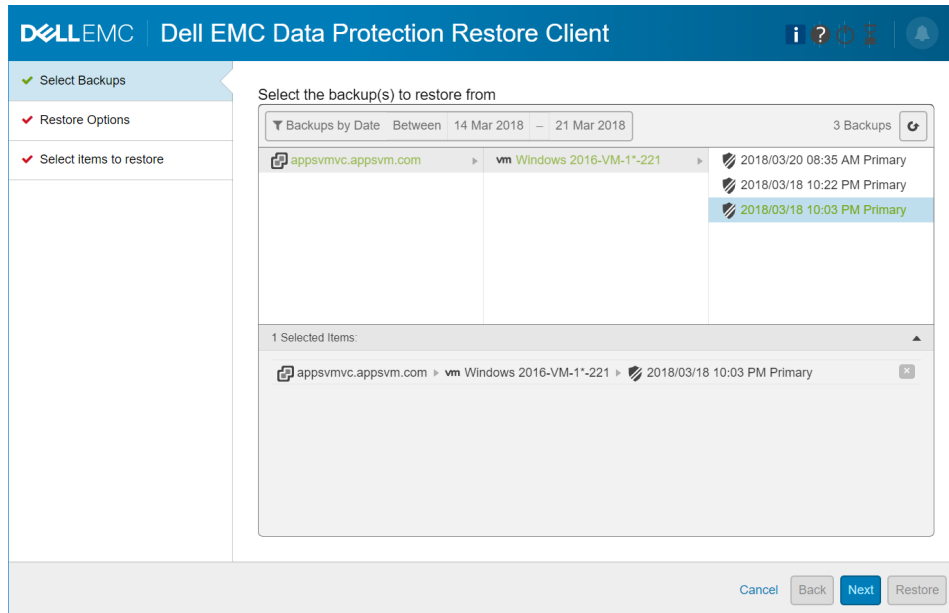
The **Dell EMC Data Protection Restore Client** login window appears.



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.

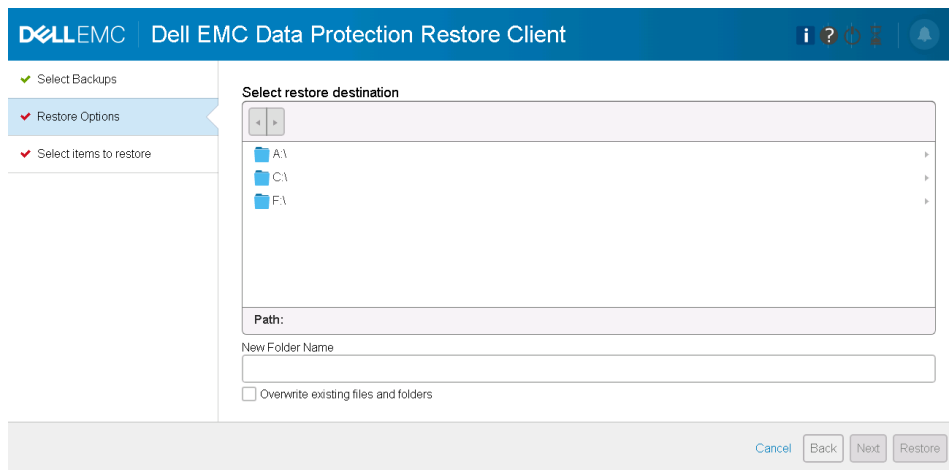
3. On the **Select Backups** page, use the drop-down list to view the available backups. You can set the backup filter to view backups on a specific day or within a specific date range. Select a backup and double-click or drag and drop to move the backup to the **Selected Items** pane. Click **Next**.



**Figure 50. 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.

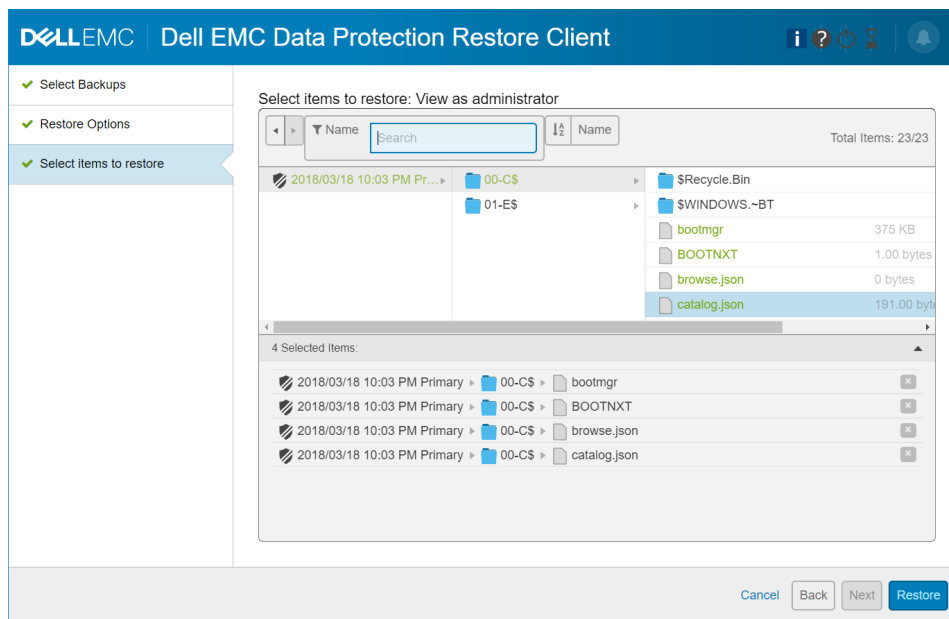
4. On the **Restore Options** page, go to the file system drive where you want to restore the items and select an existing folder, or specify a new folder name in the restore destination, and then click **Next**.



**Figure 51. 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.

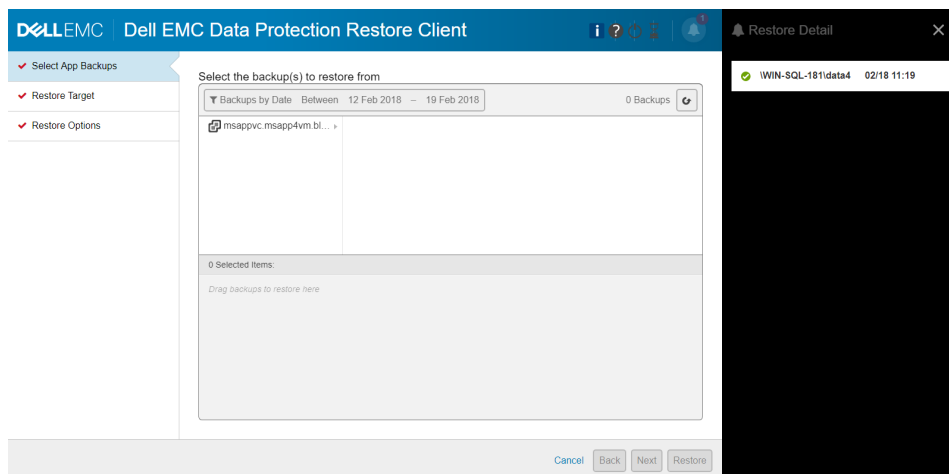
- On the **Select items to restore** page, browse and select the files and folders available for recovery. Note that you can sort items by Name, File size, or Date, and you can also search for a specific file or folder name. To mark an item for recovery, double-click the item, or drag and drop the item into the **Selected Items** pane.



**Figure 52. Select items to restore**

- When finished selecting items, click **Finish**.
- Click **Yes** when you are prompted to continue the restore.
- To enable the polling feature so that you can monitor the status of the restore, click the hourglass icon that is 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.
- Once the polling feature is enabled, you can monitor the status of the restore by clicking the icon that is 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 53. Restore Monitoring**

- NOTE:** vProxy FLR Agent creates and maintains a file on each discovered file system (volume) that has information about the volume's original path. The file name is in the form "DellEMC\_VolumeID\_path.info", where the path is in URL-encoded form of the last discovered path of the file system. These files are used during the FLR mount operation and are re-created again if they are found missing.

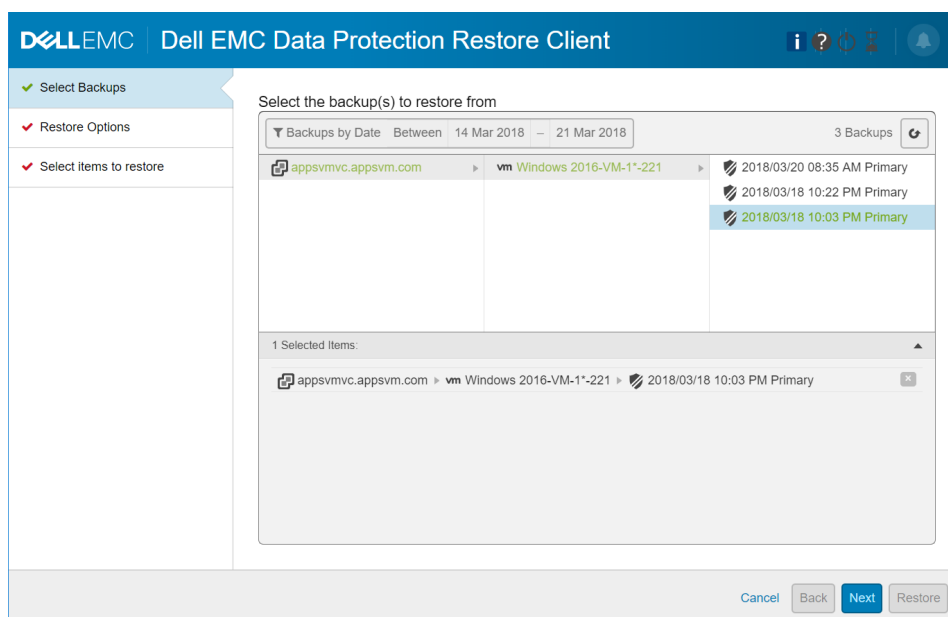
## Restoring specific folders or files from different virtual machines in Admin mode

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.

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 54. Select the backup(s) to restore from**

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. Select 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.

