Dell EMC NetWorker

Version 18.1

VMware Integration Guide

302-004-429

REV 07

DELL EMC

Published February 2019

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

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

Published in the USA.

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

CONTENTS

FIGURES

TABLES

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 at https://support.emc.com.

Purpose

This document describes how to configure the NetWorker software to protect a VMware environment.

Audience

This document is part of the NetWorker documentation set and is intended for use by system administrators during the configuration of the NetWorker software.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
07	February 28, 2019	Added troubleshooting item "Increase the vCenter query timeout before starting a VMware backup action." Updates to file-level restore limitations for user requirements for FLR Agent installation on Linux, and the local Linux account requirement for mounting a virtual machine. Updates to "NetWorker VMware Protection Solution best practices with the vProxy appliance" for recommendation to enable the vCenter server's Datastore Browser feature.
06	February 5, 2019	Updates to vProxy incoming and outgoing port requirements.
05	January 25, 2019	Updates to Prerequisites section of the appendix "NetWorker VMware Protection in VMware Cloud on Amazon Web Services."
04	January 7, 2019	Updates to "NetWorker VMware Protection Solution best practices with the vProxy appliance" for recommendations when installing third party tools/

Table 1 Revision history (continued)

Revision	Date	Description
		applications in the virtual appliance, and the vCenter server's Datastore Browser feature. Updates to the section "Domain user setup required for file-level recovery."
03	August 3, 2018	Added section "Renaming a NetWorker 9.1 and later server with legacy VMware Backup appliance" for upgrades from a NetWorker 8.2.x release to 9.1 and later.
02	July 18, 2018	Removed troubleshooting item "Backups failing for virtual machines containing both hotadd disks and disks that do not support hotadd mode such as IDE and SATA."
01	July 7, 2018	First release of this document for NetWorker 18.1.

Related documentation

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

- *NetWorker Online Software Compatibility Matrix*
  Provides compatibility information, including specific software and hardware configurations that NetWorker supports. To access the matrix, go to http://compatibilityguide.emc.com:8080/CompGuideApp/.
- *NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *NetWorker Network Data Management Protocol (NDMP) User Guide*
  Describes how to use the NetWorker software to provide data protection for NDMP filers.
- *NetWorker Cluster Integration Guide*
  Contains information related to configuring NetWorker software on cluster servers and clients.
- *NetWorker Installation Guide*
  Provides information on how to install, uninstall, and update the NetWorker software for clients, storage nodes, and servers on all supported operating systems.
- *NetWorker Updating from a Previous Release Guide*
  Describes how to update the NetWorker software from a previously installed release.
- *NetWorker Release Notes*
  Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.
- *NetWorker Data Domain Boost Integration Guide*
  Provides planning and configuration information on the use of Data Domain devices for data deduplication backup and storage in a NetWorker environment.

- *NetWorker Performance Optimization Planning Guide*
  Contains basic performance tuning information for NetWorker.
- *NetWorker Server Disaster Recovery and Availability Best Practices Guide*
  Describes how to design, plan for, and perform a step-by-step NetWorker disaster recovery.
- *NetWorker Snapshot Management Integration Guide*
  Describes the ability to catalog and manage snapshot copies of production data that are created by using mirror technologies on storage arrays.
- *NetWorkerSnapshot Management for NAS Devices Integration Guide*
  Describes how to catalog and manage snapshot copies of production data that are created by using replication technologies on NAS devices.
- *NetWorker Security Configuration Guide*
  Provides an overview of security configuration settings available in NetWorker, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- *NetWorker VMware Integration Guide*
  Provides planning and configuration information on the use of VMware in a NetWorker environment.
- *NetWorker Error Message Guide*
  Provides information on common NetWorker error messages.
- *NetWorker Licensing Guide*
  Provides information about licensing NetWorker products and features.
- *NetWorker REST API Getting Started Guide*
  Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.
- *NetWorker REST API Reference Guide*
  Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.
- *NetWorker 18.1 with CloudBoost 18.1 Integration Guide*
  Describes the integration of NetWorker with CloudBoost.
- *NetWorker 18.1 with CloudBoost 18.1 Security Configuration Guide*
  Provides an overview of security configuration settings available in NetWorker and Cloud Boost, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- NetWorker Management Console Online Help
  Describes the day-to-day administration tasks performed in the NetWorker Management Console and the NetWorker Administration window. To view the online help, click **Help** in the main menu.
- NetWorker User Online Help
  Describes how to use the NetWorker User program, which is the Windows client interface, to connect to a NetWorker server to back up, recover, archive, and retrieve files over a network.

Special notice conventions that are used in this document

The following conventions are used for special notices:

NOTICE

Identifies content that warns of potential business or data loss.

Note

Contains information that is incidental, but not essential, to the topic.

Typographical conventions

The following type style conventions are used in this document:

Table 2 Style conventions

Bold	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.
Italic	Used for full titles of publications that are referenced in text.
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
Monospace italic	Used for variables.
`Monospace bold`	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://support.emc.com
- https://community.emc.com

Where to get support

The Support website at https://support.emc.com provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may enable you to resolve a product issue before you contact Support.

To access a product specific Support page:

1. Go to https://support.emc.com/products.
2. In the **Find a Product by Name** box, type a product name, and then select the product from the list that appears.
3. Click ».
4. (Optional) To add the product to **My Saved Products**, in the product specific page, click **Add to My Saved Products**.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for by solution number, for example, 123456, or by keyword.

To search the Knowledgebase:

1. Go to https://support.emc.com.
2. Click **Advanced Search**.
   The screen refreshes and filter options appear.
3. In the **Search Support or Find Service Request by Number** box, type a solution number or keywords.
4. (Optional) To limit the search to specific products, type a product name in the **Scope by product** box, and then select the product from the list that appears.
5. In the **Scope by resource** list box, select **Knowledgebase**.
   The **Knowledgebase Advanced Search** panel appears.
6. (Optional) Specify other filters or advanced options.
7. Click 🔍.

Live chat

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

1. Go to https://support.emc.com.
2. Click **Chat with Support**.

Service requests

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

1. Go to https://support.emc.com.
2. Click **Create a Service Request**.

Note

To create a service request, you must have a valid support agreement. Contact a sales representative for details about obtaining a valid support agreement or with questions about an account. If you know the service request number, then directly enter the service request number in the `Service Request` field to get the valid details.

To review an open service request:

1. Go to https://support.emc.com.
2. Click **Manage service requests**.

Online communities

Go to the Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all products.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Introduction to NetWorker VMware Protection with the vProxy appliance

This chapter contains the following topics:

Introduction to NetWorker VMware Protection with vProxy appliance

NetWorker 18.1 releases provide you with the ability to perform virtual machine protection and recovery by using the NetWorker VMware Protection solution with the vProxy appliance, also known as NVP.

NVP features the following:

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

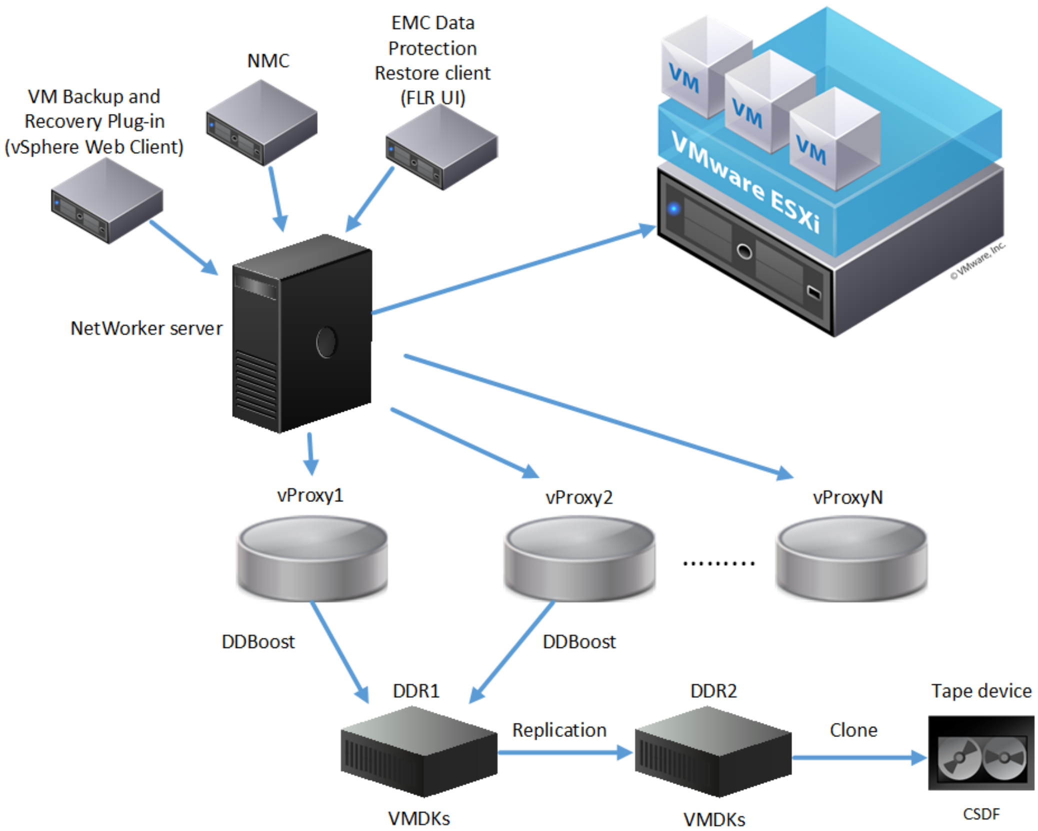
Note

If upgrading to NetWorker 18.1, you can continue to use the legacy NetWorker VMware Protection Solution with the VMware Backup appliance (VBA) to run existing VMware Backup appliance protection policies. However, you will not be able to create any new policies using the VMware Backup Appliance, and you cannot recover backups performed with the VMware Backup appliance by using the vProxy appliance.

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.
- NMC server—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.
- 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.

Table 3 NetWorker VMware Protection with vProxy appliance requirements

Component	Requirements
NetWorker	NetWorker 18.1 server software with NMC. **Note** The NetWorker storage node should be the same version as the NetWorker server.
vProxy Appliance	Version 2.3.0-3 System requirements for the vProxy include: • CPU: 4 * 2 GHz (4 virtual sockets, 1 core for each socket). • Memory: 8GB. • Disks: 2 disks (59 GB and 98 GB). • Internet Protocol: IPv4 only; dual stack and IPv6 not supported. • SCSI controller: Maximum 4. • NIC: One vmxnet3 NIC with one port.
vCenter server	• Version 5.5, 5.5 U2, 5.5 U3a, 5.5 U3b, 5.5 U3d, 6.0, 6.0 U1b, 6.0 U2, 6.5, 6.50b. **Note** Version 6.5 and later is required to perform Microsoft SQL Server application-consistent protection. • Linux or Windows platform, or VC appliance.
ESX/ESXi server	• Version 5.5, 5.5 U2, 5.5 U3a, 5.5 Ub, 6.0 U1, 6.0 U1b, 6.0 U2, 6.5, 6.50b. **Note** Version 6.5 and later is required to perform Microsoft SQL Server application-consistent protection. • Automatically enables Changed Block Tracking (CBT) on each virtual machine.
VMware Tools	Version 10 or later. **Note** Version 10.1 and later is required to perform Microsoft SQL Server application-consistent protection.

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

Component	Requirements
Data Domain	• A minimum of one configured DD Boost device is required. Additionally, you must specify one pool that contains the DD Boost device. • Data Domain system OS at DDOS version 5.7, 6.0.0.30, 6.0.1-10, or 6.1. If using DDOS 5.7.x, 5.7.1 is recommended. **Note** The NetWorker compatibility matrix at http://compatibilityguide.emc.com:8080/CompGuideApp/ provides detailed information on NetWorker and DD Boost version compatibility. • A Data Domain user account with administrator privileges, which you will use to manage file-level restore and instant access restore.

Port requirements

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

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	VMware View in NMC
vCenter server	NetWorker server	9090	vSphere Client's VM Backup and Recovery plug-in
Dell EMC Data Protection Restore Client interface	NetWorker server	9090	File-level recovery in the Dell EMC Data Protection Restore Client
ESXi servers	Data Domain	111, 2049, 2052	File-level recovery and instant recovery

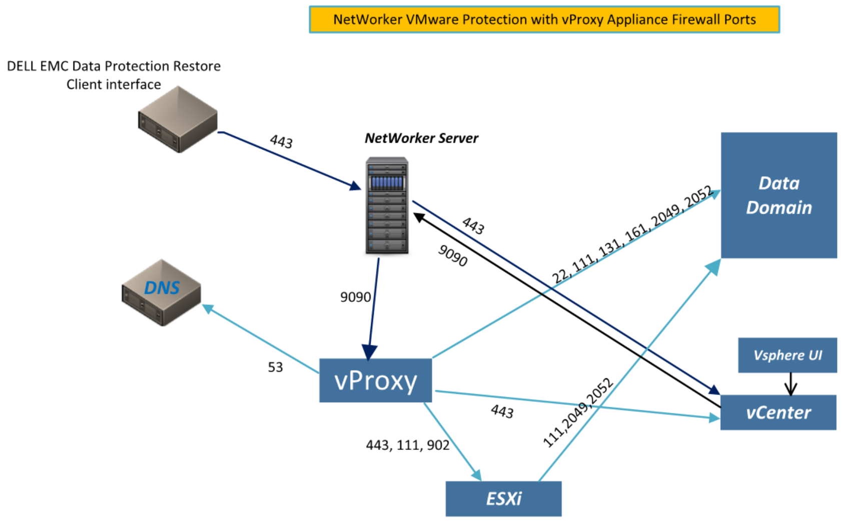
Table 4 Incoming port requirements (continued)

From	To	Port	Purpose
Virtual machines	Data Domain	111, 2049 The *NetWorker Data Domain Boost Integration Guide* also provides information about firewall ports required for DD Boost.	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	Data Domain management
vProxy Appliance	ESXi server	443, 902	Backup and recovery operations
vProxy Appliance	vCenter server	443	Backup and recovery operations

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



vProxy limitations and unsupported features

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

Note

Review the VMware limitations:

- vSphere 5.5—https://www.vmware.com/pdf/vsphere5/r55/vsphere-55-configuration-maximums.pdf
- vSphere 6.0—https://www.vmware.com/pdf/vsphere6/r60/vsphere-60-configuration-maximums.pdf
- vSphere 6.5—https://www.vmware.com/pdf/vsphere6/r65/vsphere-65-configuration-maximums.pdf

Limitations to SQL Server application consistent data protection

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

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

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

vProxy appliance configured with dual stack or IPv6 only is not supported

The vProxy appliance does not support dual stack (IPv4 and IPv6) or IPv6 only addressing. If you want to run backups and restores using the vProxy appliance, use IPv4 addressing for the vProxy and disable IPv6.

vCenter version not updated in RAP database after upgrade

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

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

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

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

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

vProxy cannot perform recoveries from policies run with VMware Backup appliance

After upgrading to a NetWorker release with the vProxy appliance, any policies run with the VMware Backup appliance cannot be recovered with the vProxy appliance. If you want to recover these backups you must continue to use the VMware Backup appliance.

No new policies can be created with VMware Backup appliance

After upgrading to a NetWorker release with the vProxy appliance, new policies can only be created with the vProxy appliance. You can continue to run and edit existing VMware Backup Appliance policies, but once you delete a VMware Backup appliance policy, it is no longer available. A message appears each time you run a VMware Backup Appliance policy recommending that you use the vProxy appliance.

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

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

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

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

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

Datastore names cannot contain special characters

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

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

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

Data Domain Boost over fibre channel not supported

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

Data Domain SMT not supported

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

Only hotadd and NBD transport modes supported

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

Note

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

Specify NBD for datastores if proxies should use NBD mode only

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

Backup of individual folders within a Virtual Machine is not supported

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

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

When you use VMware View, the map view does not appear when the configuration for one or more Virtual Machines in the vCenter is incomplete. To avoid this issue, remove the incomplete Virtual Machine configurations from vCenter.

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

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

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

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

VMware snapshot for backup is not supported for independent disks

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

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

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

Restricted data zones not supported

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

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 http://compatibilityguide.emc.com:8080/CompGuideApp/.

Note

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

Recommendations and considerations

This section provides information about performance and scalability, best practices, and a configuration checklist.

Performance and scalability

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

Table 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	50 (10G network)		VMware uses Network File Copy (NFC) protocol to read VMDK using NBD transport mode. You need one VMware NFC connection for each VMDK file being backed up. The VMware Documentation provides more information on vCenter NFC session connection limits.
Virtual machines concurrent backups per vCenter server	100	100	Can be achieved with a combination of the number of proxies multiplied by the number of configured hotadd sessions per vProxy.
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

Table 6 Performance and scalability factors (continued)

Component	Maximum limit	Recommended count	Notes
			than 100 proxy streams run concurrently against any given vCenter.
Number of workflows per VMware policy	64	8	Ensure that you do not to exceed 2000 virtual machines per VMware policy.
Number of virtual machines per workflow	2000		Ensure that you do not to exceed 2000 virtual machines per VMware policy. Note that the maximum of 2000 virtual machines per workflow is only applicable to the first FULL backup to Data Domain, and does not apply to CBT-based incremental backups of the virtual machines. However, ensure that you do not exceed 100 connections per vCenter at any time during the backup window.
Number of vCenter servers per policy	5	3	Per policy you can use 5 vCenter servers in the respective workflows and trigger concurrent backups.
Number of concurrent recoveries		50	It is recommended to use hotadd transport mode for recoveries. For large concurrent restores, it is highly recommended that multiple target datastores are used for optimal performance
Number of files/directories per file level recovery (User and Admin mode)	20000 or less		File-level recovery is recommended for quickly recovering a small set of files. Image-level or VMDK-level recoveries are optimized and recommended for recovering a large set of files/folders.
Number of parallel instant access sessions	32		You can perform up to 32 parallel instant recovery sessions using `nsrvproxy_recover`, provided that you satisfy the following prerequisites: • For the backups being restored, you must select **Performance** backup optimization mode during VMware type group creation in NMC. • Data Domain OS version 6.0.0.30 is supported. • Data Domain platforms supported include DD6300 (EOS-T2), DD6800 (EOS-T3), DD9300 (EOS-T4), and DD9800. • The ESXi host requires the following default values to be updated to the maximum supported: Under NFS, update **NFS.MaxVolumes**. Under Net, update **Net.TcpipHeapSize**. Under Net, update **Net.TcpipHeapMax**. The VMware knowledgebase article at https://kb.vmware.com/kb/2239 provides more information. Additionally, refer to the VMware Documentation for concurrent virtual machine migration limits.

Table 6 Performance and scalability factors (continued)

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

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 adds additional backup and recovery capabilities that quiesce certain processes on the guest operating system prior to backup.
- Installation of third-party tools or applications in the virtual appliance for the purposes of monitoring the appliance status and protecting the appliance from computer viruses can have a negative impact on system performance. Therefore, it is recommended that you do not install any additional tools or applications in the appliance.

Configuration recommendations

- Ensure that the vCenter server's **Datastore Browser** feature is enabled, which allows you to browse all datastores associated with the vSphere environment. NetWorker VMware Protection requires this feature to download configuration files for a virtual machine during backup and recovery operations.
  This feature is enabled by default, but you can verify the feature status by opening the `vpxd.cfg` file within your vCenter configuration, and ensuring that the entry for **`enableHttpDatastoreAccess`** is either set to **`true`** or is not contained in the file. Information on how to locate the `vpxd.cfg` file within your vCenter configuration is provided in the VMware documentation.
- vProxy remote site configurations with a storage node communication latency greater than 50 ms require a storage node in the remote site.
- 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.

- For best practices related to SQL Server application-consistent protection, review the software and security requirements in the section Enable the Microsoft VM App Agent for SQL Server application-consistent protection.
- During policy configuration, assign virtual machines to a protection group based on logical grouping to allow for better scheduling of backups that will help you avoid resource contention and create more organized logs for review.
- When you plan the backups, ensure that NetWorker VMware Protection supports the disk types that you use in the environment. Currently, NetWorker VMware Protection does not support the following disk types:
  - Independent (persistent and non-persistent)
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode
- The vProxy Appliance leverages Changed Block Tracking (CBT) by default. If CBT is disabled on the virtual machine, then it will enable CBT automatically. If you add a disk to the virtual machine after the first full backup, for the next policy run a full backup will be performed automatically for the newly added disk, and an incremental backup will be performed for the existing disk. For information on disabling CBT, refer to the section Enabling or disabling Changed Block Tracking.
- When backing up thin-provisioned Virtual Machines or disks for Virtual Machines on NFS datastores, an NFS datastore recovery does not preserve thin provisioning. VMware knowledge base article 2137818 at http://kb.vmware.com/kb/2137818 provides more information.
- It is recommended that you set an appropriate NetWorker server/storage parallelism value, according to the available resources, to reduce queuing. For example, 5 vProxy appliances with backup and clone operations will require more than 125 parallel sessions. Therefore, setting the parallelism for the NetWorker server to 128 or higher (while also setting the server with 32+ GB memory and 8+ CPUs) will suit such an environment. The *NetWorker Performance Optimization Planning Guide* provides more details.
  If you require a larger number of parallel image backups, also consider setting the maximum number of vCenter SOAP sessions to larger value. Note that this requires careful planning and additional resources on the vCenter Server You can configure this by modifying the following line in the vCenter `vpxd.cfg` file:

  ```
  <vmacore><soap><maxSessionCount> N </maxSessionCount></soap></
  vmacore>
  ```

  This applies specifically to SDK sessions as opposed to VI client sessions:
- Each Virtual Machine backup to a Data Domain system consumes more than one session on the Data Domain device. The default device configuration is `target sessions=20` and `max session=60`, however it is recommended that you configure additional devices for more than 10 parallel backups.
- Virtual Machines with extremely high IO may face hangs during consolidation due to the ESXi forced operation called synchronous consolidate. Plan your backups of such Virtual Machines according to the amount of workload on the Virtual Machine.

- When you work with the vCenter database either directly or by using scripts, do not change the name attribute for the `vmfolder` object. VMware knowledge base article at https://support.emc.com/kb/190755 provides more information.
- Resource contention can occur at various points during the backup cycle. When NetWorker runs larger policies, issues due to contention of resources can occur, which impact all running operations. Adjust your resources and times for other larger policies to avoid overlaps, and avoid resource contention.
  For example, you configure one pool named Bronze, with one device. If you set up a policy where every day at 10 pm two policies called 'Bronze1' and 'Bronze2' with 400 virtual machines each start writing to the device in the 'Bronze' pool, then the long wait for device availability may cause unexpected delays or timeouts. To fix this, set the policy start times 4 hours apart and add more devices, to allow for stable backups.

Transport mode recommendations

Review the following recommendations for transport mode settings:

- Use hotadd transport mode for faster backups and restores and less exposure to network routing, firewall, and SSL certificate issues. The vProxy appliance currently supports a maximum of 25 concurrent hotadd sessions. To support hotadd mode, deploy the vProxy on an ESXi host that has a path to the storage that holds the target virtual disk(s) for backup.

  Note

  Hotadd mode requires VMware hardware version 7 or later. Ensure that all virtual machines that you back up with Hotadd mode are using Virtual Machine hardware version 7 or later.

  For sites that contain a large number of virtual machines that do not support hotadd requirements, NBD transport mode will be used. This can cause congestion on the ESXi host management network. Plan your backup network carefully for large scale NBD installs. You may consider configuring one of the following options:

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

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

- Upgrade all Data Domain systems to use DDOS version 5.7, 6.0.0.30, 6.0.1-10, or 6.1. The Data domain Retention Lock feature is also supported for vProxy backup and clone actions but requires DDOS 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. By default, only NFS v3 is enabled from the ESXi host. If using NFS v4, you might be required to disable and use NFS v3 instead in order to avoid issues with file-level restore operations.
- For virtual machines within in application-consistent data protection policy, network zoning must be configured to enable network connectivity between the virtual machines and the Data Domain system.

NetWorker configuration

- Ensure that the relevant devices are mounted.
- Ensure that vProxy IP addresses are populated in DNS, and that the NetWorker server has name resolution for the vProxy host names.
- 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.

Accessing Knowledge Base Articles

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

CHAPTER 2

Deploy the vProxy appliance and configure the NetWorker datazone

This chapter contains the following topics:

Deploying the vProxy appliance

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

- The vCenter server.
- The ESXi host.

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

Deploy the vProxy OVA on a vCenter server

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

Before you begin

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

Procedure

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

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

- In the **Default gateway** field, specify the IP address of the gateway host.
- In the **Network Netmask/Prefix** field, specify the netmask for an IPv4 Network IP address. vProxy backups do not support the use of IPv6 Network IP addresses.

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 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`***

---

d. Expand **Password settings**, and then perform the following tasks:

- In the **Root password** field, specify a password for the root account or leave the field blank to use the default password. The default password is *changeme*.
- In the **Admin password** field, specify a password for the admin account or leave the field blank to use the default password. The default password is *a3dp@m8n*.

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.

Deploy the vProxy OVA on an ESXi host

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

Before you begin

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

Procedure

1. Log into the ESXi host with an administrator account.
2. From the **File** menu, select **Deploy OVF Template**.
3. On the **Source** window, type a URL path to the OVA package or click **Browse** and navigate to the OVA package location, and then click **Next**.
4. On the **OVF Template Details** window, review the product details such as the product name, version, vendor, publisher, and download size, and then click **Next**.

5. On the **Accept License Agreements** window, the EULA appears. Review the EULA and then click **Accept**.
6. On the **Name and Location** window, specify a name for the virtual appliance, and optionally the inventory location, for example a datacenter or VM folder. Click **Next**.
7. If the location you selected in the previous step has more than one available host, the **Host / Cluster** window appears. Select the ESXi host or cluster on which you want to deploy the virtual appliance, and then click **Next**.
8. On the **Resource Pool** window, perform one of the following tasks, and then click **Next**.
   - When you deploy the virtual appliance in a cluster with multiple hosts, select the specific host in the cluster on which to deploy the virtual appliance.

     Note

     If DRS is enabled, the target host is automatically selected.
   - When you deploy the virtual appliance on a host with a resource pool or vApp, select the resource pool or vApp on which to deploy virtual appliance.
9. On the **Storage** window, select the destination datastore on which to store the virtual appliance files, and then click **Next**.
10. On the **Disk Format** window, select the disk format.

    EMC recommends 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.

Configure the network settings

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

Procedure

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

   The default password for the root account is **`changeme`**.
3. Use the `/opt/emc/vproxy/bin/config_network.sh` command to configure the network settings.

   For example: `/opt/emc/vproxy/bin/config_network.sh` ***`fqdn IP address netmask gateway "dns_server1, dns_server2, ... dns_serverN"`*** where:
   - *fqdn* is the Fully Qualified Domain Name of the appliance.

- *IP address* is the IP address of the appliance.
- *netmask* is the netmask of the appliance.
- *gateway* is the name or IP address of the gateway host.
- *" dns_server1, dns_server2, ... dns_serverN"* is a comma-separated list of IP addresses or hostnames for the DNS servers, enclosed in quotes.

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

Note

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

VMware vCenter server management

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

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

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

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

Add the vCenter server using NMC's VMware View

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

Procedure

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

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

   Note

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

Edit a vCenter server using VMware View in NMC

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

Procedure

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

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

   Note

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

Results

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

Note

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

Add the vCenter server using the NetWorker Management Web UI

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

Procedure

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

   The NetWorker login page displays.
2. In the NetWorker login page:

   a. Type the **Username** and **password** credentials for the administrator user.

   b. Type the NetWorker server IP address.

   c. Type the port that will be used for communication between the NetWorker server and the vCenter server.

   d. Click **Log in**.

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

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

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

   Note

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

   ---
9. Click **Save**.

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

Results

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

Edit a vCenter server using the NetWorker Management Web UI

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

Procedure

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

   The **Edit vCenter** dialog displays, with the **Hostname** field greyed out as this field cannot be changed in this dialog.
3. In the **Username** field, specify a new vCenter user account that has permissions to perform backups.
4. In the **Password** field, specify the password for this vCenter user account.

5. If the vCenter server is deployed in the Cloud and this option is currently unselected, select the **Deployed in Cloud** checkbox.

   Note

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

   ---

6. Click **Save**.

Results

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

Note

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

Configuring and registering the vProxy appliance

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

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

Configure and register the vProxy in NMC

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

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

Procedure

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. On the taskbar, click the **Enterprise** icon .
3. In the navigation tree, highlight a host:

   a. Right-click **NetWorker**.

   b. Select **Launch Application**. The **NetWorker Administration** window appears.
4. On the taskbar, click the **Devices** button .
5. In the **Device** window's left navigation pane, right-click **VMware Proxies** and select **New VMware Proxy Wizard**.

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

The **Select the VMware Proxies to Configure and Register** page displays. On this page, the **VMware Proxy Selection** pane displays the location of the deployed but unregistered vProxy appliance(s) within the vCenter/ESXi server.

7. Select the checkbox next to the vProxy appliance(s) you want to configure.
8. (Optional) If you want to override the common configuration options for the selected vProxy, click the **Edit** button to open the **Configure VMware Proxy** dialog. When finished, click **OK** to save the settings.
9. Click **Next**.

   The **VMware Proxies Configuration and Registration Summary** page displays.
10. Verify that the details are correct, and then click **Configure**.

Results

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

Additional method to add and configure the vProxy in NMC

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

Procedure

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

   The **Create NSR VMware Proxy** dialog displays.
6. On the **General** tab, specify the FQDN of the vProxy appliance in the **Name** field.
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. In the **User ID** field, specify the `admin` user account.
   c. In the **Password** field, specify the password for the `admin` user account on the vProxy appliance. The default password is `a3dp@m8n`.
   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.

8. Click **OK**.

Add and configure the vProxy in the NetWorker Management Web UI

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

Before you begin

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

Procedure

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

   The **VMware Proxies** pane opens on the **Proxies** tab, which displays any vProxies that have already been configured. You can choose to display hidden columns by clicking the blue icon in the lower left corner of the table.
2. In the **Proxies** tab, click the **+** icon and select **Actions** > **Add Proxies**.
3. On the **Selection** page, ensure that the correct vCenter is selected.

   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. The default password is `a3dp@m8n`.

   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.

6. Click **Finish**.

Results

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

Installing the vCenter plug-in

After you add the vCenter host, install either the HMTL5 or flash-based vCenter plug-in to enable virtual machine backup and recovery in the **vSphere Client** or **vSphere Web Client**.

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

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

Install the vCenter plug-in using VMware View in NMC

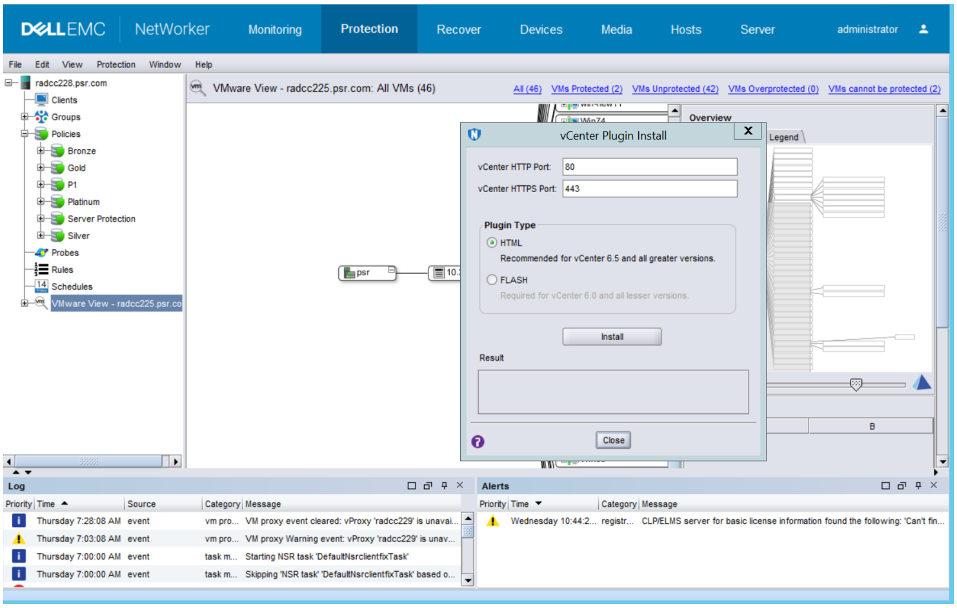
You can also use **VMware View** in NMC to install either the HMTL5 or flash-based vCenter plug-in to enable virtual machine backup and recovery in the **vSphere Client** or **vSphere Web Client**. Perform the following steps.

Procedure

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

   The **vCenter Plugin Install** dialog displays.

Figure 3 Install vCenter Plugin in NMC



vCenter Plugin Install

vCenter HTTP Port: 80

vCenter HTTPS Port: 443

Plugin Type

● HTML

Recommended for vCenter 6.5 and all greater versions.

○ FLASH

Required for vCenter 6.0 and all lesser versions.

Install

Result

Close

Log

Priority	Time	Source	Category	Message
i	Thursday 7:28:08 AM	event	vm pro...	VM proxy event cleared: vProxy 'radcc229' is unavai...
⚠	Thursday 7:03:08 AM	event	vm pro...	VM proxy Warning event: vProxy 'radcc229' is unav...
i	Thursday 7:00:00 AM	event	task m...	Starting NSR task 'DefaultNsrclientfixTask'
i	Thursday 7:00:00 AM	event	task m...	Skipping 'NSR task' 'DefaultNsrclientfixTask' based o...

Alerts

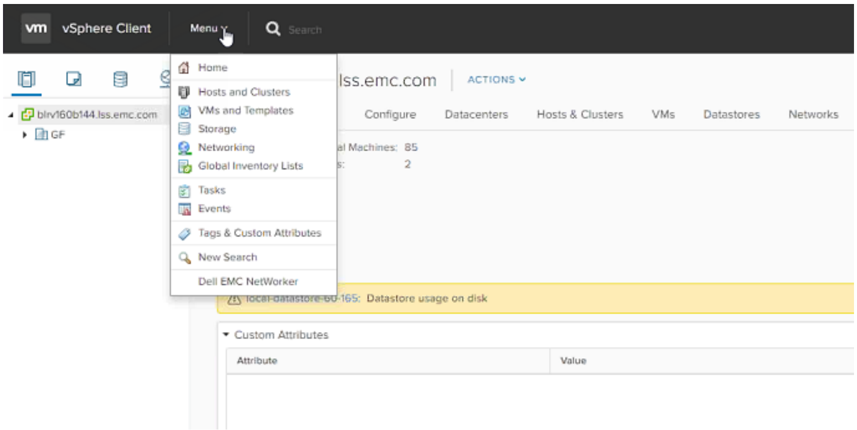
Priority	Time	Category	Message
⚠	Wednesday 10:44:2...	registr...	CLP/ELMS server for basic license information found the following: 'Can't fin...

4. If a security warning appears, click **Continue** to dismiss the warning.
5. Select the **Plugin Type** that you want to install. **HTML5** will install the **Dell EMC NetWorker** interface in the **vSphere Client**, which is introduced in NetWorker 18.1. **FLASH** will install the **VM Backup and Recovery** interface in the **vSphere Web Client**, which was introduced in NetWorker 9.1.
6. Provide the required HTTP and HTTPS ports that are configured for the vCenter server, or leave the default values 80 and 443.
7. Click **Install**.

Results

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

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



Note

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

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

In vSphere version 6.5 and later and NetWorker 18.1, the html-5 based vCenter plug-in appears as **Dell EMC NetWorker** in the **vSphere Client**. If you need to remove the HTML5-based plug-in and then reinstall the plug-in, perform the following steps.

Procedure

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

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

In NetWorker 9.2.x and earlier versions, the vCenter plug-in for vProxy backup and recovery is a flash-based plug-in that appears as **VM Backup and Recovery** in the left pane of the **vSphere Web Client**. vSphere versions 6.5 and later and NetWorker 18.1 support both this plug-in and the html-5 based vCenter plug-in that appears as **Dell EMC NetWorker** in the **vSphere Web Client**. If upgrading to NetWorker 18.1 and you no longer require the flash-based plug-in, perform the following steps in order to manually remove **VM Backup and Recovery** from the **vSphere Web Client**.

Procedure

1. Stop the **vSphere Web Client** services.
2. Log into vCenter Server's MOB at **`http://`*`vcenter-server`*`/mob`**.
3. Click the **content** link.
4. Click the **ExtensionManager** link.
5. Click on the **UnregisterExtension** link.

6. Enter the value `com.emc.networker` and click the **Invoke Method** link.
7. Enter the value `com.emc.networker.backup` and click the **Invoke Method** link.
8. Enter the value `com.emc.networker.recover` and click the **Invoke Method** link.
9. On the vCenter server, manually remove the plug-in from the `/vsphere-client-serenity` folder. On vCenter 6.0 and 6.5, the path is `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` on Linux, and `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` on Windows.
10. Restart the **vSphere Web Client** services.

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

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

Procedure

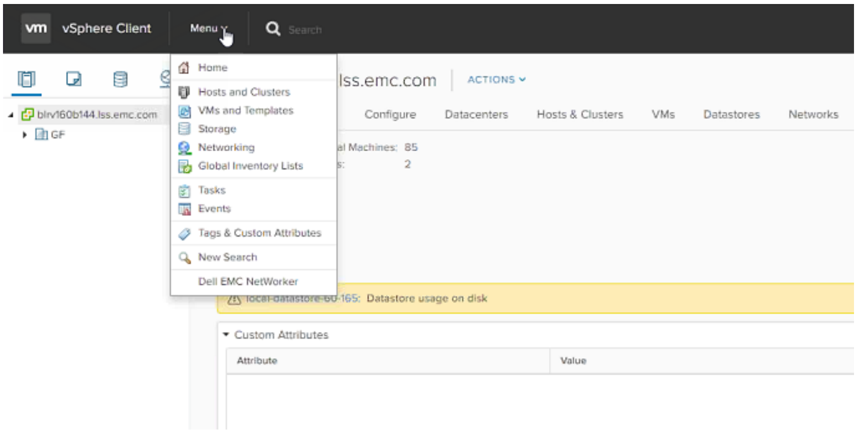
1. Select **Protection** > **VMware vCenters**in the left pane.
2. In the **Protection** window's **VMware vCenters** pane, click the **Install** icon.

   The **Install vCenter Plugin** dialog displays.
3. Select the **Plugin Type** that you want to install. **HTML** will install the **Dell EMC NetWorker** interface in the **vSphere Client**, which is introduced in NetWorker 18.1 for vSphere version 6.5. **Flash** will install the flash-based **VM Backup and Recovery** interface in the **vSphere Web Client**, which was introduced in NetWorker 9.1 for vSphere versions 6 and earlier.
4. Provide the required HTTPS port that is configured for the vCenter server, or leave the default value 443.
5. Type the username and password for the NetWorker administrator user.
6. Click **Install**.

Results

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

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



Note

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

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 sections Creating a VMware backup action, Creating a workflow provide more information.

- Restore of SQL Server instance or individual SQL Server databases—The **Dell EMC Data Protection Restore Client** includes an **App** mode that allows you to restore an entire SQL Server instance to the original virtual machine and original instance, and restore individual SQL Server databases to the original database on the original virtual machine, to multiple instances on the same virtual machine, or to an alternate location (different virtual machines/SQL instances on the same or a different vCenter), as well as the ability to roll-forward transaction log backups. The section Restoring SQL Server application-consistent backups provides more information.

During advanced application-consistent backup for both SQL Server FULL backup and transaction log backup, vProxy installs or upgrades the **vProxy Agent** and **MSVMAPPAGENT** software packages. On a new virtual machine without these software packages installed, the **vProxy Agent** uses the VM Administrator Credentials from the backup action to install the vProxy Agent, using the vCenter VIX API to copy packages into the guest virtual machine and run the install. Once the vProxy Agent is installed in the virtual machine, vProxy communicates with the **vProxy Agent** to install the **MSVMAPPAGENT** package.

On a system with vProxy and **MSVMAPPAGENT** already installed, vProxy performs a version check of the **MSVMAPPAGENT** by running the `Msvmagent_discovery.exe` program to report the installed program version and, if necessary, perform an upgrade if the vProxy software repository contains a later version.

Note

Ensure that you manually uninstall in-guest agents (VM app agent for Microsoft Applications) from an alternate virtual machine that is not protected by a SQL application-consistent backup workflow. Also, if you are restoring to an alternate virtual machine that is not protected by a SQL application-consistent workflow, note that the agents will not be automatically uninstalled once the restore is complete. If you want to remove these agents, you must manually uninstall the agents.

The following table provides a list of the **MSVMAPPAGENT** binaries that are called by the vProxy, and the operations these binaries perform.

Table 7 MSVMAPPAGENT binaries called by vProxy

Binary	Purpose	When called
`Msvmagent_discovery.exe`	Provides functions for listing program version and for validating that SQL is installed and for listing SQL Instances and databases.	Called by vProxy to report agent version and determine if an upgrade is required. Also called by vProxy to validate that SQL Server services are running in the virtual machine. Also called by vProxy to report running SQL instances and databases to support SQL alternate restore selection.