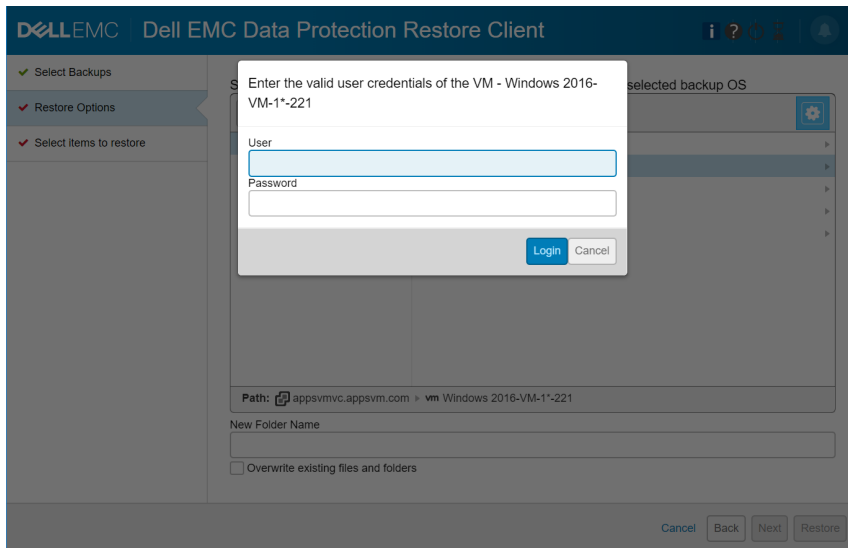


Figure 55. Select restore location

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 required, 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.

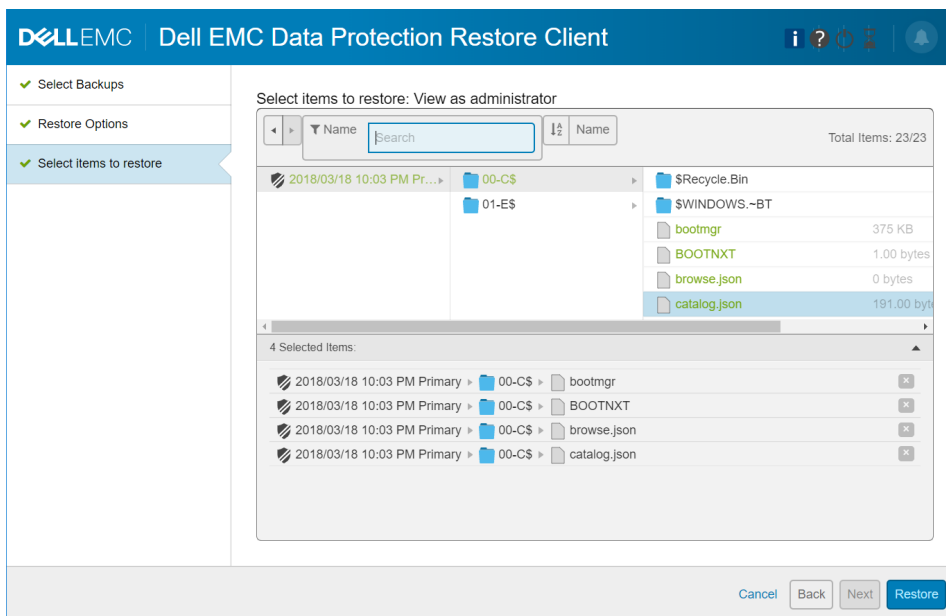
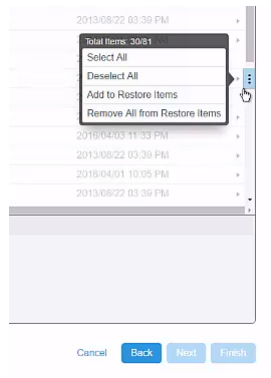



Figure 56. Select items to restore

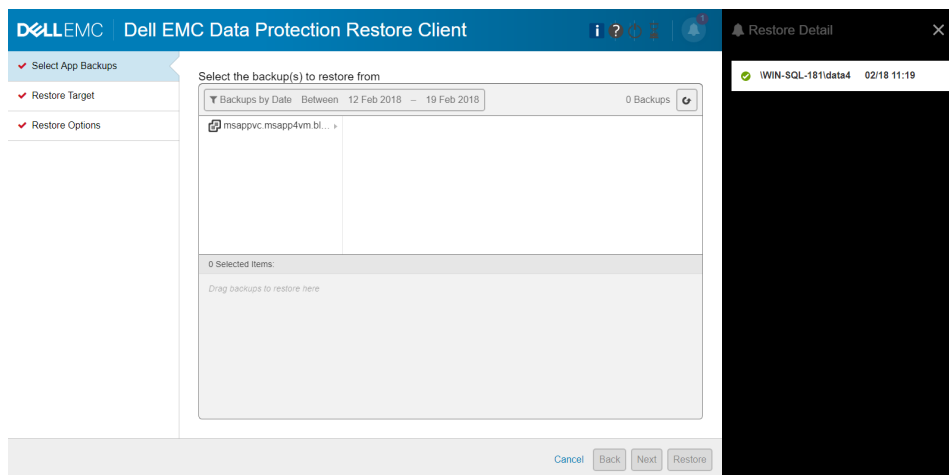
Within this window, you can also discover and select the total number of items available for recovery by scrolling to the far right of the directory structure and right-clicking the icon that is located on the vertical scroll bar, as shown in the following figure.



**Figure 57. 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 that is 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 that is 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 58. Restore Monitoring**

**NOTE:** vProxy FLR Agent creates and maintains a file on each discovered file system (volume) that has information about the volume’s original path. The file name is in the form “DellEMC\_VolumeID\_path.info”, where the path is in URL-encoded form of the last discovered path of the file system. These files are used during the FLR mount operation and are re-created again if they are found missing.

## Restoring SQL Server application-consistent backups (Windows platforms only)

NetWorker 19.8 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.

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.

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.

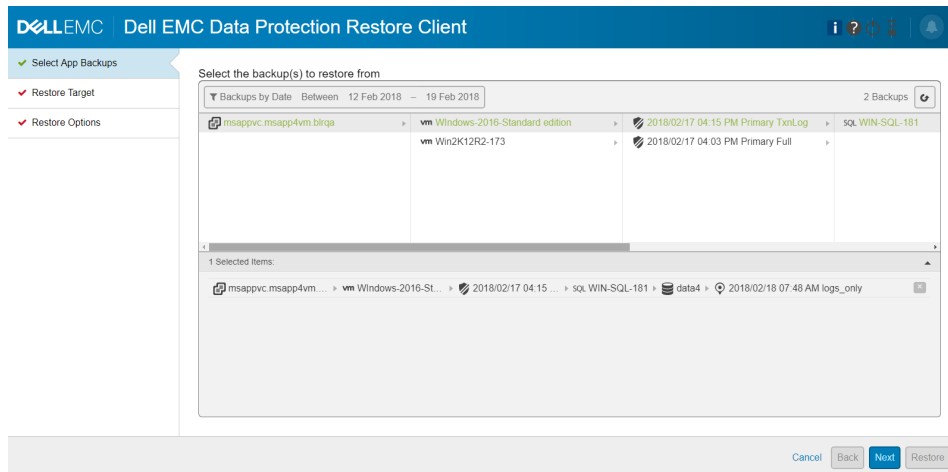
**NOTE:** The polling feature, which enables monitoring of in-progress restore operations, is turned off by default. To turn on the polling feature, click the hourglass icon located in the upper right-hand corner of the window and set to **ON**.

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.

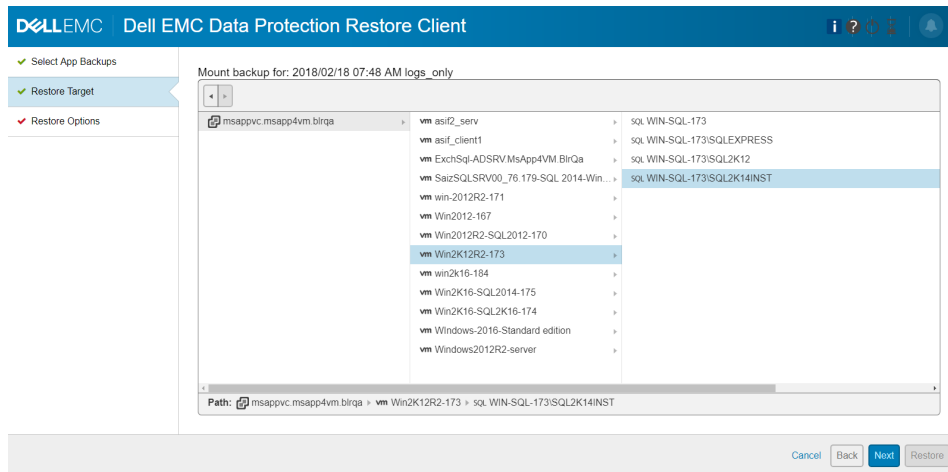


**Figure 59. Select App Backups page**

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 60. 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**.



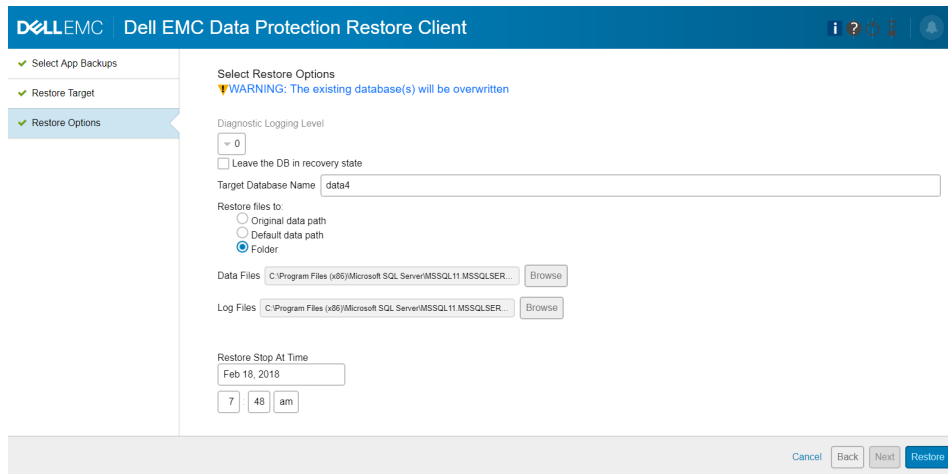


Figure 61. Restore Options page


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.

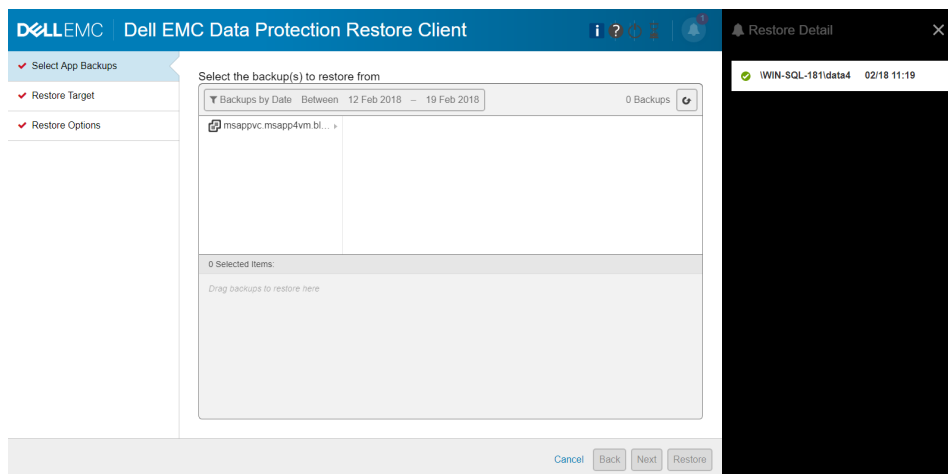


Figure 62. Restore Monitoring

# 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.

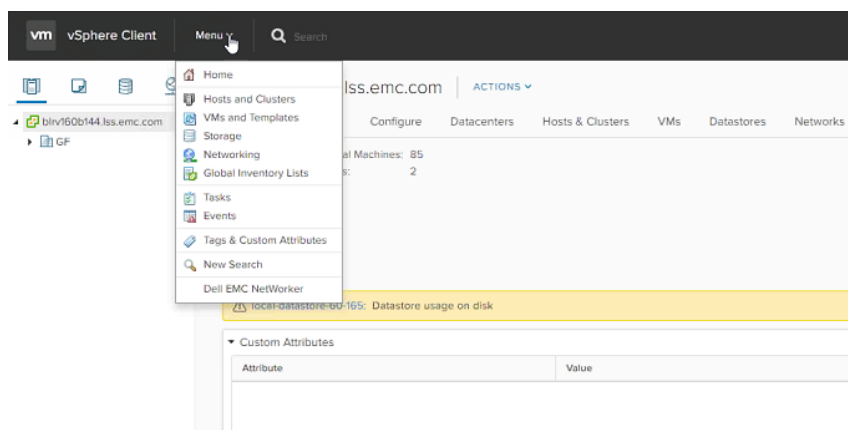
**NOTE:** Backup and recovery operations in the **vSphere Client Dell EMC NetWorker** interface are not supported for SQL Server advanced application-consistent protection policies. Perform these operations from the NMC **NetWorker Administration** window or the **Dell EMC Data Protection Restore Client**.

## 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**.

**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.

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 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 63. 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**.

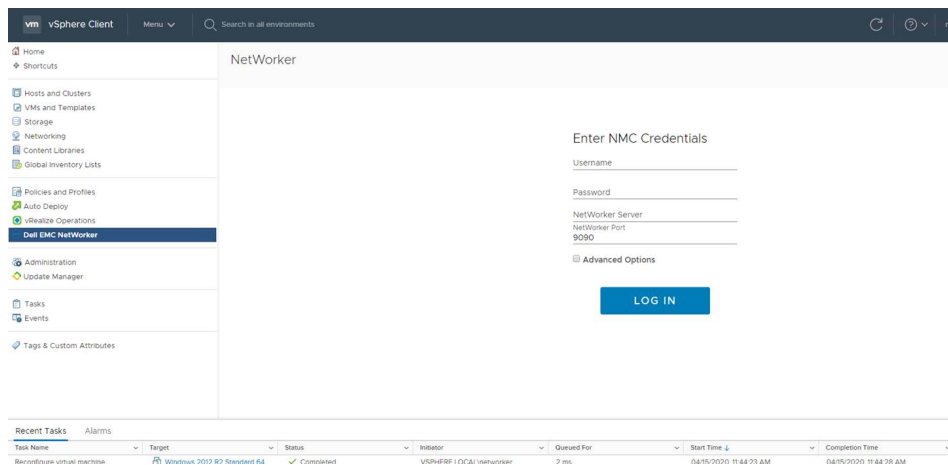


Figure 64. NetWorker connection information in the vSphere Client

#### 4. Click **Log in**.

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

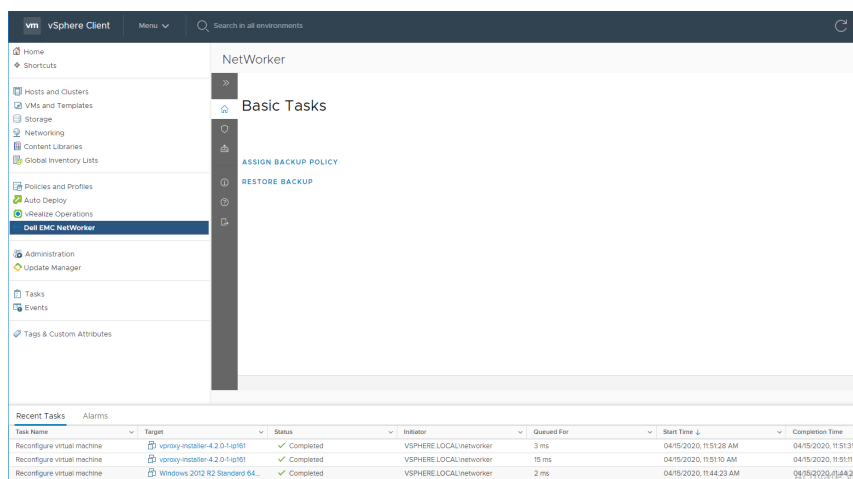



Figure 65. Dell EMC NetWorker Basic Tasks pane

## 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.

Ensure that the virtual machine you want to restore to is in powered OFF state.

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.

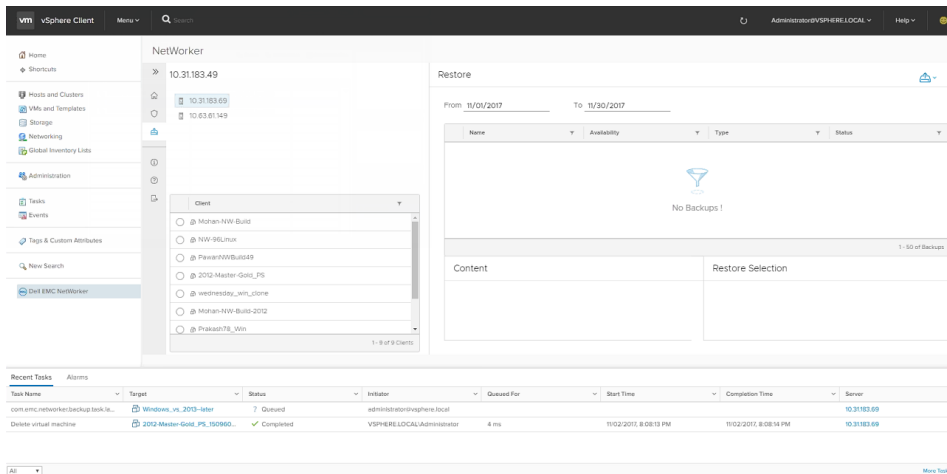


Figure 66. Restore pane with available virtual machine backups

**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.

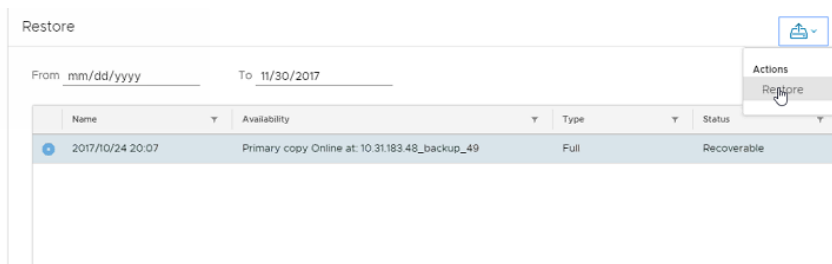


Figure 67. Select Restore from the Action drop-down

The **Restore** wizard opens on the **Basic Config** page.

6. From the **Destination** drop-down, leave the default **Restore to original location** selected.

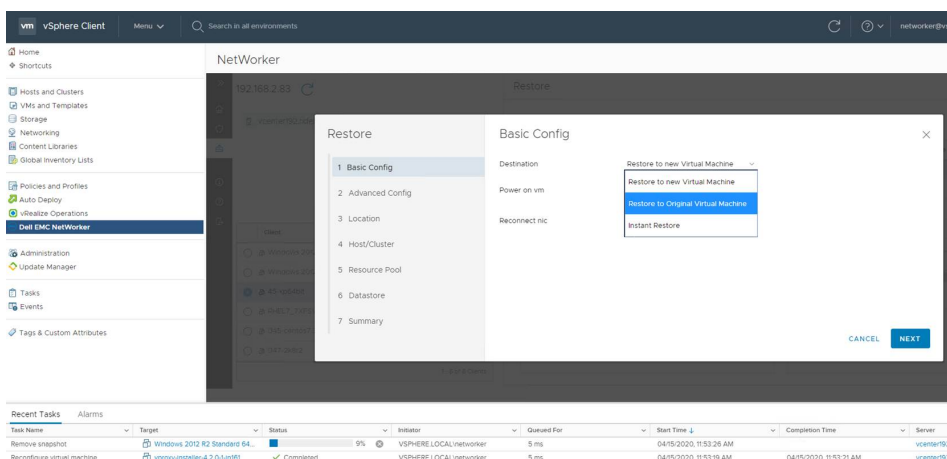


Figure 68. Restore to original location

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.
- c. **Parallelism**—Select this checkbox to perform parallel disks recovery based on available HotAdd or NBD sessions.

**NOTE:** The Max Parallelism attribute is 12 disks at a time. If no sufficient HotAdd or NBD sessions are available then the count will be exponentially decreased with power of two, it might be sequential if only one session is available.

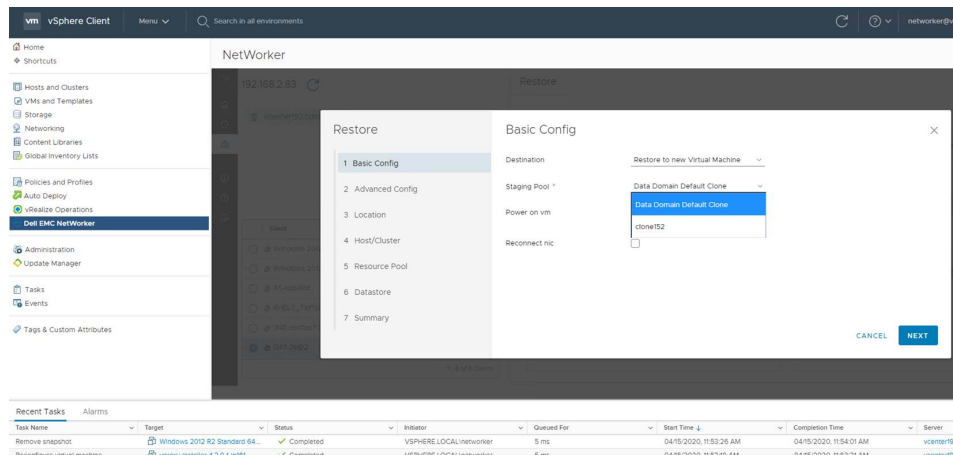
8. Click **Next**.
9. In the **Summary** page, review the information and then click **Finish** to start the recovery.