Table 7 MSVMAPPAGENT binaries called by vProxy (continued)

Binary	**Purpose**	**When called**
		Note If `Msvmagent_discovery.exe` does not find running SQL Server services, the program returns a failure to the vProxy and the overall NetWorker Application Consistent backup workflow cannot proceed. To resolve the issue, remove virtual machines that do not have SQL from the NetWorker Application Consistent workflow. You can also use the action logs to diagnose the failure, and contact Dell EMC support if required.
`Msvmagentcatsnap.exe`	Catalogs the SQL VSS Full backup that was performed by VMware Tools as an App Agent VSS Full backup of SQL Server instances. Catalog is written to Data Domain.	Called by vProxy once the virtual machine image snapshot has completed.
`Msvmagent_appbackup.exe`	Performs transaction log backup.	Called by vProxy for transaction log backup workflows. The `Msvmagent_appbackup.exe` program will back up all SQL instances in the virtual machine. `Msvmagent_appbackup.exe` performs transaction log backup only, and does not create a virtual machine image backup.
`Msvmagent_snapshotrestore.exe`	Performs restore of SQL VSS Full backup.	Called by vProxy during restore of SQL Database FULL backup. Prior to the restore, the virtual machine image backup is mounted on the target virtual machine. The `Msvmagent_snapshotrestore.exe` copies the VSS manifest documents from the backup, and uses those documents to perform a VSS-aware restore of the SQL database. The SQL database files are copied from the mounted backup VMDK to the original location of the database, and during the VSS post restore, the SQL VSS Writer completes recovery of the backup. If transaction logs are to be restored, or if the NORECOVERY option has been specified, the database will be left in a NORECOVERY state. The msvmagent_snapshotrestore.exe

Table 7 MSVMAPPAGENT binaries called by vProxy (continued)

Binary	Purpose	When called
		command also supports SQL Alternate restore and instructs SQL the SQL instance to be restored and to change database name and file locations as selected by the customer.
`Msvmagent_apprestore.exe`	Performs restore of individual SQL transaction log backup.	Called by vProxy during restore of the transaction log backup. For each transaction log restore, `Msvmagent_apprestore.exe` receives the Data Domain path for the backup and performs a SQL VDI restore of the transaction log backup. For intermediate transaction logs, the database is left in the NORECOVERY state. For the final transaction log restore, the database is either recovered or left in the NORECOVERY state if you specify this option. The STOPAT feature may also be used for the final transaction log restore if you specify this option. The msvmagent_apprestore.exe command also supports SQL Alternate restore and instructs SQL the SQL instance to be restored and to change database name and file locations as selected by the customer.

MSVMAPPAGENT binaries are installed to `C:\Program Files\DPSAPPS \MSVMAPPAGENT\bin`. Logs are located in `C:\Program Files\DPSAPPS \MSVMAPPAGENT\log`.

Software and security requirements

In order to perform SQL Server application-consistent data protection for virtual machines, the **MSVMAPPAGENT** requires the following:

- The**MSVMAPPAGENT** runs under the SYSTEM account for data protection operations. Configure all SQL Server instances in the virtual machine to grant NT AUTHORITY\SYSTEM account rights to perform SQL database backup and recovery operations:
  Add **SYSTEM** account to SQL logins.

  Grant **SYSTEM** account the sysadmin role.
- Network connectivity, host name resolution, and firewall ports between the Data Domain device and the virtual machines that are part of SQL Server application-consistent protection policies and restore to alternate operations. This connectivity is required to allow **MSVMAPPAGENT** to perform client direct operations to Data Domain.
- VMware vCenter server version 6.5 and later.
- VMware ESXi server version 6.5 and later.
- VMware Tools version 10.1 and later.

- Enable the UUID attribute (*disk.EnableUUID=TRUE*) in the **vSphere Client**.
- The virtual machine must use SCSI disks only, and the number of available SCSI slots must at least match the number of disks. For example, a virtual machine with 7 disks will only require one SCSI controller, but a virtual machine with 8 disks will require 2 SCSI controllers.
- The vProxy requires live network connectivity to the ESXi where the targeted SQL virtual machine resides.

Note

The **MSVMAPPAGENT** does not require installation of the NetWorker client.

The following table provides a list of special characters known to be supported in SQL database names for English and non-English locales.

Table 8 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 **Note** Restore to an alternate location for a SQL database with an apostrophe in the file name or destination file path will fail to restore.	Supported	Supported
$ Dollar	Supported	Supported
: Colon	Supported	Supported

Table 8 Supported characters in SQL database names (continued)

Special character	FULL and transaction log backup	FULL and transaction log restore
. Period	Supported	Supported

Unsupported features and configurations

The following features and configurations are not supported for SQL application-consistent protection:

- The **MSVMAPPAGENT** only supports stand-alone SQL Server instances, and does not support SQL Server Always-On Availability Group and SQL Server Clustered Failover instances.
- The **MSVMAPPAGENT** does not support interoperability with other backup agents, including SQL backup products from Dell EMC. If another backup product is running at the same time as **MSVMAPPAGENT**, the **MSVMAPPAGENT** has safeguards to prevent issues. For example, if another product is performing in-guest backups, **MSVMAPPAGENT** may skip databases for transaction log backups.
- If using the **VM Backup and Recovery** user interface in the **vSphere Web Client** for vSphere versions earlier than 6.5, backup and recovery operations are not supported for SQL Server advanced application-consistent protection policies. For SQL backups, perform these operations from the NMC **NetWorker Administration** window or the **Dell EMC NetWorker** user interface in the **vSphere Client**. For SQL recoveries, perform these operations from the **Dell EMC Data Protection Restore Client**.

Additionally, the following items are not supported due to VMware restrictions and feature limitations:

- Changing pools between backup actions, for example, between a SQL full and transaction log backup.
- Application-consistent quiescing for virtual machines with IDE disks.
- Dynamic disks on the virtual machine.
- Read-only volumes mounted on the SQL virtual machine.
- VMware encrypted virtual machines.
- VMware Fault Tolerant virtual machines.
- RDM storage.

The vProxy appliance performs validation of the environment for these VMware restrictions. If validation fails, the VMware policy with SQL Server application-consistent data protection will not run.

Additional vProxy backup configuration options

The following section provides additional configuration options for vProxy backups.

Configure a backup to support VMware encryption

NetWorker 18.1 supports encrypted virtual machine backups. When configuring a virtual machine backup with VMware encryption, perform the following steps.

Before you begin

Review the known limitations for configuring a backup to support VMware encryption. To backup or restore encrypted virtual machines, ensure that the vProxy appliance is also encrypted, and that the vProxy is manually mapped to the backup policy.

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

Procedure

1. Establish encryption for the virtual machine.

   a. Set up the Key Management Service (KMS).

   b. Create a VM encryption policy.

   c. Assign the encryption policy to the virtual machine(s) you want to encrypt.
2. Encrypt the vProxy appliance.
3. Open the `/opt/emc/vproxy/conf/VixDiskLib.config` file with a Linux text editor.
4. In the file, search for *vixDiskLib.transport.hotadd.NoNFCSession* and change the value to `0`.

   Changing this value to 0 overrides a VMware VDDK bug that inhibits hot-adding an encrypted virtual machine. The *VMware Release Notes* provide more information.
5. Save and close the file.
6. Run the following:

   ```
   systemctl restart vbackupd.service
   ```
7. Set the following additional permissions for the **vCenter user account** role, which is described in the section Create a customized role:

   `Cryptographic operations > Add disk`

   `Cryptographic operations > Direct access`

   `Cryptographic permissions- Register VM`

VMware encryption support limitations

The following limitations apply to backups with VMware encryption enabled.

- As a result of disabling **NoNFCSession**, backup and restore in VMware Cloud on Amazon Web Services (AWS) is not supported. This VMware limitation is addressed in the VDDK update.
- When restoring from an encrypted virtual machine backup, the restored data is unencrypted.
- Restoring virtual machines requires that the target vCenter is configured for the same Key Management Service (KMS) host as the source vCenter.

- Application-consistent quiesce snapshot backups on an encrypted virtual machine will fail back to a file system-consistent snapshot. This process generates an error message in vCenter, which can be ignored. This is a VMware limitation.
- When restoring a virtual machine as a new image, by default, new virtual machines are not encrypted. If you want to apply encryption to the new virtual machine, apply the required storage policy.
  In cases where a boot order other than the default was implemented before the image-level backup was performed, the original boot order is not restored. In this instance, you must select the correct boot device after the restore completes. Alternatively, you can enter the non-default boot order to the VMX file so that the restored virtual machine starts without any reconfiguration. This limitation does not affect virtual machines that use the default boot order.

Configure a backup to support vSAN encryption

NetWorker 18.1 supports all backup and recovery functionality for encrypted vSAN virtual machines, including the restore of an encrypted vSAN virtual machine to a different vCenter that has a non-encrypted datastore.

When performing backups or restores of virtual machines residing on vSAN datastores, it is highly recommended to deploy the vProxy on a vSAN datastore. A vProxy deployed on any one vSAN datastore can be used for backing up virtual machines from other vSAN or non-vSAN datastores (encrypted or non-encrypted) by using hotadd or nbdssl transport modes, as applicable. Both **Capacity** and **Performance** Optimization modes are fully supported for vSAN encrypted virtual machines.

The *VMware Administering VMware VSAN Guide* provides more information about VSAN encryption.

When configuring a virtual machine backup with vSAN encryption, perform the following steps.

Procedure

1. Set the following permissions for the **vCenter user account** role, which is described in the section Create a customized role:

   `Cryptographic operations > Add disk`

   `Cryptographic operations > Direct access`

2. Create the backup group.

   Note

   To back up the vSAN virtual machine, use the vProxy deployed in the vSAN datastore.

Enabling or disabling Changed Block Tracking

The vProxy appliance uses changed block tracking (CBT) automatically upon the first virtual machine backup so that only changed disk areas on the virtual machine get backed up. Some virtual machines, however, do not support CBT and you may be required to disable CBT for those virtual machines.

A vCenter administrator can control the application of CBT by using the custom field **EMC vProxy Disable CBT**. You can set this custom field to **true** to disable CBT, or **false** to enable CBT. If you do not set this field for a virtual machine, or the field is not present, CBT is enabled by default for that virtual machine.

To set CBT for virtual machines, perform the following:

1. Log into the **vSphere Client** (vSphere versions 6 and earlier) or **vSphere Web Client** (vSphere versions 6.5 and later) as an administrator.
2. Click on a virtual machine in the vCenter tree, and then click the **Summary** tab.
3. Edit the virtual machine attributes:
    - In vSphere versions 6.x and earlier, click **Edit** in the **Annotation** box.
    - In vSphere versions 6.5 and later, click **Edit** under **Custom Attributes**.
4. Locate the **EMC vProxy Disable CBT** field, or create a string for **EMC vProxy Disable CBT**. The string must match the field name exactly and is case-sensitive.
5. Set the value to **true** to disable CBT on the virtual machine, or to **false** (or leave the field blank) to enable CBT on the virtual machine. Setting or resetting the field for one virtual machine does not affect the other virtual machines in the vCenter.
6. Refresh **VMware View** in the NMC **NetWorker Administration** window.

Fixing CBT if corrupted on virtual machine

If CBT becomes corrupted on the virtual machine, warnings similar to the following appear in the backup logs:

```
WARN: Change block tracking needs to be reset.
WARN: Change Block Tracking could not be reset, causing full backup:
Second attempt failed.
NOTICE: Change block tracking cannot be reset by proxy. Please
remediate VM.
```

If these messages appear, you can use PowerCLI commands to disable and then enable CBT without powering off the virtual machines as described in the VMware knowledgebase article at https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1031873, or perform the following steps to clean up CBT:

1. Power down the virtual machine.
2. Remove CBT flags.
3. Delete CTK files from the datastore.
4. Power ON the virtual machine.

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

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

Create vCenter user account

Procedure

1. From a web browser, type the following:

    ```
    https://<IP_address_vCenter_Server>:5480
    ```

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

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

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

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

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

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

Create a customized role

Procedure

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

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

Table 9 Minimum required vCenter user account privileges

Setting	vCenter 5.5 and later required privileges
Alarms	• Create alarm • Modify alarm
Datastore	• Allocate space • Browse datastore • Configure datastore

Table 9 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 and later required privileges
	• Low level file operations • Move datastore • Remove datastore • Remove file • Rename datastore
Extension	• Register extension • Unregister extension • Update extension
Folder	• Create folder
Global	• Cancel task • Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Settings • Set custom attribute
Host	• Configuration > Storage partition configuration **Note** Not applicable to vCenter 5.5.
Network	• Assign network • Configure
Resource	• Assign virtual machine to resource pool • Migrate powered off virtual machine • Migrate powered on virtual machine
Sessions	• Validate session
Tasks	• Create task • Update task
vApp	• Export • Import • vApp application configuration

Table 9 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 and later required privileges
Virtual Machine	
Configuration	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Configure managed by • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Set annotation • Settings • Swapfile placement • Upgrade virtual machine compatibility
Guest Operations	• Guest operation modifications • Guest operation program execution • Guest operation queries
Interactions	• Configure CD media • Console interaction • Device Connection • Guest operating system management by VIX API • Power off • Power on • Reset • VMware Tools install

Table 9 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 and later required privileges
Inventory	• Create new • Register • Remove • Unregister
Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Mark as Template
Snapshot Management	• Create snapshot • Remove Snapshot • Revert to snapshot

vSphere Client user accounts

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

Note

In high-security environments, you can restrict the vCenter user account permissions required to configure and administer the vProxy appliance. Table 9 on page 60 provides the account permission categories.

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

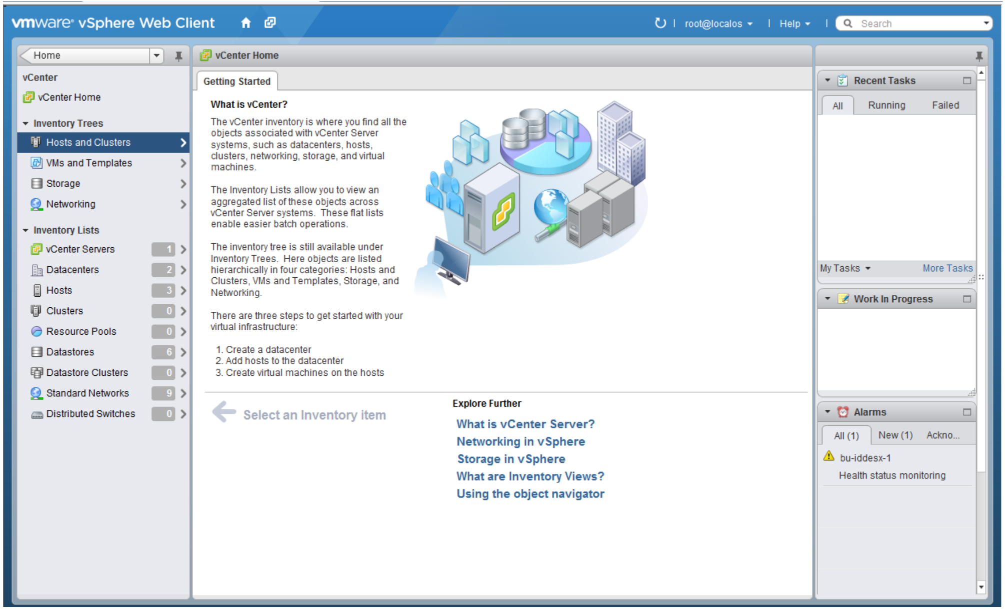
Procedure

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

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

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

Figure 6 Hosts and Clusters in the vSphere Web Client



What is vCenter?

The vCenter inventory is where you find all the objects associated with vCenter Server systems, such as datacenters, hosts, clusters, networking, storage, and virtual machines.

The Inventory Lists allow you to view an aggregated list of these objects across vCenter Server systems. These flat lists enable easier batch operations.

The inventory tree is still available under Inventory Trees. Here objects are listed hierarchically in four categories: Hosts and Clusters, VMs and Templates, Storage, and Networking.

There are three steps to get started with your virtual infrastructure:

1. Create a datacenter
2. Add hosts to the datacenter
3. Create virtual machines on the hosts

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

Note

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

---

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

   The **Add Permission** dialog box opens.

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

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

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

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

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

Adding a NIC for VMXNET 3 on the vProxy appliance

The following section describes how to set up a virtual network interface card (vNIC) of type VMXNET 3 for the vProxy appliance. You can also use this procedure to swap a NIC to VMXNET 3 on the vProxy appliance.

Before you begin

This procedure is required for custom setup using dual NIC, but is otherwise optional for vProxy appliances unless you are swapping a NIC.

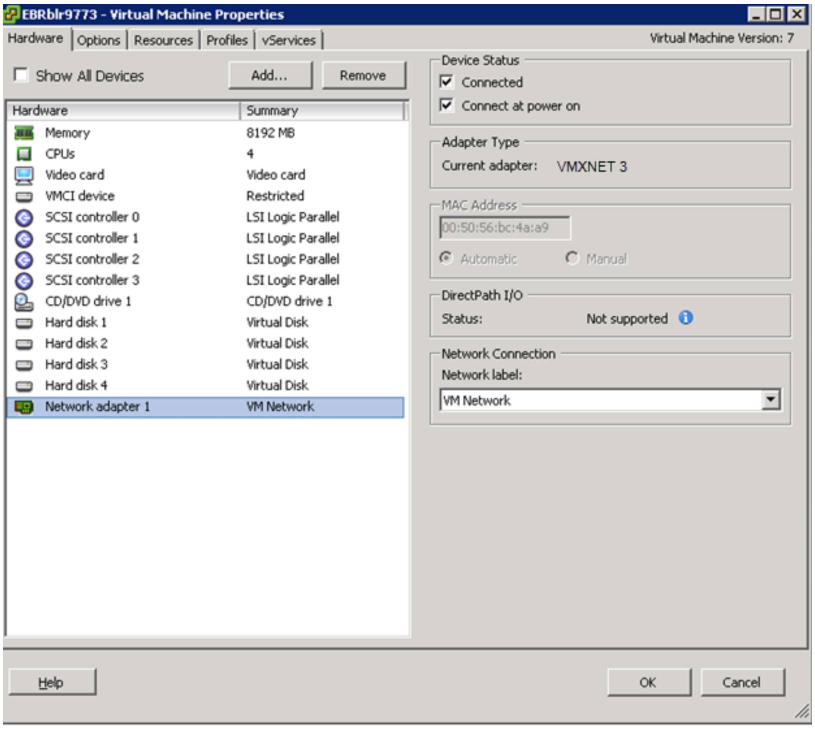
If setting up dual NIC, review the section Dual vNIC setup and configuration requirements, and then use the following steps to configure the appliance before the steps outlined in the section Configuring the vProxy in NetWorker.

Procedure

1. Log in to the vProxy appliance console in the **vSphere Client**.
2. Right-click the vProxy appliance and select **Power** > **Shutdown Guest**.
3. Add the second NIC to the vProxy appliance:

   a. Right click the vProxy appliance, and then select **Edit Settings**. The **Virtual Machine Properties** window appears.

   Figure 7 Swap network for NICs in the Virtual Machine Properties window



EBRblr9773 - Virtual Machine Properties

Hardware | Options | Resources | Profiles | vServices — Virtual Machine Version: 7

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
SCSI controller 1	LSI Logic Parallel
SCSI controller 2	LSI Logic Parallel
SCSI controller 3	LSI Logic Parallel
CD/DVD drive 1	CD/DVD drive 1
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Hard disk 4	Virtual Disk
Network adapter 1	VM Network

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: VMXNET 3

MAC Address
00:50:56:bc:4a:a9
● Automatic ○ Manual

DirectPath I/O
Status: Not supported

Network Connection
Network label: VM Network

   b. (Optional, to be performed when swapping a NIC) In the **Hardware** tab, select **Network adapter 1** in the list, and then click **Remove.**

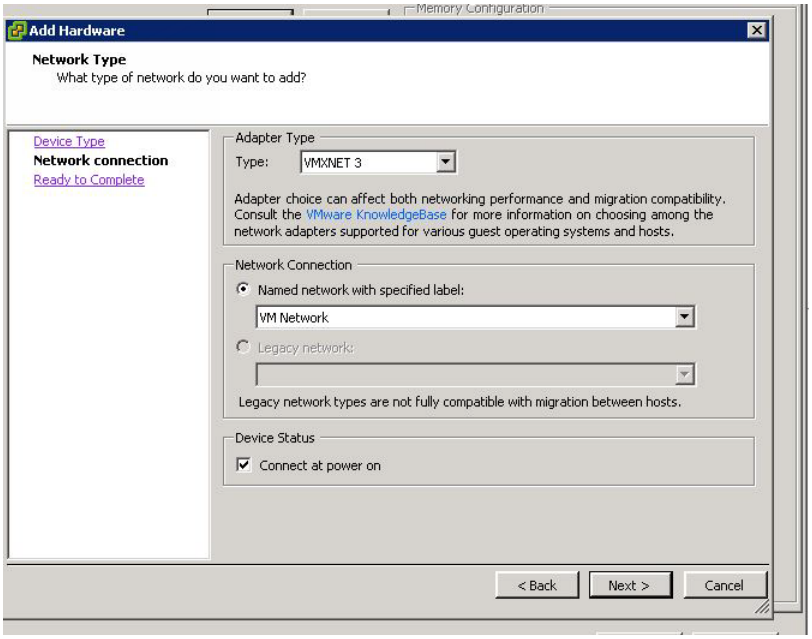
   c. In the **Hardware** tab, click **Add.**

      The **Add Hardware** wizard opens.

   d. In the **Device Type** page, select **Ethernet Adapter** and click **Next**.

e. In the **NetWork Type** page, change the value in the **Adapter Type** field to **VMXNET 3**, and assign this vNIC to the appropriate virtual machine port group. Select the **Connect at power on** checkbox if it is not selected.

Figure 8 Change Adapter Type



Network Type

What type of network do you want to add?

Adapter Type

Type: VMXNET 3

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

Network Connection

● Named network with specified label: VM Network

○ Legacy network:

Legacy network types are not fully compatible with migration between hosts.

Device Status

☑ Connect at power on

f. Select the appropriate virtual machine port group for the production network/VLAN, and then click **Next**.

g. In the **Ready to Complete** page, verify the information and then click **Finish**.

4. Right click the vProxy appliance and select **Power > Power On**.

5. Configure the second NIC on the vProxy appliance:

a. After you power on the vProxy appliance, log in as root to the vProxy appliance Console by using the **vSphere Client**.

b. Type `yast2` to invoke the YaST configuration tool.

c. Select **Network Devices** and press **Enter**.

The **Network Devices** dialog appears.

d. Select **Network Settings** and press **Enter**.

The **Network Settings** dialog appears.

e. In the **Overview** tab, select the Second Ethernet Adapter labeled **eth1**.

f. Use the tab key to select **Edit** and press **Enter**.

g. From the Network Card Setup, use the tab key to access **Statically assigned IP Address** and select using the spacebar. Use the tab key to select **IP Address** and enter the IP Address, the Subnet Mask, and the host name of the vProxy appliance. Ensure that these settings come from the production network/VLAN.

h. Use the tab key to select **Edit**, and then press **Enter**.

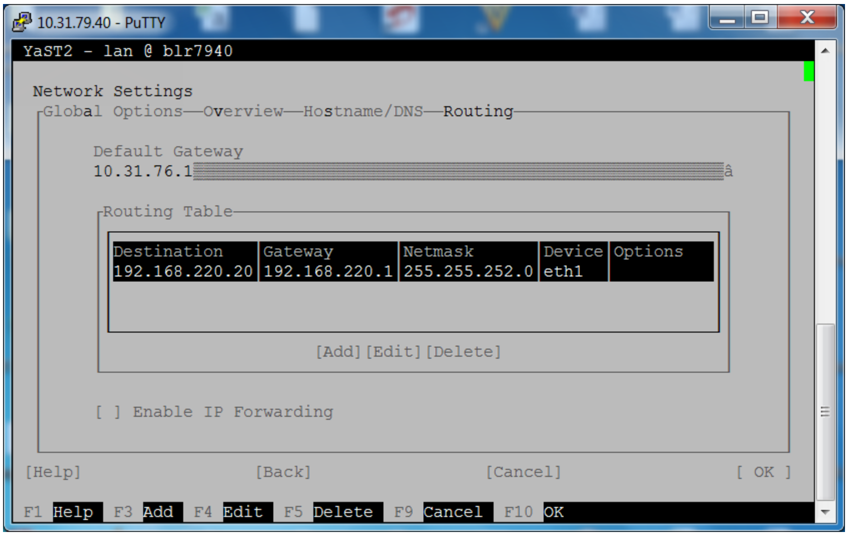
i. (Optional when setting up second NIC) From **Network Settings**, use the tab key to select **Overview**. Use the right-arrow key to select **Hostname/DNS**. Use the tab key to select and then specify the following fields:

- Host name
- Domain name for the production network
- Policy for DNS configuration
- Name Server 1 for production network
- Name Server 2 for backup network
- Domain Search for both production and backup network.

When setting up a second NIC, carefully review the following sections including operating system routes since you may need to be define these routes as custom routes.

j. From **Network Settings**, use the tab key to select **Hostname/DNS**.Use the right-arrow key to select **Routing**, and update the routing table by setting the Default Gateway to the gateway/address for the backup network, if not already set.

Figure 9 Routing table with backup network gateway



```
YaST2 - lan @ blr7940

 Network Settings
┌Global Options──Overview──Hostname/DNS──Routing──────────────────────────┐
│                                                                          │
│     Default Gateway                                                      │
│     10.31.76.1                                                           │
│                                                                          │
│    ┌Routing Table──────────────────────────────────────────────────┐     │
│    │ Destination    Gateway       Netmask       Device Options     │     │
│    │ 192.168.220.20 192.168.220.1 255.255.252.0 eth1               │     │
│    │                                                               │     │
│    │                    [Add] [Edit] [Delete]                      │     │
│    └───────────────────────────────────────────────────────────────┘     │
│                                                                          │
│     [ ] Enable IP Forwarding                                             │
└──────────────────────────────────────────────────────────────────────────┘
[Help]                  [Back]                  [Cancel]                [ OK ]
F1 Help  F3 Add  F4 Edit  F5 Delete  F9 Cancel  F10 OK
```

k. Use the tab key to select **Add to the Routing table**.

l. Add the following entry to the Routing table:

- Destination: IP address for the vCenter Server
- Device: eth1
- Gateway: gateway/address for your production network
- Netmask: Same as the netmask for eth1 entered earlier

m. Use the tab key to select **OK**, and then press **Enter**.

n. Use the tab key to select **Quit**, and then press **Enter**.

6. Restart the vProxy appliance.

7. Login to the vProxy appliance and confirm that you can ping the vCenter production network IP.

   You can now proceed with registering the vProxy appliance with the NetWorker server on the backup subnet/VLAN. This will require selecting the vCenter server running on the production network in the drop-down.

Dual vNIC setup and configuration requirements

This section outlines NetWorker support for enabling the vProxy appliance to support dual vNIC. Enabling dual vNIC on the vProxy appliance can provide the following benefits:

- You can separate the backup data traffic going to the back-end from the production network so that backups do not negatively impact performance in your environment.
- You can use a separate private or isolated physical network infrastructure for your backup network and send the backup data in this isolated network unencrypted, leading to performance gains.
- You can dedicate a NIC to backup traffic so that you do not impact production performance if using an older host with a slower physical NIC.

Along with the configuration required when downloading and deploying the vProxy appliance, the vProxy appliance requires the following for dual vNIC setup. Review these items before performing the steps in the section Adding a NIC for VMXNET 3 on the vProxy appliance:

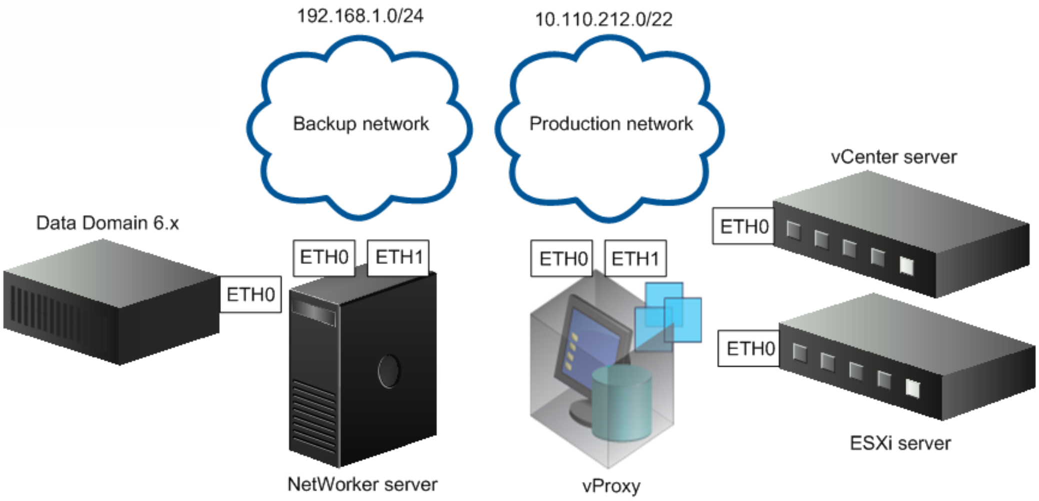
- During deployment of the vProxy appliance, ensure that you assign an IP address from the backup subnet/VLAN that follows the normal rules for a proxy appliance (for example, has a DNS server, associated PTR on that DNS server, and so on).
- Before registering the vProxy appliance with the NetWorker server on the backup subnet/VLAN, add static routes for the production network/VLAN. This is required for communicating with the vCenter server.
- Power on the vProxy appliance, and when you log in, ensure that you can perform nslookup for the backup subnet FQDN of the vProxy and the NetWorker server.
- In order to use Instant Access restore, emergency restore, and file-level restore with dual NIC configured, the destination ESXi requires a VMkernel port connected to the backup subnet/VLAN. You can configure the vmkernel port on a separate VLAN by using the steps in the following knowledgebase article: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2001426.
- Configure the two vNICs with separate and unique subnets in order to facilitate the direction of network traffic. All backup traffic will flow out of the first vNIC. All production traffic (which includes vCenter Server traffic, VMTools requests used by file-level restore, and so on) will flow out of the second vNIC. Further details for vProxy appliance NIC connectivity are provided in the bullets below.
- Proxies with multiple NICs rely on the operating system routes and require reliable bi-directional communications with the respective subnets on which the NICs are configured with Data Domain systems.

  Note

  You may be required to define operating system routes as custom routes.

- Set up the NetWorker server with dual network adapters, with eth0 connected to the backup subnet/VLAN and eth1 connected to the production network/VLAN.

Figure 10 Backup and production traffic with dual network adapters



You can use a non-routable private address space for the subnet used for the backup traffic/data, providing that:

- All devices/vNICs using a private IP address exist on the same physical switch, and
- There is a DNS server on the non-routed private network so that the proxies can perform a reverse lookup for its host name.

Note

A private address space-based network is an optional example and not a requirement.

Verify vNIC connectivity

You can verify that the vNIC is associated to the correct network by running a test using ping or traceroute against the IP of the NetWorker server and/or vCenter and other required components. If the IP is not reachable, you may need to swap the network for NICs.

1. Right-click the vProxy appliance and select **Edit Settings**.
2. in the Hardware tab of the **Virtual Machine Properties** window, select **Network adaptor** and **Network connection** on the right of the screen.
3. In the **Network connection** page, select the correct network label.
4. Click **OK** to complete the configuration change.

For systems with swapped NICs or dual vNIC configurations, you can use the `proxycp.jar` command line utility on the vProxy appliance to test connectivity.

To download the `proxycp.jar` command line utility:

1. Log into the vProxy appliance by using the **vSphere Client** or a putty session.
2. If required, run **`sudo su -`** to switch to the root user.
3. In a command prompt, use which curl. For example:

```
blrv071b219:~ # which curl
/usr/bin/curl
blrv071b219:~ #
```

4. Run the following command:

   ```
   curl -O ftp://valid_ftp_needed/software/scripts/proxycp.jar
   ```

   For sites where direct download using `curl` is unavailable, use `WinSCP` to transfer the script to the VMware Backup appliance or external proxy.

5. Change the permissions on `proxycp.jar`:

   ```
   chmod 755 /usr/local/avamar/bin/proxycp.jar
   ```

After downloading `proxycp.jar`, you can use the following command tools to test connectivity:

- `proxycp.jar --vctest --dryrun`—Tests connectivity to vCenter and returns many details of the vCenter.
- `proxycp.jar --testconn`—connects to vCenter to perform tests at set intervals, similar to "ping tests".
- `proxycp.jar --testwebservice`—Tests connectivity to the Avamar MC SDK.
- `proxycp.jar --portcheck [--timeout <Num> ]` - Tests proxy connectivity to vCenter by discovering all nodes and hosts in the environment and then checking connectivity of each proxy to every single ESX host. Also checks for Data Domain in the environment and checks connectivity from the proxy. If running in a slower environment you can change the timeout value from the default of 10 seconds to 60 seconds.

Dual NIC configuration, and particularly operating system routes, can be very complex and require careful planning by the administrator. When complete the setup and verified working functionality of the configuration, make note of the configuration details including NIC Type, IPs, operating system routes and any other custom settings since these may be required if you need to recreate the OVA for operations such as proxy upgrades and storage failures.

Migrating policies from VMware Backup appliance to vProxy appliance

New installations of NetWorker 18.1 use the NetWorker VMware Protection solution with the vProxy appliance. When you upgrade from a NetWorker 9.0.x and earlier release, you can continue to use the VMware Backup appliance, migrate to use only the vProxy appliance, or use a combination of the VMware Backup appliance and vProxy appliance. If you choose to use the vProxy appliance only, workflow migration is required to convert existing VMware Backup appliance policies to vProxy appliance policies.

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

Note

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

Co-existence of the VMware Backup appliance and vProxy appliance

After upgrading to a NetWorker 9.1.x or 9.2 release and migrating from the VMware Backup appliance to the vProxy appliance, you might still require the VMware Backup appliance. For example, if you want to recover from a backup performed with the VMware Backup appliance that has not expired, you must keep the VMware Backup appliance and at least one of the VMware Backup appliance's external proxies.

If you plan to continue using the VMware Backup appliance, make note of the following information:

- NetWorker 9.1 and later releases require the same version of the VMware Backup appliance as NetWorker 9.0.1, which is 1.5.1.7. If you are upgrading from NetWorker 9.0.1, you do not need to upgrade the VMware Backup appliance version. If you are upgrading from an earlier release, for example, from NetWorker 8.2.3 with version 1.1.3.7, you will need to upgrade the VMware Backup appliance version to 1.5.1.7 after upgrading the NetWorker server to 9.1 and later.
- Backups run with VMware Backup appliance policies cannot be recovered using the vProxy appliance. These backups must be recovered with the VMware Backup appliance.
- You cannot create new policies with the VMware Backup appliance. You can only run or edit existing policies.
- You cannot run policies with VMware Backup appliance GSAN internal storage.
- Different plug-ins are available in the vSphere Web Client for VMware Backup appliance policies and vProxy appliance policies. For the VMware Backup appliance, this is the **EMC Backup and Recovery** plug-in. For the vProxy appliance, this is the **VM Backup and Recovery** plug-in. The two plug-ins can co-exist on the same vCenter.

It is recommended to migrate all VMware Backup appliance policies to the vProxy appliance. Note that you can still use the **EMC Backup and Recovery** plug-in within the **vSphere Web Client** for operations that are related to the backup of still-to-be migrated VMware Backup appliance policies, or for image-level recovery of any backups performed with the VMware Backup appliance. However, after a policy has been migrated to the vProxy appliance, it is no longer accessible from the VMware Backup appliance. You must manage all such migrated policies as native NetWorker vProxy policies from NMC, or by using the **VM Backup and Recovery** plug-in within the **vSphere Web Client** for NetWorker 9.1 and later vProxy-based policies.

Additionally, for file-level recovery in the **EMC Data Protection Restore Client**, you must use vProxy appliance backups after migrating. Recovery from older backups that were created using the VMware Backup appliance can still be performed using the **EMC Backup and Recovery** plug-in, but you must retain at least one external proxy node.

The following table provides a list of supported and unsupported VMware Backup appliance operations in an upgraded NetWorker 9.1 and later environment.

Table 10 Supported and unsupported VMware Backup appliance operations in a NetWorker 9.1 and later environment

Supported operations	**Unsupported operations**
• Scheduled backups of VMware Backup appliance policies that were created before upgrading to NetWorker 9.1 or 9.2	• Create new VMware Backup appliance protection policies

Table 10 Supported and unsupported VMware Backup appliance operations in a NetWorker 9.1 and later environment

Supported operations	Unsupported operations
• On demand (adhoc) backups of virtual machines protected by a VMware Backup appliance from NMC's **Protection** window • On demand (adhoc) backups of virtual machines protected by a VMware Backup appliance from the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • Edit existing VMware Backup appliance protection policies (for example, to modify an existing action to point to a different VMware Backup appliance) • Modify the VMware Backup appliance protection group to add virtual machines to an existing group or remove virtual machines from an existing group • Image-level recovery (to a new virtual machine, revert, VMDK-level and instant access) from VMware Backup appliance backups run before or after the upgrade by using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • File-level recovery from VMware Backup appliance backups run before or after the upgrade by using the **Dell EMC Data Protection Restore Client** (VBA) • Emergency restore from VMware Backup appliance backups run before or after the upgrade • Create checkpoints after the upgrade by running an integrity check using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • Rollback to a desired checkpoint (to checkpoints taken after the upgrade) • Deploy and manage VMware Backup appliance external proxies after the upgrade by selecting a desired VMware Backup appliance • Resurrect VMware Backup appliance backups run before or after the upgrade by using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • Disaster recovery of VMware Backup appliance in case of a VMware Backup appliance failure • Restore to the same vCenter with a newly deployed VMware Backup appliance by using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • Recovery of VMware Backup appliance backups from a secondary site (restore to a different vCenter) with a newly deployed VMware Backup appliance by using the	• Image-level recovery of VMware Backup appliance backups by using the **VM Backup and Recovery** plug-in in the **vSphere Web Client** • Image-level recovery of VMware Backup appliance backups by using the NMC **Recovery** wizard • File-level recovery from VMware Backup appliance backups by using the NMC **Recovery** wizard • File-level recovery from VMware Backup appliance backups by using the **Dell EMC Data Protection Restore Client** (vProxy) • Manage VMware Backup appliance policies by using the **VM Backup and Recovery** plug-in in the **vSphere Web Client** • Manage vProxy policies by using the **VM Backup and Recovery** plug-in in the **vSphere Web Client**

Table 10 Supported and unsupported VMware Backup appliance operations in a NetWorker 9.1 and later environment

Supported operations	Unsupported operations
EMC Backup and Recovery plug-in in the **vSphere Web Client**	

Migration pre-requisites

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

These requirements include verification of the following items:

- The Data Domain OS (DD-OS) is DDOS version 5.7, 6.0.0.30, 6.0.1-10, or 6.1. Note that use of the DD Retention Lock feature on vProxy backup and clone actions requires DDOS 6.1.
- The NetWorker server and storage node version is NetWorker 18.1.
- The vProxy is available on the vCenter server and is version 2.1.0.17 for NetWorker 18.1.
- The vCenter server is a minimum of version 5.5.

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.

Additionally, if you used IPv6 only or dual stack (IPv4 and IPv6) for the VMware Backup appliance and are migrating to use the vProxy appliance, ensure that you switch to IPv4 only. The vProxy appliance does not support either IPv6 or dual stack (IPv4 and IPv6), and so the migration from the VMware Backup appliance to the vProxy appliance will not work with these configurations. If you previously used IPv4 only, no configuration change is necessary.

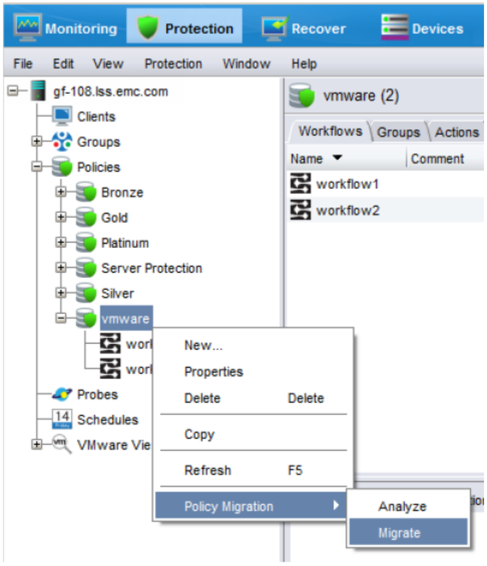
Policy migration to vProxy by using NMC

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

Procedure

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

Figure 11 Migrating a VMware Backup appliance policy to vProxy in NMC



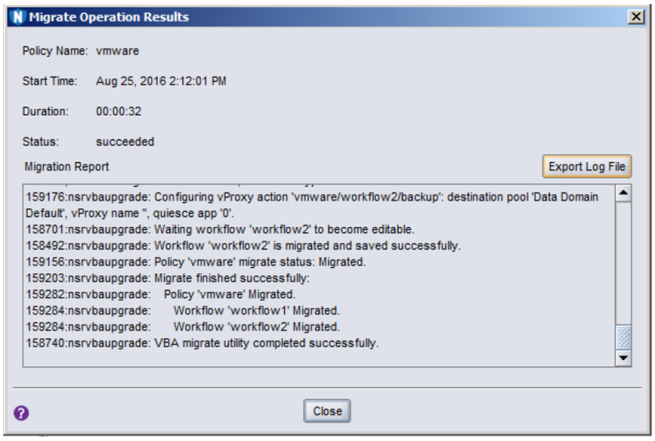
Note

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

Results

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

Figure 12 Migrate Operation Results dialog



Policy Name: vmware

Start Time: Aug 25, 2016 2:12:01 PM

Duration: 00:00:32

Status: succeeded

Migration Report

```
159176:nsrvbaupgrade: Configuring vProxy action 'vmware/workflow2/backup': destination pool 'Data Domain
Default', vProxy name '', quiesce app '0'.
158701:nsrvbaupgrade: Waiting workflow 'workflow2' to become editable.
158492:nsrvbaupgrade: Workflow 'workflow2' is migrated and saved successfully.
159156:nsrvbaupgrade: Policy 'vmware' migrate status: Migrated.
159203:nsrvbaupgrade: Migrate finished successfully:
159282:nsrvbaupgrade:   Policy 'vmware' Migrated.
159284:nsrvbaupgrade:     Workflow 'workflow1' Migrated.
159284:nsrvbaupgrade:     Workflow 'workflow2' Migrated.
158740:nsrvbaupgrade: VBA migrate utility completed successfully.
```

Policy migration to vProxy by using the command line

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

Before you begin

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

Procedure

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

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

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

Renaming a NetWorker 9.1 and later server with legacy VMware Backup appliance

When a NetWorker 8.2.x release is upgraded to NetWorker 9.1 and 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 specified in the section Disaster Recovery.

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.

Updating the vProxy appliance

When you upgrade the NetWorker server to NetWorker 18.1, you must also upgrade the vProxy appliance to the latest version for NetWorker 18.1. There is no procedure to automatically update the vProxy appliance version. To update the vProxy appliance, you must delete the currently deployed appliance from NMC and vCenter, and then deploy and register the new vProxy appliance on the same vCenter.

Procedure

1. Delete the vProxy appliance from NMC, as described in the section Deleting the vProxy host.
2. Log in to the vCenter server by using the **vSphere Client**.
3. Remove the vProxy appliance from the vCenter by powering off the appliance and then deleting the vProxy virtual machine from the disk.
4. Deploy the new vProxy appliance and configure the network settings, as described in the section "Deploy the vProxy appliance".