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.

## vCenter HTML5 UI Staging Pool Selection to recover from non-Boost Devices

With NetWorker 19.3, the support for staging pool selection is introduced. You can select a staging pool when recovering from non-boost device and perform the following restore operations using the HTML5 UI plugin.

- Restore to new virtual machine
- Restore to original virtual machine
- Instant restore




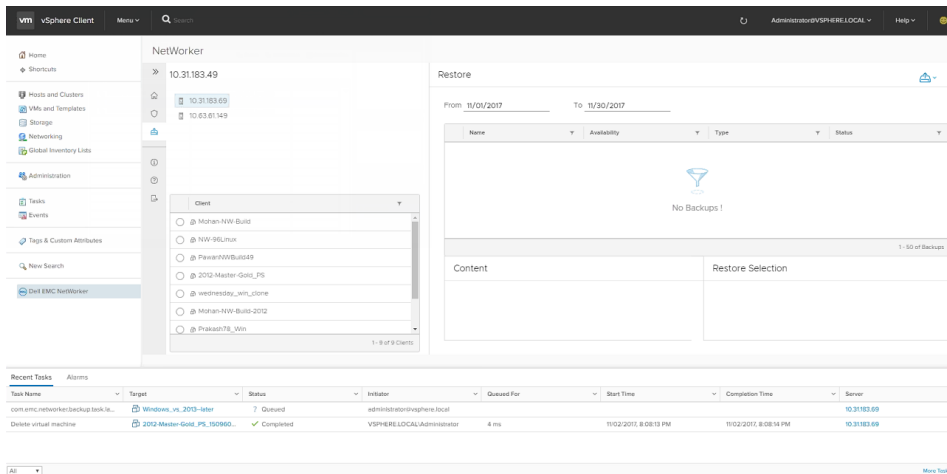
**Figure 69. Staging Pool Selection**

**NOTE:** NetWorker 19.3 and later does not support Flash plug-in. This feature cannot be used with vCenter Flash plug-in. You must only use HTML5 plug-in.

## 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.

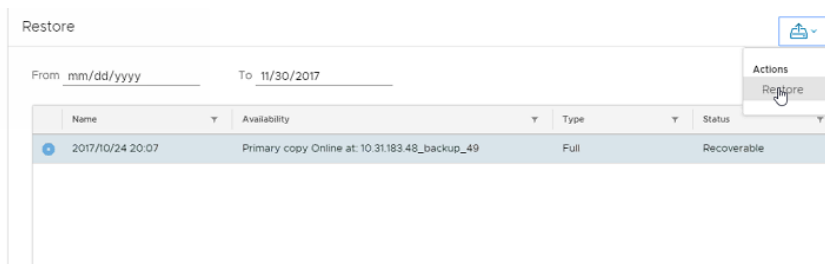
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane. When a connection to the NetWorker server is established, links to **Basic Tasks** appear in the right pane.
2. From the **Basic Tasks** pane, click **Restore Backup**, or click the Restore icon  in the vertical navigation bar. A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.



**Figure 70. 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.

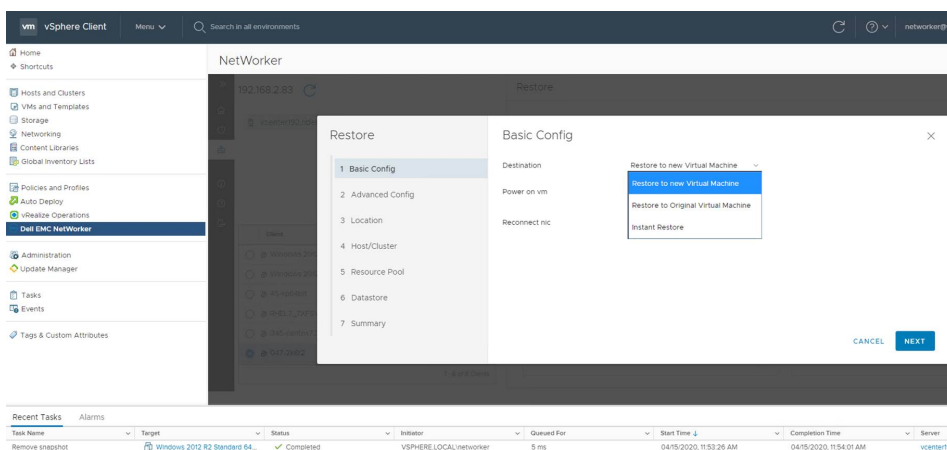
3. From the **Client** pane, click the radio button next to the virtual machine that you want to recover. A list of available restore points for that virtual machine display in the right pane. You can also specify a date range to view only the virtual machine backups that were performed within that range.
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 71. 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 72. 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.

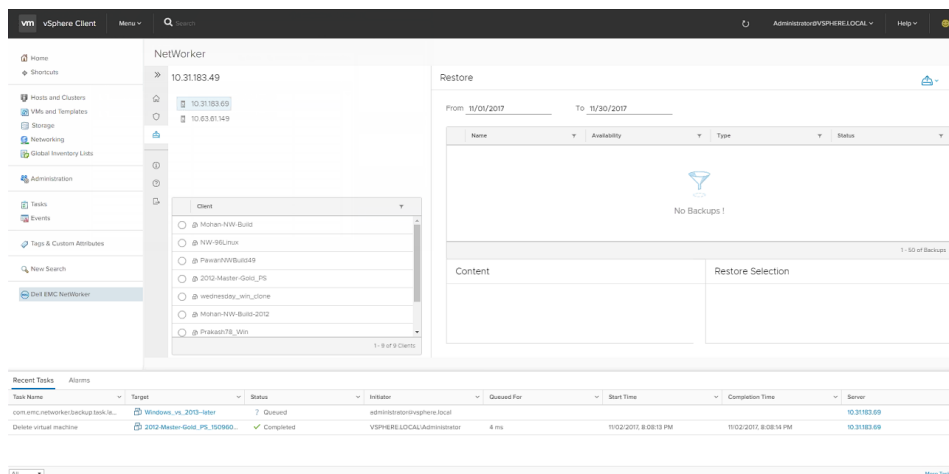
- b. **Power on vm**—Select this checkbox to automatically power on the virtual machine after the restore completes.
  - c. **Reconnect nic**—Select this checkbox to automatically reconnect the network interface card after the restore completes.
8. Click **Next**.  
The **Advanced Config** page displays.
  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.

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.

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 73. 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.

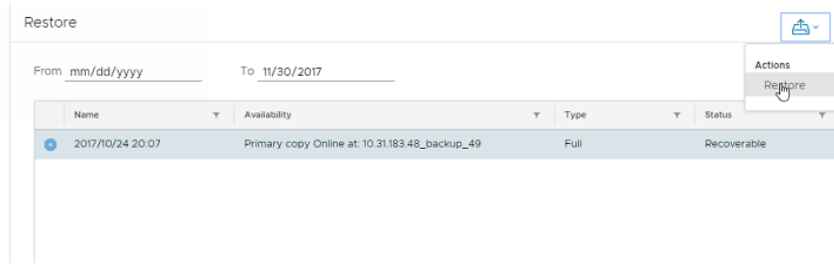


Figure 74. Select Restore from the Action drop-down

The **Restore** wizard opens on the **Basic Config** page.

- From the **Destination** drop-down, select **Restore to different (existing) virtual machine**.

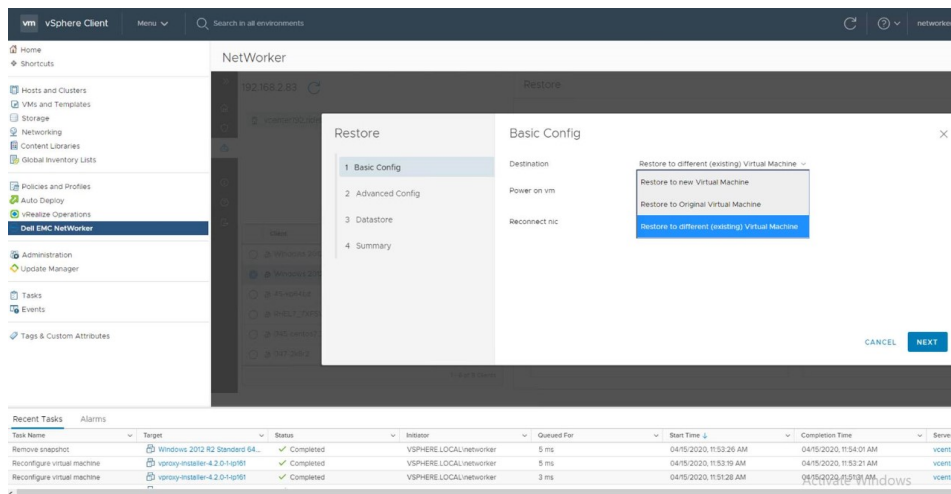


Figure 75. Restore virtual disks to existing virtual machine

- (Optional) Select from the following options:
  - Reconnect nic**—Select this checkbox to automatically reconnect the network interface card after the restore completes.
  - Power on vm**—Select this checkbox to automatically power on the virtual machine after the restore completes.
- Click **Next**.  
The **Advanced Config** page displays.
- 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.
- Click **Next**.  
The **Datastore** page displays.
- For each virtual disk listed in the **Datastore** pane, select a **Destination Datastore** from the drop-down, and then click **Next**.
- 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.

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.




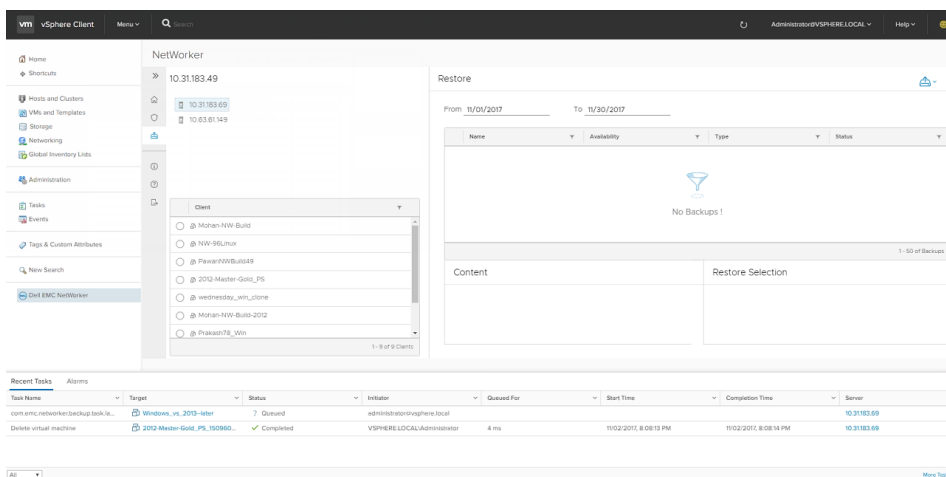
# Instant recovery of a virtual machine

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.