   Note

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

5. Add the newly deployed vProxy appliance to the NetWorker server and configure the appliance, as described in the section Configuring the vProxy in NetWorker.
6. After vProxy appliance registration completes, verify that a valid certificate appears in the NMC **NetWorker Administration** window by enabling diagnostic mode and adding the column **VM vProxy certificate**.

Deleting the vProxy host

Perform the following steps to delete the resource for the vProxy appliance in NetWorker.

Procedure

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. On the taskbar, click the **Enterprise** icon.
3. In the navigation tree, highlight a host:

   a. Right-click **NetWorker**.

   b. Select **Launch Application**. The **NetWorker Administration** window appears.

4. On the taskbar, click the **Devices** button.
5. In the expanded left navigation pane, select **VMware Proxies**,
6. In the right pane, right-click on the VMware proxy, and then select **Delete**.
7. When prompted, click **Yes** to delete the VMware proxy.

After you finish

When you delete a vProxy resource after failed registration, a warning appears to manually unregister the vProxy appliance.

Redeploying a vProxy

The procedure to redeploy a vProxy appliance requires you to perform the same steps that you performed when you deployed the original vProxy host.

After you deploy the vProxy appliance, perform the following steps:

Procedure

1. Delete the vProxy by performing the steps in the section "Deleting the vProxy host".
2. Deploy the vProxy by performing the procedures in the section "Deploy the vProxy appliance".
3. Configure the vProxy using the steps in the section "Configuring the vProxy in NetWorker".

Un-registering and re-registering a vProxy after removal

When registration fails for a vProxy appliance that was previously registered to a NetWorker server but was removed due to a disaster recovery, or because the previous removal did not complete successfully, you must un-register the vProxy appliance manually before you can re-register the appliance.

Procedure

1. Start the `nsradmin` utility.
2. In Visual mode, select the **NSR VMWare proxy** resource.
3. In the **Options** menu, select the **Hidden item** view.
4. Press the ESC key to return to the **NSR VMWare proxy** resource view, and then select **Edit** from the **Options** menu.
5. Navigate to operation property and select **Unregister**.
6. Press the ESC key and then confirm that you want to save the changes to the resource.
7. Select **Edit** from the **Options** menu and repeat step 5, only this time selecting **Register**.
8. Press the ESC key and then confirm that you want to save the changes to the resource.

Results

The vProxy registration starts. You can now exit the `nsradmin` utility.

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.

Procedure

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

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

   The default password for the root account is **changeme**.

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.

CHAPTER 3

Protecting virtual machines

This chapter contains the following topics:

Preparing the NetWorker data zone

Review the following requirements.

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

Configure the Data Domain System

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

Procedure

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

   Note

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

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

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

Creating VMware data protection policies in NMC for the vProxy appliance

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:

- Creating a policy.
- Creating a workflow.
- Creating a VMware protection group.
- Creating an action.

Overview of data protection policies

Data protection policy is a concept that provides you with the ability to design a data protection solution for the 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.

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

Policies
Policies provide you with the ability to develop 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
Workflows define the start time for a series of actions, the frequency in which the actions run, the order of actions in a sequence, and the protection group to which the workflow applies.

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

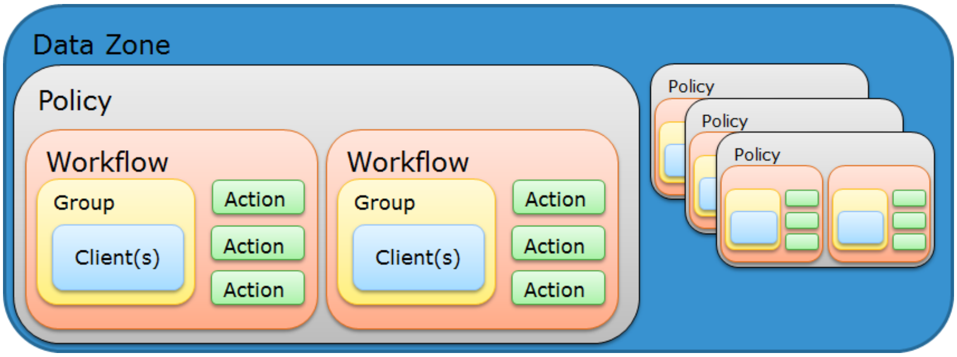
Actions are the key resources in a workflow for a data protection policy and define a specific task, for example, a backup, clone, or snapshot. NetWorker uses a work list to define the task. A work list is composed of one or several work items. Work items include client resources, virtual machines, save sets, or tags. You can chain multiple actions together to occur sequentially or concurrently in a workflow. All chained actions use the same work list.

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

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 13 Data Protection Policy



Default data protection policies

NetWorker provides you with preconfigured data protection policies that you can use immediately to protect the environment, modify to suit the environment, or use an example to create resources and configurations. To use these preconfigured data protection policies, you must add clients to the appropriate group resource.

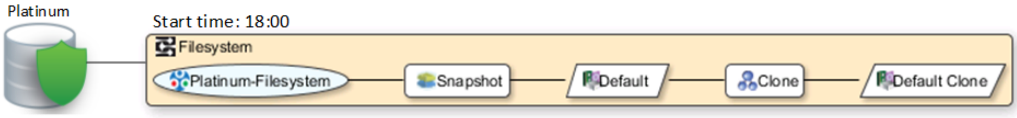
Note

NetWorker also includes a preconfigured 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 14 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

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.

Procedure

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

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

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

   Note

   This name cannot contain spaces or special characters such as + or %. After you create a policy, the **Name** attribute is read-only.
4. In the **Comment** box, type a description for the policy.
5. From the **Send Notifications** list, select whether to send notifications for the policy:
   - To avoid sending notifications, select **Never**.
   - To send notifications with information about each successful and failed workflow and action after all the actions in the policy complete, select **On Completion**.
   - To send a notification with information about each failed workflow and action after all the actions in the policy complete, select **On Failure**.
6. In the **Send notification** attribute, when you select the **On Completion** option or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file or you can send an email notification.

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

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

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

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

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

  ```
  mail -s subject recipient
  ```

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

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

- On Windows, to send a notification email, type the following command:

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

  where:

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

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

After you finish

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

Creating a workflow

The policy workflow defines a list of actions to perform sequentially or concurrently, a schedule window during which the workflow can run, and the client resource or save set 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.

Create a workflow in a new policy

Procedure

1. In the **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. This name cannot contain spaces or special characters such as + or %.

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

   The maximum number of allowed characters for the **Comment** field is 128.

6. From the **Send Notifications** list, select how to send notifications for the workflow:

   - To use the notification configuration that is defined in the policy resource to specify when to send a notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after the workflow completes all the actions, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after the workflow completes all the actions, select **On Failure**.

7. In the **Send notification** attribute, when you select the **On Completion** option or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file or you can send an email notification.

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

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

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

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

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

     ```
     mail -s subject recipient
     ```

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

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

   - On Windows, type the following command:

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

     where:

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

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

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

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

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

      The default value is 9:00 PM.

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

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

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

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

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

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

After you finish

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

Create a workflow in an existing policy

A policy can contain one or more unique workflows.

Before you begin

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

Procedure

1. In the **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. This name cannot contain spaces or special characters such as + or %.
7. In the **Comment** box, type a description for the workflow.

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

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

   Use the default mailer program on Linux to send email messages or the `smtpmail` application on Windows:
   - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

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

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

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

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

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

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

       The default value is 9:00 PM.

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

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

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

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

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

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

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

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

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

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

Create or edit a VMware group

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

Before you begin

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

Procedure

1. In the **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. This name cannot contain spaces or special characters such as + or %.

   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 xxx 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 xxx 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

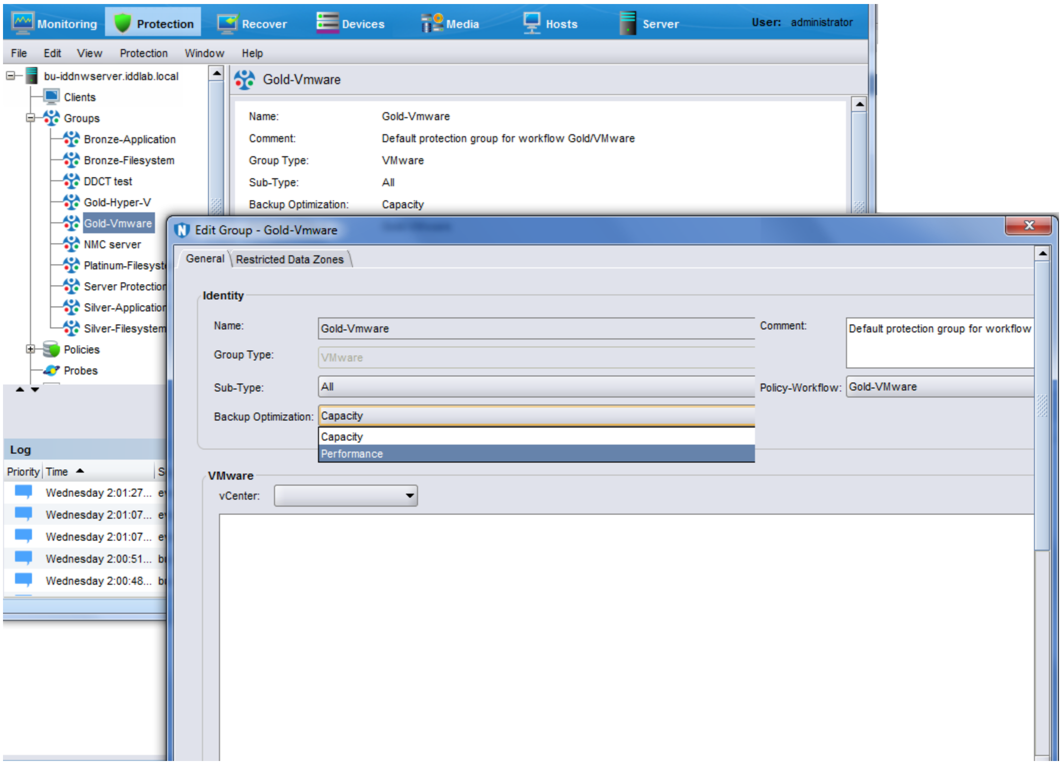
NetWorker supports two types of backup optimization modes for vProxy backup to Data Domain systems—**Optimized for Capacity**, and **Optimized for Performance**. You can apply the optimization mode to vProxy protection groups during backup.

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 15 Changing the Backup Optimization mode in the vProxy protection group



User: administrator

Gold-Vmware

Name: Gold-Vmware
Comment: Default protection group for workflow Gold/VMware
Group Type: VMware
Sub-Type: All
Backup Optimization: Capacity

Wednesday 2:01:27...
Wednesday 2:01:07...
Wednesday 2:01:07...
Wednesday 2:00:51...
Wednesday 2:00:48...

Edit Group - Gold-Vmware

Name: Gold-Vmware
Comment: Default protection group for workflow
Group Type: VMware
Sub-Type: All
Policy-Workflow: Gold-VMware
Backup Optimization: Capacity
vCenter:

Software and storage requirements for Optimized for Performance mode

Using **Optimized for Performance** requires DDOS version 5.7.x or version 6.0.0.30 and later. If using a DDOS 5.7 version, DDOS 5.7.1 or later is recommended for this mode. When you request **Optimized for Performance** mode but it is not supported by the DDOS version, the backup automatically falls back to using **Optimized for Capacity**. 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 (DDOS version 5.7 and later).

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.

VMware actions

Actions are the key resources in a workflow for a data protection policy. 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.

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 (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.

Creating 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 vProxy. The *NetWorker Administration Guide* provides information about other action types.

Before you begin

Create the policy and workflow that contain the action.

Procedure

1. In the 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.
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 occurs 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 or monthly schedule for the action:
   - To specify a schedule for each day of the week, select **Weekly by day**.
   - To specify a schedule for each day of the month, select **Monthly by day**.
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 11 Schedule icons

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

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

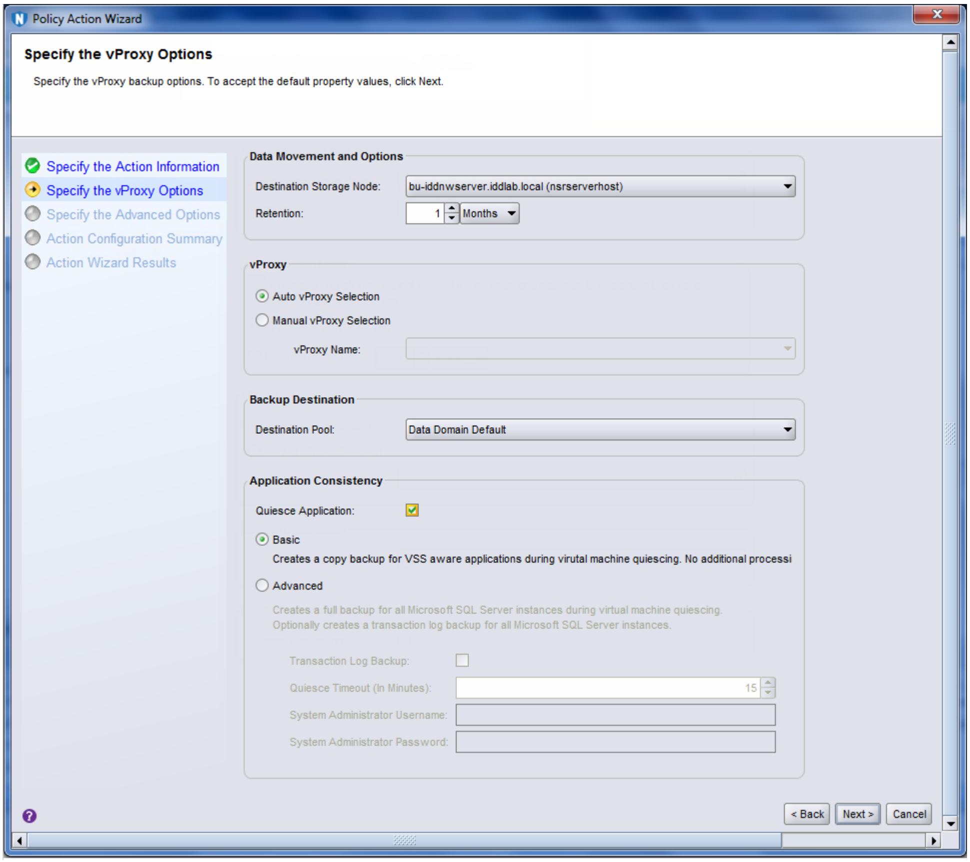
Note

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

11. Click **Next**.

    The **Specify vProxy Options** page appears.

Figure 16 Specify vProxy Options page



Policy Action Wizard

Specify the vProxy Options

Specify the vProxy backup options. To accept the default property values, click Next.

Specify the Action Information
Specify the vProxy Options
Specify the Advanced Options
Action Configuration Summary
Action Wizard Results

Data Movement and Options

Destination Storage Node: bu-iddnwserver.iddlab.local (nsrserverhost)

Retention: 1 Months

vProxy

● Auto vProxy Selection

○ Manual vProxy Selection

vProxy Name:

Backup Destination

Destination Pool: Data Domain Default

Application Consistency

Quiesce Application: ☑

● Basic

Creates a copy backup for VSS aware applications during virutal machine quiescing. No additional processi

○ Advanced

Creates a full backup for all Microsoft SQL Server instances during virtual machine quiescing.
Optionally creates a transaction log backup for all Microsoft SQL Server instances.

Transaction Log Backup: □

Quiesce Timeout (In Minutes): 15

System Administrator Username:

System Administrator Password:

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

    Note

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

    ---

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

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

14. 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.

15. 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.

16. In the **vProxy** section, select one of the following options:

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

17. 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.

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

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

    When you select the option, the following fields display:

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

      Note

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

    - **Quiesce Timeout**—Specify the amount of time, in minutes, to wait for the quiesce operation on the virtual machine to time out before failing. If not selected, the backup action will proceed even if quiescing was not performed, unless a validation problem occurs. If an application-consistent backup cannot complete due to a problem with validation, the backup action will fail even if this checkbox is not selected.
    - **System Administrator Username and Password**—Specify the virtual machine credentials for a user with administrative privileges. All virtual machines in the workflow should use the same System Administrator username/password.

Note

Selecting the **Advanced** option will apply application-consistent processing for all virtual machines within the parent workflow. When selecting this option, ensure that the policy's workflow and client groups are provisioned specifically for virtual machines that require advanced application-consistent protection. NetWorker will always attempt to perform advanced application processing for virtual machines in a workflow that contains a backup action with advanced application processing enabled. The section Creating an action for application-consistent data protection provides more information.

19. Click **Next**.

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

20. Although the **Retries**, **Retry Delay**, and the **Inactivity Timeout** options appear, this action does not support these options and you can ignore these values.
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.

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. Click **Next**.

    The **Action Configuration Summary** page appears.

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

After you finish

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

Creating a clone action

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

Procedure

1. In the 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.

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

5. From the **Action Type** list, select **Clone**.
6. If you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is dimmed.
7. 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.

8. Specify a weekly or monthly schedule for the action:

    - To specify a schedule for each day of the week, select **Weekly by day**.
    - To specify a schedule for each day of the month, select **Monthly by day**.

9. 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 12 Schedule icons

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

10. Click **Next**.

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

11. 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.

12. Click **Next**.

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

13. 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.

14. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. This value should not exceed 25.

15. 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.

16. 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**.
17. 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.
18. 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.
19. 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.
20. (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.
21. Click **Next**.

The **Action Configuration Summary** page appears.

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

After you finish

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

Creating an action for Microsoft SQL Server application-consistent protection

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

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

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

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

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

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

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

Starting, stopping, and restarting policies

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

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

Procedure

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

   A confirmation message appears.

   Note

   You cannot stop, restart, or start individual actions.

   ---
3. Click **Yes**.

Enabling a VMware group with Dynamic Association and applying rules in NMC

When you create or edit a VMware protection group in NMC, 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. Note that you can only use the NMC **NetWorker Administration** window 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, virtual machine tags in the **vSphere Web Client** allow you to attach metadata to the objects in the vSphere inventory to make these objects easier to sort and search. Tags are supported in vSphere versions 6.5 and later.

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

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

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

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

  VMfolder - Name, path, tag

  Datacenter - Name, path, tag

  ResourcePool - Path, tag

  VirtualMachine - Name, tag

  vApp - Name, tag

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

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

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

Note

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

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

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

Before you begin

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

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

Procedure

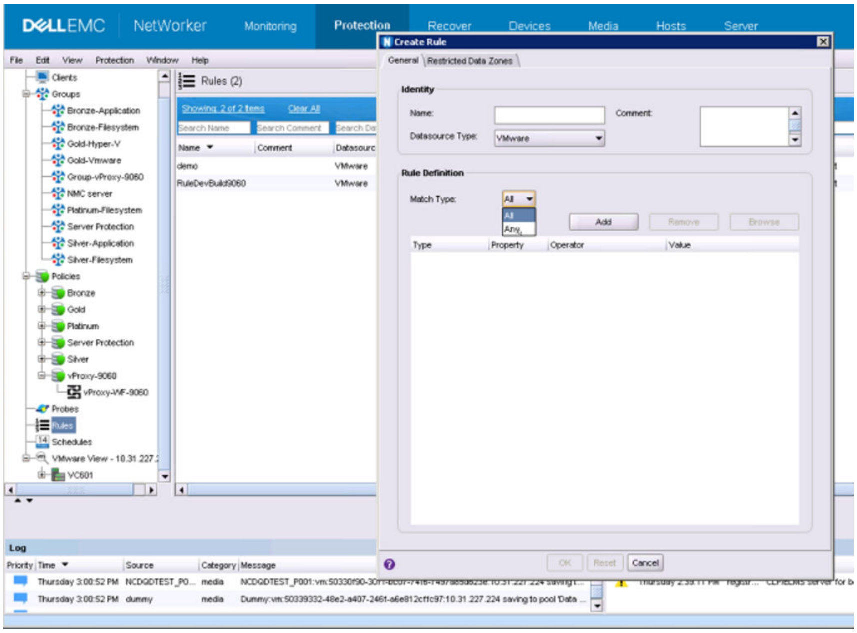
1. In the **NetWorker Administration** window, click **Protection**, and then select **Rules** in the left navigation pane.

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

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

   The **Create Rule** window displays.

Figure 17 Create a new rule to apply to a VMware group



```
Thursday 3:00:52 PM  NCDQDTEST_PO...  media  NCDQDTEST_P001:vm:50330f90-30...10.31.227.224 saving t...
Thursday 3:00:52 PM  dummy            media  Dummy:vm:50339332-48e2-a407-2461-a6e812cffc97:10.31.227.224 saving to pool 'Data ...
```

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

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

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

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

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

   Note

   Tags are only supported in vSphere versions 6.5 and later.

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

Note

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

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

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

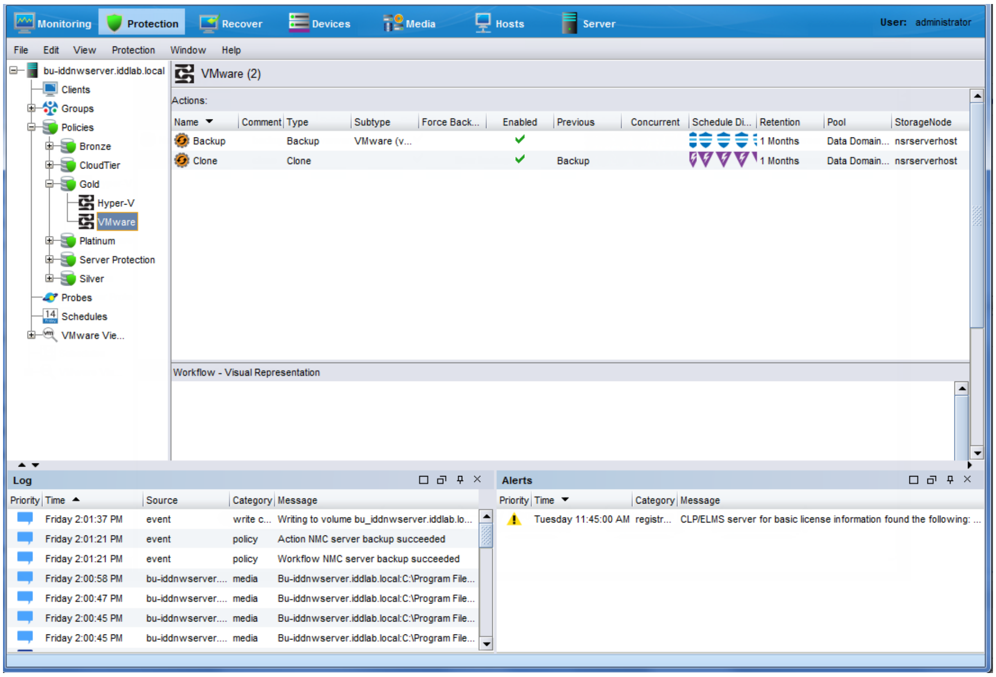
Results

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

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 18 VMware protection policy in the Protection window



Actions:

Name	Comment	Type	Subtype	Force Back...	Enabled	Previous	Concurrent	Schedule Di...	Retention	Pool	StorageNode
Backup		Backup	VMware (v...		✓				1 Months	Data Domain...	nsrserverhost
Clone		Clone			✓	Backup			1 Months	Data Domain...	nsrserverhost

Log

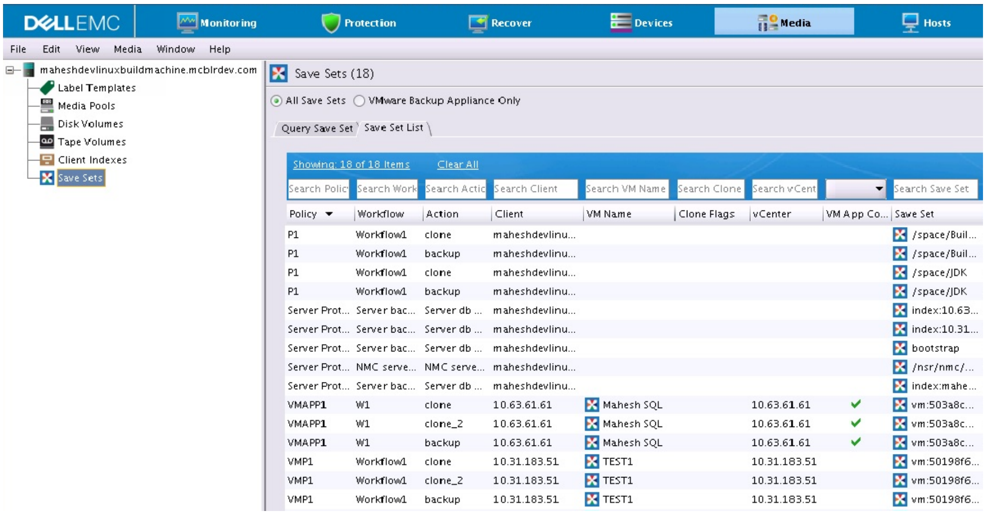
Priority	Time	Source	Category	Message
	Friday 2:01:37 PM	event	write c...	Writing to volume bu_iddnwserver.iddlab.lo...
	Friday 2:01:21 PM	event	policy	Action NMC server backup succeeded
	Friday 2:01:21 PM	event	policy	Workflow NMC server backup succeeded
	Friday 2:00:58 PM	bu-iddnwserver....	media	Bu-iddnwserver.iddlab.local:C:\Program File...
	Friday 2:00:47 PM	bu-iddnwserver....	media	Bu-iddnwserver.iddlab.local:C:\Program File...
	Friday 2:00:45 PM	bu-iddnwserver....	media	Bu-iddnwserver.iddlab.local:C:\Program File...
	Friday 2:00:45 PM	bu-iddnwserver....	media	Bu-iddnwserver.iddlab.local:C:\Program File...

Alerts

Priority	Time	Category	Message
⚠	Tuesday 11:45:00 AM	registr...	CLP/ELMS server for basic license information found the following: ...

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 19 VMware protection policy save sets in Media window



Save Sets (18)

● All Save Sets ○ VMware Backup Appliance Only

Query Save Set | Save Set List

Showing: 18 of 18 Items   Clear All

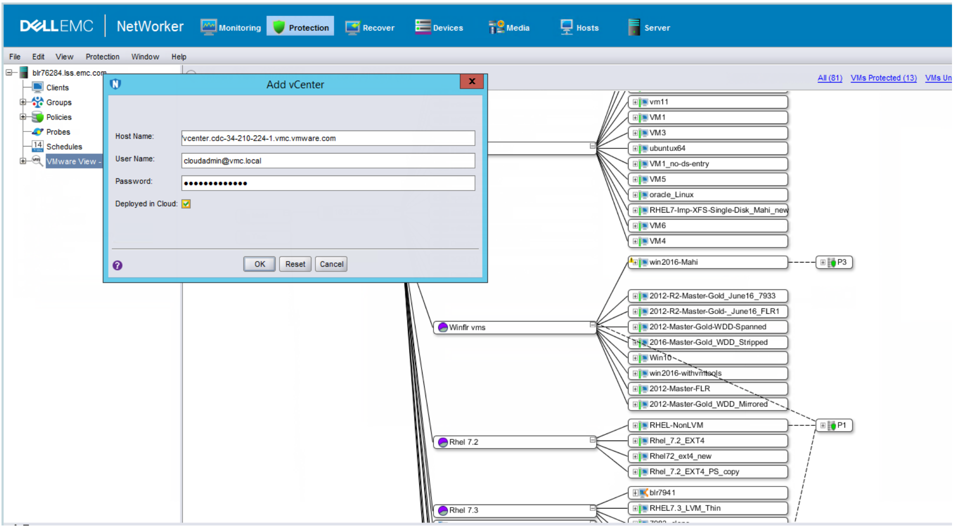
Policy	Workflow	Action	Client	VM Name	Clone Flags	vCenter	VM App Co...	Save Set
P1	Workflow1	clone	maheshdevlinu...					/space/Buil...
P1	Workflow1	backup	maheshdevlinu...					/space/Buil...
P1	Workflow1	clone	maheshdevlinu...					/space/JDK
P1	Workflow1	backup	maheshdevlinu...					/space/JDK
Server Prot...	Server bac...	Server db ...	maheshdevlinu...					index:10.63...
Server Prot...	Server bac...	Server db ...	maheshdevlinu...					index:10.31...
Server Prot...	Server bac...	Server db ...	maheshdevlinu...					bootstrap
Server Prot...	NMC serve...	NMC serve...	maheshdevlinu...					/nsr/nmc/...
Server Prot...	Server bac...	Server db ...	maheshdevlinu...					index:mahe...
VMAPP1	W1	clone	10.63.61.61	Mahesh SQL		10.63.61.61	✓	vm:503a8c...
VMAPP1	W1	clone_2	10.63.61.61	Mahesh SQL		10.63.61.61	✓	vm:503a8c...
VMAPP1	W1	backup	10.63.61.61	Mahesh SQL		10.63.61.61	✓	vm:503a8c...
VMP1	Workflow1	clone	10.31.183.51	TEST1		10.31.183.51		vm:50198f6...
VMP1	Workflow1	clone_2	10.31.183.51	TEST1		10.31.183.51		vm:50198f6...
VMP1	Workflow1	backup	10.31.183.51	TEST1		10.31.183.51		vm:50198f6...

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 20 Add a vCenter server to VMware View in NMC



Add vCenter

Host Name: vcenter.cdc-34-210-224-1.vmc.vmware.com

User Name: cloudadmin@vmc.local

Password: •••••••••••••

Deployed in Cloud: ☑

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

Note

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

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

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

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

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

Map view of the VMware environment

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

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

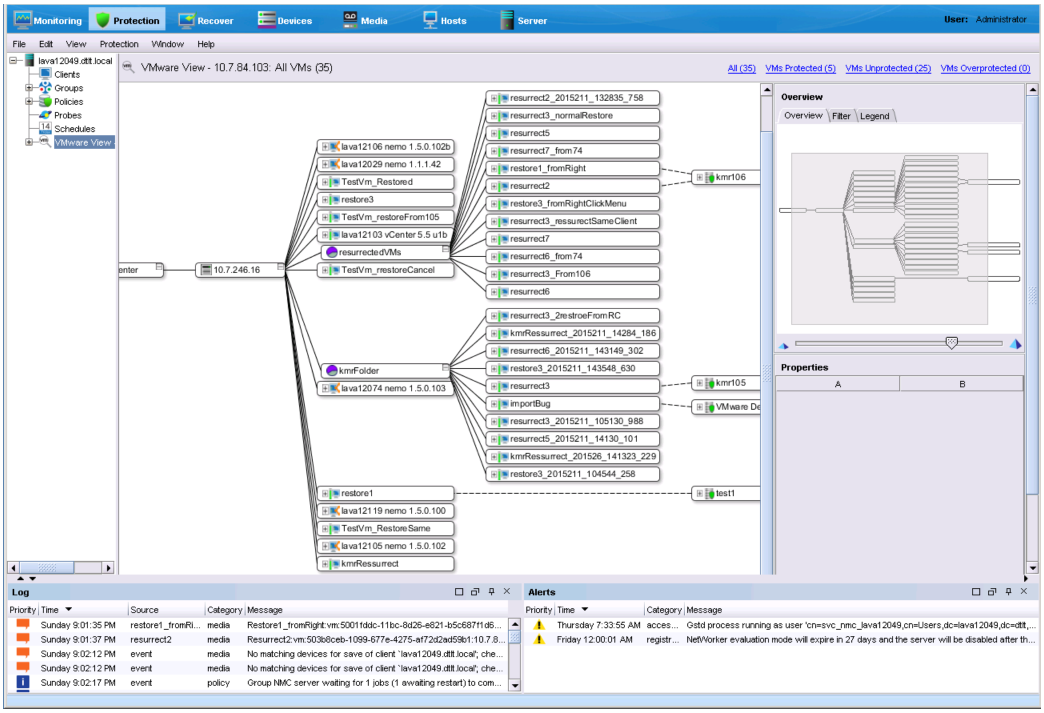
You can use several operations to navigate within the map view:

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

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

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

Figure 21 Map view of VMware environment in NMC



Log

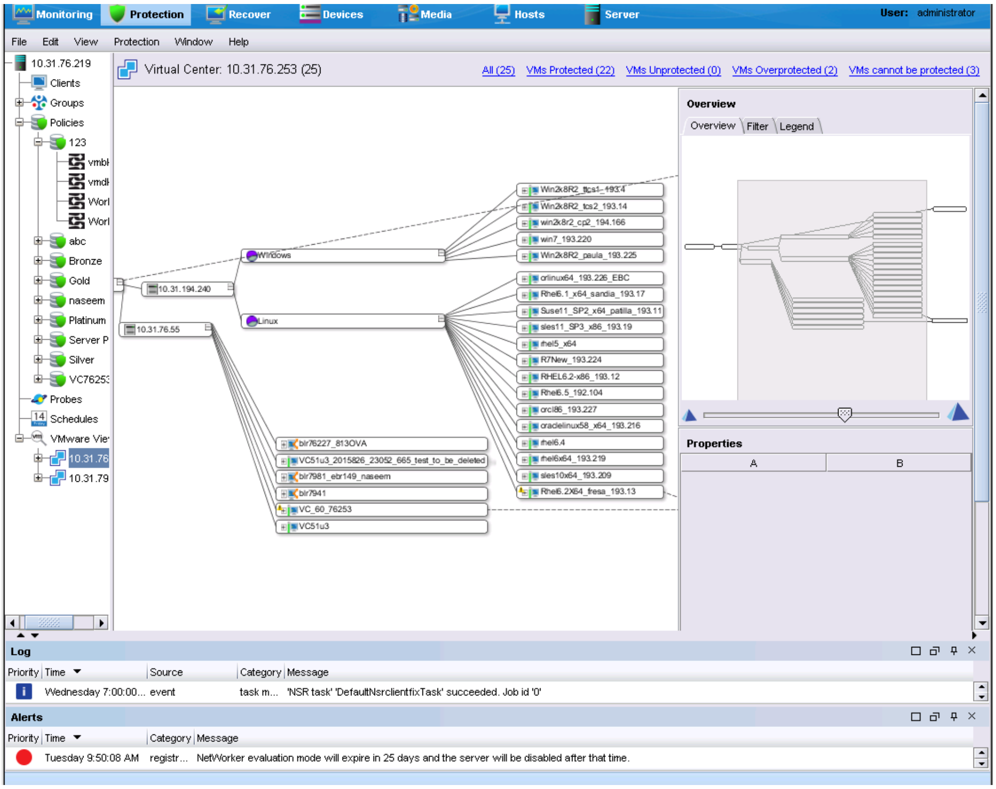
Priority	Time	Source	Category	Message
	Sunday 9:01:35 PM	restore1_fromRi...	media	Restore1_fromRight:vm:5001fddc-11bc-8d26-e821-b5c687f1d6...
	Sunday 9:01:37 PM	resurrect2	media	Resurrect2:vm:503b8ceb-1099-677e-4275-af72d2ad59b1:10.7.8...
	Sunday 9:02:12 PM	event	media	No matching devices for save of client `lava12049.dtlt.local'; che...
	Sunday 9:02:12 PM	event	media	No matching devices for save of client `lava12049.dtlt.local'; che...
i	Sunday 9:02:17 PM	event	policy	Group NMC server waiting for 1 jobs (1 awaiting restart) to com...

Alerts

Priority	Time	Category	Message
⚠	Thursday 7:33:55 AM	acces...	Gstd process running as user 'cn=svc_nmc_lava12049,cn=Users,dc=lava12049,dc=dtlt,...
⚠	Friday 12:00:01 AM	registr...	NetWorker evaluation mode will expire in 27 days and the server will be disabled after th...

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 22 Cluster with child elements in VMware View



Priority	Time	Source	Category	Message
i	Wednesday 7:00:00...	event	task m...	'NSR task' 'DefaultNsrclientfixTask' succeeded. Job id '0'

Priority	Time	Category	Message
●	Tuesday 9:50:08 AM	registr...	NetWorker evaluation mode will expire in 25 days and the server will be disabled after that time.

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 23 Filtering results in VMware View

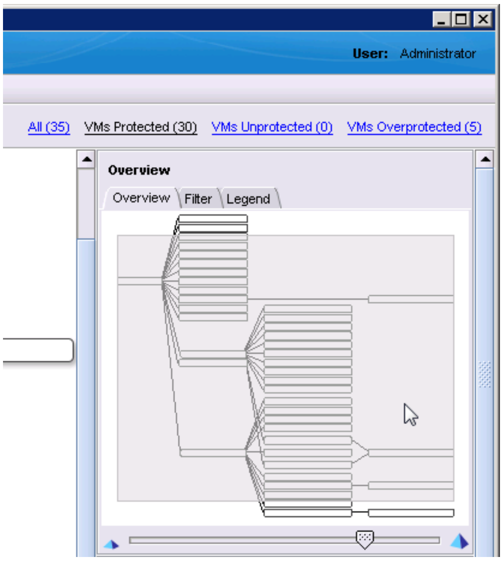


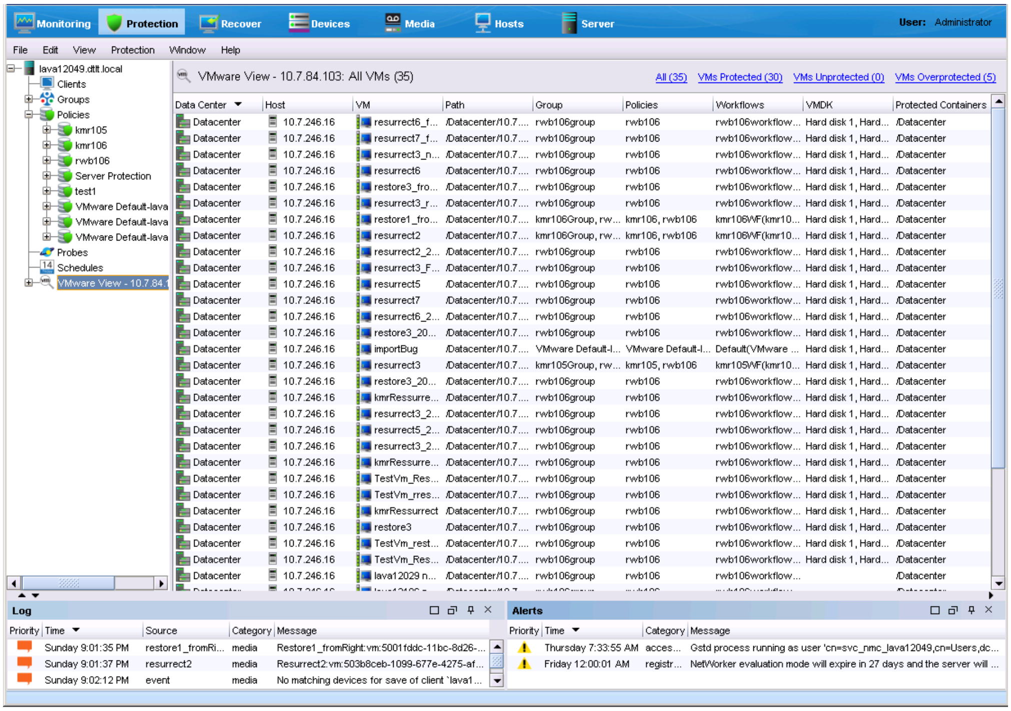
Table view of the VMware environment

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 24 VMware table view



VMware View - 10.7.84.103: All VMs (35)

Data Center	Host	VM	Path	Group	Policies	Workflows	VMDK	Protected Containers
Datacenter	10.7.246.16	resurrect6_f...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect7_f...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_n...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect6	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore3_fro...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_r...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore1_fro...	/Datacenter/10.7....	kmr106Group, rw...	kmr106, rwb106	kmr106WF(kmr10...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect2	/Datacenter/10.7....	kmr106Group, rw...	kmr106, rwb106	kmr106WF(kmr10...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect2_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_F...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect5	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect7	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect6_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore3_20...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	importBug	/Datacenter/10.7....	VMware Default-l...	VMware Default-l...	Default(VMware ...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3	/Datacenter/10.7....	kmr105Group, rw...	kmr105, rwb106	kmr105WF(kmr10...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore3_20...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	kmrRessurre...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect5_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	kmrRessurre...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	TestVm_Res...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	TestVm_rres...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	kmrRessurrect	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore3	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	TestVm_rest...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	TestVm_Res...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	lava12029 n...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...		/Datacenter

Log

Priority	Time	Source	Category	Message
	Sunday 9:01:35 PM	restore1_fromRi...	media	Restore1_fromRight:vm:5001fddc-11bc-8d26-...
	Sunday 9:01:37 PM	resurrect2	media	Resurrect2:vm:503b8ceb-1099-677e-4275-af...
	Sunday 9:02:12 PM	event	media	No matching devices for save of client `lava1...

Alerts

Priority	Time	Category	Message
⚠	Thursday 7:33:55 AM	acces...	Gstd process running as user 'cn=svc_nmc_lava12049,cn=Users,dc...
⚠	Friday 12:00:01 AM	registr...	NetWorker evaluation mode will expire in 27 days and the server will ...

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

Note

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

Assigning protection groups to virtual machines

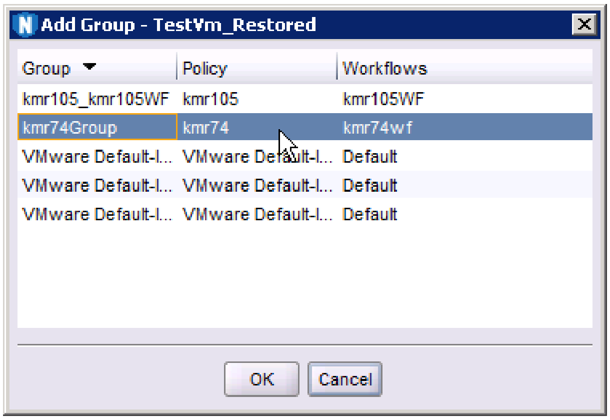
From within the map or table view of the VMware environment, you can assign protection groups at any level, for example, you can assign a group to the entire datacenter, a cluster, a resource pool, a virtual machine, or even a VMDK by using **VMware View**.