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.

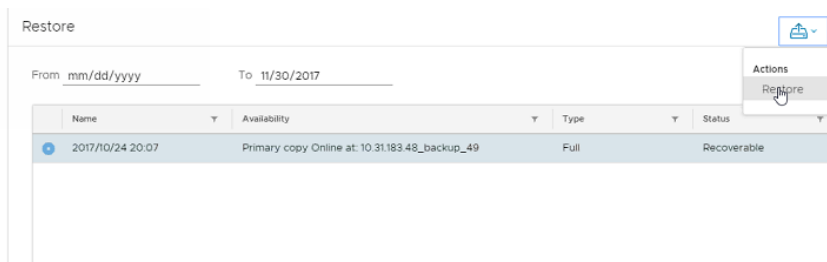
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane. When a connection to the NetWorker server is established, links to **Basic Tasks** appear in the right pane.
2. From the **Basic Tasks** pane, click **Restore Backup**, or click the Restore icon  in the vertical navigation bar. A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.



**Figure 76. 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 77. 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**.

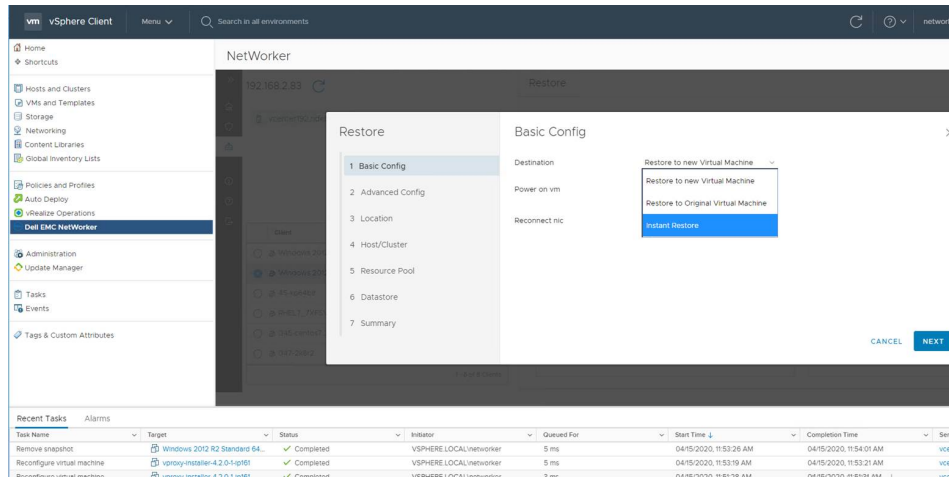


Figure 78. Instant Restore

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.

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 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 16. 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: <ol style="list-style-type: none"> <li>1. Edit the /usr/lib/systemd/system/vrecoverd.service file.</li> <li>2. Search for the for the <i>ExecStart=</i> string.</li> <li>3. Edit the <i>--program-log-level=</i> argument with one of the following values: <ul style="list-style-type: none"> <li>• warn</li> <li>• info</li> <li>• trace</li> <li>• debug</li> </ul> </li> <li>4. Reload the unit config file into systemd: <b>systemctl daemon-reload</b></li> <li>5. Restart the recovery engine: <b>systemctl restart vrecoverd.service</b></li> </ol>

**Table 16. Recovery log files (continued)**

Log file	Log location and name	Logging levels
DD Boost recovery log	For image level recoveries, <code>/opt/emc/vrproxy/runtime/logs/vrecoverd/vrecoverd-boost.log</code> .  For file-level recoveries or SQL application-consistent recoveries, <code>/opt/emc/vrproxy/runtime/logs/vflrd/vflrd-boost.log</code> .	To modify the logging level: <ol style="list-style-type: none"> <li>1. Edit the <code>/usr/lib/systemd/system/vrecoverd.service</code> file.</li> <li>2. Search for the for the <code>ExecStart=</code> string.</li> <li>3. Edit the <code>--boost-log-level=</code> argument with one of the following values: <ul style="list-style-type: none"> <li>• none</li> <li>• error</li> <li>• warn</li> <li>• info</li> <li>• trace</li> <li>• debug</li> <li>• all</li> </ul> </li> <li>4. Reload the unit config file into systemd: <b><code>systemctl daemon-reload</code></b></li> <li>5. Restart the recovery engine: <b><code>systemctl restart vrecoverd.service</code></b></li> </ol>
VDDK recovery log	<code>/opt/emc/vrproxy/runtime/logs/vrecoverd/vrecoverd-vddk.log</code>	To modify the logging level: <ol style="list-style-type: none"> <li>1. Edit the <code>/opt/emc/vproxy/conf/VixDiskLib.config</code> file.</li> <li>2. Edit the <code>vixDiskLib.transport.LogLevel =</code> to specify one of the following values: <ul style="list-style-type: none"> <li>• 0—No logging</li> <li>• 1—Errors only</li> <li>• 2—Warnings and Errors</li> <li>• 3—Important information messages, errors and warnings</li> <li>• 4 —All messages, including debug messages.</li> </ul> </li> <li>3. Restart the recovery engine: <b><code>systemctl restart vrecoverd.service</code></b></li> </ol>

## vProxy backups and restores using Direct Fiber channel

You can perform backup and recovery of the VMware virtual machines through fiber channel using vProxy. vProxy uses the VMDirect passthrough capability of vSphere. You can enable DFC to leverage on the FC connectivity to DD for vProxy backup and recovery.

### Configuring Direct Fibre Channel (DFC) for vProxy

You can configure the DFC for vProxy by performing the following procedure:

- You must have a fiber channel connectivity that is established in between ESXI hosting the vProxy and the Data Domain device.
- Fiber channel connectivity in between NetWorker storage node and Data Domain device.

**NOTE:**

- On a Fiber channel setup, instant access and FLR are not supported.
- Only NBD transport mode is supported.
- Hotadd is not supported.

1. Configuring VMDirect path on vProxy.
  - a. Go to vSphere client, select the ESXI , and then select the vProxy where you want to configure the DFC.

- b. Power off the vProxy.
  - c. Select the vProxy, click **Edit Settings**.
  - d. Click **Add Hardware**, in the **Add Hardware** window select PCI Device, and click **Next**.
  - e. In the Specify the physical PCI/PCIe Device to connect to drop down menu, select the Fiber channel PCI/PCIe device, and click **Next**.
  - f. Review the selected options and click **Finish**, then click **OK**.
  - g. Power On the vProxy.  
The DFC path is enabled on vProxy.
2. Creating a DDBoost enabled device.
- a. In NMC, click **Devices**.
  - b. In the left panel, right-click **Devices** and select **New Device Wizard**.
  - c. On the **Select the Device** page, select **Data Domain** and click **Next**.
  - d. On the **Data Domain Preconfiguration Checklist** page, click **Next**.
  - e. On the **Specify the Data Domain Configuration Options** page:
  - f. On the **Specify the Data Domain Configuration Options** page, Under **Data Domain System Name**, Select **Use an existing Data Domain System**
  - g. In the **Data Domain DDBoost Username** field, type the username of the Data Domain user.
  - h. In the **Data Domain DDBoost Password** field, type the password of the Data Domain user.
  - i. On the **Specify the Data Domain Configuration Options** page, Under **Data Domain System Name**, Select **Use an existing Data Domain System**
  - j. In the **Data Domain DDBoost Username** field, type the username of the Data Domain user.
  - k. In the **Data Domain DDBoost Password** field, type the password of the Data Domain user.
  - l. In the **Data Domain Management Credentials**, select **use the DDBoost Credentials**.
  - m. Click **Next**.
  - n. On the **Select the Folder to Use as Devices** page, click **New Folder** to create a folder for the device.
  - o. Select the newly created folder.
  - p. Specify the required values in the other fields.
  - q. Click **Next**.
  - r. On the **Configure Pool Information** page, under **Pool Type**, select one of the following pool types:
    - Backup
    - Backup Clone
  - s. Under **Pool**, perform one of the following tasks to select the pool:
    - Select **Create and use a new pool**, and type the pool number in the text box.
    - Select **Use an existing pool**, and select the pool from the drop-down list box.
  - t. Specify the required values in the other fields.
  - u. Click **Next**.
  - v. On the **Select Storage Nodes and Fibre Channel Options** page, select the storage node.
  - w. Select **Enable Fibre Channel for this device** and type the **Fibre Channel Host Name**, click **Next**.
  - x. On the **Select SNMP Monitoring Options** page, specify the required field values, and click **Next**.
  - y. On the **Review the Device Configuration Settings** page, review the configuration settings, and click **Configure**.
  - z. On the **Device Configuration Results** page, click **Finish**.

## vProxy DFC limitations

The following features are unavailable for virtual machines that are configured with DirectPath:

- Instant access
- FLR

# Backing up and recovering a vCenter server

The following sections describe 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.

## Topics:

- [vCenter deployments overview](#)
- [Best practices for vCenter server backup and restore](#)
- [Protecting an embedded PSC](#)
- [Protecting external deployment models](#)
- [vCenter server restore workflow](#)
- [Platform Services Controller restore workflow](#)
- [Additional considerations](#)
- [Command reference](#)

## 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 vCenter server backup and restore

Review the following recommendations and best practices when planning a vCenter server backup and restore.

 **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 server 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.

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 that is 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.

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, select one of the following proxy selection option:
  - Take control of an existing proxy already deployed in vCenter

**Figure 79. Proxy selection**

- Use a proxy already deployed in the ESX but not registered with NetWorker. This option preprovisions the proxy from the OVA on the ESXi. It does not registers it. The proxy is unregistered after the recovery.

Disk Name	Datastore
Hard disk 1	Datastore2

**Figure 80. Proxy selection**

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 in 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**.

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 if 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 with one external PSC where PSC fails

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 **vc-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 **vc-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


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 but one remains


1. Repoint the vCenter instance (insert link) to one of the functional PSCs in the same SSO domain.
 


 **NOTE:** Log in to all vCenter servers one by one to determine which vCenter login fails. This will be the vCenter server 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 login 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

-  **NOTE:** In this scenario, none of the vCenter logins (SSO user) have been successful.
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

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

**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.

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.