Procedure

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

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

   Figure 25 Add group in VMware View



Group	Policy	Workflows
kmr105_kmr105WF	kmr105	kmr105WF
kmr74Group	kmr74	kmr74wf
VMware Default-I...	VMware Default-I...	Default
VMware Default-I...	VMware Default-I...	Default
VMware Default-I...	VMware Default-I...	Default

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

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

Assigning a group to a disconnected ESX server

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

Note

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

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

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

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

Note

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

Connect to the NetWorker server in the vSphere Client

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

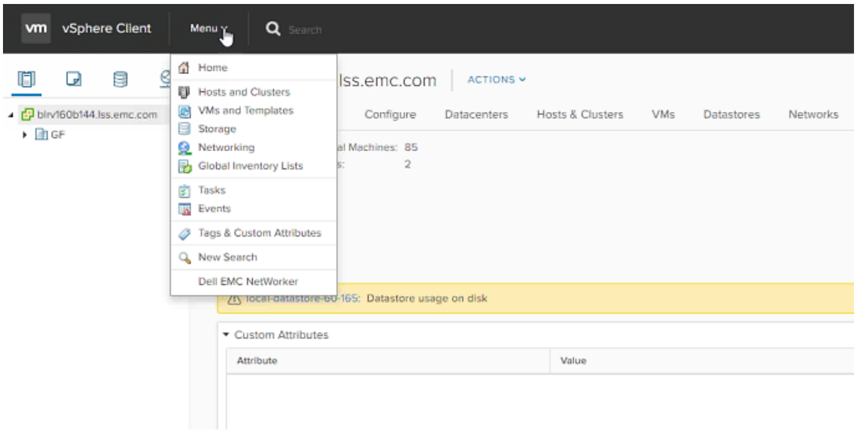
Before you begin

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

Procedure

1. Login to the **vSphere Client** as an administrator, or as a non-administrator Active Directory user that you created using the steps in the section Using the 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 26 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:

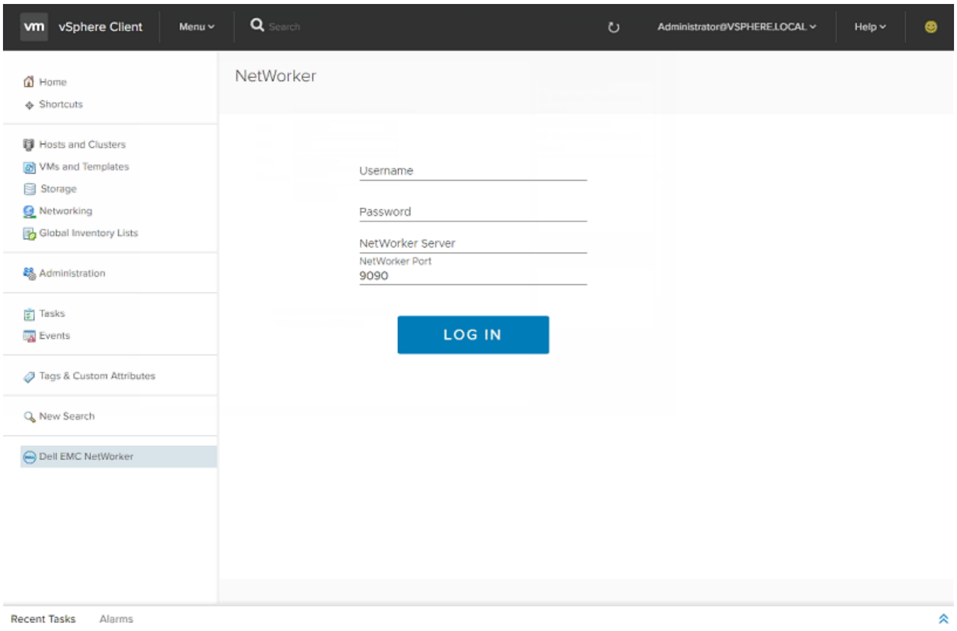
   a. In the **Username** field, type the NetWorker administrator username.

   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 27 NetWorker connection information in the vSphere Client



Username

Password

NetWorker Server

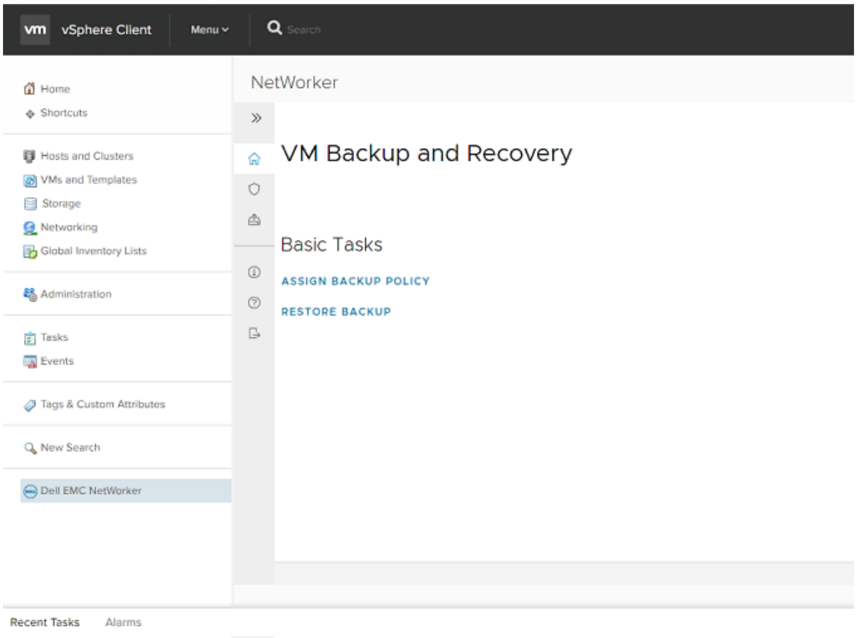
NetWorker Port
9090

4. Click **Log in**.

Results

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

Figure 28 Dell EMC NetWorker Basic Tasks pane



Accessing the vCenter plug-in as a non-administrator Active Directory user

You can only access the vCenter plug-in (the **Dell EMC NetWorker** interface) in the **vSphere Client** if you are an NetWorker administrator or a non-administrator Active Directory user associated with appropriate privileges in NetWorker. The following procedure describes how to access the plug-in as a non-administrator Active Directory user.

Before you begin

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

Procedure

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

   ```
   CN=VMwareTeam,CN=Users,DC=vproxy,DC=com
   ```

cn=VMwareUser,cn=Users,dc=vproxy,dc=com
where *VMwareTeam* is the security group name, and *VMwareUser* is the Active Directory user name.

4. Log in to the **vSphere Web Client** as the Active Directory user, in the format **<tenant>\<domain>\<userid>**. For example:

   default\vproxy\VMwareUser

Results

The Active Directory user that you create using these steps will only have access to the **vSphere Client Dell EMC NetWorker** interface, and cannot be used to log in to **NetWorker Management Console**. If you also need to provide access to NMC, then add those required privileges accordingly.

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

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

Procedure

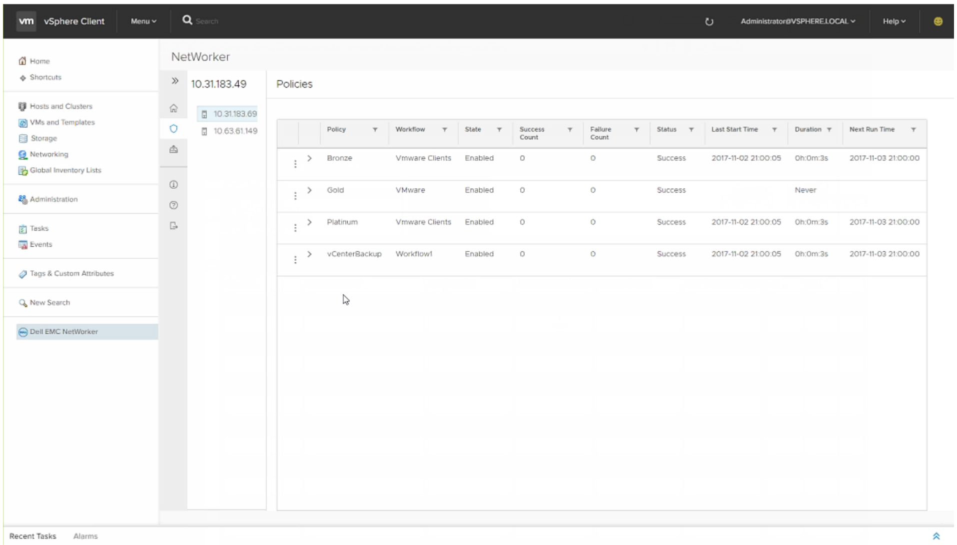
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

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

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

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

   Figure 29 Policies pane with available vProxy policies

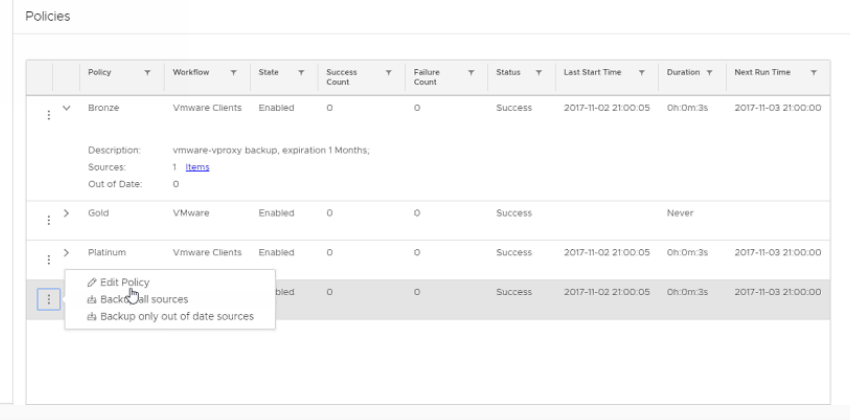


Policy	Workflow	State	Success Count	Failure Count	Status	Last Start Time	Duration	Next Run Time
Bronze	Vmware Clients	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00
Gold	VMware	Enabled	0	0	Success		Never	
Platinum	Vmware Clients	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00
vCenterBackup	Workflow1	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00

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 30 Policy backup options

   Policies

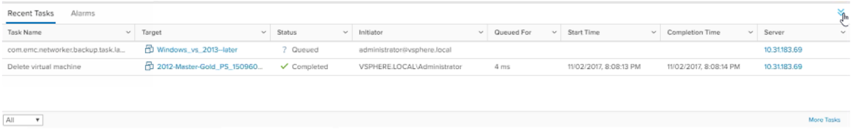
Policy	Workflow	State	Success Count	Failure Count	Status	Last Start Time	Duration	Next Run Time
Bronze	Vmware Clients	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00
Gold	VMware	Enabled	0	0	Success		Never	
Platinum	Vmware Clients	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00
		bled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00

   Description: vmware-vproxy backup, expiration 1 Months;
   Sources: 1 Items
   Out of Date: 0

Results

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

Figure 31 Recent Tasks pane



Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
com.emc.networker.backup.task.la...	Windows_vs_2013--later	? Queued	administrator@vsphere.local				10.31.183.69
Delete virtual machine	2012-Master-Gold_PS_150960...	✓ Completed	VSPHERE.LOCAL\Administrator	4 ms	11/02/2017, 8:08:13 PM	11/02/2017, 8:08:14 PM	10.31.183.69

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

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

Procedure

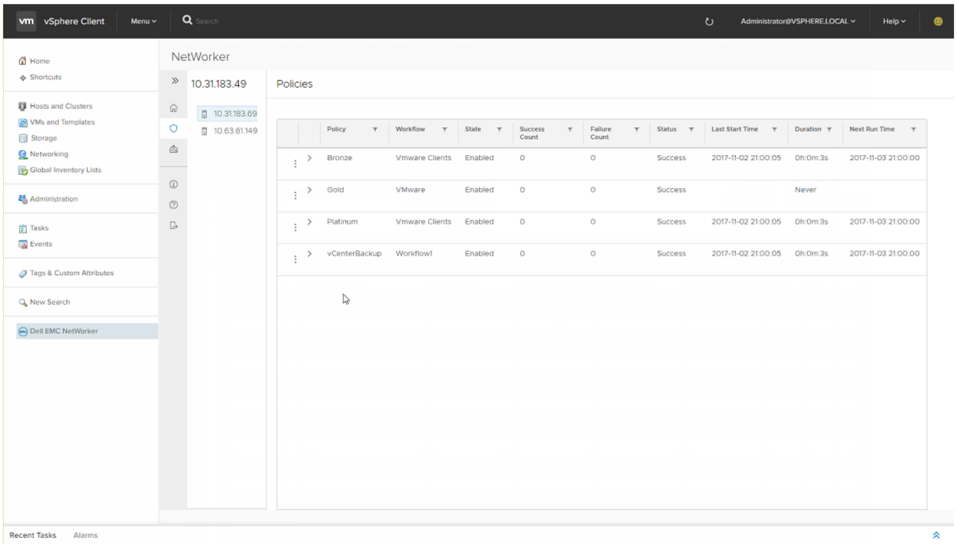
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

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

2. Click **Assign Backup Policy**.

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

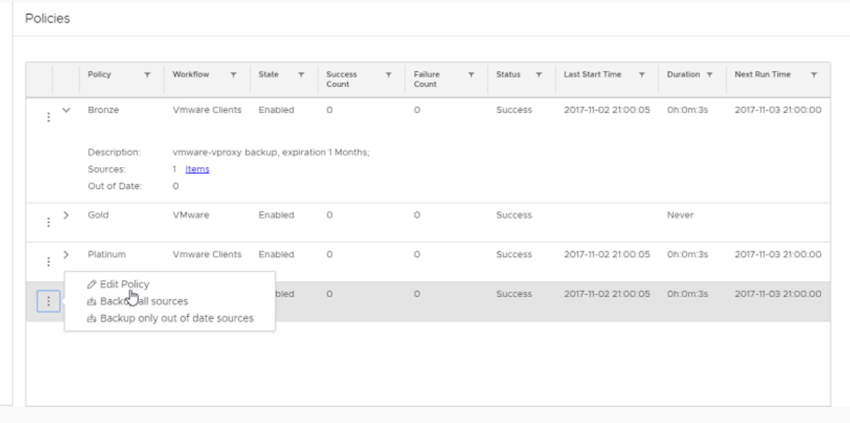
Figure 32 Policies pane with available vProxy policies



Policy	Workflow	State	Success Count	Failure Count	Status	Last Start Time	Duration	Next Run Time
Bronze	Vmware Clients	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00
Gold	VMware	Enabled	0	0	Success		Never	
Platinum	Vmware Clients	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00
vCenterBackup	Workflow1	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00

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

Figure 33 Edit a vProxy policy

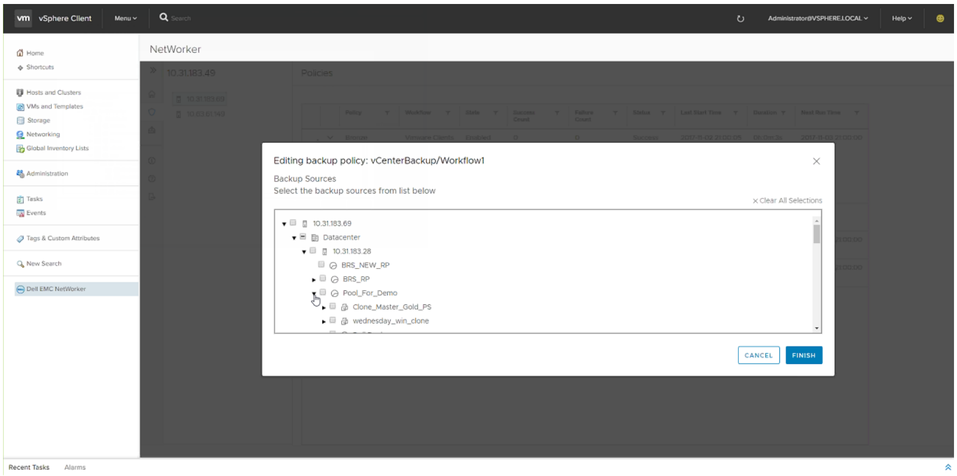


Policy	Workflow	State	Success Count	Failure Count	Status	Last Start Time	Duration	Next Run Time
Bronze	Vmware Clients	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00
Description:	vmware-vproxy backup, expiration 1 Months;							
Sources:	1 Items							
Out of Date:	0							
Gold	VMware	Enabled	0	0	Success		Never	
Platinum	Vmware Clients	Enabled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00
		bled	0	0	Success	2017-11-02 21:00:05	0h:0m:3s	2017-11-03 21:00:00

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

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

Figure 34 Backup sources in the Editing backup policy dialog



Editing backup policy: vCenterBackup/Workflow1

Backup Sources

Select the backup sources from list below

× Clear All Selections

- ▾ □ 10.31.183.69
  - ▾ ⊟ Datacenter
    - ▾ □ 10.31.183.28
      - □ BRS_NEW_RP
      - ▸ □ BRS_RP
      - ▾ □ Pool_For_Demo
        - ▸ □ Clone_Master_Gold_PS
        - ▸ □ wednesday_win_clone

CANCEL FINISH

Results

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

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

The flash-based vCenter plug-in, which displays as the **VM Backup and Recovery** interface in the vSphere Web Client, was introduced in NetWorker 9.1. New and upgraded users of NetWorker version 18.1 can still use this plug-in to run virtual machine backups from the vProxy workflows created in NMC, and add virtual machines to those vProxy workflows.

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

Note

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

Connect to the NetWorker server in the vSphere Web Client

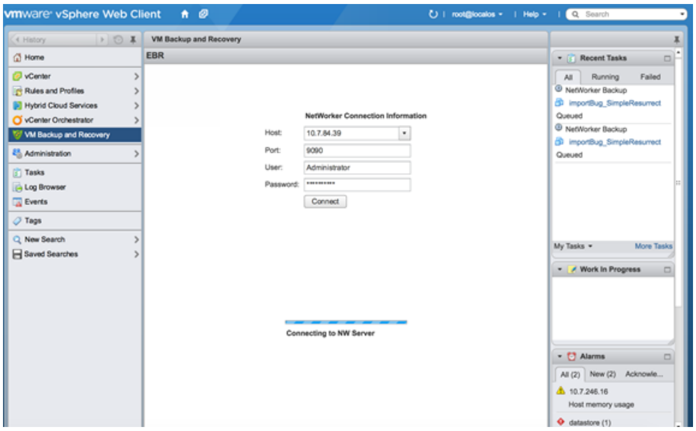
After installing the vCenter plug-in, you must establish a connection to the NetWorker server before performing any vProxy operations in the vSphere Web Client.

Procedure

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

   The required NetWorker connection information appears in the right pane.

Figure 35 NetWorker connection information in the vSphere Web Client



VM Backup and Recovery

EBR

NetWorker Connection Information

Host: 10.7.84.39

Port: 9090

User: Administrator

Password: **********

Connect

Connecting to NW Server

NetWorker Backup
importBug_SimpleResurrect
Queued

NetWorker Backup
importBug_SimpleResurrect
Queued

10.7.246.16
Host memory usage

datastore (1)

3. Enter the following information for the NetWorker server:

   a. In the **Host** field, type the IP address of the NetWorker server.

   b. In the **Port** field, type **9090**.

   c. In the **User** field, type the NetWorker administrator username.

   d. In the **Password** field, type the NetWorker administrator password.

4. Click **Connect**.

Results

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

Accessing the vCenter plug-in as a non-administrator Active Directory user

You can only access the vCenter plug-in (the VM Backup and Recovery interface) in the vSphere Web Client if you are an NetWorker administrator or a non-administrator Active Directory user associated with appropriate privileges in NetWorker . The following procedure describes how to access the plug-in as a non-administrator Active Directory user.

Before you begin

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

Procedure

1. Create a **vmwareAdmin** group in NetWorker that contains the following privileges at a minimum:

   - View Security Settings
   - View Application Settings
   - Remote Access All Clients
   - Operate NetWorker
   - Monitor NetWorker
   - Operate Devices and Jukeboxes
   - Recover Local Data
   - Recover Remote Data

- Backup Local Data

2. Create an Active Directory user within your desired security group.
3. Add the user and group to the NetWorker Management Console's **External Roles** attribute. For example:

   ```
   CN=VMwareTeam,CN=Users,DC=vproxy,DC=com
   cn=VMwareUser,cn=Users,dc=vproxy,dc=com
   ```

   where *VMwareTeam* is the security group name, and *VMwareUser* is the Active Directory user name.
4. Log in to the **vSphere Web Client** plug-in as the Active Directory user, in the format `<tenant>\<domain>\<userid>`. For example:

   ```
   default\vproxy\VMwareUser
   ```

Results

The Active Directory user that you create using these steps will only have access to the **vSphere Web Client VM Backup and Recovery** interface, and cannot be used to log in to NetWorker Management Console. If you also need to provide access to NMC, then add those required privileges accordingly.

Starting a vProxy policy in the vSphere Web Client

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

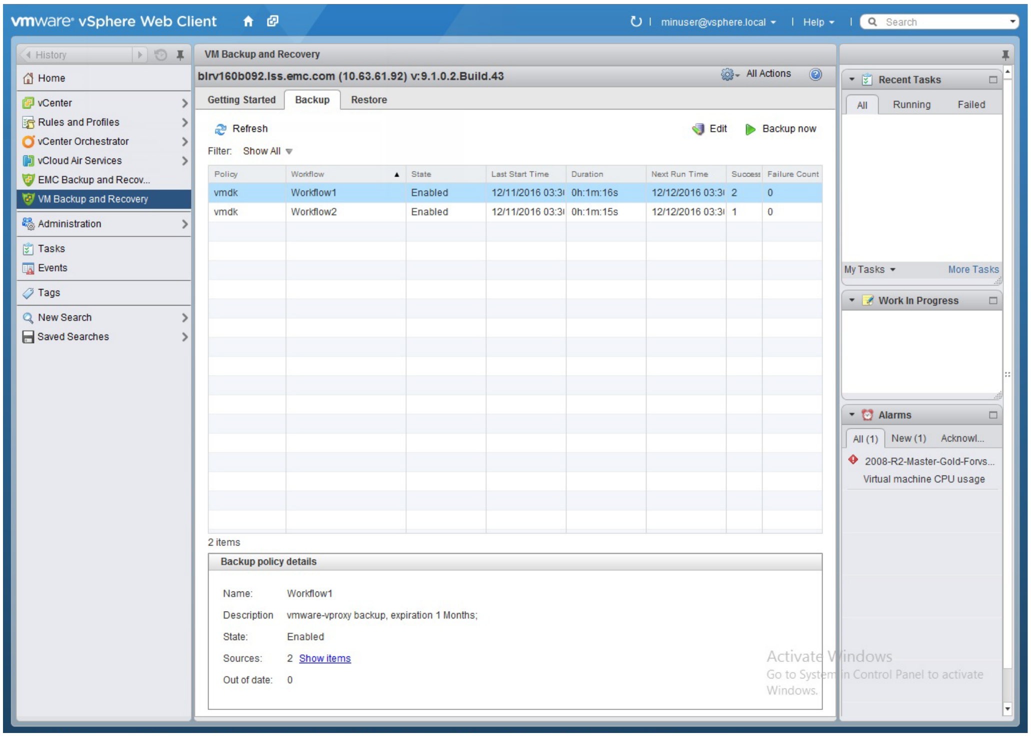
Procedure

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

   When a connection to the NetWorker server is established, the **Getting Started** pane appears.
2. Click the **Backup** tab to open the **Backup** pane.

   Any vProxy policies created in NMC display.

Figure 36 Backup pane with vProxy policy



blrv160b092.lss.emc.com (10.63.61.92) v:9.1.0.2.Build.43

Filter: Show All

Policy	Workflow	State	Last Start Time	Duration	Next Run Time	Success	Failure Count
vmdk	Workflow1	Enabled	12/11/2016 03:3	0h:1m:16s	12/12/2016 03:3	2	0
vmdk	Workflow2	Enabled	12/11/2016 03:3	0h:1m:15s	12/12/2016 03:3	1	0

2 items

Backup policy details

Name: Workflow1

Description vmware-vproxy backup, expiration 1 Months;

State: Enabled

Sources: 2 Show items

Out of date: 0

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

Results

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

Note

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

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

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

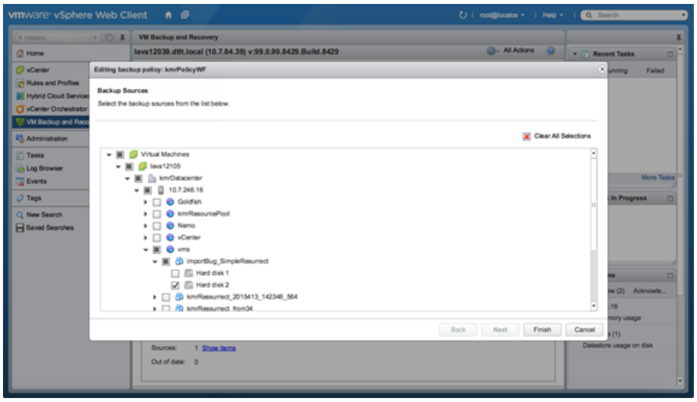
Procedure

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

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

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

Figure 37 Backup sources in the Editing backup policy window



Editing backup policy: kmrPolicyWF

Backup Sources

Select the backup sources from the list below.

☒ Clear All Selections

- ■ Virtual Machines
  - ■ lava12105
    - ■ kmrDatacenter
      - ■ 10.7.246.16
        - □ Goldfish
        - □ kmrResourcePool
        - □ Nemo
        - □ vCenter
        - ■ vms
          - ■ importBug_SimpleResurrect
            - □ Hard disk 1
            - ☑ Hard disk 2
          - □ kmrResurrect_2015413_142346_564
          - □ kmrResurrect_from34

Sources: 1 Show items

Out of date: 0

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

Results

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

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 NetWorker VMware Protection backups for the VMware Backup Appliance (VBA).

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.enableUUDI* variable for the virtual machine is set to `False`.

```
Unable to find VSS metadata files in directory C:\Program Files
\DPSAPPS\MSVMAPPAGENT\tmp\VSSMetadata.xxxx.
```

To resolve this issue, ensure that the *disk.enableUUDI* variable for the virtual machines included in an SQL Server application-consistent backup is set to `True`.

Failed to lock Virtual Machine for backup: Another EMC vProxy operation 'Backup' is active on VM

This error message appears when a backup fails for a virtual machine, when previous backups of the virtual machine was abruptly ended and the VM annotation string was not cleared.

To resolve this issue, clear the annotation string value for the virtual machine.

1. Connect to the vCenter server and navigate **Home** > **Inventory** > **Hosts and Clusters**.
2. Select the virtual machine, and then select the **Summary** tab.
3. Clear the value that appears in the **EMC Proxy Session** field.

“Loading backup job data”

This message can appear for up to five minutes when you select a large number of VMs (approximately 100 VMs) for a single backup job. This issue can also apply to lock/unlock, refresh, or delete actions for large jobs. This is expected behavior when you select a very large number of jobs. This message disappears when the action is completed, which can take up to five minutes.

“The following items could not be located and were not selected {client name}.”

This error can occur when the backed up VM(s) cannot be located during Edit of a backup job. This is a known issue.

Windows 2008 R2 VMs may fail to backup with “disk.EnableUUID” configured to “true.”

Windows 2008 R2 backups may fail if the VM is configured with the *disk.EnableUUID* parameter set to *true*. To correct this problem, manually update the vmx configuration parameter *disk.EnableUUID* to *false* by using the vSphere Web Client:

1. Shut down the VM by right clicking the VM and selecting **Shut Down Guest OS**.
2. Right click the VM and select **Edit Settings**.
3. Click **VM Options**.
4. Expand the **Advanced** section and click **Edit Configuration**.
5. Locate the name *disk.EnableUUId* and set the value to *false*.
6. Click **OK** on the next two pages.
7. Right click the VM and select **Power On**.

After you update the configuration parameter, the backups of the Windows 2008 R2 VM should succeed.

When VMs are moved in or out of different cluster groups, associated backup sources may be lost

When you move hosts into clusters with the option to retain the resource pools and vApps, the containers get recreated, not copied. As a result, the container is no longer the same container even though the name is the same. To resolve this issue, validate or recreate any backup jobs that protect containers after moving hosts in or out of a cluster.

vMotion operations are not allowed during active backup operations

The vSphere vMotion feature enables the live migration of running virtual machines from one physical server to another. You cannot run vMotion operations on the vProxy appliance or VMware Backup appliance during active backup operations. This is expected behavior. Wait until all backup operations have completed prior to performing a vMotion operation.

Backups fail if certain characters are used in the virtual machine name, datastore, folder, or datacenter names

When you use spaces or special characters in the virtual machine name, datastore, folder, or datacenter names, the .vmx file is not included in the backup. The vProxy appliance and VMware Backup appliance do not back up objects that include the following special characters, in the format of character/escape sequence:

- & %26
- + %2B
- / %2F
- = %3D
- ? %3F
- % %25
- \ %5C
- ~ %7E
-] %5D

NSRCLONE failed for one or more savesets

This message appears during a clone action and NetWorker does not clone all save sets.

Error messages similar to the following also appear:

```
[CLONE SKIPPED SAVESETS]
ssid/cloneid;
Action clone 'name' with job id 5 is
exiting with status 'failed', exit code 1
NSRCLONE failed for one or more savesets
```

To resolve this issue, increase the values in the **max target sessions** and **target sessions** attributes for the clone device. The *NetWorker Administration Guide* describes how to modify the properties of a device.

Lock placed on virtual machine during backup and recovery operations continues for 24 hours if vProxy appliance fails

During vProxy backup and recovery operations, a lock is placed on the virtual machine. If a vProxy appliance failure occurs during one of these sessions, the lock gets extended to a period of 24 hours, during which full backups and transaction log backups will fail with the following error until the lock is manually released:

```
Cannot lock VM 'W2K8R2-SQL-2014' (vm-522): Another EMC vProxy
operation 'Backup' is active on VM vm-522.
```

Workaround

To manually release the lock on the virtual machine:

1. Open the **vSphere Web Client**.
2. Click on 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 a NetWorker 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:

Case	Description
Database has been restored	When a database has been restored, this database will be skipped during transaction log backup because there is no Backup Promotion.
System Database	System databases are automatically skipped for transaction log backup.
Database State	Database is not in a state that allows backup. For example, the database is in the NORECOVERY state.
Recovery Model	Database is in SIMPLE recovery model, which does not support transaction log backup
Other Backup Product	Most recent backup for the database was performed by a different backup product.
New Database	Database was created after most recent full backup.
Backup Failure	Database was in state to allow backup, backup was attempted, but backup failed.

All skipped databases will be backed up as part of the next full backup. Also, a skipped database will not result in `msvmagent_appbackup.exe` failure. The only instance in which `msvmagent_appbackup.exe` would potentially fail is if all databases failed to back up.

The `msvmagent_appbackup.exe` program generates a history report of the databases, if the database backup status was success/skipped/failed, and a reason if they were skipped or failed if applicable. This history report is visible in the action logs for the vProxy, which are available on the NetWorker server and also available on the client 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*.

vProxy backup log files

You can use vProxy session log files to troubleshoot backup failures.

The following table provides information about the vProxy backup log files. located in `/opt/emc/vproxy/runtime/logs/vbackupd/` on the vProxy host. Note that old daemon and session logs are located in `/opt/emc/vproxy/runtime/logs/recycle/`.

Table 13 Backup log files

Log file	Log location	Description
Session logs	`<session-uuid>.log`	Contains processing details for a session. Sessions display as “Recycled” when the session is deleted. The log level is configured in the session request.
Daemon logs	`<daemon>-engine.log`	Records requests and problem events which may require administrative action in vProxy or vCenter. Error and Panic messages from the session logs are also recorded in the daemon log. The log level is set

Table 13 Backup log files (continued)

Log file	Log location	Description
		in `/usr/lib/systemd/system/<daemon>.service`, for example, "--engine-log-level <level>".
DD Boost backup log	`<daemon>-boost.log`	The log level is set in `/usr/lib/systemd/system<daemon>.service`, for example, "--boost-log-level <level>"
VDDK backup log	`<daemon>-vddk.log`	The log level is set in `/opt/emc/vproxy/conf/VixDiskLib.config` (vixDiskLib.transport.LogLevel = <level>)

On the NetWorker server, the location of log files for individual backups differ on Windows and LINUX:

- Linux—`/nsr/logs/policy/`*`policy_name`*
- Windows—`C:\Program Files\EMC NetWorker\logs\policy\`*`policy_name`*

where *policy_name* is the name of the policy resource associated with the backup action.

Additional logging with the VMBackup broker

Debug logging of the `vmbackup` broker of `nsrd` is disabled by default. To turn on additional logging, you can touch an empty file at *`<nsr>`*`/tmp/vmbackup_logging`. Enabling of additional logging can be performed while other operations are in progress, and a NetWorker restart is not required. To turn off additional logging, you can remove the same file.

NMC function to collect vProxy log bundle information

NetWorker 18.1 features an NMC function to collect vProxy log bundle information from a virtual machine. To collect log bundle information, perform the following steps in NMC:

1. From NMC's **NetWorker Administration**, open the **Devices** window.
2. From the left pane, select **VMware Proxies** to display the virtual machine proxy devices.
3. Right-click the virtual machine that you want to collect log bundle information from, and then from the menu, click **Log Bundle**.

Note

If you are accessing NMC from a remote machine that cannot communicate with vProxy, NMC fails to collect the log bundle.

Logs for SQL application-consistent data protection

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

Note

In order to increase the debug level for SQL application-consistent virtual machine (MSVMAPPAGENT) backups, use `dbgcommand`, For example, `dbgcommand -p <nsrd-pid> Debug=9`. Once you complete the debugging session, ensure that you reset the debug level of `nsrd` to zero by running `dbgcommand <nsrd-pid> Debug=0`.

MSVMAPPAGENT logs

You can access logs related to MSVMAPPAGENT from the following locations:

- Discovery log: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmagent_discovery.log`
- FULL backup: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmcatsnap.log`
- Transaction log backup: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmagent_appbackup.log`
- Restore of FULL backup: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmagent_snapshotrestore.log`
- Restore of transaction log backup: `C:\Program Files\DPSAPPS\MSVMAPPAGENT\logs\msvmagent_apprestore.log`

vProxy logs

You can access these vProxy logs from the following locations:

- FULL and transaction log backups: `/opt/emc/vproxy/runtime/logs/vbackupd/BackupVmSessions-sessionnumber.log`
- InspectBackup logs: `/opt/emc/vproxy/runtime/logs/vsessionsd/inspectBackup-sessionnumber.log`
- Mount session logs: `/opt/emc/vproxy/runtime/logs/vflrd/mount-sessionnumber.log`
- Browse session logs: `/opt/emc/vproxy/runtime/logs/vflrd/browse-sessionnumber.log`
- Recover App sessions logs: `/opt/emc/vproxy/runtime/logs/vflrd/application-sessionnumber.log`. Note that a few minutes after completion, these logs are moved to `/opt/emc/vproxy/runtime/logs/recycle/`.

CHAPTER 4

Recover virtual machines and data

This chapter contains the following topics:

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**.

Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only)

Before you perform an instant recovery of a virtual machine or file-level restore (User mode), ensure that you provide the management credentials for the Data Domain resource. For instant recovery, these credentials are required when performing the recovery using the NMC **Recover** wizard or the **VM Backup and Recovery** interface in the **vSphere Web Client**.

Procedure

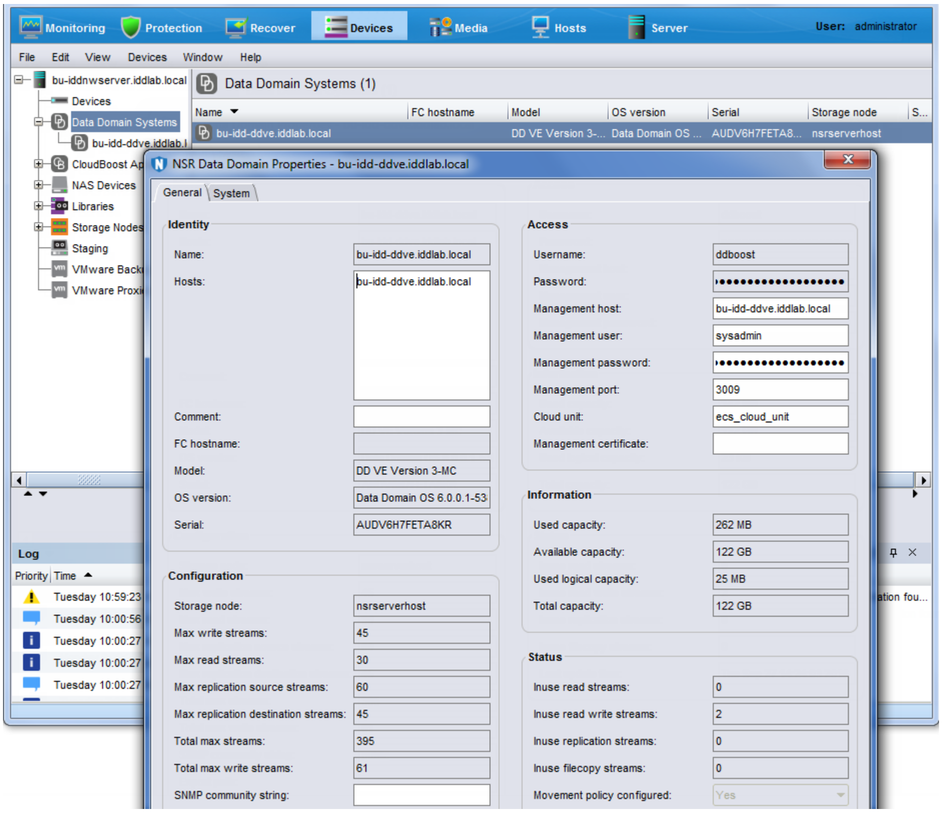
1. In the NMC Administration window, click **Devices**.

   The **Devices** window displays.

2. In the expanded left navigation pane, select **Data Domain Systems**.
3. In the right details pane, right-click the Data Domain system, and then select **Properties**.

   The **NSR Data Domain Properties** window displays.

Figure 38 NSR Data Domain Properties



Data Domain Systems (1)

Name	FC hostname	Model	OS version	Serial	Storage node	S...
bu-idd-ddve.iddlab.local		DD VE Version 3-...	Data Domain OS ...	AUDV6H7FETA8...	nsrserverhost	

NSR Data Domain Properties - bu-idd-ddve.iddlab.local

Identity

Name: bu-idd-ddve.iddlab.local

Hosts: bu-idd-ddve.iddlab.local

Comment:

FC hostname:

Model: DD VE Version 3-MC

OS version: Data Domain OS 6.0.0.1-53

Serial: AUDV6H7FETA8KR

Access

Username: ddboost

Password: ••••••••••••••••••

Management host: bu-idd-ddve.iddlab.local

Management user: sysadmin

Management password: ••••••••••••••••••

Management port: 3009

Cloud unit: ecs_cloud_unit

Management certificate:

Information

Used capacity: 262 MB

Available capacity: 122 GB

Used logical capacity: 25 MB

Total capacity: 122 GB

Configuration

Storage node: nsrserverhost

Max write streams: 45

Max read streams: 30

Max replication source streams: 60

Max replication destination streams: 45

Total max streams: 395

Total max write streams: 61

SNMP community string:

Status

Inuse read streams: 0

Inuse read write streams: 2

Inuse replication streams: 0

Inuse filecopy streams: 0

Movement policy configured: Yes

Priority	Time
⚠	Tuesday 10:59:23
	Tuesday 10:00:56
i	Tuesday 10:00:27
i	Tuesday 10:00:27
	Tuesday 10:00:27

ation fou...

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 a domain user

To perform a file-level restore as a domain user in the NMC **NetWorker Administration** window's **Recovery** wizard or the **Dell EMC Data Protection Restore Client**, you need to register a tenant user and provide the FLR Domain user permissions by performing the following steps.

Note

Steps 1 through 3 provide high level information for running `authc_config`. More detailed steps might be required if configuring AD authentication in the NetWorker environment. The *NetWorker Security Configuration Guide* provides more information.

Procedure

1. Create a tenant user on NetWorker by running the `authc_config` command. For example, open a command prompt and cd to `C:\Users\Administrator`, and then type `authc_config -u administrator -e add-tenant -D tenant-name=FLR -D tenant-alias FLR -p` *`password`*
2. Obtain the tenant ID by running the following command:

   ```
   authc_config -u administrator -e find-tenant -D tenant-
   name=FLR -p password
   Tenant Id : 4
   Tenant Name : FLR
   Tenant Alias : FLR
   Tenant Details:
   ```

3. Register the domain user by running the following command:

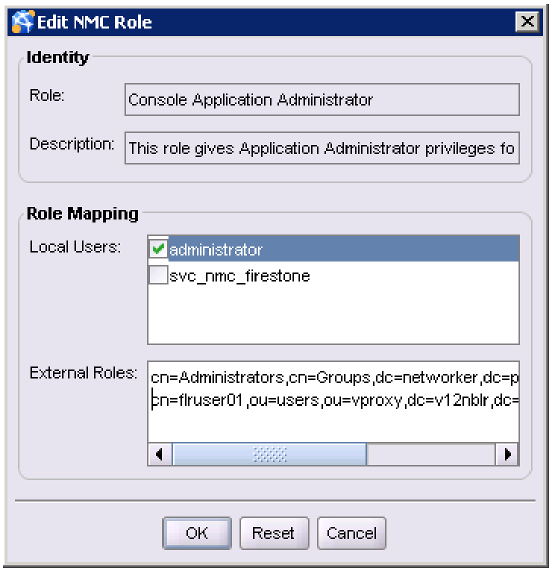
   ```
   authc_config -u administrator -e add-config -D config-tenant-
   id=3 -D config-name=FLRtest
   -D config-server-address=ldap://10.63.60.31:389/
   OU=vproxy,DC=v12nblr,DC=com -D config-domain=v12nblr
   -D config-user-
   dn=CN=flruser01,OU=users,OU=vproxy,DC=v12nblr,DC=com -D
   config-user-dn-password=password
   -D config-user-object-class=inetOrgPerson -D config-user-
   search-path=OU=users -D config-user-id-attr=cn
   -D config-group-search-path=OU=users -D config-group-name-
   attr=cn -D config-group-object-class=group
   -D config-group-member-attr=member -D config-active-
   directory=y -p password
   ```

4. Launch the **NetWorker Management Console**.
5. In the **NetWorker Management Console**, click **Setup** to open the **Setup** window.
6. Under **Users and Roles** in the left navigation pane, select **NMC Roles**. The roles display in the right pane.
7. For the **Console Application Administrator**, **Console Security Administrator** and **Console User** NMC roles, perform the following

   a. From the right pane, right-click **NMC role** and select **Properties**.

b. In the **Edit NMC Role** dialog, add the Domain FLR user by typing `cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com` in the **External roles** field, and then click **OK**.

Figure 39 Add Domain FLR user



Role: Console Application Administrator

Description: This role gives Application Administrator privileges fo

Local Users:
☑ administrator
□ svc_nmc_firestone

External Roles:
cn=Administrators,cn=Groups,dc=networker,dc=p
cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=

8. Navigate to the NMC **Enterprise** window, right-click the server and select **Launch Application...** to open the NMC **Administration** window.
9. Click **Server** to open the **Server** window.
10. In the left navigation pane, select **User Groups** to display the users in the right pane.
11. Type the Domain FLR user details in the **External Roles** field for the following User groups:
    - Application Administrators: `cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com`
    - Users: `cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com`
    - VMware FLR Users: `cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com`
12. Type the Domain FLR user details in the **External Roles** field for the following User group:
    - VMware FLR Users: `cn=flrusergroup,ou=users,ou=vproxy,dc=v12nblr,dc=com`

    In the example, the Domain FLR user "cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com" is part of the Domain FLR group "cn=flrusergroup,ou=users,ou=vproxy,dc=v12nblr,dc=com" in Active Directory.
13. After registering the user as external domain, log in to the virtual machine as a domain user.
14. Re-launch the NMC **NetWorker Administration** window or the **Dell EMC Data Protection Restore Client** with the Domain FLR user in the following format:
    - In **NetWorker Administration**, v12nblr\flruser01

- In the **Dell EMC Data Protection Restore Client**, FLR\v12nblr\flruser01

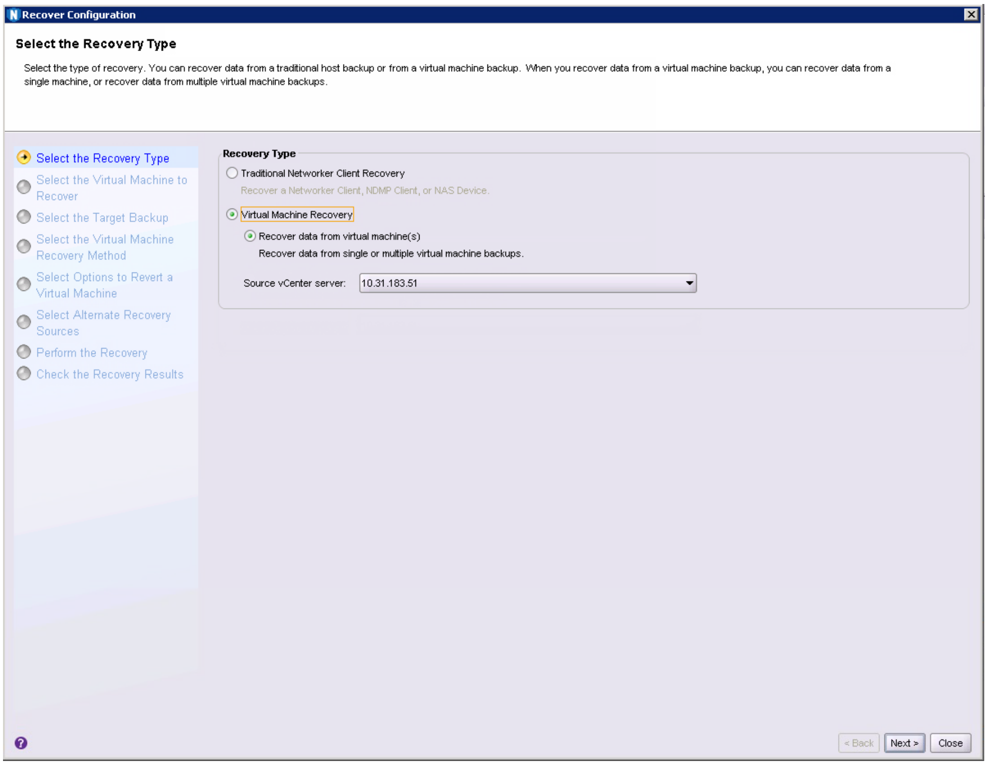
Results

You can now perform file level recovery in the **NetWorker Administration Recovery** wizard or the **Dell EMC Data Protection Restore Client** as a domain user.

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 40 Virtual machine recovery in the NMC Recovery wizard



Recover Configuration

Select the Recovery Type

Select the type of recovery. You can recover data from a traditional host backup or from a virtual machine backup. When you recover data from a virtual machine backup, you can recover data from a single machine, or recover data from multiple virtual machine backups.

Recovery Type

○ Traditional Networker Client Recovery

Recover a Networker Client, NDMP Client, or NAS Device.

● Virtual Machine Recovery

● Recover data from virtual machine(s)

Recover data from single or multiple virtual machine backups.

Source vCenter server: 10.31.183.51

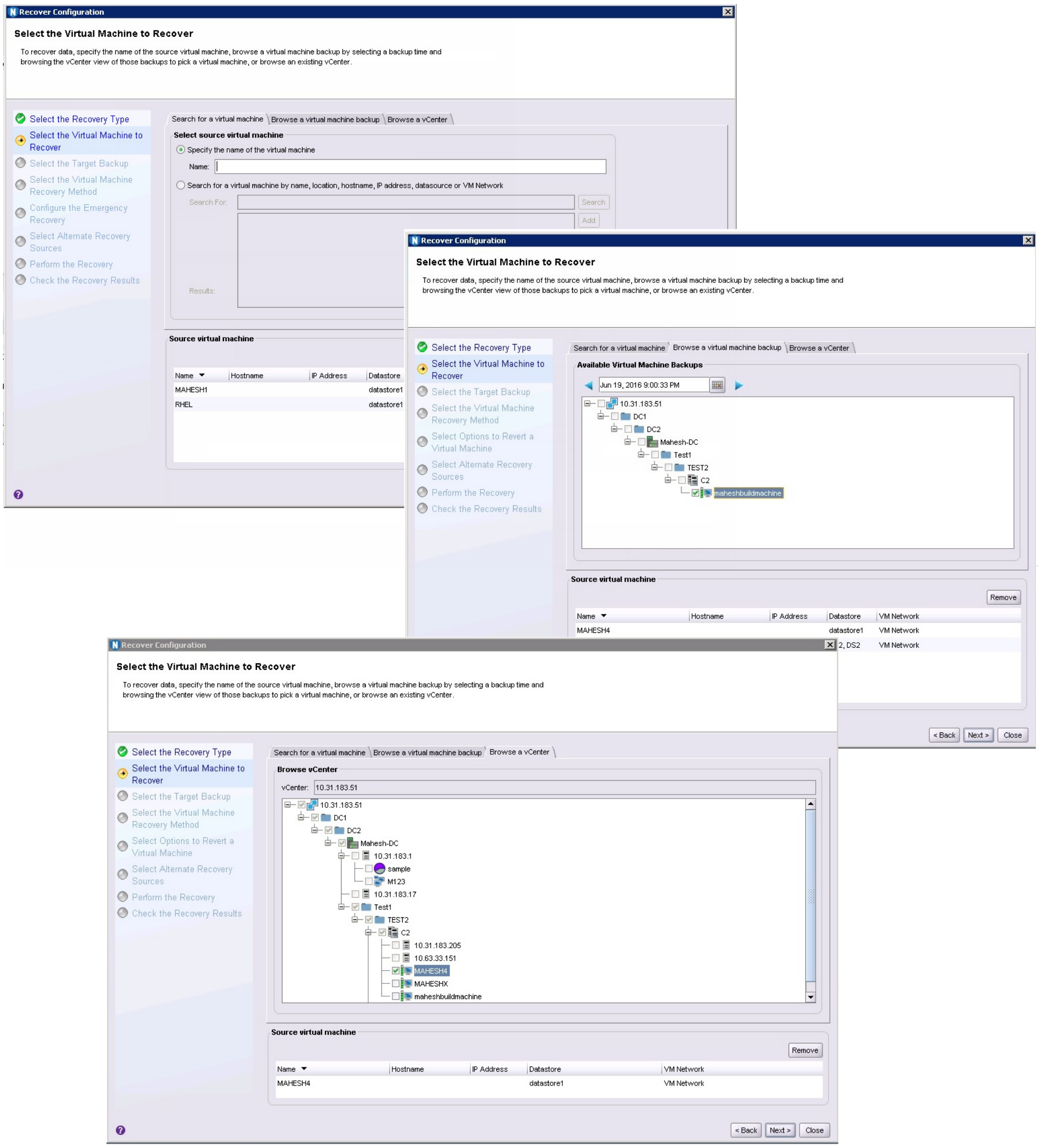
Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Select Options to Revert a Virtual Machine
Select Alternate Recovery Sources
Perform the Recovery
Check the Recovery Results
< Back
Next >
Close

After selecting the **Virtual Machine Recovery** type, you can perform recovery of individual virtual machines, or (for revert and virtual machine recovery options) recovery from multiple virtual machines.

Procedure

1. In the **Select the Recovery Type** page, select **Virtual Machine Recovery**, and then select a vCenter server to recover from using the **Source vCenter server** drop-down. Click **Next**.
2. In the **Select the Virtual Machine to Recover** page, enter the name of the source virtual machine(s) to recover from, or perform a search for the virtual machine. Additionally, you can use the tabs on this page to choose a single virtual machine or multiple virtual machines from a selected backup, or browse the source vCenter to determine the required virtual machine source. When you locate and choose the desired virtual machine(s), click **Next**.

Figure 41 Select the Virtual Machine to Recover



Recover Configuration

Select the Virtual Machine to Recover

To recover data, specify the name of the source virtual machine, browse a virtual machine backup by selecting a backup time and browsing the vCenter view of those backups to pick a virtual machine, or browse an existing vCenter.

- Select the Recovery Type
- Select the Virtual Machine to Recover
- Select the Target Backup
- Select the Virtual Machine Recovery Method
- Configure the Emergency Recovery
- Select Alternate Recovery Sources
- Perform the Recovery
- Check the Recovery Results

Search for a virtual machine | Browse a virtual machine backup | Browse a vCenter

Select source virtual machine

● Specify the name of the virtual machine

Name:

○ Search for a virtual machine by name, location, hostname, IP address, datasource or VM Network

Search For:

Results:

Source virtual machine

Name	Hostname	IP Address	Datastore
MAHESH1			datastore1
RHEL			datastore1

Recover Configuration

Select the Virtual Machine to Recover

To recover data, specify the name of the source virtual machine, browse a virtual machine backup by selecting a backup time and browsing the vCenter view of those backups to pick a virtual machine, or browse an existing vCenter.

- Select the Recovery Type
- Select the Virtual Machine to Recover
- Select the Target Backup
- Select the Virtual Machine Recovery Method
- Select Options to Revert a Virtual Machine
- Select Alternate Recovery Sources
- Perform the Recovery
- Check the Recovery Results

Search for a virtual machine | Browse a virtual machine backup | Browse a vCenter

Available Virtual Machine Backups

Jun 19, 2016 9:00:33 PM

Source virtual machine

Name	Hostname	IP Address	Datastore	VM Network
MAHESH4			datastore1	VM Network
			2, DS2	VM Network

Recover Configuration

Select the Virtual Machine to Recover

To recover data, specify the name of the source virtual machine, browse a virtual machine backup by selecting a backup time and browsing the vCenter view of those backups to pick a virtual machine, or browse an existing vCenter.

- Select the Recovery Type
- Select the Virtual Machine to Recover
- Select the Target Backup
- Select the Virtual Machine Recovery Method
- Select Options to Revert a Virtual Machine
- Select Alternate Recovery Sources
- Perform the Recovery
- Check the Recovery Results

Search for a virtual machine | Browse a virtual machine backup | Browse a vCenter

Browse vCenter

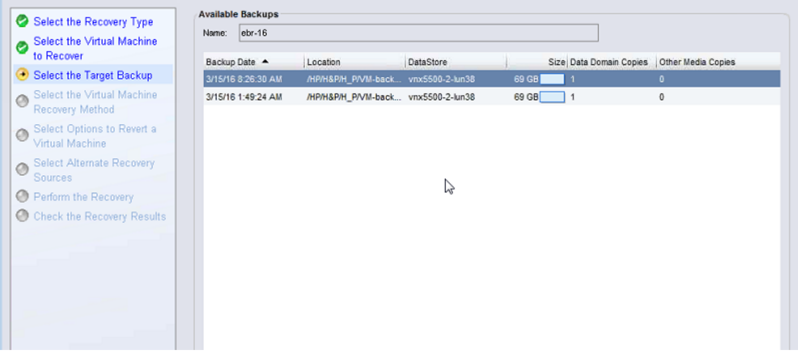
vCenter: 10.31.183.51

Source virtual machine

Name	Hostname	IP Address	Datastore	VM Network
MAHESH4			datastore1	VM Network

3. In the **Select the Target Backups** page, select the virtual machine backup(s) you want to restore from the **Available Backups** pane. This pane lists both primary backups and, if available, clone copies. If you selected recovery from multiple virtual machines, you can switch between virtual machines to browse each machine's available backups by using the **Virtual Machine Name** drop-down. Click **Next**.

Figure 42 Select the Target Backup (individual virtual machine)

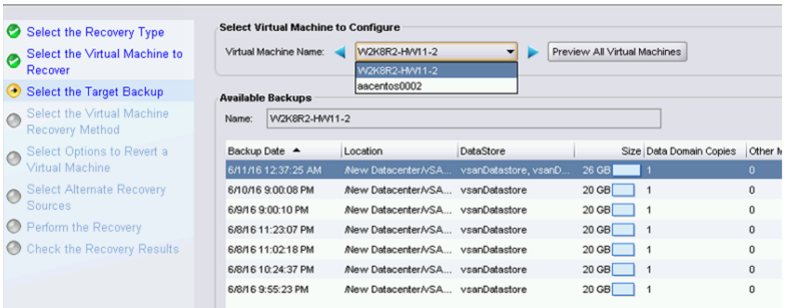

Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Select Options to Revert a Virtual Machine
Select Alternate Recovery Sources
Perform the Recovery
Check the Recovery Results

Available Backups

Name: ebr-16

Backup Date ▲	Location	DataStore	Size	Data Domain Copies	Other Media Copies
3/15/16 8:26:30 AM	/HP/H&P/H_P/VM-back...	vnx5500-2-lun38	69 GB	1	0
3/15/16 1:49:24 AM	/HP/H&P/H_P/VM-back...	vnx5500-2-lun38	69 GB	1	0

Figure 43 Select the Target Backup (multiple virtual machines)


Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Select Options to Revert a Virtual Machine
Select Alternate Recovery Sources
Perform the Recovery
Check the Recovery Results
Preview All Virtual Machines
W2K8R2-HW11-2
aacentos0002

Select Virtual Machine to Configure

Virtual Machine Name: W2K8R2-HW11-2

Available Backups

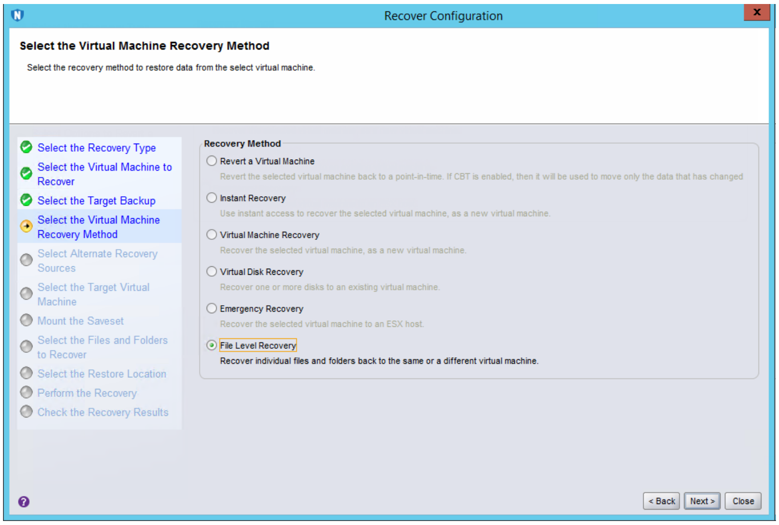
Name: W2K8R2-HW11-2

Backup Date ▲	Location	DataStore	Size	Data Domain Copies	Other M
6/11/16 12:37:25 AM	/New Datacenter/VSA...	vsanDatastore, vsanD...	26 GB	1	0
6/10/16 9:00:08 PM	/New Datacenter/VSA...	vsanDatastore	20 GB	1	0
6/9/16 9:00:10 PM	/New Datacenter/VSA...	vsanDatastore	20 GB	1	0
6/8/16 11:23:07 PM	/New Datacenter/VSA...	vsanDatastore	20 GB	1	0
6/8/16 11:02:18 PM	/New Datacenter/VSA...	vsanDatastore	20 GB	1	0
6/8/16 10:24:37 PM	/New Datacenter/VSA...	vsanDatastore	20 GB	1	0
6/8/16 9:55:23 PM	/New Datacenter/VSA...	vsanDatastore	20 GB	1	0

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 44 Select the Virtual Machine Recovery method


Recover Configuration
Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Select Alternate Recovery Sources
Select the Target Virtual Machine
Mount the Saveset
Select the Files and Folders to Recover
Select the Restore Location
Perform the Recovery
Check the Recovery Results
< Back
Next >
Close

Select the Virtual Machine Recovery Method

Select the recovery method to restore data from the select virtual machine.

Recovery Method

○ Revert a Virtual Machine
Revert the selected virtual machine back to a point-in-time. If CBT is enabled, then it will be used to move only the data that has changed

○ Instant Recovery
Use instant access to recover the selected virtual machine, as a new virtual machine.

○ Virtual Machine Recovery
Recover the selected virtual machine, as a new virtual machine.

○ Virtual Disk Recovery
Recover one or more disks to an existing virtual machine.

○ Emergency Recovery
Recover the selected virtual machine to an ESX host.

● File Level Recovery
Recover individual files and folders back to the same or a different virtual machine.

Results

Subsequent wizard options change based on the recovery option selected, as described in the following sections.

Revert (or rollback) a virtual machine backup

The first virtual machine recovery option available in the NMC Recovery wizard is to revert, or rollback, a virtual machine backup. With a Revert a virtual machine backup recovery, you use an existing virtual machine to rollback the VMDKs as a virtual machine.

Note

When you revert a virtual machine, the current virtual machine is removed in the process. You cannot use the **Revert a Virtual Machine** recovery option when the ESXi has been removed from the vCenter and then added back to the vCenter. In this case, use the **Virtual Machine recovery** option instead.

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

Procedure

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

   a. Select **Revert a Virtual Machine**.

   b. Click **Next**.

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

2. In the **Revert Type** pane of the **Select Options to Revert a Virtual Machine** page:

   a. Select **Revert both VM configuration and data** to revert both the configuration information (such as operating system, virtual machine size) and data for a virtual machine. When you select this revert type, the **Delete existing disk on disk configuration mismatch** option appears in the **Revert Options** pane to allow you to overwrite an existing disk if a configuration mismatch occurs.

   b. Select **Revert VM Data Only** to revert only the virtual machine data without changing the virtual machine configuration.

3. In the **Revert Options** pane of the **Select Options to Revert a Virtual Machine** page, choose from the following options

   a. Select **Revert all disks on this virtual machine** to rollback all VMDKs, or select **Revert one or more disks only** and then select a specific disk drive to rollback only that disk.

   b. Select the **Power on virtual machine** checkbox to power on the virtual machine after the restore.

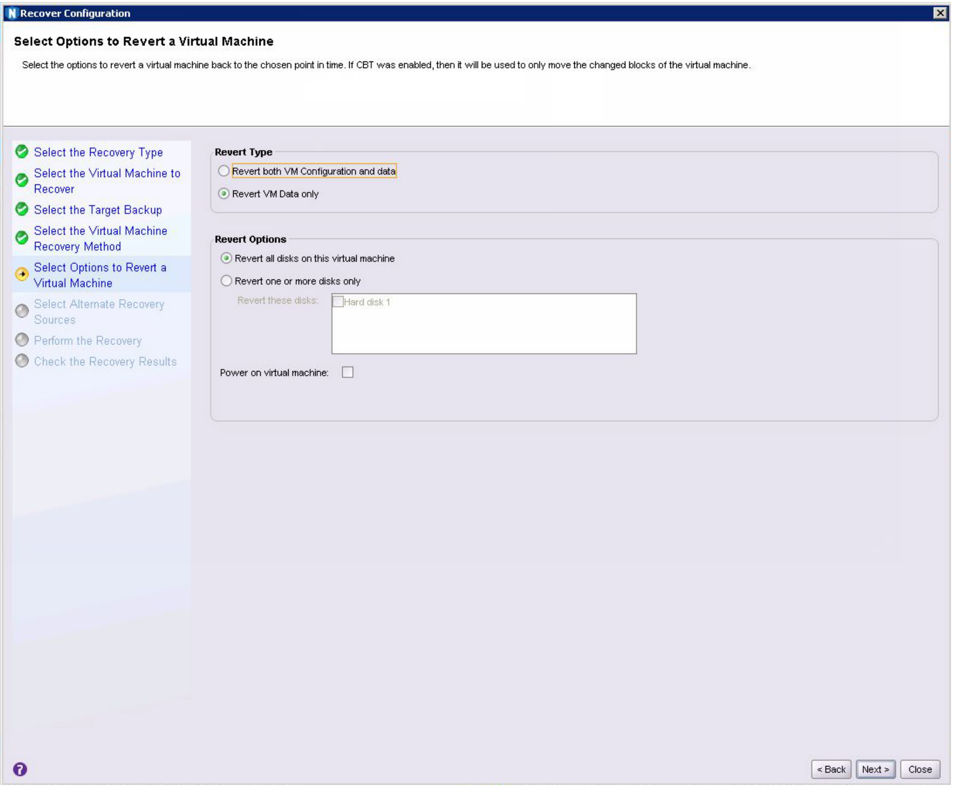
   c. Select **Delete existing disk on disk configuration mismatch** if you want to be presented with the option of deleting the existing disk if a disk configuration mismatch is detected. Note that this option only appears when you select the **Revert both VM configuration and data** revert type in step two.

   d. Click **Next**.

Note

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

Figure 45 Choose Disks to Revert



Recover Configuration

Select Options to Revert a Virtual Machine

Select the options to revert a virtual machine back to the chosen point in time. If CBT was enabled, then it will be used to only move the changed blocks of the virtual machine.

Revert Type

○ Revert both VM Configuration and data

● Revert VM Data only

Revert Options

● Revert all disks on this virtual machine

○ Revert one or more disks only

Revert these disks: □ Hard disk 1

Power on virtual machine: □

Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Select Options to Revert a Virtual Machine
Select Alternate Recovery Sources
Perform the Recovery
Check the Recovery Results
< Back
Next >
Close

Note

The entire VMDK will be rolled back unless you have CBT enabled, in which case only the changed blocks will be moved.

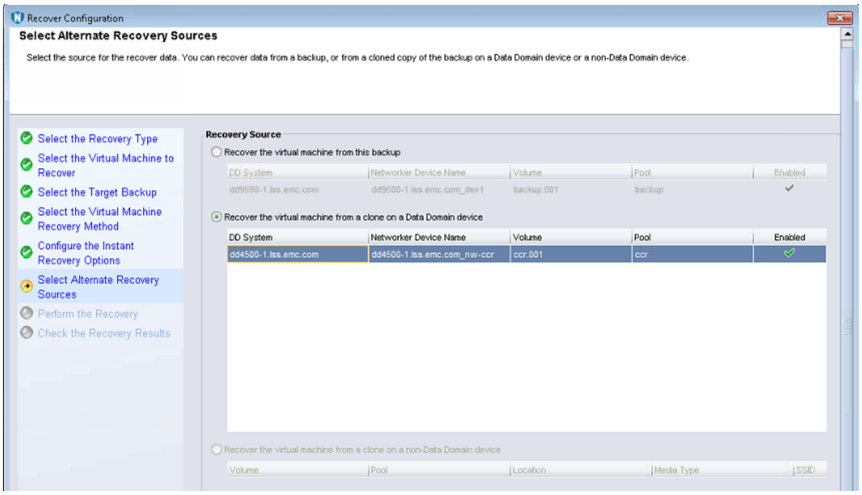
4. In the **Select Alternate Recovery Sources** page:

   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 46 Select Alternate Recovery Sources



Recover Configuration

Select Alternate Recovery Sources

Select the source for the recover data. You can recover data from a backup, or from a cloned copy of the backup on a Data Domain device or a non-Data Domain device.

- ✓ Select the Recovery Type
- ✓ Select the Virtual Machine to Recover
- ✓ Select the Target Backup
- ✓ Select the Virtual Machine Recovery Method
- ✓ Configure the Instant Recovery Options
- Select Alternate Recovery Sources
- Perform the Recovery
- Check the Recovery Results

Recovery Source

○ Recover the virtual machine from this backup

DD System	Networker Device Name	Volume	Pool	Enabled
dd9500-1.lss.emc.com	dd9500-1.lss.emc.com_dev1	backup.001	backup	✓

● Recover the virtual machine from a clone on a Data Domain device

DD System	Networker Device Name	Volume	Pool	Enabled
dd4500-1.lss.emc.com	dd4500-1.lss.emc.com_nw-ccr	ccr.001	ccr	✓

○ Recover the virtual machine from a clone on a non-Data Domain device

Volume	Pool	Location	Media Type	SSID

5. In the **Perform the Recovery** page:

   a. Specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct.

   b. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the reversion is complete.

Instant Recovery of a virtual machine

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

Before you begin

Before you begin, make note of the following:

- For the Data Domain resource, ensure that you provide the management credentials and, if required, enter the export path appropriately.
- Ensure that the free space on the Data Domain system is equal to or greater than the total disk size of the virtual machine being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target virtual machine fails.
- Ensure that you have at least one proxy that is not restricted to a specific datastore. For the vProxy, select **Properties** and then select **Configuration**, and verify that datastores is left blank.
- Do not perform an instant recovery of virtual machines in resource pools and other similar containers that are part of a currently running protection group.

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

Procedure

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

   a. Select **Instant Recovery**.

   b. Click **Next**.

2. In the **Configure the Instant Recovery Options** page:

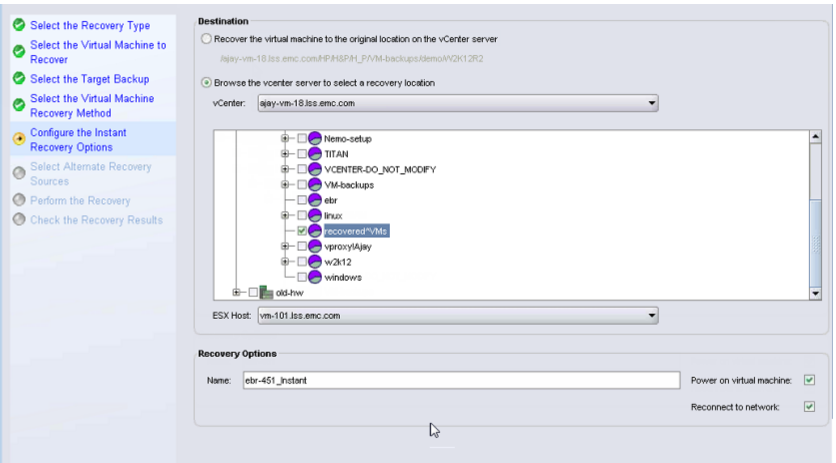
   a. Select the location where you want to restore the virtual machine in the vCenter environment.

      This does not have to be the original location, and can also be on a different vCenter server.

   b. Ensure that you select the **Power on virtual machine** and **Reconnect to network** options.

   c. Click **Next**.

   Figure 47 Configure the Instant Recovery

   
Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Configure the Instant Recovery Options
Select Alternate Recovery Sources
Perform the Recovery
Check the Recovery Results

   Destination

   ○ Recover the virtual machine to the original location on the vCenter server

   /ajay-vm-18.lss.emc.com/HP/H&P/H_P/VM-backups/demo/W2K12R2

   ● Browse the vcenter server to select a recovery location

   vCenter: ajay-vm-18.lss.emc.com

   □ Nemo-setup
   □ TITAN
   □ VCENTER-DO_NOT_MODIFY
   □ VM-backups
   □ ebr
   □ linux
   ☑ recovered^VMs
   □ vproxy!Ajay
   □ w2k12
   □ windows
   □ old-hw

   ESX Host: vm-101.lss.emc.com

   Recovery Options

   Name: ebr-451_Instant

   Power on virtual machine: ☑

   Reconnect to network: ☑

3. In the **Select Alternate Recovery Sources** page:

   a. Select the original backup, or a clone copy if one is available.

   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the DD Boost clone pool.

   c. Click **Next**.

4. In the **Perform the Recovery** page:

   a. Specify a name for the recovery.

   b. Check the summary at the bottom of the page to ensure all the details are correct.

   c. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the instant recovery is complete. When the instant recovery is complete and ready for use, you can then storage vMotion the virtual machine to a datastore, or perform a file level recovery to the target file system, and then stop the completed instant recovery to free up those resources.
To stop an instant recovery in NMC:

1. Navigate to the **Recover** window.
2. Right-click the entry for the recovery within the Recover sessions pane.
3. Select **Stop** from the drop-down.

Note

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

Virtual machine recovery

The next virtual machine recovery option available in the NMC Recovery wizard is to perform a recovery of a virtual machine backed up with the vProxy Appliance to a new virtual machine.

Note

Recoveries of virtual machines backed up with the VMware Backup Appliance should still be performed with the **EMC Backup and Recovery** user interface in the **vSphere Web Client**.

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

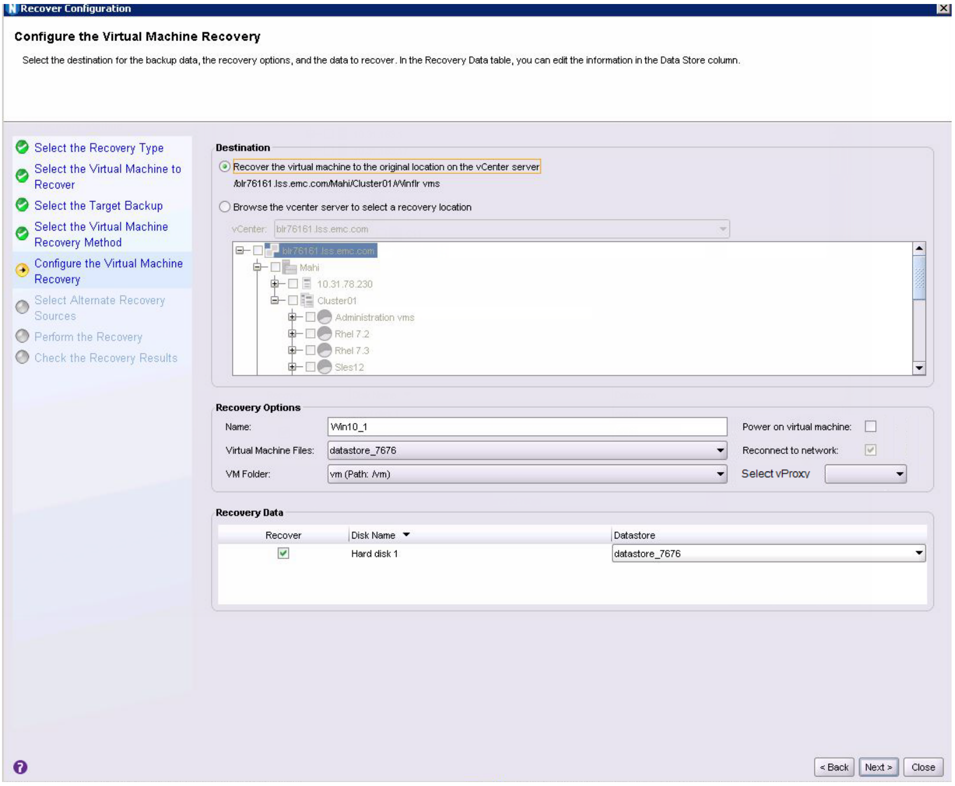
Procedure

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

   b. Click **Next**.
2. In the **Configure the Virtual Machine Recovery** page, select the location where you want to restore the virtual machine in the vCenter environment
   a. In the **Destination** pane, select the option to recover the new virtual machine to the original location, or browse to select a new location on the same vCenter server or a different vCenter server.

   b. In the **Recovery Options** pane, choose a vProxy for the virtual machine recovery from the **Select vProxy** drop-down, specify the name of the new virtual machine, and then optionally select the virtual machine file datastore and folder where you want to recover the files. You can recover the virtual machine to a Blue folder by using the **VM Folder** drop-down, as shown in the following figure. The folder can be the default folder, or a new folder.

Figure 48 Configure the virtual machine recovery



Recover Configuration

Configure the Virtual Machine Recovery

Select the destination for the backup data, the recovery options, and the data to recover. In the Recovery Data table, you can edit the information in the Data Store column.

Destination

● Recover the virtual machine to the original location on the vCenter server

/blr76161.lss.emc.com/Mahi/Cluster01/Winflr vms

○ Browse the vcenter server to select a recovery location

vCenter: blr76161.lss.emc.com

Recovery Options

Name: Win10_1

Virtual Machine Files: datastore_7676

VM Folder: vm (Path: /vm)

Power on virtual machine: □

Reconnect to network: ☑

Select vProxy

Recovery Data

Recover	Disk Name	Datastore
☑	Hard disk 1	datastore_7676

Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Configure the Virtual Machine Recovery
Select Alternate Recovery Sources
Perform the Recovery
Check the Recovery Results
blr76161.lss.emc.com
Mahi
10.31.78.230
Cluster01
Administration vms
Rhel 7.2
Rhel 7.3
Sles12
< Back
Next >
Close

If you have a single disks, or multiple disks with multiple datastores, you can perform the following:

- Choose to recover a collection of all the available hard drives.
- Select a different datastore than the original datastore.
- Select a different datatore for each disk you want to recover.
- Specify the datastore where the virtual machine configuration files reside.

Optionally, select the **Power on virtual machine** and **Reconnect to network** options to power on and reconnect after the recovery, and then click **Next**.

3. In the **Select Alternate Recovery Sources** page:

   a. Select the original virtual machine backup, or a clone copy if one is available.

   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the staging pool.

   c. Click **Next**.

Note

If selecting a clone from **Select Alternate Recovery Sources**, additionally review the "Selecting alternate recovery sources" section.

---

4. In the **Perform the Recovery** page:

   a. Specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct.

   b. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the virtual machine recovery is complete.

Virtual Disk Recovery

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

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

Procedure

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

   a. Select **Virtual Disk Recovery**.

   b. Click **Next**.

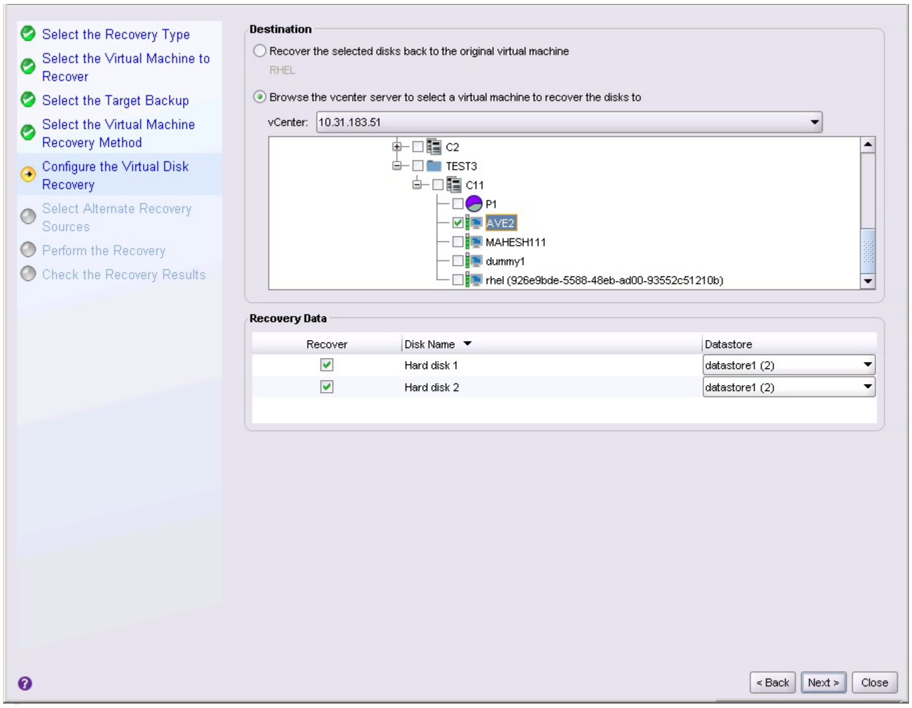
2. In the **Configure the Virtual Disk Recovery** page:

   a. Select the virtual machine where you want to restore the VMDKs. This can be the original virtual machine, or another existing virtual machine.

   b. Select the desired disks from the **Recovery Data** pane, and select a datastore.

   c. Click **Next**.

Figure 49 Configure the Virtual Disk Recovery


Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Configure the Virtual Disk Recovery
Select Alternate Recovery Sources
Perform the Recovery
Check the Recovery Results
C2
TEST3
C11
P1
AVE2
MAHESH111
dummy1
rhel (926e9bde-5588-48eb-ad00-93552c51210b)
< Back
Next >
Close

Destination

○ Recover the selected disks back to the original virtual machine
RHEL

● Browse the vcenter server to select a virtual machine to recover the disks to

vCenter: 10.31.183.51

Recovery Data

Recover	Disk Name	Datastore
☑	Hard disk 1	datastore1 (2)
☑	Hard disk 2	datastore1 (2)

3. In the **Select Alternate Recovery Sources** page:

   a. Select the original virtual disk backup, or a clone copy if one is available.

   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the staging pool.

   c. Click **Next**.

4. In the **Perform the Recovery** page:

   a. Specify a name for the recovery.

   b. Check the summary at the bottom of the page to ensure all the details are correct.

   c. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the disk recovery is complete.

Note

When you start a VMDK recovery, the virtual machine will be powered off automatically without issuing a warning message.

Emergency Recovery

The next virtual machine recovery option available in the NMC Recovery wizard is an Emergency Recovery. An Emergency Recovery is required when you need to restore the virtual machine to an ESXi host.

Before you begin

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

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

Note

During an Emergency Recovery, the vProxy gets associated with the ESXi host and is unavailable for other operations on the vCenter server. Wait until the recovery completes before initiating any other operations on the vProxy.

To complete the Recovery wizard with the Emergency Recovery method, perform the following:

Procedure

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

   a. Select **Emergency Recovery**.

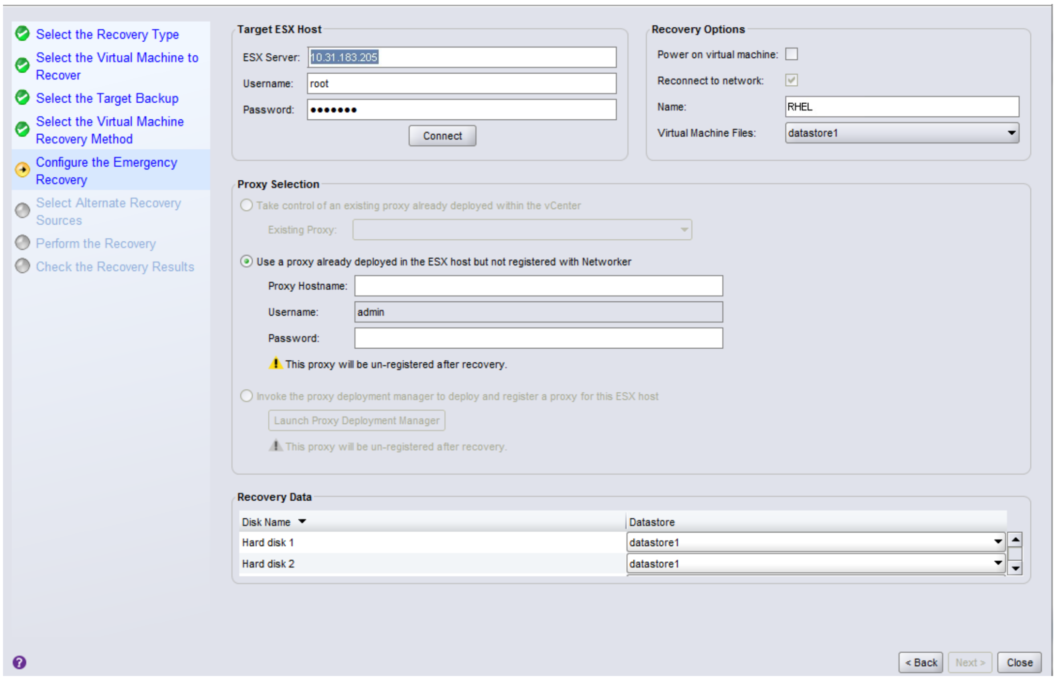
   b. Click **Next**.

2. In the **Configure the Emergency Recovery** page:

   a. Specify the target ESXi server in the vCenter environment.

   b. Click **Connect**.

Figure 50 Configure the Emergency Recovery


Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Configure the Emergency Recovery
Select Alternate Recovery Sources
Perform the Recovery
Check the Recovery Results
Connect
Launch Proxy Deployment Manager
< Back
Next >
Close

Target ESX Host

ESX Server: 10.31.183.205

Username: root

Password: •••••••

Recovery Options

Power on virtual machine: □

Reconnect to network: ☑

Name: RHEL

Virtual Machine Files: datastore1

Proxy Selection

○ Take control of an existing proxy already deployed within the vCenter

Existing Proxy:

● Use a proxy already deployed in the ESX host but not registered with Networker

Proxy Hostname:

Username: admin

Password:

⚠ This proxy will be un-registered after recovery.

○ Invoke the proxy deployment manager to deploy and register a proxy for this ESX host

⚠ This proxy will be un-registered after recovery.