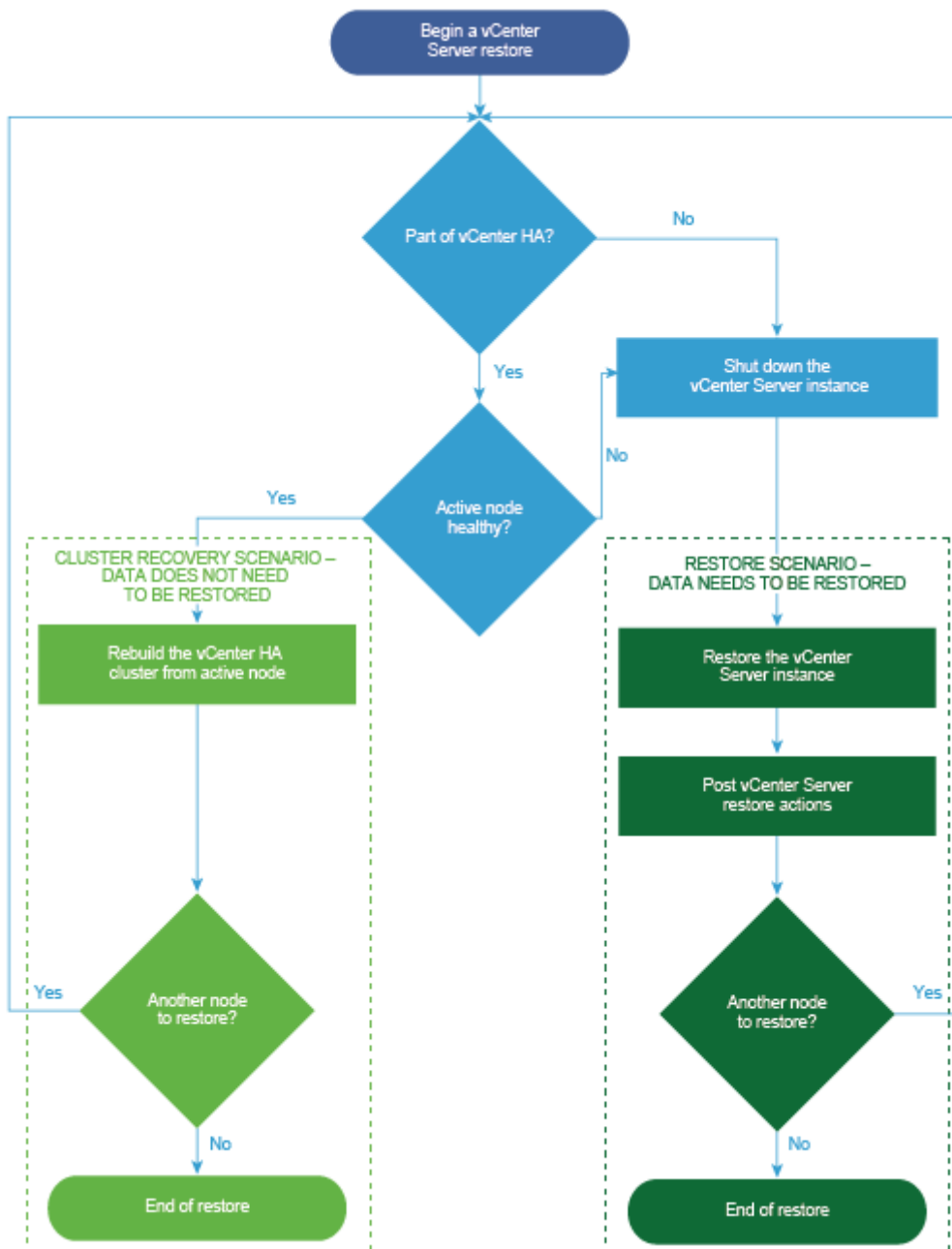


Figure 81. vCenter server restore workflow

# Platform Services Controller restore workflow

The following diagram shows the restore workflow for a Platform Services Controller (PSC).

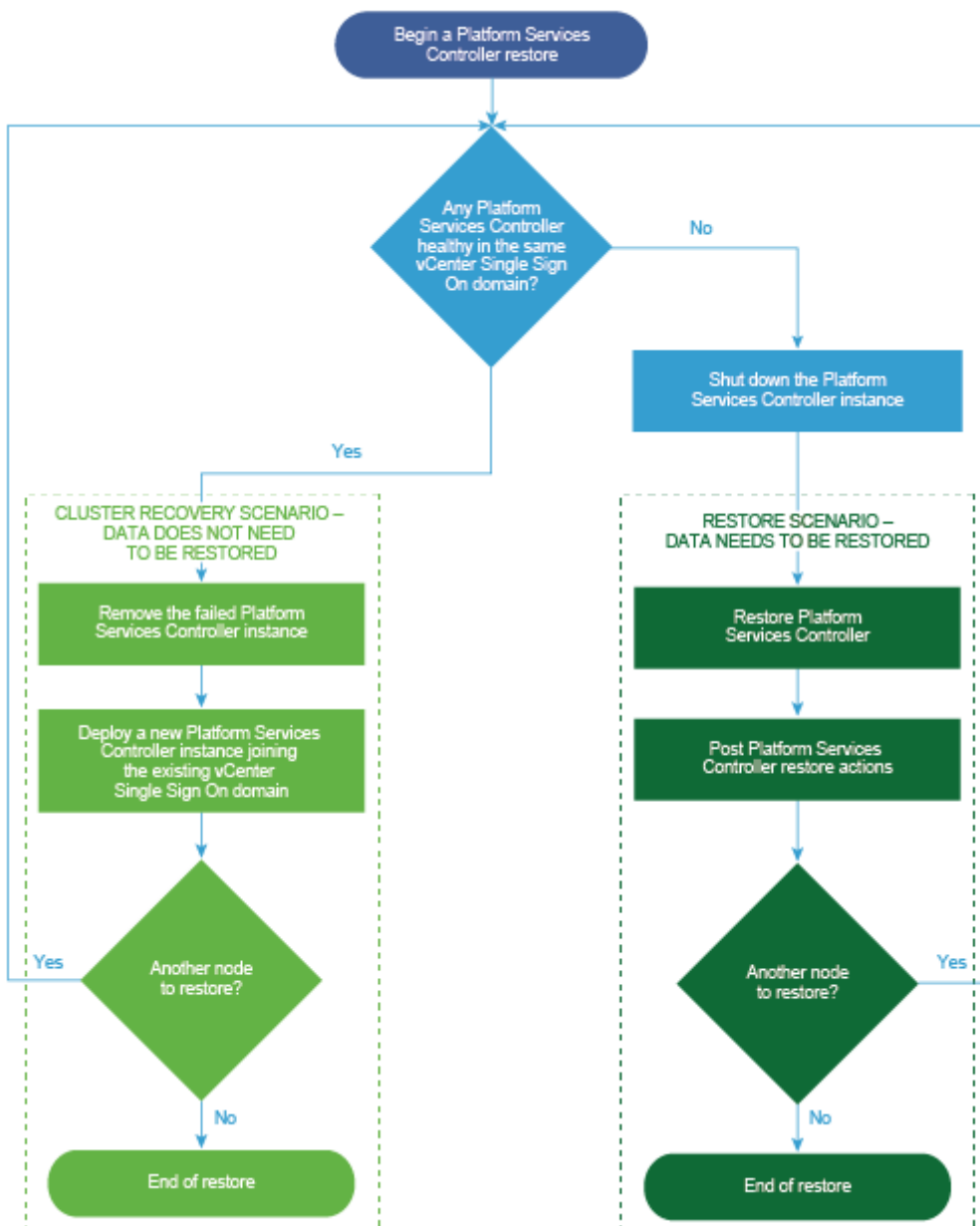


Figure 82. PSC restore workflow

## 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-vmmdir/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%\vmmdir\`

- 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 stuning.

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 and PSC, or obtain the status:

```
service-control -status/start/stop -all
```

You can use other Replication topology commands, as in the following example.

### 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.

# NetWorker VMware Protection in VMware Cloud on Amazon Web Services

This appendix includes the following topics:

## Topics:

- [Introduction to NetWorker VMware Protection in VMware Cloud on AWS](#)
- [Prerequisites](#)
- [Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS](#)
- [NetWorker VMware Protection for VMware Cloud on AWS best practices](#)
- [Unsupported NetWorker operations](#)
- [Limitations](#)

## Introduction to NetWorker VMware Protection in VMware Cloud on AWS

NetWorker 19.3 or later 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/](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

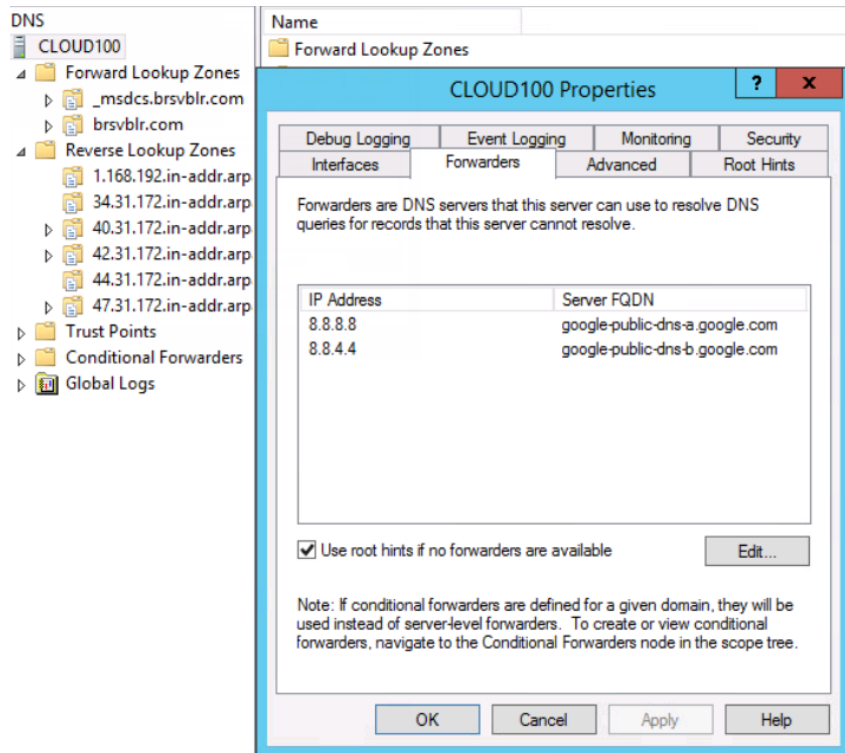


Figure 83. Enable internet access for Forwarders

## 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**.

Review the [Pre-requisites](#) section.