Recovery Data

Disk Name	Datastore
Hard disk 1	datastore1
Hard disk 2	datastore1

The **Proxy Selection** and **Recovery Data** panes get populated with the ESXi server details.

3. In the **Proxy Selection** pane, if a proxy is not discovered, add a new proxy which is deployed in vCenter but not added to NetWorker.
4. For the disks in the **Recovery Data** pane:

   a. Select a datastore.

   b. Optionally, select the **Power on virtual machine** and **Reconnect to network** options.

   c. Click **Next**.
5. In the **Select Alternate Recovery Sources** page:

   a. Select the original disk backup, or a clone copy if one is available.

   b. If recovering from a clone that is not on a Data Domain device, or recovering from a Data Domain Cloud Tier device, specify the staging pool.
6. In the **Perform the Recovery** page:

   a. Specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct.

   b. Click **Run Recovery**.

Results

The **Check the Recovery Results** page will display a progress bar with the duration of the recovery, and a log file entry when the Emergency Recovery is complete.

Note

The progress bar may not update correctly when you perform an Emergency Recovery directly to the ESXi host.

File Level recovery (Admin mode only)

The final virtual machine recovery option available in the NMC Recovery wizard is File Level recovery. With file level recovery, you can recover individual files from backups of virtual machines or VMDKs to a primary or secondary vCenter server, and for application-consistent backups, you can also restore the transaction log from Data Domain to the SQL database.

Before you begin

NetWorker only supports file level recovery operations from a primary or cloned backup if the save set is on a Data Domain device. If a cloned backup does not exist on the Data Domain device, you must manually clone a save set from the tape device to Data Domain before launching the **Recovery** wizard.

For the Data Domain resource, ensure that you provide the management credentials and, if required, type the export path appropriately. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only) provides detailed steps.

Additionally, if recovering to a virtual machine on a secondary vCenter, ensure that a vProxy appliance has been deployed on the secondary vCenter server and configured with the NetWorker server.

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

Note

For file-level recovery of high-density file systems (more than few hundred files/ folders), it is recommended to use either the **NetWorker Management Web UI** or the **Dell EMC Data Protection Restore Client** (User or Admin mode, as applicable) instead of the NMC **Recovery** wizard.

To complete the Recovery wizard with the file level recovery method, perform the following:

Procedure

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

   a. Select **File Level recovery**.

   b. Click **Next**.

2. In the **Select Alternate Recovery Sources** page:

   a. Select the primary backup to recover from, or select the **Recover the Virtual machine from a clone on a Data Domain device** option.

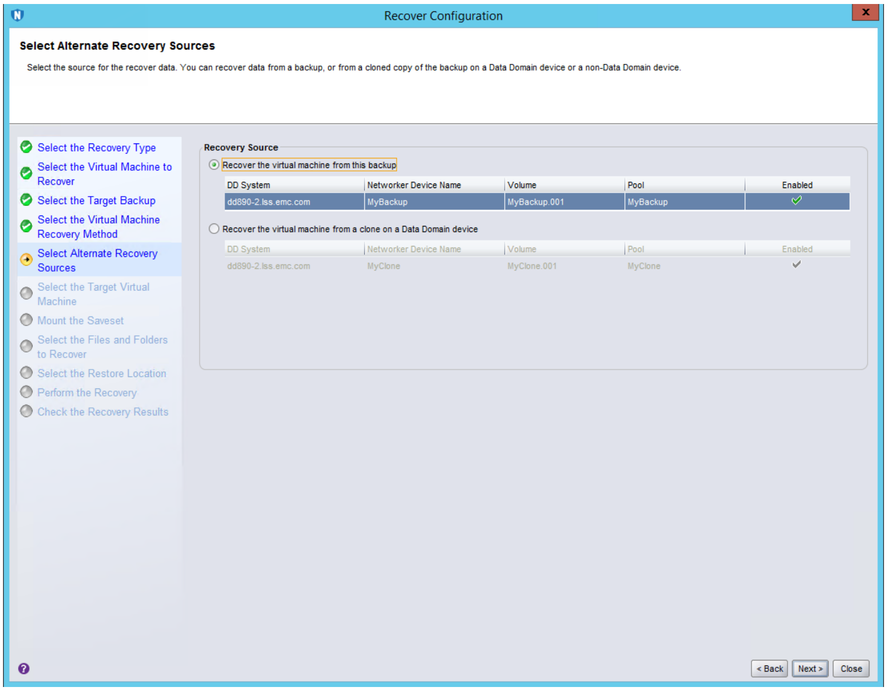
   b. Select the clone copy that you want to recover files from.

   c. Click **Next**.

   Note

   If selecting a clone from **Select Alternate Recovery Sources**, additionally review the section "Selecting alternate recovery sources".

Figure 51 Select Alternate Recovery Sources for file level recovery



Recover Configuration
Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Select Alternate Recovery Sources
Select the Target Virtual Machine
Mount the Saveset
Select the Files and Folders to Recover
Select the Restore Location
Perform the Recovery
Check the Recovery Results
< Back
Next >
Close

Select Alternate Recovery Sources

Select the source for the recover data. You can recover data from a backup, or from a cloned copy of the backup on a Data Domain device or a non-Data Domain device.

Recovery Source

● Recover the virtual machine from this backup

DD System	Networker Device Name	Volume	Pool	Enabled
dd890-2.lss.emc.com	MyBackup	MyBackup.001	MyBackup	✓

○ Recover the virtual machine from a clone on a Data Domain device

DD System	Networker Device Name	Volume	Pool	Enabled
dd890-2.lss.emc.com	MyClone	MyClone.001	MyClone	✓

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.

---

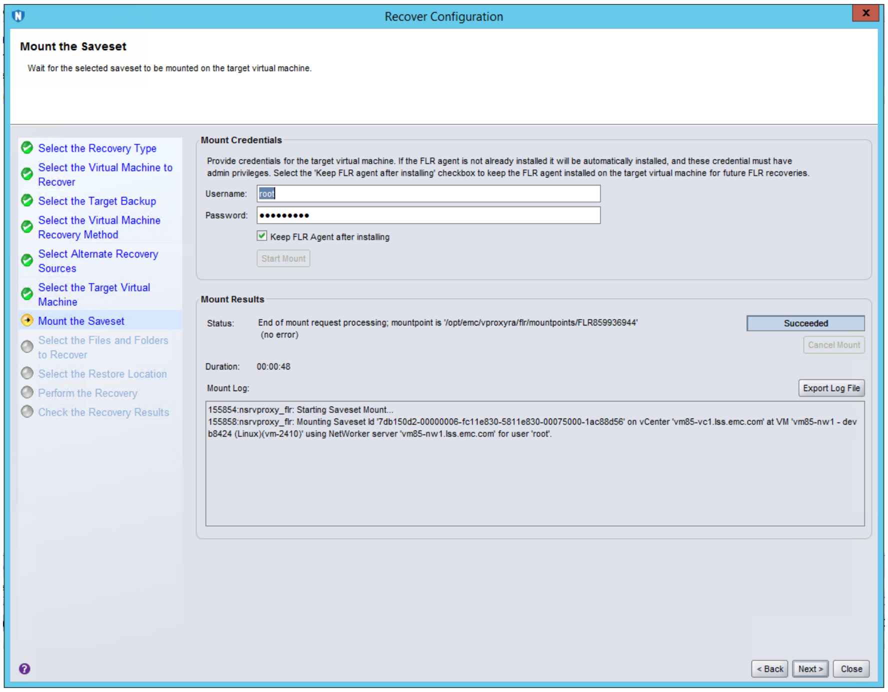
4. In the **Mount The Saveset** page:

   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 52 Mount the save set for file level recovery


Recover Configuration
Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Select Alternate Recovery Sources
Select the Target Virtual Machine
Mount the Saveset
Select the Files and Folders to Recover
Select the Restore Location
Perform the Recovery
Check the Recovery Results
Start Mount
Cancel Mount
Export Log File
< Back
Next >
Close

Mount the Saveset

Wait for the selected saveset to be mounted on the target virtual machine.

Mount Credentials

Provide credentials for the target virtual machine. If the FLR agent is not already installed it will be automatically installed, and these credential must have admin privileges. Select the 'Keep FLR agent after installing' checkbox to keep the FLR agent installed on the target virtual machine for future FLR recoveries.

Username: root

Password: •••••••••

☑ Keep FLR Agent after installing

Mount Results

Status: End of mount request processing; mountpoint is '/opt/emc/vproxyra/flr/mountpoints/FLR859936944' (no error) Succeeded

Duration: 00:00:48

Mount Log:

```
155854:nsrvproxy_flr: Starting Saveset Mount...
155858:nsrvproxy_flr: Mounting Saveset Id '7db150d2-00000006-fc11e830-5811e830-00075000-1ac88d56' on vCenter 'vm85-vc1.lss.emc.com' at VM 'vm85-nw1 - dev
b8424 (Linux)(vm-2410)' using NetWorker server 'vm85-nw1.lss.emc.com' for user 'root'.
```

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

Note

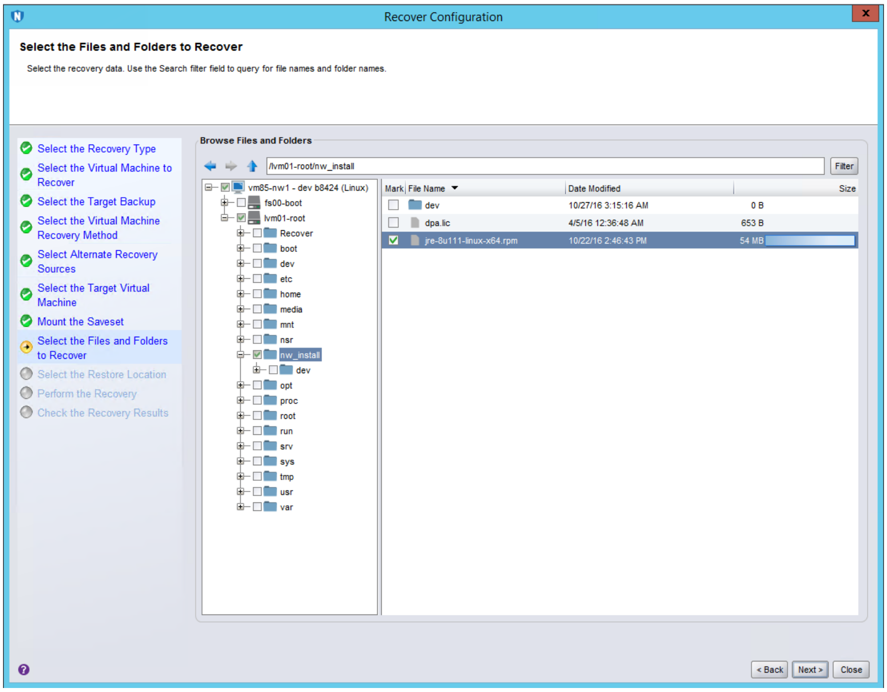
This user should have privileges to install the **FLR Agent**, which is required to perform file level recovery. For Linux virtual machines, this requires the root user account.

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 53 Select the files and folders to recover



Recover Configuration

Select the Files and Folders to Recover

Select the recovery data. Use the Search filter field to query for file names and folder names.

Browse Files and Folders

/lvm01-root/nw_install

Mark	File Name	Date Modified	Size
□	dev	10/27/16 3:15:16 AM	0 B
□	dpa.lic	4/5/16 12:36:48 AM	653 B
☑	jre-8u111-linux-x64.rpm	10/22/16 2:46:43 PM	54 MB

Select the Recovery Type
Select the Virtual Machine to Recover
Select the Target Backup
Select the Virtual Machine Recovery Method
Select Alternate Recovery Sources
Select the Target Virtual Machine
Mount the Saveset
Select the Files and Folders to Recover
Select the Restore Location
Perform the Recovery
Check the Recovery Results
Filter
vm85-nw1 - dev b8424 (Linux)
fs00-boot
lvm01-root
Recover
boot
dev
etc
home
media
mnt
nsr
nw_install
dev
opt
proc
root
run
srv
sys
tmp
usr
var
< Back
Next >
Close

6. In the **Select the Restore Location** page:

   a. Select the folder that you want to recover the files to, or create a folder.

   b. Click **Next**.

   Note

   NetWorker does not currently support creating folders with spaces in the folder name.

   ---

7. In the **Perform the Recovery** page:

   a. Specify a name for the recovery.

   b. To ensure all the details are correct, check the summary at the bottom of the page

   c. Click **Run Recovery**.

Results

The **Check the Recovery Results** page displays the duration of the recovery, and a log file entry when the file level recovery is complete.

Selecting alternate recovery sources in the NMC Recovery wizard

The NMC Recovery wizard contains a step for each virtual machine recovery method where you can select an alternate source to recover from, for example, a clone copy on a Data Domain or non-Data Domain device. If the primary source is present, it is recommended that you recover from the primary source. However, if both the primary source and clone copies are present and enabled and you want to recover from a clone copy, perform the following.

Procedure

1. In the **Select Alternative Recovery Sources** page, select the clone you want to recover from, either a clone on a Data Domain device or non-Data Domain device.

   Additionally, make note of the name indicated in the **Volume** column for all of the volumes you do not want to recover from, as you will require this information in steps 5 and 6.

2. Click **Close** to display the **Save Progress** dialog, and then specify a name for the recover and click **Save** to save your progress.
3. In the NMC **Administration** window, click **Devices** to display the **Devices** window.
4. In the left navigation pane, select **Devices**. The list of devices displays in the right pane.
5. For each volume you do not want to recover from that you made note of in step 1, locate the corresponding device, and make note of that device name.
6. For each device you identify as corresponding with those volumes, right-click the device and select **Unmount** from the drop-down, and then also select **Disable** from the drop-down.

   Note

   Ensure that no backups are currently running to these devices prior to unmounting.

7. In the NMC **Administration** window, click **Recover** to display the **Recover** window, and locate the saved recovery
8. Right-click the saved recovery and select Open Recover.

   The Recovery wizard re-opens on the **Select Alternative Recovery Sources** page.

9. In the **Recovery Source** pane of the **Select Alternative Recovery Sources** page, select either **Recover the virtual machine from a clone on a Data Domain device**, or **Recover the virtual machine from a clone on a non-Data Domain device**. Click **Next**.

   Note

   If you want to recover from a clone on a non-Data Domain device, manually change the staging pool to a different pool, and ensure that your selected pool does not already contain copies for this backup. If the primary source is present and you select a clone to recover from using the same staging pool that contains the existing copy, the recovery may become unresponsive.

10. In the **Perform the Recovery** page, specify a name for the recovery and check the summary at the bottom of the page to ensure all the details are correct. Click **Run Recovery**.

    The **Check the Recovery Results** page will display the duration of the recovery, and a log file entry when the recovery is complete.

11. In the NMC **Administration** window, click **Devices** to return to the **Devices** window, and in the left navigation pane, select **Devices** to display the list of devices in the right pane.

12. For each device that you unmounted and disabled in step 6, right-click the device and select **Enable** from the drop-down, and then select **Mount** from the drop-down.

Monitoring and verifying Virtual Machine recoveries

After selecting Run Recovery to complete the Recovery wizard, there are multiple ways you can monitor the progress of the virtual machine recovery, and then verify when the recovery is complete.

NMC Recover and Monitoring windows

To monitor the progress of the virtual machine recovery, use the **Recover sessions** pane in the **Monitoring** window, or the **Currently Running** pane of the **Recover** window.

To verify that the virtual machine recovery is complete, use the **Configured Recovers** pane in the **Recover** window.

Check the Recovery results in the NMC Recovery wizard

The final step of the **Recovery** wizard also allows you to check the recovery results. Upon completion of the virtual machine recovery, an entry for the log file appears in the **Recovery log** pane. Click **Export log** to save and view the log file.

Recovery configuration information storage

When you create a recover configuration by using the Recovery wizard, NetWorker saves the configuration information in an NSR recover resource in the resource database of the NetWorker server. NetWorker uses the information in the NSR recover resource to perform the recover job operation.

When a recover job operation starts, NetWorker stores:

- Details about the job in the nsrjobsd database.
- Output sent to stderr and stdout in a recover log file. NetWorker creates one log file for each recover job.

  NOTICE

  NetWorker removes the recover log file and the job information from the job database based on value of the *Jobsdb retention in hours* attribute in the properties of the NetWorker server resource. The default jobsdb retention is 72 hours.

vProxy recovery in the NetWorker Management Web UI

The NetWorker Management Web UI contains the same vProxy recovery functionality that is available in the **NetWorker Management Console** through the **Recovery** wizard, including support for all image-level recovery types and file-level recovery.

When logged in to the NetWorker Management Web UI, the landing page displays options for **Monitoring**, **Protection**, and **Recovery** in the left pane. If not already selected, select **Recover**, and then select **VMware Recovery**.

In the **VMware Recovery** window's **Select vCenter** drop-down, choose the vCenter server that contains the virtual machines or objects that you want to recover. Then, select **List and Search** to view only the available virtual machine backups, or **Browse vCenter** to navigate to the location within the vCenter that contains the virtual machine or objects that you want to recover. When you select an item, the backup details display in a table within the right pane. You can choose to display hidden columns such as the virtual machine UUID by clicking the blue icon in the lower left corner of the table.

From the **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down to choose from one of the image-level recovery types available, or file level recovery. Additionally, ensure that you specify the correct time range of the backup(s) that you want to recover.

Revert (or rollback) a virtual machine backup

Select **Revert** to rollback one or more virtual machine disks (VMDKs) as a virtual machine to the original virtual machine. Additionally, you can rollback the virtual machine configuration.

Note

You cannot use the **Revert** recovery type when the ESXi has been removed from the vCenter and then added back to the vCenter. In this case, use the **Virtual Machine recovery** method instead.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **Revert**.

   The **Recover** wizard launches.
3. In the **Configuration** page:

   a. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.

   b. Select **Power On** to power on the virtual machine after the recovery completes.

   Note

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

   c. Select **Revert VM configuration** to restore the virtual machine with the same configuration details used at the time of backup. Additionally, select the **Delete existing disk on config mismatch** option if you want to continue with the removal of the existing disk if the configuration details do not match. If you do not select **Revert VM configuration**, the recovery will revert only the virtual machine data without changing the virtual machine configuration.

   d. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

   e. Click **Next**.

   The **Disk Selection** page displays
4. In the **Disk Selection** page, choose one or more of the available hard disks, and then click **Next**.

Note

The entire VMDK will be rolled back unless you have CBT enabled, in which case only the changed blocks will be moved.

The **Summary** page displays.

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

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Recover to a new virtual machine

Select **New Virtual Machine** to recover a virtual machine backed up with the vProxy appliance to a new virtual machine.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **New Virtual Machine**.

   The **Recover** wizard launches.
3. In the **Configuration** page:

   a. From the **Destination vCenter** drop-down, select a different destination vCenter server if required, or leave the default selection of the same vCenter server.

   b. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.

   c. In the **Virtual Machine Name** field, specify the name of the new virtual machine.

   d. Select **Power On** to power on the virtual machine after the recovery completes.

   e. Select **Reconnect NIC** to reconnect the network interface card after the recovery completes.

   f. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

   g. Click **Next**.

   The **Destination Location** page displays.
4. In the **Destination Location** page, select the location where you want to recover the virtual machine. If the target location contains a specific folder that you need to select, select the desired folder from the **VM Folder** drop-down. Click **Next**.

   The **Disk Selection** page displays.
5. In the **Disk Selection** page, 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. Additionally, you can use the **VM**

Configuration Files drop-down to select the datastore where the virtual machine configuration files will reside. Click **Next**.

Note

The entire VMDK will be rolled back unless you have CBT enabled, in which case only the changed blocks will be moved.

The **Summary** page displays.

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

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Instant Restore of a virtual machine

When you select **Instant Restore**, the virtual machine backup is read directly from the Data Domain device and the VMDKs will be restored directly on a Data Domain device. You can perform one instant recovery session at a time.

Before you begin

Before you begin, make note of the following:

- For the Data Domain resource, ensure that you provide the management credentials and, if required, enter the export path appropriately.
- Ensure that the free space on the Data Domain system is equal to or greater than the total disk size of the virtual machine being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target virtual machine fails.
- Ensure that you have at least one proxy that is not restricted to a specific datastore. For the vProxy, select **Properties** and then select **Configuration**, and verify that datastores is left blank.
- Do not perform an instant recovery of virtual machines in resource pools and other similar containers that are part of a currently running protection group.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **Instant Restore**.

   The **Recover** wizard launches.
3. In the **Configuration** page:

   a. From the **Destination vCenter** drop-down, select a different destination vCenter server if required, or leave the default selection of the same vCenter server.

   b. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.

   c. In the **Virtual Machine Name** field, specify the name of the new virtual machine.

   d. Select **Power On** to power on the virtual machine after the recovery completes.

   e. Select **Reconnect NIC** to reconnect the network interface card after the recovery completes.

   f. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

   g. Click **Next**.

   The **Destination Location** page displays.

4. In the **Destination Location** page, select the location in the vCenter server where you want to recover the virtual machine, and then click **Next**.

   The **Summary** page displays.

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

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.
Note that the status might not update to "Completed" or "Succeeded" upon a successful instant recovery. If this occurs, cancel the corresponding NetWorker restore task in the **vSphere Client** and the status will update correctly in the NetWorker Management Web UI.

Note

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

Virtual Disk (VMDK) recovery

Select **Virtual Disk** to recover the disks from the virtual machine backup to an existing virtual machine.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **Virtual Disk**.

   The **Recover** wizard launches.

3. In the **Configuration** page:

   a. From the **Destination vCenter** drop-down, select a different destination vCenter server if required, or leave the default selection of the same vCenter server.

   b. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.

   c. Select **Power On** to power on the virtual machine after the recovery completes.

   d. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

e. Click **Next**.

The **Virtual Machine Selection** page displays.

4. In the **Virtual Machine Selection** page, select the location of the virtual machine in the vCenter server where you want to recover the virtual disk(s), and then click **Next**.

   Note

   This location can be the original virtual machine, or another existing virtual machine.

   The **Disk Selection** page displays.

5. In the **Disk Selection** page, choose one or more of the available hard disks, and select a **Destination Datastore** for each selected disk. The default **Destination Datastore** selected is the original datastore, however, you can select a different datastore for each disk you want to recover. Click **Next**.

   The **Summary** page displays.

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

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Note

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

Emergency Recovery

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

Before you begin

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

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

Note

During an Emergency Recovery, the vProxy gets associated with the ESXi host and is unavailable for other operations on the vCenter server. Wait until the recovery completes before initiating any other operations on the vProxy.

To complete the Recovery wizard with the Emergency Recovery method, perform the following:

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. From the **Image Level** drop-down, select **Emergency**.

   The **Recover** wizard launches.

3. In the **Configuration** page:

   a. From the **ESX Server** drop-down, select the IP of the ESX server in the vCenter environment where you want to restore the virtual machine backup.

   b. Specify the root **Username** and **Password** for the ESX Server.

   c. In the **Virtual Machine Name** field, specify the name of the new virtual machine.

   d. Select **Power On** to power on the virtual machine after the recovery completes.

   Note

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

   ---

   e. Select **Reconnect NIC** to reconnect the network interface card after the recovery completes.

   f. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

   g. Click **Next**.

   The **VMware Proxy Configuration** page displays.

4. In the **VMware Proxy Configuration** page:

   a. For **Proxy Selection Type**, if the desired proxy has been discovered, select an existing vProxy for the recovery. Alternatively, you can use a new vProxy that is deployed in the vCenter but not yet added in NetWorker by selecting **Register a new VMware Proxy**.

   b. From the **Select Proxy** drop-down, select one of the registered vProxies.

   c. Click **Next**.

      The **Disk Selection** page displays.

5. In the **Disk Selection** page, 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. Additionally, you can use the **VM Configuration Files** drop-down to select the datastore where the virtual machine configuration files will reside. Click **Next**.

   The **Summary** page displays.

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

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Note

The progress bar may not update correctly when you perform an Emergency Recovery directly to the ESXi host.

File Level recovery

Select **File Level** to recover individual files from backups of virtual machines or VMDKs to a primary or secondary vCenter server.

Before you begin

NetWorker only supports file level recovery operations from a primary or cloned backup if the save set is on a Data Domain device. If a cloned backup does not exist on the Data Domain device, you must manually clone this save set to Data Domain before launching the **Recovery** wizard.

For the Data Domain resource, ensure that you provide the management credentials and, if required, type the export path appropriately. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only) provides detailed steps.

Additionally, if recovering to a virtual machine on a secondary vCenter, ensure that a vProxy appliance has been deployed on the secondary vCenter server and configured with the NetWorker server.

Note

File level recovery in the NetWorker Management Web UI can only be performed by an administrator.

Procedure

1. In the **VMware Recovery** window's **Backups and Clones** pane, select from one of the available primary or cloned backups, and then select the **Recovery** drop-down.
2. Select **File Level**.

   The **Recover** wizard launches.
3. In the **Configuration** page:

   a. From the **Destination vCenter** drop-down, select a different destination vCenter server if required, or leave the default selection of the same vCenter server.

   b. From the **Proxy** drop-down, select **Automatic** to use the default vProxy appliance, or choose another vProxy.

   c. Select **Overwrite** to overwrite files in the destination location that have the same name as files being recovered.

   d. Select **Terminate mount session** to release the disk mount after the recovery completes.

   e. If required, set a **Debug** level if you want to enable debug logs. The default level is 0.

   f. Click **Next**.

   The **Destination Virtual Machine** page displays.
4. In the **Destination Virtual Machine** page, the location of the original virtual machine backup displays by default in blue. If you do not want to recover to the original location, navigate to the desired virtual machine in the vCenter server where you want to recover the objects, and click **Next**.

   The **Mount Configuration** page displays.

5. In the **Mount Configuration** page, type the user credentials to access the virtual machine that you want to recover objects to in order to initiate the disk mount. This user should have privileges to install the **FLR Agent**, which is required to perform file level recovery. For Linux virtual machines, this requires the root user account. Optionally, select **Keep FLR agent after installation** if you do not want to remove the **FLR Agent** from the virtual machine upon recovery completion. Click **Mount**.

   The disk mount initializes and a progress bar displays.

   Note

   You cannot browse the contents of the virtual machine backup until the mounting of the destination virtual machine completes successfully.

6. When the mount completes successfully, click **Next**.

   The **Source Data** page displays.

7. In the **Source Data** page, select individual folders to browse the contents of the backup, and select the objects you want to recover. You can select all objects in a folder by clicking the checkbox to the left of the **Name** field in the **Contents** pane.

   When any objects in a folder are selected, that folder is highlighted in blue in the **Folders** pane. After selecting the objects that you want to recover, click **Next**.

   The **Destination Location** page displays.

8. In the **Destination Location** page, browse the folder structure of the destination virtual machine to select the folder where you want to recover the objects. Click **Next**.

   The **Summary** page displays.

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

Results

The wizard exits and a message displays along the top of the **VMware Recovery** window to indicate that a recovery request was submitted. Select **Monitoring** in the left pane to view the duration and status of the recovery operation.

Monitor recovery operations in the NetWorker Management Web UI

After initiating a recovery operation in the NetWorker Management Web UI, select **Monitoring** in the left pane to view the status and progress of the recovery in the right pane.

In addition to the progress and completion status of individual recovery operations, a column displays the recovery type. You can choose to display hidden columns by clicking the blue icon in the lower left corner of the table.

If you need to troubleshoot recovery operations, you can view the vProxy logs by clicking the menu in the first column and selecting **View Messages** from the drop-down.

vProxy file-level restore and SQL restore in the Dell EMC Data Protection Restore Client

You can also use the **Dell EMC Data Protection Restore Client** to perform granular recovery from a primary or cloned vProxy backup on a Data Domain device. The **Dell**

EMC Data Protection Restore Client allows you to restore specific files and folders from virtual machines in **User** and **Admin** modes, and also restore individual SQL databases from SQL server application-aware backups. The **Dell EMC Data Protection Restore Client** is part of the NetWorker client installation.

Note

Before you start a file-level restore, review the prerequisites in the section File-level restore prerequisites, as well as File-level restore and SQL restore limitations to ensure that you can perform file-level restores in your configuration.

Pre-requisites for file-level restore and SQL restore

Review the following information before performing a file-level restore or SQL restore in the **Dell EMC Data Protection Restore Client**.

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 platform versions

The **Dell EMC Data Protection Restore Client** supports file-level restore for the following platforms and operating system versions:

- RedHat Enterprise Linux versions 6.x and 7.x
- SuSE Linux Enterprise Server versions 11.x and 12.x
- Debian version 9.1
- Ubuntu version 17.10
- CentOS version 7.2
- OEL version 7.2
- Windows 64-bit platforms

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/Ubuntu ext4 file systems.

Procedure

1. Log in to the system console as a non-root user.
2. Run the `sudo passwd root` command.

   Enter the new password twice to set a password for the root account.
3. Run the `sudo passwd -u root` command to unlock the root account.
4. Specify the root user credentials in the **Dell EMC Data Protection Restore Client** and proceed to complete the file-level restore operation at least once.

   While performing the file-level restore operation for the first time, remember to select **`Keep FLR agent`**.
5. After performing the above steps at least once, you can revert the root account to the locked state and use non-root account for future file-level restore requests. Non-root user can lock the root account with the `sudo passwd -l root` command.

NetWorker privileges required by File-level restore and SQL database/instance level restore users

A new user group, **VMware FLR Users**, requires NetWorker privileges for User and Admin logins to perform file-level restore and SQL database/instance level restore operations in the **Dell EMC Data Protection Restore Client**.

Specify the following privileges for the VMware FLR Users group by using the NMC **NetWorker Administration** window or `nsradmin`.

Table 14 FLR privilege requirements

User	Admin
Remote Access All Clients	Remote Access All Clients
Operate NetWorker	Operate NetWorker
Monitor NetWorker	Monitor NetWorker
Operate Devices and Jukeboxes	Operate Devices and Jukeboxes
Recover Local Data	Recover Local Data
Backup Local Data	Backup Local Data
	View Security Settings

Operating system utilities required for file-level restore

On Linux and Windows, the installed operating system must include several standard utilities in order to use file-level restore. Depending on the target operating system for restore and the types of disks or file systems in use, some of these standard utilities, however, may not be included.

The following utilities and programs may be required for performing file-level restore.

On Windows:

- msiexec.exe
- robocopy.exe
- diskpart.exe
- cmd.exe

On Linux:

- blkid
- udevadm
- readlink
- rpm
- rsync
- bash

Note

On Linux LVM, LVM2 rpm version 2.02.117 or later is required. Also, additional binaries required on Linux LVM include dmsetup, lvm, and vgimportclone.

Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only)

Before you perform an instant recovery of a virtual machine or file-level restore (User mode), ensure that you provide the management credentials for the Data Domain resource. For instant recovery, these credentials are required when performing the recovery using the NMC **Recover** wizard or the **VM Backup and Recovery** interface in the **vSphere Web Client**.

Procedure

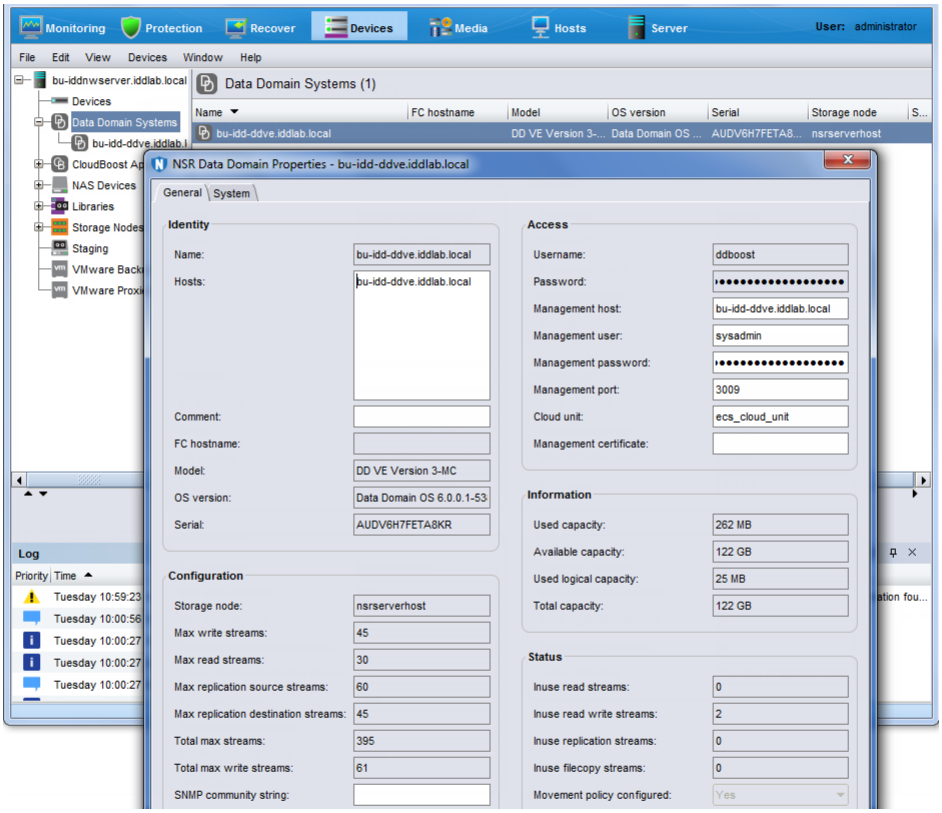
1. In the NMC Administration window, click **Devices**.

   The **Devices** window displays.

2. In the expanded left navigation pane, select **Data Domain Systems**.
3. In the right details pane, right-click the Data Domain system, and then select **Properties**.

   The **NSR Data Domain Properties** window displays.

Figure 54 NSR Data Domain Properties



Data Domain Systems (1)

Name	FC hostname	Model	OS version	Serial	Storage node	S...
bu-idd-ddve.iddlab.local		DD VE Version 3-...	Data Domain OS ...	AUDV6H7FETA8...	nsrserverhost	

NSR Data Domain Properties - bu-idd-ddve.iddlab.local

Identity

Name:	bu-idd-ddve.iddlab.local
Hosts:	bu-idd-ddve.iddlab.local
Comment:	
FC hostname:	
Model:	DD VE Version 3-MC
OS version:	Data Domain OS 6.0.0.1-53
Serial:	AUDV6H7FETA8KR

Configuration

Storage node:	nsrserverhost
Max write streams:	45
Max read streams:	30
Max replication source streams:	60
Max replication destination streams:	45
Total max streams:	395
Total max write streams:	61
SNMP community string:	

Access

Username:	ddboost
Password:	••••••••••••••••••
Management host:	bu-idd-ddve.iddlab.local
Management user:	sysadmin
Management password:	••••••••••••••••••
Management port:	3009
Cloud unit:	ecs_cloud_unit
Management certificate:	

Information

Used capacity:	262 MB
Available capacity:	122 GB
Used logical capacity:	25 MB
Total capacity:	122 GB

Status

Inuse read streams:	0
Inuse read write streams:	2
Inuse replication streams:	0
Inuse filecopy streams:	0
Movement policy configured:	Yes

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 a domain user

To perform a file-level restore as a domain user in the NMC **NetWorker Administration** window's **Recovery** wizard or the **Dell EMC Data Protection Restore Client**, you need to register a tenant user and provide the FLR Domain user permissions by performing the following steps.

Note

Steps 1 through 3 provide high level information for running `authc_config`. More detailed steps might be required if configuring AD authentication in the NetWorker environment. The *NetWorker Security Configuration Guide* provides more information.

Procedure

1. Create a tenant user on NetWorker by running the `authc_config` command. For example, open a command prompt and cd to `C:\Users\Administrator`, and then type `authc_config -u administrator -e add-tenant -D tenant-name=FLR -D tenant-alias FLR -p` *`password`*
2. Obtain the tenant ID by running the following command:

   ```
   authc_config -u administrator -e find-tenant -D tenant-
   name=FLR -p password
   Tenant Id : 4
   Tenant Name : FLR
   Tenant Alias : FLR
   Tenant Details:
   ```

3. Register the domain user by running the following command:

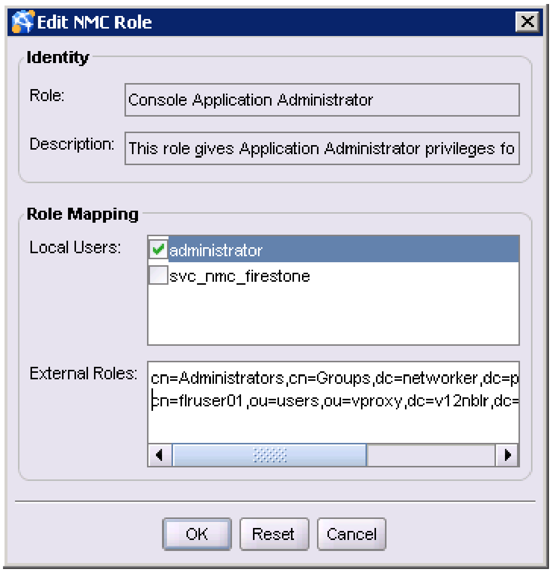
   ```
   authc_config -u administrator -e add-config -D config-tenant-
   id=3 -D config-name=FLRtest
   -D config-server-address=ldap://10.63.60.31:389/
   OU=vproxy,DC=v12nblr,DC=com -D config-domain=v12nblr
   -D config-user-
   dn=CN=flruser01,OU=users,OU=vproxy,DC=v12nblr,DC=com -D
   config-user-dn-password=password
   -D config-user-object-class=inetOrgPerson -D config-user-
   search-path=OU=users -D config-user-id-attr=cn
   -D config-group-search-path=OU=users -D config-group-name-
   attr=cn -D config-group-object-class=group
   -D config-group-member-attr=member -D config-active-
   directory=y -p password
   ```

4. Launch the **NetWorker Management Console**.
5. In the **NetWorker Management Console**, click **Setup** to open the **Setup** window.
6. Under **Users and Roles** in the left navigation pane, select **NMC Roles**. The roles display in the right pane.
7. For the **Console Application Administrator**, **Console Security Administrator** and **Console User** NMC roles, perform the following

   a. From the right pane, right-click **NMC role** and select **Properties**.

   b. In the **Edit NMC Role** dialog, add the Domain FLR user by typing **`cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com`** in the **External roles** field, and then click **OK**.

Figure 55 Add Domain FLR user



Role: Console Application Administrator

Description: This role gives Application Administrator privileges fo

Local Users:

- ☑ administrator
- □ svc_nmc_firestone

External Roles:

```
cn=Administrators,cn=Groups,dc=networker,dc=p
cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=
```

8. Navigate to the NMC **Enterprise** window, right-click the server and select **Launch Application...** to open the NMC **Administration** window.
9. Click **Server** to open the **Server** window.
10. In the left navigation pane, select **User Groups** to display the users in the right pane.
11. Type the Domain FLR user details in the **External Roles** field for the following User groups:
    - Application Administrators: `cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com`
    - Users: `cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com`
    - VMware FLR Users: `cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com`
12. Type the Domain FLR user details in the **External Roles** field for the following User group:
    - VMware FLR Users: `cn=flrusergroup,ou=users,ou=vproxy,dc=v12nblr,dc=com`

    In the example, the Domain FLR user "cn=flruser01,ou=users,ou=vproxy,dc=v12nblr,dc=com" is part of the Domain FLR group "cn=flrusergroup,ou=users,ou=vproxy,dc=v12nblr,dc=com" in Active Directory.
13. After registering the user as external domain, log in to the virtual machine as a domain user.
14. Re-launch the NMC **NetWorker Administration** window or the **Dell EMC Data Protection Restore Client** with the Domain FLR user in the following format:
    - In **NetWorker Administration**, v12nblr\flruser01
    - In the **Dell EMC Data Protection Restore Client**, FLR\v12nblr\flruser01

Results

You can now perform file level recovery in the **NetWorker Administration Recovery** wizard or the **Dell EMC Data Protection Restore Client** as a domain user.

Create a user in the NetWorker authentication service (User mode file-level restore only)

When performing file-level restore in User Mode, you must create a user in the Networker Management Console (NMC) using the **Manage Authentication Service Users** option, and make note of the password as you will require this information when logging in to the **Dell EMC Data Protection Restore Client**.

Before you begin

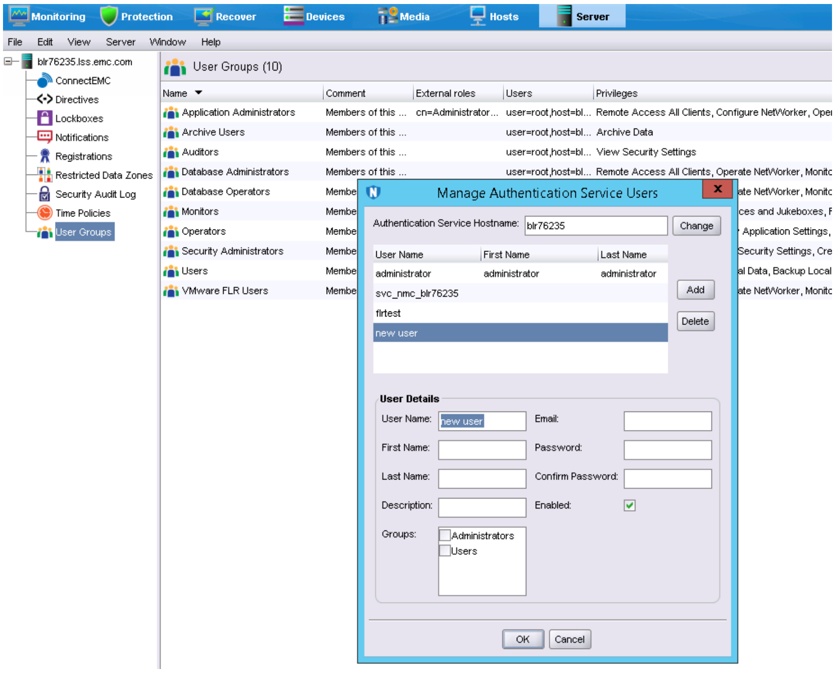
For file-level restores on Linux virtual machines, the root account credentials are required for the target virtual machine in order to install the **FLR Agent**. During the file-level restore session, if non-root credentials are provided for the target virtual machine, the **FLR Agent** installation fails, even if this user has privileges similar to a root user. To perform a file-level restore using a non-root user, ensure that the **FLR Agent** has already been installed on the target virtual machine using the root user account.

For file-level restores on Windows virtual machines, if the provided credentials for the target virtual machine do not have administrative privileges, the**FLR Agent** installation fails. To perform a file-level restore using a non-administrator user, ensure that the **FLR Agent** is already installed on the target machine using administrative privileges.

Procedure

1. In the NMC **NetWorker Administration** window, click **Server** to open the **Server** window.
2. In the left navigation pane, highlight **User Groups**, and then right-click and select **Manage Authentication Service Users**.

   Figure 56 Manage Authentication service users



Name	Comment	External roles	Users	Privileges
Application Administrators	Members of this ...	cn=Administrator...	user=root,host=bl...	Remote Access All Clients, Configure NetWorker, Oper
Archive Users	Members of this ...		user=root,host=bl...	Archive Data
Auditors	Members of this ...		user=root,host=bl...	View Security Settings
Database Administrators	Members of this ...		user=root,host=bl...	Remote Access All Clients, Operate NetWorker, Monitc
Database Operators	Membe			ate NetWorker, Monitc
Monitors	Membe			ces and Jukeboxes, F
Operators	Membe			Application Settings,
Security Administrators	Membe			Security Settings, Cre
Users	Membe			al Data, Backup Local
VMware FLR Users	Membe			ate NetWorker, Monitc

Authentication Service Hostname: blr76235

User Name	First Name	Last Name
administrator	administrator	administrator
svc_nmc_blr76235		
flrtest		
new user		

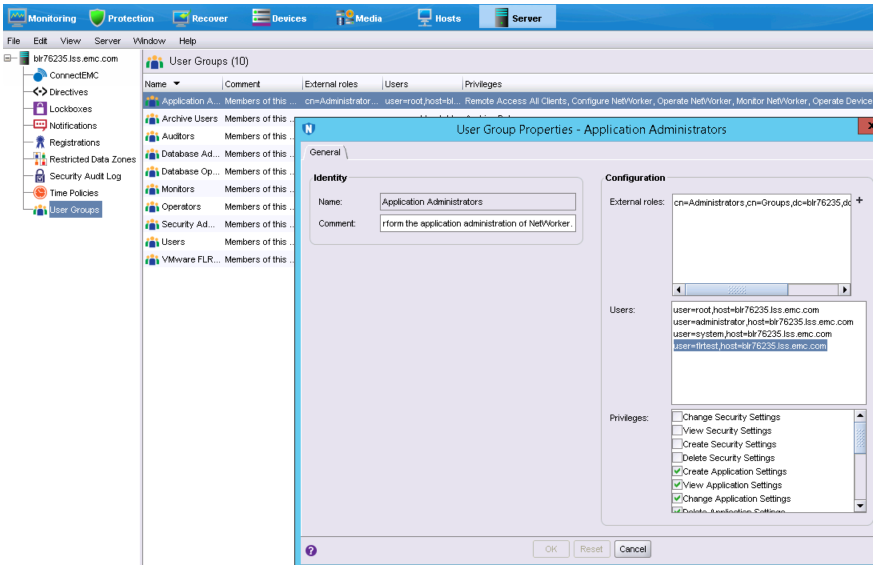
User Details

User Name: new user
Email:
First Name:
Password:
Last Name:
Confirm Password:
Description:
Enabled: ☑
Groups: □ Administrators □ Users

3. In the **Manage Authentication Service Users** dialog box, click **Add**.
4. For the new user **user1**, provide a username, password and other details, and then select the checkbox next to **Users** in the **Group** field and click **OK**.

5. Right-click **Application Administrators** and select **Properties**. In the **User Group Properties**, create an entry for the user created in step 4 (for example, **user1**), in the format `user=user1,host=NW server FQDN`.

Figure 57 Application Administrators user group properties



User Groups (10)

Name	Comment	External roles	Users	Privileges
Application A...	Members of this ...	cn=Administrator...	user=root,host=bl...	Remote Access All Clients, Configure NetWorker, Operate NetWorker, Monitor NetWorker, Operate Device
Archive Users	Members of this ...			
Auditors	Members of this ...			
Database Ad...	Members of this ...			
Database Op...	Members of this ...			
Monitors	Members of this ...			
Operators	Members of this ...			
Security Ad...	Members of this ...			
Users	Members of this ...			
VMware FLR...	Members of this ...			

User Group Properties - Application Administrators

Identity

Name: Application Administrators

Comment: rform the application administration of NetWorker.

Configuration

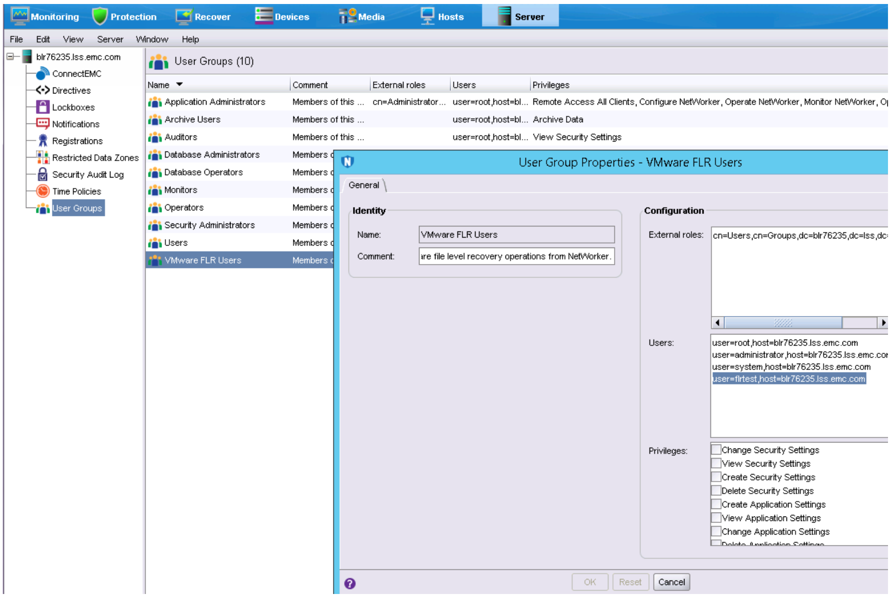
External roles: cn=Administrators,cn=Groups,dc=blr76235,dc

Users:
user=root,host=blr76235.lss.emc.com
user=administrator,host=blr76235.lss.emc.com
user=system,host=blr76235.lss.emc.com
user=flrtest,host=blr76235.lss.emc.com

Privileges:
☐ Change Security Settings
☐ View Security Settings
☐ Create Security Settings
☐ Delete Security Settings
☑ Create Application Settings
☑ View Application Settings
☑ Change Application Settings
☑ Delete Application Settings

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 58 VMware FLR Users user group properties



User Groups (10)

Name	Comment	External roles	Users	Privileges
Application Administrators	Members of this ...	cn=Administrator...	user=root,host=bl...	Remote Access All Clients, Configure NetWorker, Operate NetWorker, Monitor NetWorker, O
Archive Users	Members of this ...		user=root,host=bl...	Archive Data
Auditors	Members of this ...		user=root,host=bl...	View Security Settings
Database Administrators	Members c			
Database Operators	Members c			
Monitors	Members c			
Operators	Members c			
Security Administrators	Members c			
Users	Members c			
VMware FLR Users	Members c			

User Group Properties - VMware FLR Users

Identity

Name: VMware FLR Users

Comment: are file level recovery operations from NetWorker.

Configuration

External roles: cn=Users,cn=Groups,dc=blr76235,dc=lss,dc

Users:
user=root,host=blr76235.lss.emc.com
user=administrator,host=blr76235.lss.emc.co
user=system,host=blr76235.lss.emc.com
user=flrtest,host=blr76235.lss.emc.com

Privileges:
☐ Change Security Settings
☐ View Security Settings
☐ Create Security Settings
☐ Delete Security Settings
☐ Create Application Settings
☐ View Application Settings
☐ Change Application Settings
☐ Delete Application Settings

Results

You can now use this new user to log into the **Dell EMC Data Protection Restore Client**.

FLR Agent is required for file-level restore

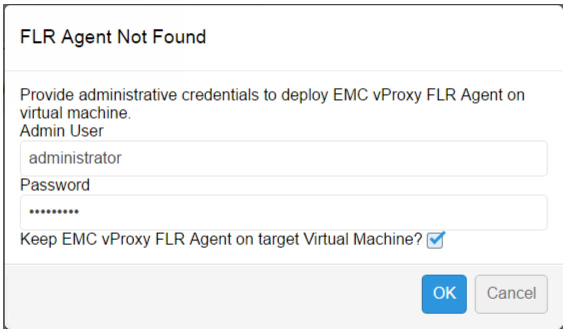
The **FLR Agent** is required for file-level restore operations and gets installed automatically on the target virtual machine when you initiate a file-level restore and provide the virtual machine credentials.

The **FLR Agent** installation on Linux virtual machines requires that you use the root account. If non-root credentials are provided for the target virtual machine, the **FLR Agent** installation fails, even if this user has privileges similar to a root user. Once the **FLR Agent** installation is completed by a root user, you can perform file-level restore operations as a non-root user.

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.

If the request to install the FLR Agent was not successful and you initiate a file-level restore, the following message appears.

Figure 59 Deploy FLR Agent if not found



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? ☑

This message provides an option to deploy the FLR Agent by providing the appropriate credentials.

On Linux, to perform a file-level restore using a non-root user, ensure that the **FLR Agent** has already been installed on the target virtual machine using the root user account. Otherwise, ensure that you are using a supported platform and the root user is specified, and click **OK**. For Linux, file-level restore is only supported on Red Hat Enterprise Linux versions 6 and 7, and SuSE Linux Enterprise Server versions 11 and 12.

On Windows, to perform a file-level restore using a non-administrator user, ensure that the **FLR Agent** is already installed on the target machine using administrative privileges. Otherwise, ensure that an administrative user is specified, and click **OK**.

FLR Agent installation on Windows virtual machines with User Account Control (UAC) enabled

Performing the FLR Agent installation on UAC-enabled Windows virtual machine requires you to either provide the credentials of the administrator user, or to 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 restore limitations

This section provides a list of limitations that apply to file-level restore and individual SQL database and instance restore.

Compatibility requirements and unsupported configurations
Review the following limitations related to file-level restore compatibility requirements and unsupported configurations.

- File-level restore and SQL instance restore in the **Dell EMC Data Protection Restore Client** is only supported on the platforms and versions identified in the section Supported platform versions. The online compatibility guide, available at https://elabnavigator.emc.com/eln/modernHomeDataProtection, provides more software compatibility information.
- 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.
- You can perform file-level restore across vCenters as long as the vCenters are configured in the same NetWorker server, and the source and target virtual machine have the same guest operating system. For example, Linux to Linux, or Windows to Windows.
- File-level restore from a Data Domain Cloud Tier device is not supported. To perform file-level restores of data that resides only on this device, first clone the data to a Data Domain device, and then recover the data from the Data Domain device.
- File-level restore does not support the following virtual disk configurations:
  - LVM thin provisioning
  - Unformatted disks
  - FAT16 file systems
  - FAT32 file systems
  - Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)

  - Two or more virtual disks mapped to single partition
  - Encrypted partitions
  - Compressed partitions

Platform-specific limitations

Review the following limitations specific to Linux and Windows operating systems.

- You can only restore files and/or folders from a Windows backup to a Windows machine, or from a Linux backup to a Linux machine.
- When you enable Admin Approval Mode (AAM) on the operating system for a virtual machine (for example, by setting `Registry/FilterAdministratorToken` to `1`), the administrator user cannot perform a file-level restore to the end user's profile, and an error displays indicating "Unable to browse destination." For any user account control (UAC) interactions, the administrator must wait for the mount operation to complete, and then access the backup folders located at `C:\Program Files (x86)\EMC\vProxy FLR Agent\flr\mountpoints` by logging into the guest virtual machine using Windows Explorer or a command prompt.
- The **FLR Agent** installation on Linux virtual machines requires you to use the root account. 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. Once the **FLR Agent** installation is completed by a root user, you can perform file-level restore operations as a non-root user.
- Mounting a Linux virtual machine for file-level restore requires a local Linux account with permissions to the file system files.
- When you perform file-level restore on Ubuntu/Debian platforms, you must enable the root account in the operating system. By default, the root account will be in locked state.
- File-level restore is not supported on Ubuntu/Debian ext4 file systems.
- When running the NetWorker server on Windows platforms, file-level restore session logs are not kept.
- For file-level restores on Windows 2012 R2 virtual machines, the volumes listed under the virtual machine display as "unknown." File-restore operations are not impacted by this issue.
- File-level restore of virtual machines with Windows dynamic disks is supported with the following limitations:
  - The restore can only be performed when recovering to a virtual machine different from the original. Also, this virtual machine cannot be a clone of the original.
  - The restore can only be performed by virtual machine administrator users.
  - If Windows virtual machines were created by cloning or deploying the same template, then all of these Windows virtual machines may end up using the same GUID on their dynamic volumes.
- File-level restore of Windows 8, Windows Server 2012 and Windows Server 2016 virtual machines is not supported on the following file systems:
  - Deduplicated NTFS
  - Resilient File System (ReFS)
  - EFI bootloader

Restore operations and performance limitations

Review the following limitations related to file-level restore operations and performance considerations.

- When a file-level restore or SQL restore operation is in progress on a virtual machine, no other backup or recovery operation can be performed on this virtual machine. Wait until the file-level restore session completes before starting any other operation on the virtual machine.
- When the backup chain for an SQL instance restore contains 30 or more transaction log backups, a message indicating the required permissions to complete this action does not display in the **Dell EMC Data Protection Restore Client**. Check the `flr-server` log for an error message similar to the following to determine what additional privileges are required:

  ```
  ERROR c.e.f.u.ProcessRestores - Failed restore attempt:
  Recover request failed: Permission denied, user does not
  have 'Create Application Settings' or 'Configure NetWorker'
  privilege to create this resource - NSR recover.
  ```
- SQL instance restore fails in the **Dell EMC Data Protection Restore Client** when the backup chain contains more than 75 transaction log backups. In such scenarios, ensure that you perform a SQL database restore for each database in the SQL instance one at a time.
- When you switch between different Data Domain devices for backup and clone operations, the SQL transaction log backup does not get promoted to FULL on the primary backup device. As a result, the transaction log backup fails with the error `Previous backup path must be specified for Transaction Log backup`. Note that this issue does not occur when the same Data Domain device is used for the backup and clone.

  If relabelling of the primary device has occurred, or you added a new Data Domain device, unselect the **Tlog backup** option for the Backup Action, and then run the SQL application-consistent workflow. After the FULL backup and clone completion, re-select the **Tlog backup** option for the Backup Action and run the SQL application-consistent workflow again. Subsequent transaction log backups and clones will complete successfully.
- For file-level restore of high-density file systems (more than few hundred files/ folders), it is recommended to use either the **NetWorker Management Web UI** or the **Dell EMC Data Protection Restore Client** (User or Admin mode, as applicable) instead of the **Recovery** wizard in the NMC **NetWorker Administration** window.
- A restore of individual SQL Server databases or instances in the **Dell EMC Data Protection Restore Client** will overwrite the existing database, even if your NetWorker version provides an option where you can unselect **Overwrite the existing DB**.
- A SQL database restore to alternate is only supported for restoring from a lower SQL version to a higher SQL version.
- The **Dell EMC Data Protection Restore Client** incorrectly allows you to select a VMware Backup appliance as a destination client for file-level restore.
- After migrating from the VMware Backup appliance to the vProxy appliance, the **Dell EMC Data Protection Restore Client** may continue to display VMware Backup appliance backups along with the new vProxy backups for virtual machines. Note, however, that you will only be able to perform file-level restore from the new vProxy backups.
- After migrating from the VMware Backup appliance to the vProxy appliance, new vProxy backups of virtual machines that were previously backed up with the

VMware Backup appliance will not be visible in the **Dell EMC Data Protection Restore Client** in Admin mode. You must log in using User mode to view and recover from these backups.

- You cannot use clone volumes for file-level restore when the primary backup volume is unmounted or unavailable. The restore will fail looking for backup volumes. If this occurs, dynamic staging allows you to use the secondary copy by staging the requested virtual machine backups from the clone to an available backup volume and then recovering the virtual machine.
- Browsing a large number of files at once may cause Internet Explorer to become slow or unresponsive. The Chrome and Mozilla browsers issue a warning when encountering a difficulty handling many files, but Internet Explorer does not.
- In a large environment where many virtual machines appear in the **Dell EMC Data Protection Restore Client**, the navigation buttons (**Back**, **Next**, **Finish**) may appear very small, requiring you to zoom in to see the options. It is recommended that you use the latest versions of the Chrome or Firefox browsers to avoid the issue.
- File-level restore supports direct restore from a cloned backup only if the clone copy is on a Data Domain device.
- File-level restore does not restore or browse symbolic links.
- When you create partitions, fill the lower ordered indices first. For example, you cannot create a single partition and place it in the partition index 2, 3, or 4. You must place the single partition in partition index 1.

Using the Dell EMC Data Protection Restore Client for file-level restore and SQL restore

The **Dell EMC Data Protection Restore Client**, which you access through a web browser, allows you to select specific virtual machine backups as file systems, and then browse the file system to locate the directories and files you want to restore. The browser also allows you to restore individual SQL databases and instances.

The login page of the **Dell EMC Data Protection Restore Client** features two tabs—an **FLR** tab for virtual machine file and folder restore, and an **App** tab for SQL database and instance restore.

Additionally, the **Dell EMC Data Protection Restore Client** operates in one of two user modes:

- User—For file-level restore, a user account that can restore folders or files to the original virtual machine, as described in the section Restoring specific folders or files to the original virtual machine (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 a different virtual machine (Admin mode).
  For SQL restore, a NetWorker administrator account or Authentication Service user that can restore individual SQL databases and instances to the original machine from any virtual machine you have access to that contains an SQL Server application-consistent backup, or restore to a different virtual machine, as described in the section Restore of SQL Server application-consistent backups.

Note

When a file-level restore operation is in progress on a virtual machine, no other backup or recovery operation can be performed on this virtual machine. Wait until the file-level restore session completes before starting any other operation on the virtual machine.

Restoring specific folders or files to the original virtual machine in User mode

To restore specific folders and files to the original virtual machine on Windows and Linux virtual machines, select the **User** tab in the **Dell EMC Data Protection Restore Client** login page. In this mode, you connect to the **Dell EMC Data Protection Restore Client** from a virtual machine that has been backed up by the vProxy Appliance.

Before you begin

For the Data Domain resource, ensure that you provide the management credentials and, if required, enter the export path appropriately. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only)provides detailed steps.

Additionally, you must create a user in the NetWorker Authentication Service by using the NetWorker Management Console (NMC), as described in the section Create a user in the NetWorker authentication service (User mode file-level restore only).

Procedure

1. Open a browser from the virtual machine that the restored files will be recovered to, and enter a URL that points to the NetWorker server host and indicates file-level restore. For example:

   ```
   https://NetWorker server:9090/flr
   ```

   Note

   For User recoveries, you must connect to the NetWorker server from a web browser on the virtual machine that will receive file-level restore data.

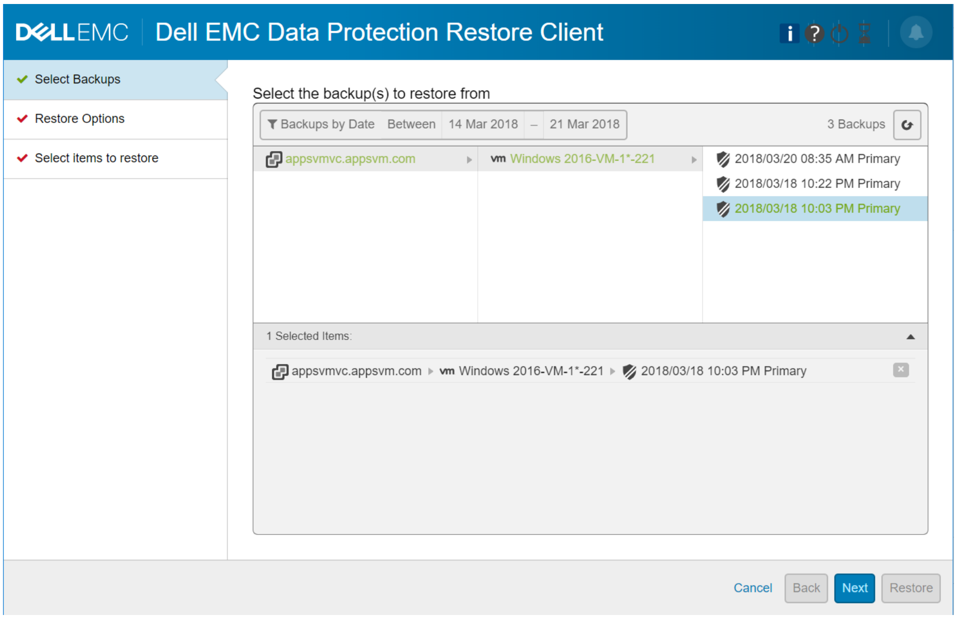
   The **Dell EMC Data Protection Restore Client** login window appears.

2. Select the **User** tab and the **FLR** tab, and then log in to the **Dell EMC Data Protection Restore Client** with the user credentials of the virtual machine to which you are logged in. This user account should also belong to the NetWorker user group "VMware FLR Users" in order to be authorized to perform file-level restore. The section NetWorker privileges required by File-level restore users provides more information.

   When you log in, the **Select Backups** page displays with a list of backups for the local virtual machine.

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

Figure 60 Select backups to restore from



Select the backup(s) to restore from

Backups by Date Between 14 Mar 2018 – 21 Mar 2018 3 Backups

appsvmvc.appsvm.com › vm Windows 2016-VM-1*-221 ›
- 2018/03/20 08:35 AM Primary
- 2018/03/18 10:22 PM Primary
- 2018/03/18 10:03 PM Primary

1 Selected Items:

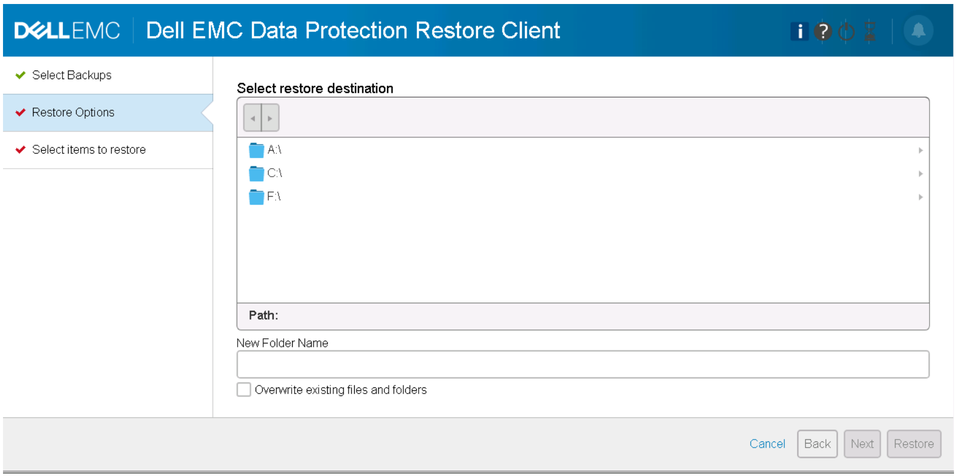
appsvmvc.appsvm.com › vm Windows 2016-VM-1*-221 › 2018/03/18 10:03 PM Primary

Note

When you click **Next**, if a folder hierarchy does not appear, the **Dell EMC Data Protection Restore Client** may not support the file system in use on the virtual machine. The section File-level restore limitations provides more information.

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

Figure 61 Select restore location



Select restore destination

- A:\
- C:\
- F:\

Path:

New Folder Name

□ Overwrite existing files and folders

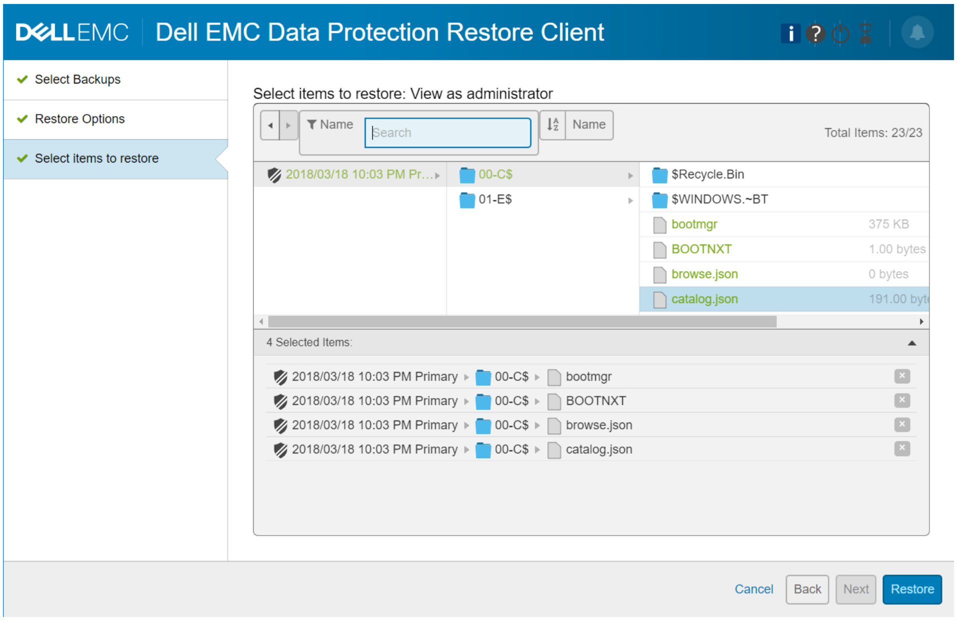
Note

Additionally, you can select the **Overwrite existing files and folders** option if you want to replace the existing files with the recovered files.

5. On the **Select items to restore** page, browse and select the files and folders available for recovery. Note that you can sort items by Name, File size, or Date,

and you can also search for a specific file or folder name. To mark an item for recovery, double-click the item, or drag and drop the item into the **Selected Items** pane.

Figure 62 Select items to restore



DELLEMC | Dell EMC Data Protection Restore Client

Select items to restore: View as administrator

Total Items: 23/23

2018/03/18 10:03 PM Pr…	00-C$	$Recycle.Bin	
	01-E$	$WINDOWS.~BT	
		bootmgr	375 KB
		BOOTNXT	1.00 bytes
		browse.json	0 bytes
		catalog.json	191.00 byt

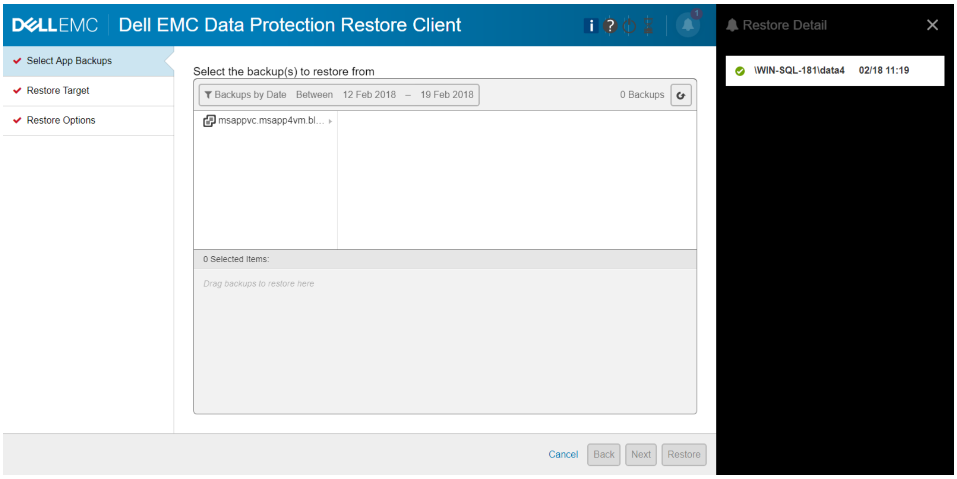
4 Selected Items:

- 2018/03/18 10:03 PM Primary ▸ 00-C$ ▸ bootmgr
- 2018/03/18 10:03 PM Primary ▸ 00-C$ ▸ BOOTNXT
- 2018/03/18 10:03 PM Primary ▸ 00-C$ ▸ browse.json
- 2018/03/18 10:03 PM Primary ▸ 00-C$ ▸ catalog.json

6. When finished selecting items, click **Finish**.
7. Click **Yes** when you are prompted to continue the restore.
8. To enable the polling feature so that you can monitor the status of the restore, click the hourglass icon located in the upper right-hand corner of the window and set to **ON**. By default, the polling feature is set to **OFF** due to the memory consumption that occurs when the server is queried every few seconds for the restore status.
9. Once the polling feature is enabled, you can monitor the status of the restore by clicking the 🔔 icon located in the upper right-hand corner of the window.

   When you click the 🔔 icon, the **Restore Detail** pane slides into view on the right side of the window, displaying the ongoing restore operations. Clicking the entry displays the progress of the restore and a recovery logs download option.

Figure 63 Restore Monitoring


DELLEMC
Dell EMC Data Protection Restore Client
✓ Select App Backups
✓ Restore Target
✓ Restore Options
Select the backup(s) to restore from
Backups by Date Between 12 Feb 2018 – 19 Feb 2018
0 Backups
msappvc.msapp4vm.bl...
0 Selected Items:
Drag backups to restore here
Cancel
Back
Next
Restore
Restore Detail

\WIN-SQL-181\data4 02/18 11:19

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

To restore specific folders or files from a different virtual machine, select the **Admin** tab in the **Dell EMC Data Protection Restore Client** login page. Once connected, you can browse, select, and restore files and folders from any virtual machine that you backed up with the vProxy Appliance. You can then restore items to the virtual machine on which you are currently logged in, or to any available destination virtual machine.

Procedure

1. Open a browser and specify a URL that points to the NetWorker server and indicates FLR, as in the following example:

   ```
   https://NetWorker server:9090/flr
   ```

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

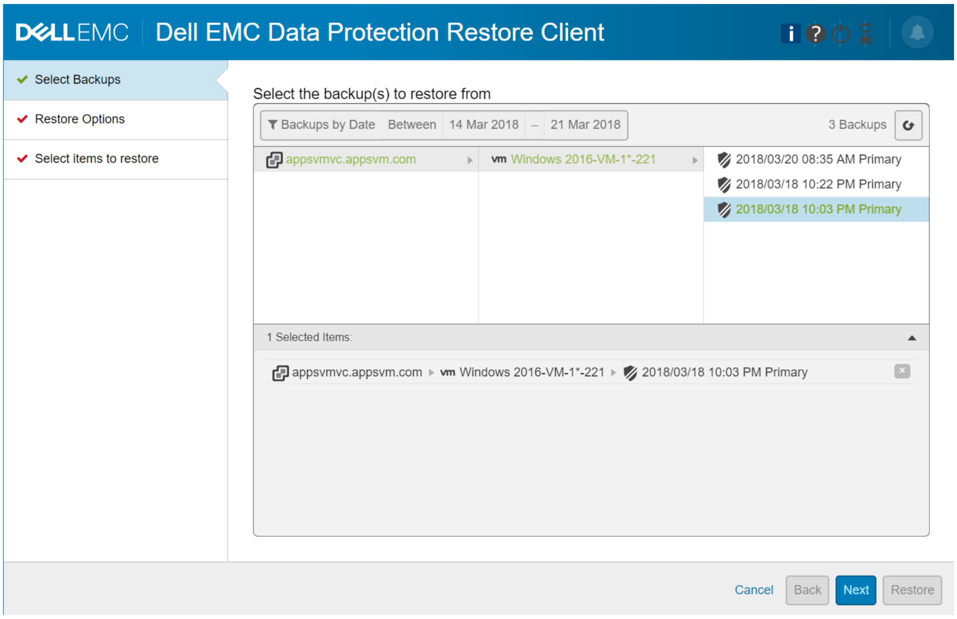
2. Click the **Admin** tab and the **FLR** tab, and then log in to the **Dell EMC Data Protection Restore Client** with the NetWorker Authentication Service User credentials.

   Note

   When using **Admin** mode, ensure that the user you specify for the NetWorker server login has the correct privileges to use this option.

   When you log in, the **Select Backups** page appears with a list of all the virtual machines that were backed up by using the vProxy Appliance. The available backups appear under each virtual machine, as shown in the following.

Figure 64 Select the backup(s) to restore from



DELL EMC | Dell EMC Data Protection Restore Client

✓ Select Backups
✓ Restore Options
✓ Select items to restore

Select the backup(s) to restore from

Backups by Date Between 14 Mar 2018 – 21 Mar 2018   3 Backups

appsvmvc.appsvm.com ▸ | vm Windows 2016-VM-1*-221 ▸ | 2018/03/20 08:35 AM Primary
2018/03/18 10:22 PM Primary
2018/03/18 10:03 PM Primary

1 Selected Items:

appsvmvc.appsvm.com ▸ vm Windows 2016-VM-1*-221 ▸ 2018/03/18 10:03 PM Primary

---

Note

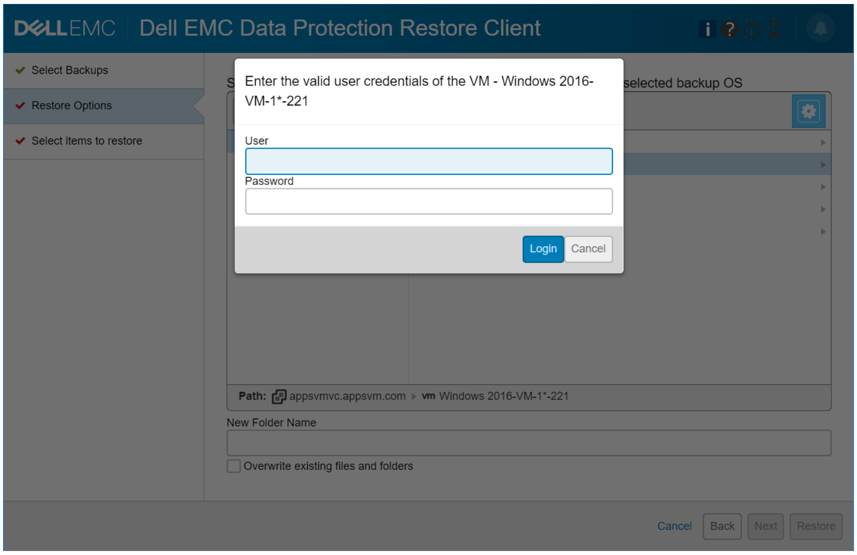
After migrating from the VMware Backup appliance to the vProxy appliance, new vProxy backups of virtual machines that were previously backed up with the VMware Backup appliance will not be visible in the **Dell EMC Data Protection Restore Client** in Admin mode. You must log in using User mode to view and recover these backups.

---

3. On the **Select Backups** page, use the arrows to the right of the entry to view the available backups. You can set the backup filter to view backups on a specific day or within a specific date range. Highlight a backup and double-click or drag and drop to move the backup to the **Selected Items** pane. Click **Next**.
4. On the **Restore Options** page, select a destination virtual machine.

   A login dialog box similar to the following figure appears for the restore destination.

Figure 65 Select restore location


DELLEMC
Dell EMC Data Protection Restore Client
✓ Select Backups
✓ Restore Options
✓ Select items to restore
selected backup OS

Enter the valid user credentials of the VM - Windows 2016-VM-1*-221

User

Password

Login
Cancel
Path: appsvmvc.appsvm.com ▸ vm Windows 2016-VM-1*-221
New Folder Name
□ Overwrite existing files and folders
Cancel
Back
Next
Restore

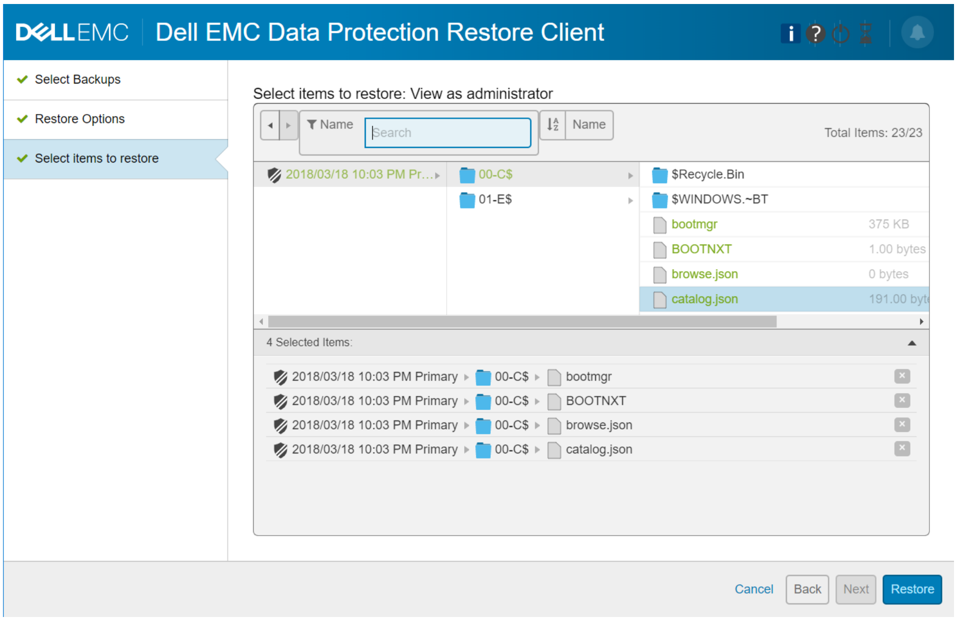
5. Log in to the destination virtual machine to initiate the mounting of the backup.
6. After you successfully log in, select the restore location. If desired, specify a new folder name in this location. Click **Next**.

Note

Additionally, you can select the **Overwrite existing files and folders** option if you want to replace the existing files with the recovered files.

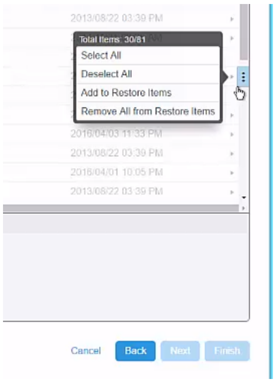
7. On the **Select items to restore** page, browse and select the files and folders available for recovery. Note that you can sort items by Name, File size, or Date, and you can also search for a specific file or folder name. To mark an item for recovery, double-click the item, or drag and drop the item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

Figure 66 Select items to restore


DELLEMC
Dell EMC Data Protection Restore Client
Select Backups
Restore Options
Select items to restore
Select items to restore: View as administrator
Name
Search
Name
Total Items: 23/23
2018/03/18 10:03 PM Pr...
00-C$
01-E$
$Recycle.Bin
$WINDOWS.~BT
bootmgr 375 KB
BOOTNXT 1.00 bytes
browse.json 0 bytes
catalog.json 191.00 byt
4 Selected Items:
2018/03/18 10:03 PM Primary ▸ 00-C$ ▸ bootmgr
2018/03/18 10:03 PM Primary ▸ 00-C$ ▸ BOOTNXT
2018/03/18 10:03 PM Primary ▸ 00-C$ ▸ browse.json
2018/03/18 10:03 PM Primary ▸ 00-C$ ▸ catalog.json
Cancel
Back
Next
Restore

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

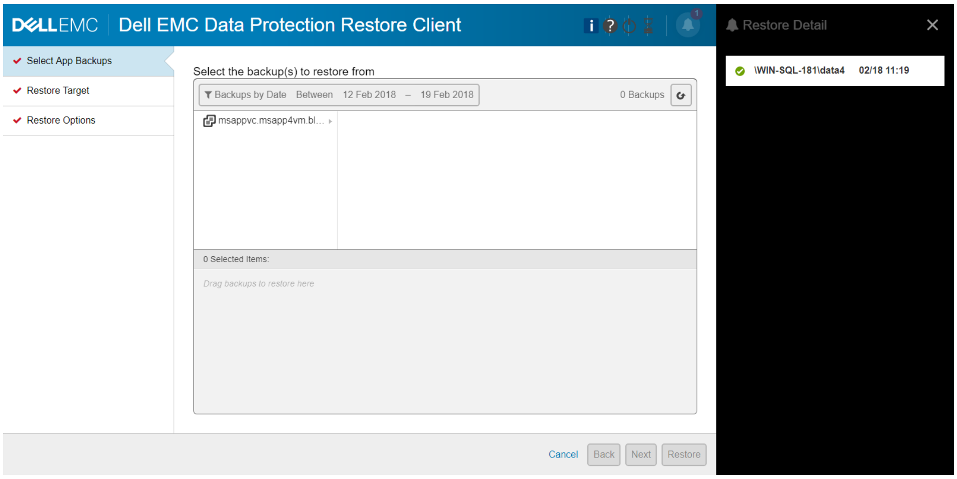
Figure 67 Total items available for recovery



8. When finished selecting items, click **Finish**.
9. Click **Yes** when you are prompted to continue with the restore.
10. To enable the polling feature so that you can monitor the status of the restore, click the hourglass icon located in the upper right-hand corner of the window and set to **ON**. By default, the polling feature is set to **OFF** due to the memory consumption that occurs when the server is queried every few seconds for the restore status.
11. Once the polling feature is enabled, you can monitor the status of the restore by clicking the icon located in the upper right-hand corner of the window.

    When you click the icon, the **Restore Detail** pane slides into view on the right side of the window, displaying the ongoing restore operations. Clicking the entry displays the progress of the restore and a recovery logs download option.

Figure 68 Restore Monitoring



Select the backup(s) to restore from

Backups by Date Between 12 Feb 2018 – 19 Feb 2018

0 Backups

msappvc.msapp4vm.bl...

0 Selected Items:

Drag backups to restore here

✓ \WIN-SQL-181\data4 02/18 11:19

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

NetWorker 18.1 allows you to restore an individual SQL database or an entire SQL instance for a virtual machine that was backed up as part of a SQL Server application-consistent protection policy. You can perform this restore to a running virtual machine, providing you with operational recovery of SQL databases and disaster recovery of SQL instances. Additionally, alternate restore allows you to restore to a database copy. Once you restore SQL database FULL backups, you can also apply SQL database transaction log backups to those databases. The individual database or instance restore target location can be the original location, or a new location on either the original virtual machine or a different virtual machine, with the ability to select the SQL instance where the database will be restored, the option to change the database name, and the option to select specific folder locations for file and log placement. Note that the ability to select a different virtual machine is only possible for individual SQL database restore. When performing SQL instance restore, you are restricted to selecting the original virtual machine and original instance.