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.

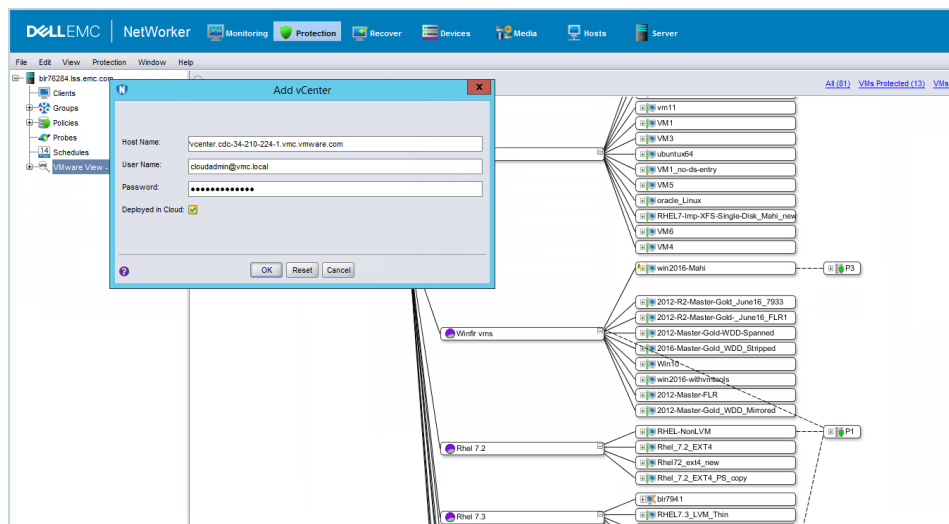


- d. In the **DNS** field, specify the IP address of the DNS servers, separated by commas.
  - e. In the **FQDN** field, specify the fully qualified domain name of the vProxy appliance.
13. Expand **Timezone settings**, and then perform the following tasks:
- a. in the **Timezone setting** field, select 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**.  
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 84. 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.

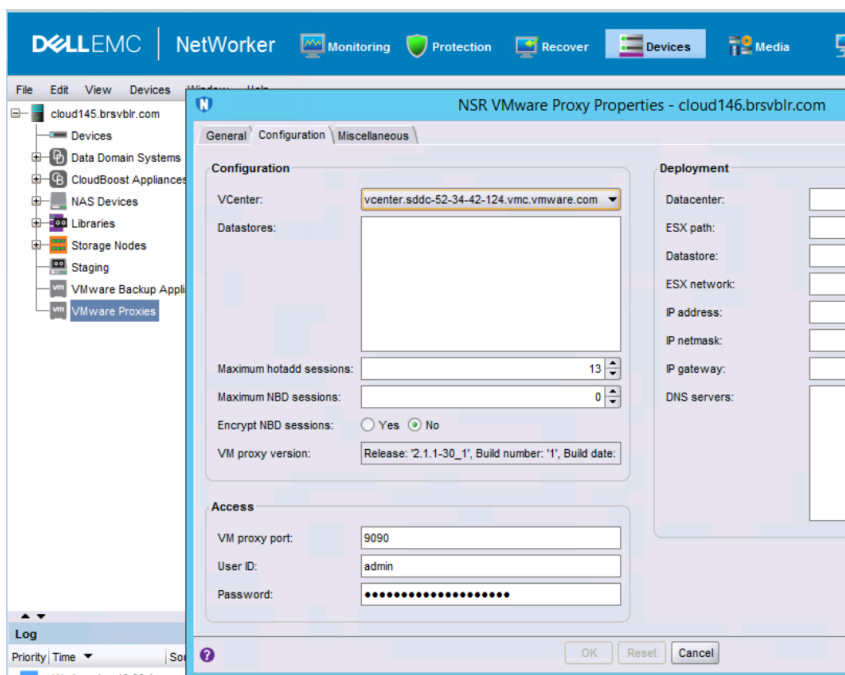


Figure 85. NSR VMware Proxy Properties

## 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.
- vProxy redeployment.

**NOTE:** These limitations are also applicable for NetWorker support for Azure VMware Solution (AVS) platform.

## Limitations

Before configuring NetWorker VMware Protection in VMware Cloud on Amazon Web Services (AWS), review the following limitations.

**VMware Cloud on AWS with SDDC version 1.8** The vProxy restores as new VM using NetWorker Management Console and NetWorker HTML5 Admin Console fail with errors stating that the vProxy is unable to register the VM onto the destination. This issue is not seen if you are using VMware Cloud on AWS version 1.7 or earlier.

The restore log displays:

```
159373:nsrvproxy_recover: vProxy Log:
2019-10-09T04:22:33Z ERROR: [@(##) Build number: 28] Error
registering VM: ServerFaultCode: Permission to perform this
operation was denied. 159373:nsrvproxy_recover: vProxy Log:
2019-10-09T04:22:33Z ERROR: [@(##) Build number: 28] Error in
registering VM "[WorkloadDatastore]
Win-GA-Repl1_1abc/Win-GA-Repl1_1abc.vmx". "ServerFaultCode:
Permission to perform this operation was denied."
```

To fix the issue, you should manually add vCenter permission to the wanted "VMs and Templates" folder that the restored VM has to be stored. The target VM folder should be associated with permissions as follows "**user=cloudadmingroup**" and "**role=cloudadmin**", and enable "**propagate to children**". After the permission is added manually, NetWorker NMC and NWUI will display the wanted folder. If correct folder is chosen in the UI, then the restore as new VM will be successful.

**When restoring as new VM, the reconnect NIC option may not work correctly.**

Edit settings of the restored new VM and change the network to "VM Network" and then click **Apply**. Reopen the edit setting configuration pane of the VM, and change the network to the correct wanted NSX-T network logical switch and then click **Connect**.

**Error registering VM**

The NetWorker VMware Protection (NVP) integration with the vProxy appliance is configured in VMware Cloud with Amazon Web Services (AWS). The NetWorker Management Console (NMC) is used to configure a Virtual Machine (VM) recovery to a new VM. The recovery fails indicating that there was a failure to register the VM due to permissions. The VM recovery wizard and recovery session log show:

```
YYYY-MM-DD HH:MM:SS ERROR:  [@(##) Build number: 28] Error registering VM: ServerFaultCode: Permission to perform this operation was denied.
YYYY-MM-DD HH:MM:SS ERROR:  [@(##) Build number: 28] Error in registering VM "[DATASTORE_NAME] VM_NAME/VM_NAME.vmx". "ServerFaultCode: Permission to perform this operation was denied."
```

The required destination folder is not listed when configuring the restore session using NMC.

On VMware Cloud on AWS, in order to perform recovery to a new VM using NetWorker Management Console (NMC), ensure that target folders in **VMs and Templates** view of the target vCenter have the following permissions. The user account for the target **VMs and Templates** folder user account can be assigned the permissions of the **CloudAdmin** role.

1. From the vSphere Web Client select the **VMs and Templates view**.
2. Expand the Data Center and select the appropriate destination folder in the tree view.
3. In the details pane, select the **Permissions** tab for the directory.
4. In the **Permissions** tab, click the **+** sign to add permissions.
5. In the **Add Permissions** window, add the appropriate user domain and search for the user account.
6. In the **Add Permissions** window, click **CloudAdmin** in the role drop-down and click **Propagate to children**.
7. The NMC displays the wanted target folder in the VM folder option to proceed with the restore-as-new.

# NetWorker VMware Protection for Azure VMware Solution

This appendix includes the following topics:

## Topics:

- [Introduction to NetWorker VMware Protection for Azure VMware Solution](#)
- [Deploy the vProxy OVA on a vCenter server running in Azure VMware Solution](#)
- [Prerequisites](#)
- [Best practices for NetWorker VMware protection running on Azure VMware Solution](#)
- [Limitations](#)
- [Unsupported NetWorker operations](#)

## Introduction to NetWorker VMware Protection for Azure VMware Solution

NetWorker and NetWorker Virtual Edition supports NetWorker VMware Protection for Azure VMware Solution.

Using either NetWorker or NetWorker Virtual Edition to protect virtual machines running in Azure VMware Solution is similar to how you protect the virtual machines in an on-premises data center. This appendix provides information about network configuration prerequisites, Azure VMware Solution best practices for NetWorker and NetWorker Virtual Edition and, NetWorker operations that are unsupported for Azure VMware Solution.

## Deploy the vProxy OVA on a vCenter server running in Azure VMware Solution

Perform the following steps to deploy the OVA for the vProxy host from a vCenter server by using the HTML5 **vSphere Web Client**.

Review the [Pre-requisites](#) section.

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**.  
The **Deploying template** task appears in the vCenter and provides status information about the deployment.

## 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 Virtual Edition, 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 and NetWorker Virtual Edition in a Azure VMware Solution. Also, ensure that you plan your firewall according to these prerequisites.

## Azure VMware Solution console

In the Azure VMware Solution 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 Azure VMware Solution 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. Ensure that you configure the inbound and outbound firewall rules of your compute gateway for Data Domain connectivity in your Azure Virtual Network (VNet).
- 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.
- Configure the inbound and outbound firewall rules of your Azure Virtual Network (VNet) security group to provide connectivity between the VMware vSphere SDDC compute gateway and Data Domain connectivity if Data Domain is running in your Azure Virtual Network (VNet).

- If you are performing replication from one Data Domain system to another, ensure that you configure the inbound rule for the security group in Azure to allow all traffic from the respective private IPs of Data Domain Virtual Editions running in your Azure Virtual Network (VNet).
- If you have more than one Data Domain running in Azure to perform replication, 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

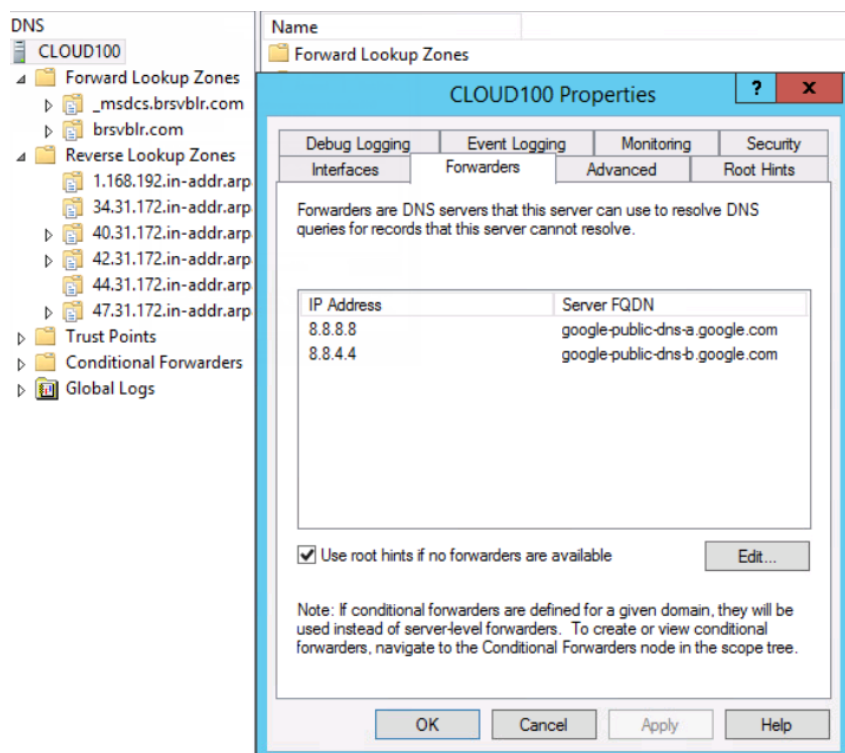


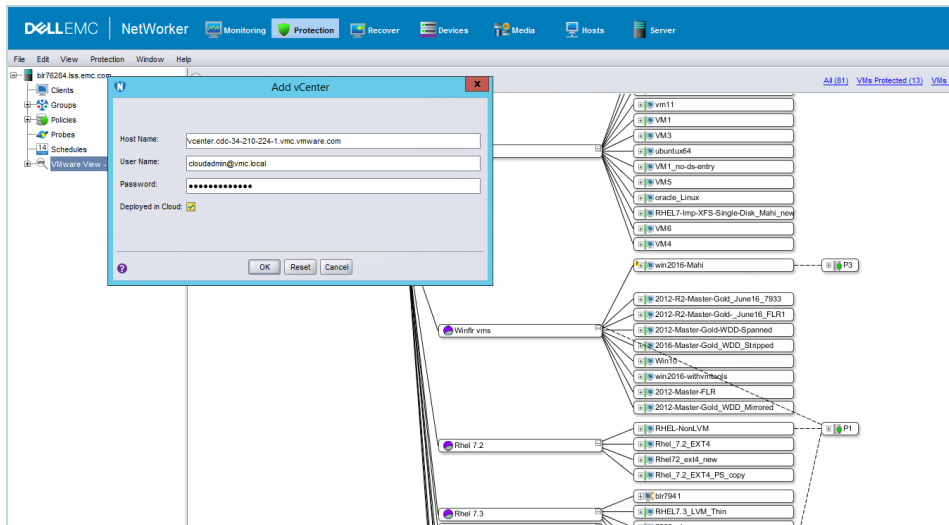
Figure 86. Enable internet access for Forwarders

## Best practices for NetWorker VMware protection running on Azure VMware Solution

Observe the following best practices when using NetWorker to protect virtual machines running in Azure VMware Solution:

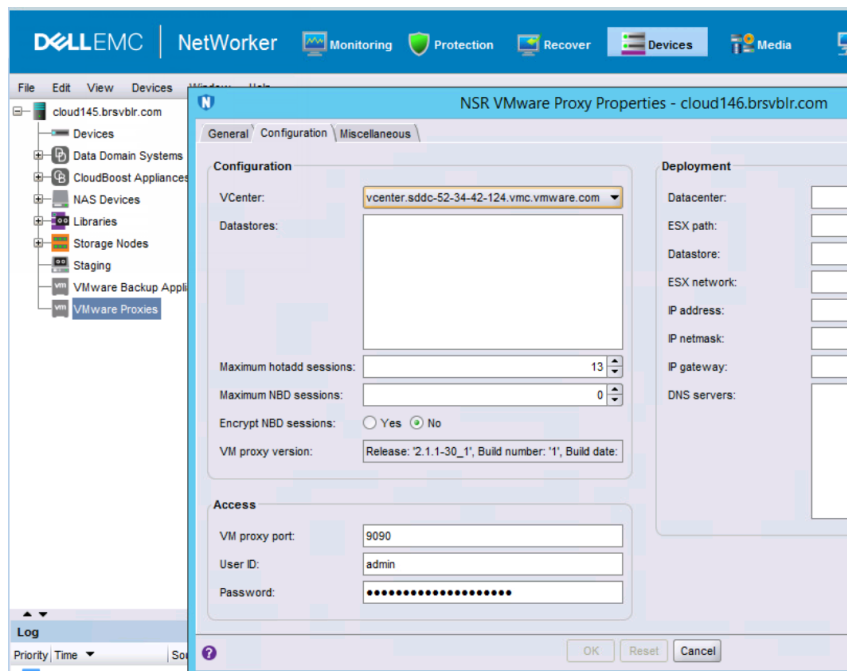
- If you are running NetWorker server prior to version 19.1.0.2, then you must disable `console events` and `console cancel`.
  1. Log in as root and run `nsradmin`.
  2. Enter `print type: nsr hypervisor; name: <vcenter_server_name>`
  3. Enter `update console cancel: no` and then type `Yes`
  4. Enter `update console events: no` and then type `Yes`
  5. Enter the command `Print`, review the settings and then exit.
- When you are deploying or configuring the Dell EMC NetWorker vProxy appliance, ensure that correct DNS server IP pointing to the internal DNS server running in the vCenter inventory is specified.
- Ensure that both forward and reverse lookup entries in the internal DNS server are specified for all the required components such as Dell EMC NetWorker server, Dell EMC NetWorker vProxy, DDVE appliance so on

- When adding the vCenter Server to NMC's **VMware View**, ensure that you select the **Deployed in Cloud** checkbox. This setting is required for any vCenter Servers running in Azure VMware Solution, If you do not select this option, then some NetWorker operations fail in the Azure VMware Solution.



**Figure 87. Add a vCenter Server to VMware View with Deployed in Cloud enabled**

- If using NSX-T, 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.
- While adding the vCenter server to the Dell EMC NetWorker server, specify the login credentials for the cloudadmin@vmc.local or an equivalent user.
  - NOTE:** Using customized roles with privileges other than the default cloudadmin role in the vCenter is not supported with NetWorker. If customized role is required, then the new role should have the same set of privileges as that of a cloudadmin role for NetWorker to perform backup and restore operations.
- When configuring the vProxy in the NetWorker Server, set the **Maximum NBD sessions** for the vProxy to zero. Azure VMware Solution does not support NBD or NBDSSL transport mode. Hence, we recommend you to always set the **Maximum NBD sessions** for all the vProxies to zero.



**Figure 88. NSR VMware Proxy Properties**

## Limitations

Before configuring NetWorker VMware Protection in Azure VMware Solution, review the following limitations.

### Restore as new VM using NMC and NetWorker HTML5 Admin Console fails with error stating that the vProxy is not able to register the VM onto the destination.

The vProxy restores as new VM using NetWorker Management Console and NetWorker HTML5 Admin Console fail with errors stating that the vProxy is unable to register the VM onto the destination.

The restore log displays:

```
159373:nsrvproxy_recover: vProxy Log:
2019-10-09T04:22:33Z ERROR: [@(##) Build number: 28] Error
registering VM: ServerFaultCode: Permission to perform this
operation was denied. 159373:nsrvproxy_recover: vProxy Log:
2019-10-09T04:22:33Z ERROR: [@(##) Build number: 28] Error in
registering VM "[WorkloadDatastore]
Win-GA-Repl1_labc/Win-GA-Repl1_labc.vmx". "ServerFaultCode:
Permission to perform this operation was denied."
```

To fix the issue, you should manually add vCenter permission to the desired "VMs and Templates" folder that the restored VM has to be stored. The target VM folder should be associated with permissions as follows "**user=cloudadmin**group" and "**role=cloudadmin**", and enable "**propagate to children**". After the permission is added manually, NetWorker NMC and NWUI will display the desired folder. If correct folder is chosen in the UI, then the restore as new VM will be successful.

### When restoring as new VM, the reconnect NIC option may not work correctly.

To fix the issue, perform one of the following workarounds:

- Edit settings of the restored new VM and change the network to "VM Network" and then click **Apply**. Reopen the edit setting configuration pane of the VM, and change the network to the correct desired NSX-T network logical switch and then click **Connect**.
- Power off the restored VM, change the network to "VM Network" and then click **Apply**. Reopen the edit setting configuration pane of the VM, change the network to the desired NSX-T network logical switch with `connected` and `connect at power on` options checked and then Power on the VM.

## Unsupported NetWorker operations

Some of the VMware features and permissions are not granted within the Azure VMware Solutions (AVS) environment. Hence, some of the dependent Dell EMC NetWorker features will be limited or not operating. Dell EMC NetWorker in Azure VMware Solutions does not support the following operations:

- File-level restore from an image-level backup.
- Instant access recovery of an image-level backup.
- Emergency restore
- Image-level backups and restores using NBD or NBDSSL transport mode.
- vProxy appliance configured with dual stack or IPv6 only is not supported.
- Application-consistent data protection for MS-SQL with the vProxy appliance.
- If datacenter is placed inside a folder in the vSphere SDDC, image backup and restore is not supported.
- NetWorker plug-in (HTML5) for vSphere Client is not supported.
- vProxy redeployment.



# Regular expressions for NetWorker vProxy dynamic policies rule definitions

This appendix includes the following topic:

## Topics:

- [Regular expression syntax accepted by dynamic policy rule definition](#)

## 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]
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

<b>Repetitions</b>	
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
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.

<b>Grouping</b>	
(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

<b>Flags</b>	
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 ).

<b>Empty strings</b>	
^	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

<b>Escape sequences</b>	
\a	bell ( ≡ \007 )
\f	form feed ( ≡ \014 )
\t	horizontal tab ( ≡ \011 )
\n	newline ( ≡ \012 )
\r	carriage return ( ≡ \015 )
\v	vertical tab character ( ≡ \013 )

<b>Escape sequences</b>	
\*	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

<b>Character class elements</b>	
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)

<b>Named character classes as character class elements</b>	
[\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} )

<b>Perl character classes (all ASCII-only)</b>	
\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_] )

<b>ASCII character classes</b>	
[[:alnum:]]	alphanumeric ( ≡ [0-9A-Za-z] )
[[:alpha:]]	alphabetic ( ≡ [A-Za-z] )
[[:ascii:]]	ASCII ( ≡ [\x00-\x7F] )
[[:blank:]]	blank ( ≡ [\t ] )
[[:cntrl:]]	control ( ≡ [\x00-\x1F\x7F] )

<b>ASCII character classes</b>	
[: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] )

<b>Unicode character class names--general category</b>	
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
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

<b>Unicode character class names--general category</b>	
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

<b>Vim character classes</b>	
\d	digits ( ≡ [0-9] ) VIM
\D	not \d VIM
\w	word character VIM
\W	not \w VIM