SQL restore functionality is provided in the **Dell EMC Data Protection Restore Client** by using the **App** mode button on the login page. In **App** restore mode, the display of virtual machines and their primary backups is limited to virtual machines that have application consistent backups. Once a primary backup is selected, an additional index is loaded that allows you to browse and select the SQL instances, databases, and the database backup versions.

The **Backup Versions** pane displays the database backup versions on the original virtual machine, with a cumulative history of FULL and transaction log backups for that database for one cycle of the backup policy. The **Backup Versions** pane refreshes with each full backup, and each subsequent transaction log backup adds the transaction log backup versions. The cumulative backup history allows you to select a database and associated backup regardless of the primary backup that is selected. When you select a SQL instance or SQL database to restore and do not select a specific backup version, the most recent backup version of the selected primary backup will be restored automatically.

The **Dell EMC Data Protection Restore Client** requires the virtual machine administrative credentials during mounting of the primary FULL backup on the original virtual machine. During the mount, NetWorker also installs or upgrades the FLR Agent and Microsoft VM App Agent, if required, on the selected virtual machine

The **Dell EMC Data Protection Restore Client** will discover and display the SQL instance on the target virtual machine once the mount completes. If the target virtual machine does not have any running SQL Instances, an error will be displayed. You may select the SQL instance from this where you want to restore the database. The ability to select a different SQL Instance is only possible for individual database restore, and when performing SQL Instance restore you are restricted to selecting the original SQL Instance.

NetWorker automates the complete restore of SQL databases, restoring the database FULL and any transaction log backups as a single operation according to the following sequence:

- The primary FULL database backup is identified, mounted on the original virtual machine, and the SQL database files from the FULL backup are restored to the original database.
- If a transaction log backup was selected, the series of transaction logs that occurred after the FULL backup to the selected transaction log are restored in sequence.

NetWorker automates the complete restore of SQL instances according to the following sequence:

- The **master** database is restored first, then **msdn**, then **model**. During this restore, the SQL instance restarts in single-user mode as required by the Microsoft SQL Server to restore the master database. When the restore completes, the SQL services restart in multi-user mode.
- Each remaining database is restored individually, and includes the backup versions present in the currently selected backup.

The **Dell EMC Data Protection Restore Client** provides the ability to monitor the restore operations while in progress by enabling the Polling feature, which is disabled by default. Once enabled, when you click the 🔔 icon, the **Restore Detail** pane slides into view on the right side of the window, displaying the ongoing restore operations. Clicking the entry displays the progress of the restore and a recovery logs download option.

Restore specific SQL databases and instances to a running virtual machine (Windows platforms only)

To restore specific SQL instances and databases to a running virtual machine in the **Dell EMC Data Protection Restore Client**, select the **App** button, and then select **User** or **Admin**. In **User** mode, you can log in and connect to the virtual machine that was backed up as part of a SQL Server application-consistent protection policy to restore to the original virtual machine. In **Admin** mode, you can browse, select, and restore from any virtual machine that you backed up as part of a SQL Server application-consistent protection policy. In both modes, you can restore the virtual machine's SQL instance(s) to the original SQL instance, or an alternate SQL instance.

Before you begin

When planning to restore to an alternate instance between virtual machines in different domains, ensure that DNS is resolved.

For the Data Domain resource, ensure that you provide the management credentials and, if required, enter the export path appropriately. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only)provides detailed steps.

Additionally, if not using the NMC Administrator account to log in, you must create a user in the NetWorker Authentication Service by using the NetWorker Management Console (NMC), as described in the section Create a user in the NetWorker authentication service (User mode file-level restore only), and you must configure

Microsoft SQL Server instances in the original virtual machine to allow SYSTEM account login and membership in the SQL sysadmin role.

Procedure

1. Open a browser from the virtual machine that the SQL databases or instances will be recovered to, and enter a URL that points to the NetWorker server host and indicates file-level restore. For example:

   ```
   https://NetWorker server IP:9090/flr
   ```

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

2. Select the **User** or **Admin** tab, and then select the **App** tab.

   Note

   For **User** mode recoveries, you must connect to the NetWorker server from a web browser on the virtual machine that the SQL database or instance will be restored to.

3. Type the user credentials, and then click **Login**.

   - For **User** mode, type the NetWorker credentials. These can be your NMC credentials, or the user account credentials specified for the NetWorker user group **VMware FLR Users**. This user must belong to the **VMware FLR Users** group in order to be authorized to perform SQL database or instance restore. The section NetWorker privileges required by File-level restore users provides more information.
   - For **Admin** mode, type the NetWorker credentials. When using this mode, ensure that the user you specify for the NetWorker server login has the correct privileges to use this option.

   When you log in, the **Select App Backups** page displays with a list of virtual machines that were backed up by the SQL Server application-consistent protection policy. The available backups (primary backups) appear under each virtual machine, and include the virtual machine FULL and transaction log backups, depending on the application-consistent policy settings. For **User** mode, this will be limited to a list of backups for the local virtual machine.

   Note

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

4. On the **Select App Backups** page, use the arrows to the right of the entry to browse and select from the available SQL Server application-consistent backups, including all SQL instances, databases, and backup versions.

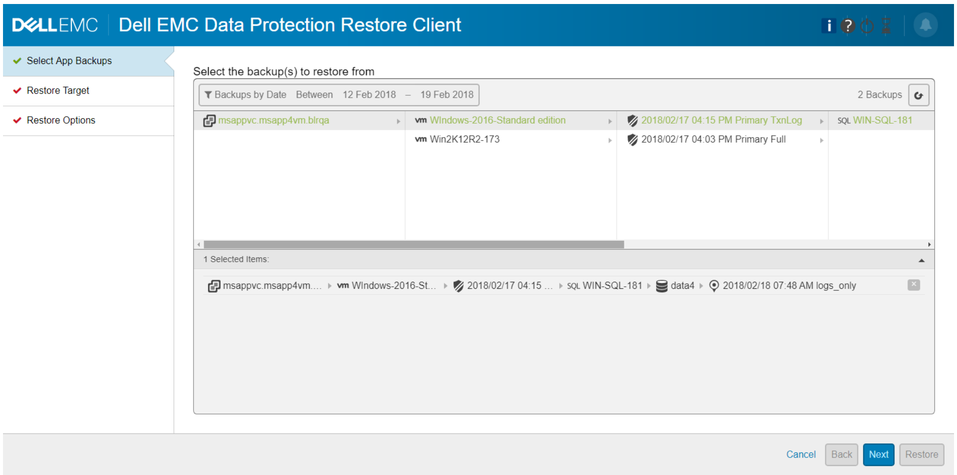
   To select a backup version, expand the SQL instance and database to display the backup versions pane, and then click the backup version item once or drag and drop the item to move the backup to the **Selected Items** pane. You may be required to scroll right to view the backup versions.

   To select a SQL database or instance, drag and drop the entry to move the item to the **Selected Items** pane. Note that you cannot drag and drop the SQL database or instance when the entry has been expanded to view its children. If you expanded the entry, reselect the virtual machine, and then select the SQL database or instance to enable drag-and-drop.

Note

The backup filter is set to the last seven days by default. You can expand the date range further back if desired.

Figure 69 Select App Backups page



Select the backup(s) to restore from

Backups by Date Between 12 Feb 2018 – 19 Feb 2018 2 Backups

msappvc.msapp4vm.blrqa
vm WIndows-2016-Standard edition
vm Win2K12R2-173
2018/02/17 04:15 PM Primary TxnLog
2018/02/17 04:03 PM Primary Full
SQL WIN-SQL-181

1 Selected Items:

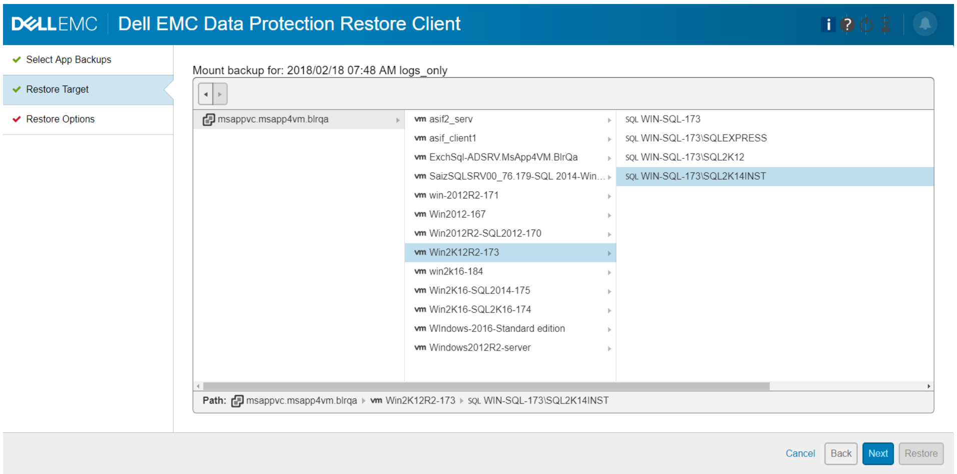
msappvc.msapp4vm.... › vm WIndows-2016-St... › 2018/02/17 04:15 ... › SQL WIN-SQL-181 › data4 › 2018/02/18 07:48 AM logs_only

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 70 Restore Target page



Mount backup for: 2018/02/18 07:48 AM logs_only

msappvc.msapp4vm.blrqa

vm asif2_serv
vm asif_client1
vm ExchSql-ADSRV.MsApp4VM.BlrQa
vm SaizSQLSRV00_76.179-SQL 2014-Win...
vm win-2012R2-171
vm Win2012-167
vm Win2012R2-SQL2012-170
vm Win2K12R2-173
vm win2k16-184
vm Win2K16-SQL2014-175
vm Win2K16-SQL2K16-174
vm WIndows-2016-Standard edition
vm Windows2012R2-server

SQL WIN-SQL-173
SQL WIN-SQL-173\SQLEXPRESS
SQL WIN-SQL-173\SQL2K12
SQL WIN-SQL-173\SQL2K14INST

Path: msappvc.msapp4vm.blrqa › vm Win2K12R2-173 › SQL WIN-SQL-173\SQL2K14INST

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.

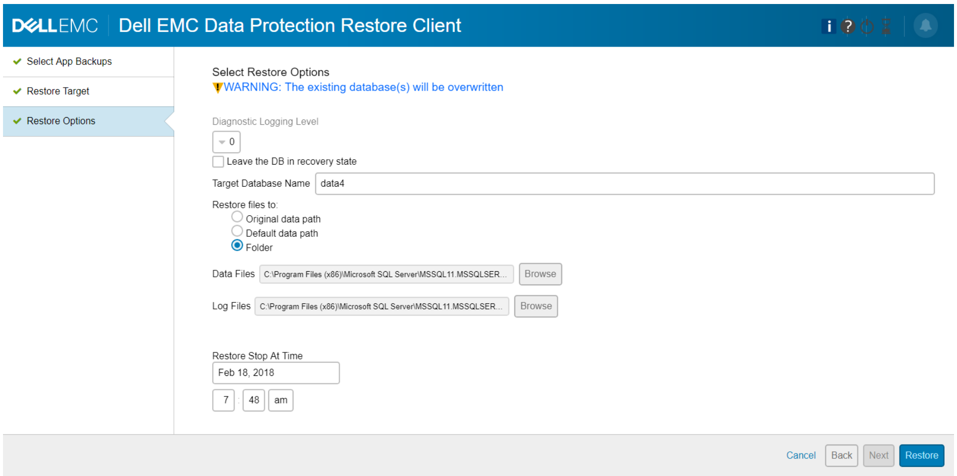
   ---

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 71 Restore Options page



✓ Select App Backups
✓ Restore Target
✓ Restore Options

Select Restore Options

WARNING: The existing database(s) will be overwritten

Diagnostic Logging Level: 0

□ Leave the DB in recovery state

Target Database Name: data4

Restore files to:
○ Original data path
○ Default data path
● Folder

Data Files: C:\Program Files (x86)\Microsoft SQL Server\MSSQL11.MSSQLSER... Browse

Log Files: C:\Program Files (x86)\Microsoft SQL Server\MSSQL11.MSSQLSER... Browse

Restore Stop At Time: Feb 18, 2018 7 : 48 am

Cancel | Back | Next | Restore

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.

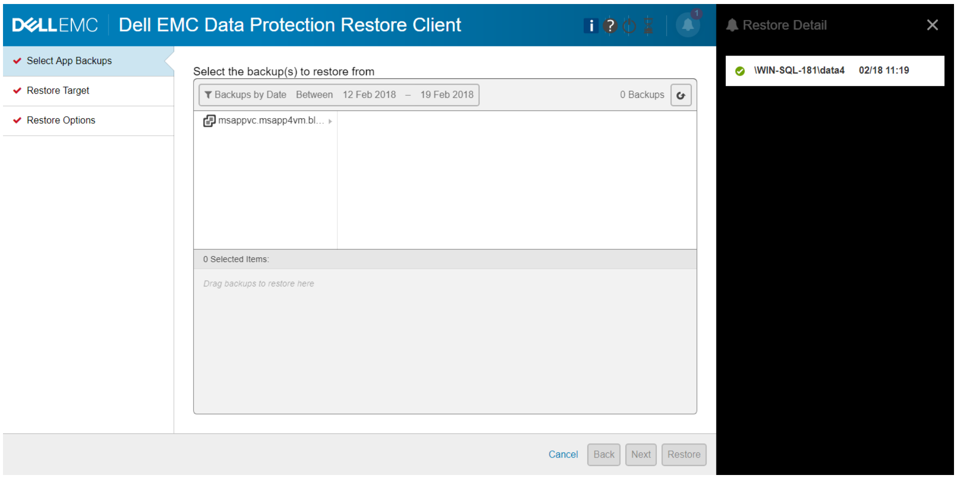
---

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 72 Restore Monitoring



Select the backup(s) to restore from

Backups by Date Between 12 Feb 2018 – 19 Feb 2018 0 Backups

msappvc.msapp4vm.bl...

0 Selected Items:

Drag backups to restore here

✓ \WIN-SQL-181\data4 02/18 11:19

vProxy recovery in the vSphere Client's Dell EMC NetWorker interface

You can also perform virtual machine image-level recoveries of vProxy backups by using the **vSphere Client** HTML-5 based **Dell EMC NetWorker** interface. Recoveries can be performed to the original virtual machine or to a new virtual machine.

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

Note

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

Connect to the NetWorker server in the vSphere Client

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

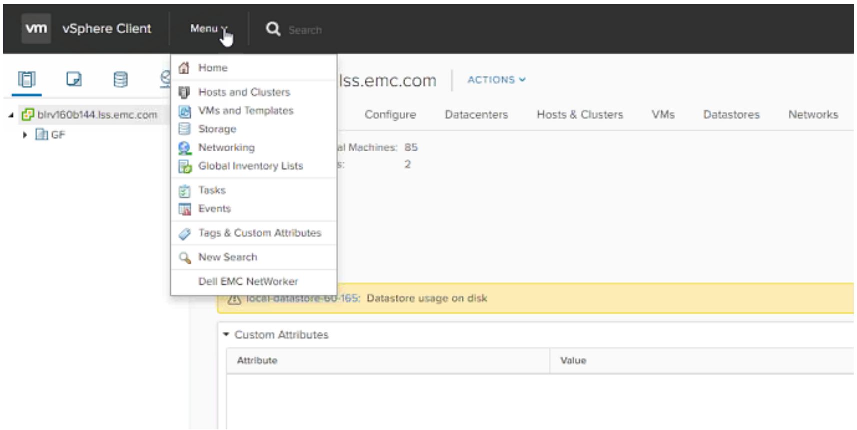
Before you begin

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

Procedure

1. Login to the **vSphere Client** as an administrator, or as a non-administrator Active Directory user that you created using the steps in the section Using the 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 73 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:

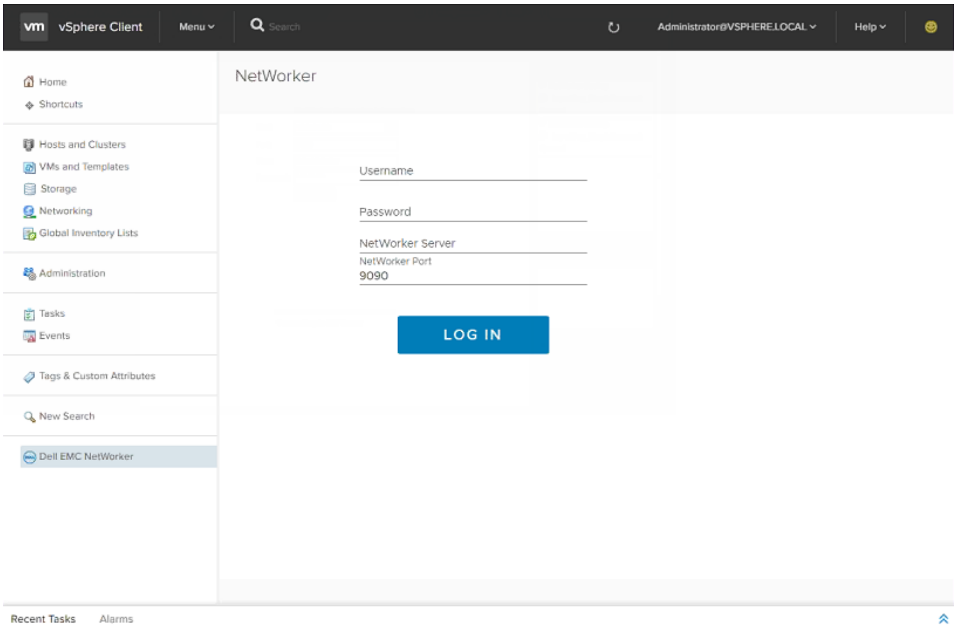
   a. In the **Username** field, type the NetWorker administrator username.

   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 74 NetWorker connection information in the vSphere Client

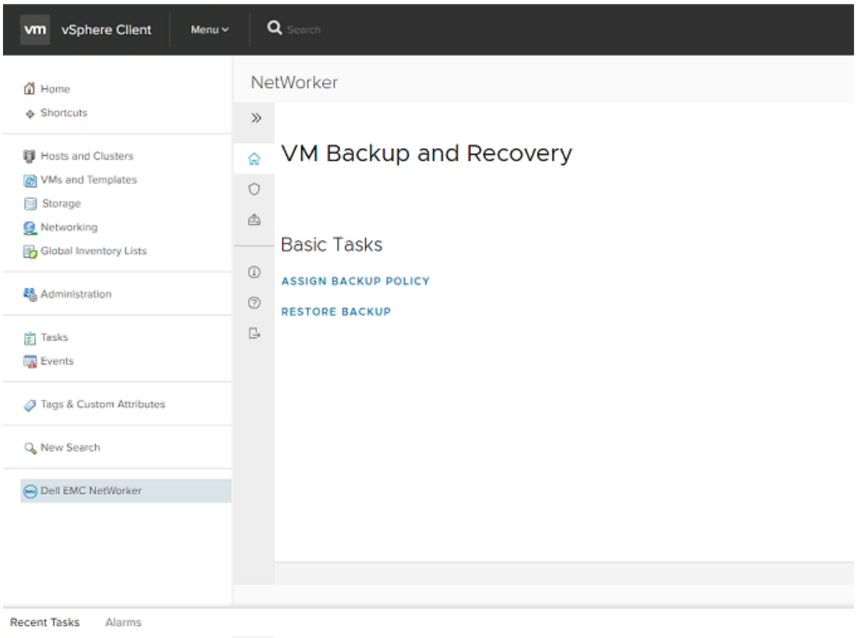


4. Click **Log in**.

Results

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

Figure 75 Dell EMC NetWorker Basic Tasks pane



Accessing the vCenter plug-in as a non-administrator Active Directory user

You can only access the vCenter plug-in (the **Dell EMC NetWorker** interface) in the **vSphere Client** if you are an NetWorker administrator or a non-administrator Active Directory user associated with appropriate privileges in NetWorker. The following procedure describes how to access the plug-in as a non-administrator Active Directory user.

Before you begin

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

Procedure

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

   ```
   CN=VMwareTeam,CN=Users,DC=vproxy,DC=com
   ```

`cn=VMwareUser,cn=Users,dc=vproxy,dc=com`
where *VMwareTeam* is the security group name, and *VMwareUser* is the Active Directory user name.

4. Log in to the **vSphere Web Client** as the Active Directory user, in the format `<tenant>\<domain>\<userid>`. For example:

   ```
   default\vproxy\VMwareUser
   ```

Results

The Active Directory user that you create using these steps will only have access to the **vSphere Client Dell EMC NetWorker** interface, and cannot be used to log in to **NetWorker Management Console**. If you also need to provide access to NMC, then add those required privileges accordingly.

Recovery to the original virtual machine

To start a vProxy image-level recovery to the original virtual machine by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

Before you begin

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

Procedure

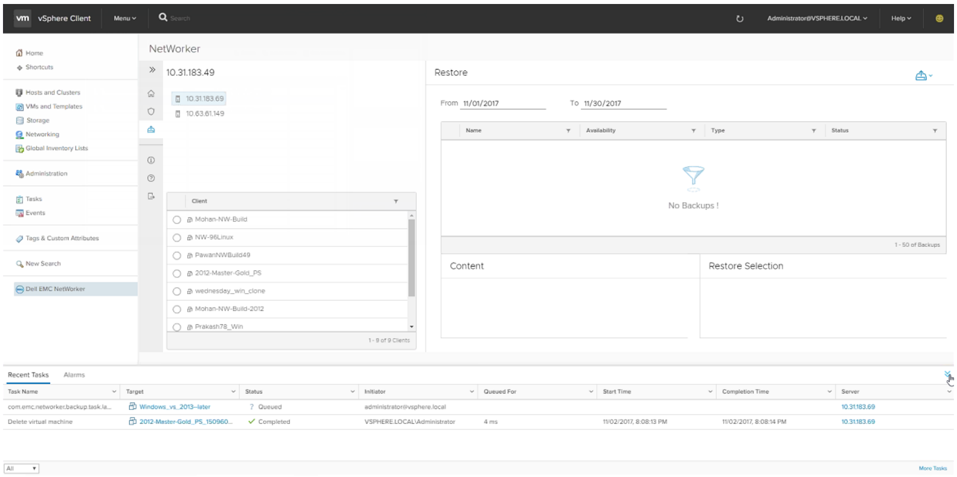
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

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

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

   A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.

   Figure 76 Restore pane with available virtual machine backups



10.31.183.49

- 10.31.183.69
- 10.63.61.149

Client
○ Mohan-NW-Build
○ NW-96Linux
○ PawanNWBuild49
○ 2012-Master-Gold_PS
○ wednesday_win_clone
○ Mohan-NW-Build-2012
○ Prakash78_Win

1 - 9 of 9 Clients

From 11/01/2017 To 11/30/2017

Name	Availability	Type	Status

1 - 50 of Backups

Recent Tasks Alarms

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
com.emc.networker.backup.task.la...	Windows_vs_2013--later	? Queued	administrator@vsphere.local				10.31.183.69
Delete virtual machine	2012-Master-Gold_PS_150960...	✓ Completed	VSPHERE.LOCAL\Administrator	4 ms	11/02/2017, 8:08:13 PM	11/02/2017, 8:08:14 PM	10.31.183.69

Note

If this list does not contain a virtual machine that was recently backed up, refresh the window.

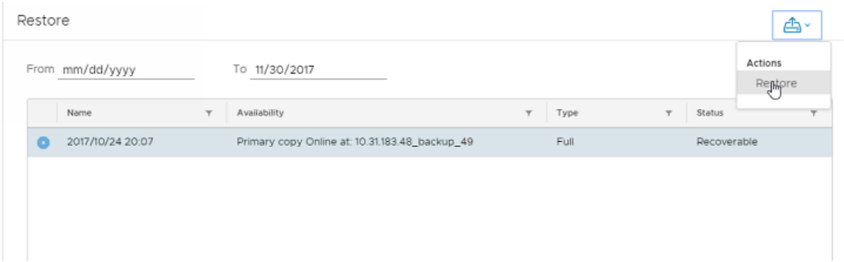
3. From the **Client** pane, click the radio button next to the virtual machine that you want to recover.

   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 77 Select Restore from the Action drop-down



Restore

From mm/dd/yyyy   To 11/30/2017

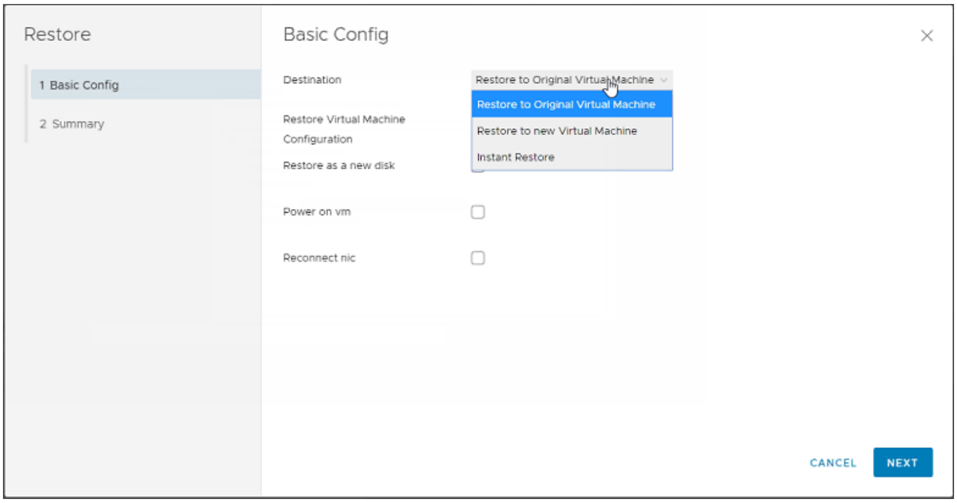
Actions
Restore

	Name	Availability	Type	Status
●	2017/10/24 20:07	Primary copy Online at: 10.31.183.48_backup_49	Full	Recoverable

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

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

   Figure 78 Restore to original location



Restore

1 Basic Config

2 Summary

Basic Config

Destination: Restore to Original Virtual Machine

- Restore to Original Virtual Machine
- Restore to new Virtual Machine
- Instant Restore

Restore Virtual Machine Configuration

Restore as a new disk

Power on vm ☐

Reconnect nic ☐

7. (Optional) Select from the following options:

   a. **Power on vm**—Select this checkbox to automatically power on the virtual machine after the restore completes.

   b. **Reconnect nic**—Select this checkbox to automatically reconnect the network interface card after the restore completes.

8. Click **Next**.

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

Results

You can monitor the progress of the recovery in the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Recovery to a new virtual machine

To start a vProxy image-level recovery to a new virtual machine by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

Procedure

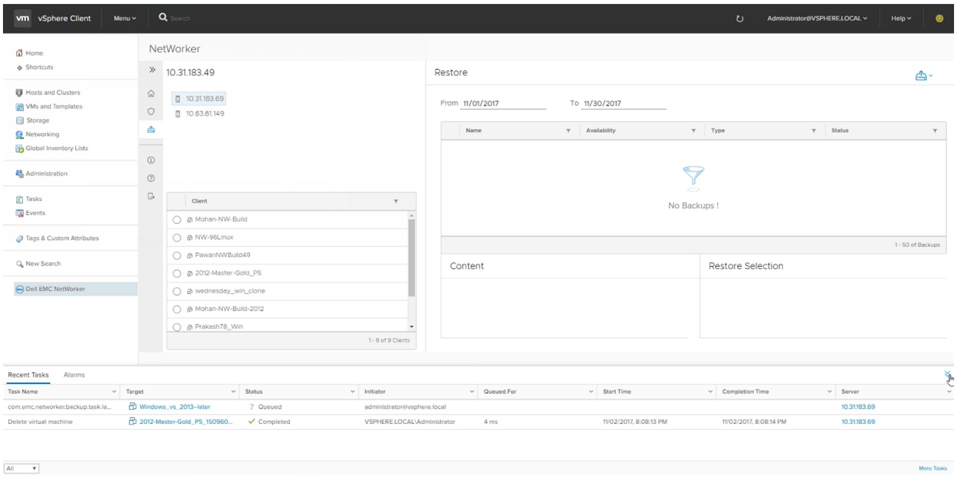
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

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

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

   A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.

   Figure 79 Restore pane with available virtual machine backups



Client
○ Mohan-NW-Build
○ NW-96Linux
○ PawanNWBuild49
○ 2012-Master-Gold_PS
○ wednesday_win_clone
○ Mohan-NW-Build-2012
○ Prakash78_Win

1 - 9 of 9 Clients

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
com.emc.networker.backup.task.la...	Windows_vs_2013--later	? Queued	administrator@vsphere.local				10.31.183.69
Delete virtual machine	2012-Master-Gold_PS_150960...	✓ Completed	VSPHERE.LOCAL\Administrator	4 ms	11/02/2017, 8:08:13 PM	11/02/2017, 8:08:14 PM	10.31.183.69

   Note

   If this list does not contain a virtual machine that was recently backed up, refresh the window.

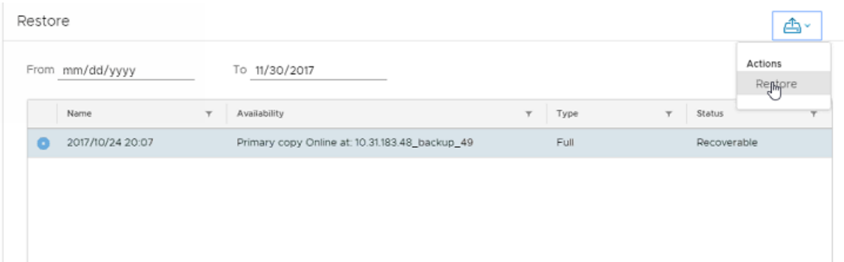
3. From the **Client** pane, click the radio button next to the virtual machine that you want to recover.

   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 80 Select Restore from the Action drop-down



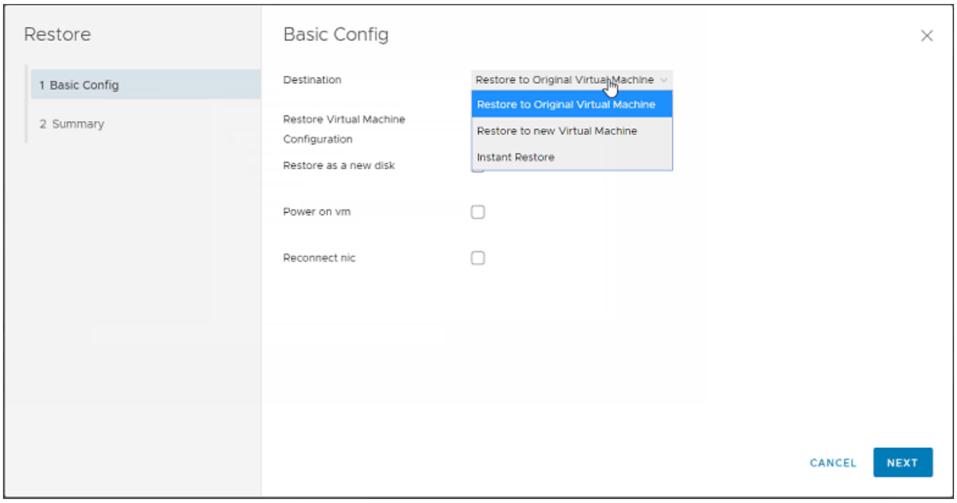
From mm/dd/yyyy To 11/30/2017

	Name	Availability	Type	Status
●	2017/10/24 20:07	Primary copy Online at: 10.31.183.48_backup_49	Full	Recoverable

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

6. From the **Destination** drop-down, select **Restore to new Virtual Machine**.

Figure 81 Restore to new virtual machine



Destination: Restore to Original Virtual Machine

Restore Virtual Machine Configuration

Restore as a new disk

Power on vm □

Reconnect nic □

7. (Optional) Select from the following options:
   a. **Restore Virtual Machine Configuration**—Select this checkbox to restore this virtual machine with the existing configuration settings.
   b. **Power on vm**—Select this checkbox to automatically power on the virtual machine after the restore completes.
   c. **Reconnect nic**—Select this checkbox to automatically reconnect the network interface card after the restore completes.

8. Click **Next**.

   The **Advanced Config** page displays.

9. From the **vCenter** drop-down, select the destination vCenter server, and then specify a name for the new virtual machine. Click **Next**.

   The **Location** page displays.

10. Expand the vCenter server tree and select a destination for recovery within the vCenter server, and then click **Next**.

    The **Host/Cluster** page displays.

11. Select a host within the destination datacenter, and then click **Next**.

    The **Resource Pool** page displays.

12. Select a resource pool, and then click **Next**.

    The **Datastore** page displays.

13. From the **Destination Datastore** drop-down, select a datastore that is compatible with the virtual machine, and then click **Next**.
14. In the **Summary** page, review the information and then click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Virtual disk recovery (restore to an existing virtual machine)

To start a VMDK recovery to an existing virtual machine by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

Procedure

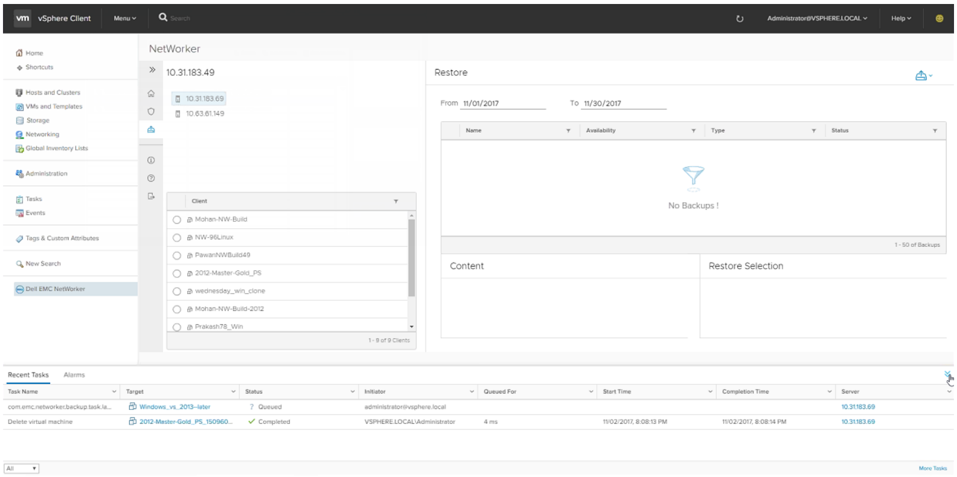
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

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

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

   A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.

   Figure 82 Restore pane with available virtual machine backups



10.31.183.49

10.31.183.69
10.63.61.149

	Client
○	Mohan-NW-Build
○	NW-96Linux
○	PawanNWBuild49
○	2012-Master-Gold_PS
○	wednesday_win_clone
○	Mohan-NW-Build-2012
○	Prakash78_Win

1 - 9 of 9 Clients

From 11/01/2017 To 11/30/2017

Name	Availability	Type	Status

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
com.emc.networker.backup.task.la...	Windows_vs_2013--later	? Queued	administrator@vsphere.local				10.31.183.69
Delete virtual machine	2012-Master-Gold_PS_150960...	✓ Completed	VSPHERE.LOCAL\Administrator	4 ms	11/02/2017, 8:08:13 PM	11/02/2017, 8:08:14 PM	10.31.183.69

   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.

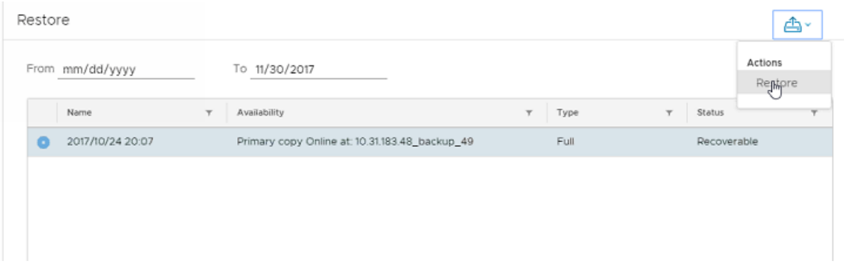
   A list of available restore points for that virtual machine displays in the right pane. You can also specify a date range to view only the virtual machine backups that were performed within that range.

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 83 Select Restore from the Action drop-down

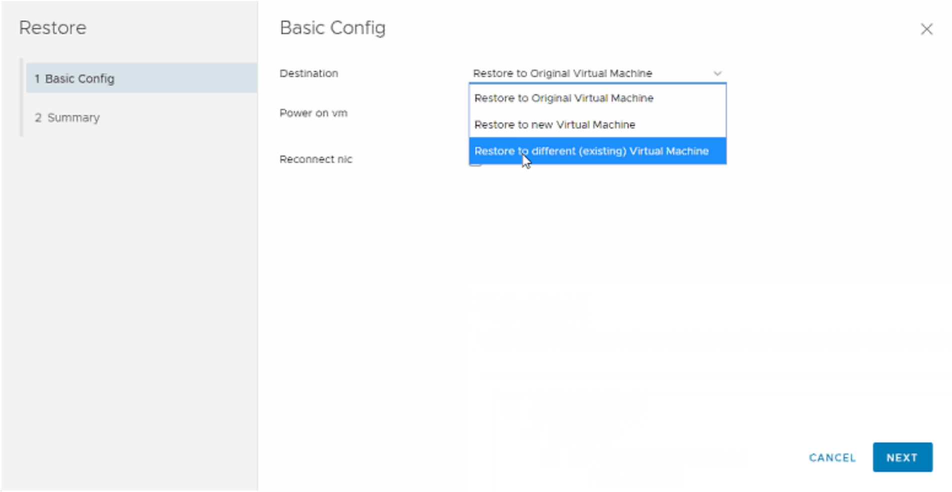


Name	Availability	Type	Status
2017/10/24 20:07	Primary copy Online at: 10.31.183.48_backup_49	Full	Recoverable

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

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

Figure 84 Restore virtual disks to existing virtual machine


Restore
1 Basic Config
2 Summary
Basic Config
Destination
Restore to Original Virtual Machine
Power on vm
Reconnect nic
Restore to Original Virtual Machine
Restore to new Virtual Machine
Restore to different (existing) Virtual Machine
CANCEL
NEXT

8. (Optional) Select from the following options:
   a. **Reconnect nic**—Select this checkbox to automatically reconnect the network interface card after the restore completes.
   b. **Power on vm**—Select this checkbox to automatically power on the virtual machine after the restore completes.
9. Click **Next**.

   The **Advanced Config** page displays.
10. In the **Host/Cluster** pane, select the location in the datacenter of the existing virtual machine(s). A list of virtual machines for this location displays in the **Virtual Machines** pane. You can click the + icon next to a virtual machine to view more details.
11. Click **Next**.

    The **Datastore** page displays.
12. For each virtual disk listed in the **Datastore** pane, select a **Destination Datastore** from the drop-down, and then click **Next**.

13. In the **Summary** page, review the information and then click **Finish** to start the recovery.

    ⚠ **WARNING**

    When you start a VMDK recovery, the virtual machine will be powered off automatically without issuing a warning message.

Results

You can monitor the progress of the recovery in the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Instant recovery of a virtual machine

To start an instant recovery to a new virtual machine by using the **Dell EMC NetWorker** interface in the **vSphere Client**, perform the following steps.

Before you begin

Note the following before performing an instant recovery in the **Dell EMC NetWorker** interface:

- Ensure that you provide the management credentials for the Data Domain resource before you initiate the recovery. If you do not configure the management credentials in NMC prior to the recovery, the recovery will fail silent without an error message. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only) provides instructions.
- Ensure that you do not perform an instant recovery of virtual machines in resource pools and other similar containers that are part of a currently running protection group.
- Ensure that the free space on the Data Domain system is equal to or greater than the total disk size of the virtual machine being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target virtual machine fails.

Procedure

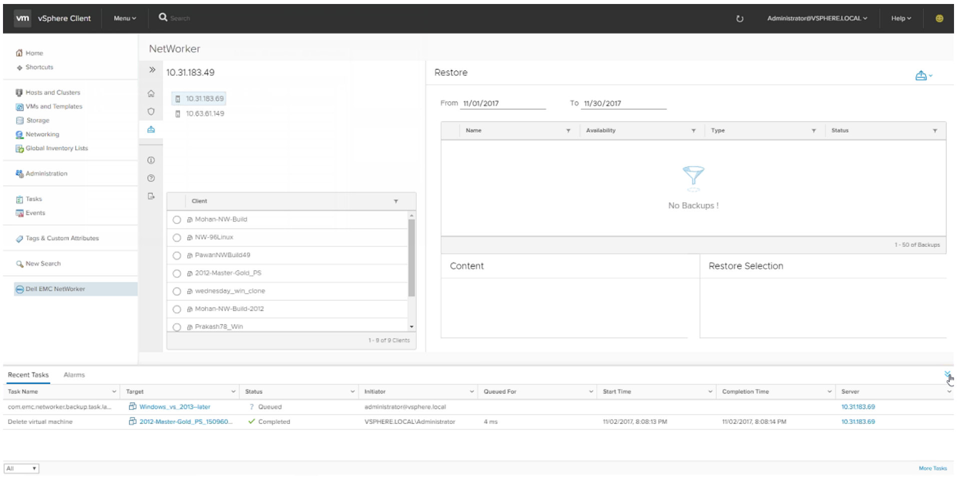
1. In the **vSphere Client**, if not already selected, click **Dell EMC NetWorker** in the left pane.

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

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

   A list of existing virtual machine client backups for the selected vCenter server host displays in the **Client** pane.

Figure 85 Restore pane with available virtual machine backups



10.31.183.49

10.31.183.69
10.63.61.149

Client
○ Mohan-NW-Build
○ NW-96Linux
○ PawanNWBuild49
○ 2012-Master-Gold_PS
○ wednesday_win_clone
○ Mohan-NW-Build-2012
○ Prakash78_Win

1 - 9 of 9 Clients

From 11/01/2017 To 11/30/2017

Name	Availability	Type	Status

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
com.emc.networker.backup.task.la...	Windows_vs_2013--later	? Queued	administrator@vsphere.local				10.31.183.69
Delete virtual machine	2012-Master-Gold_PS_150960...	✓ Completed	VSPHERE.LOCAL\Administrator	4 ms	11/02/2017, 8:08:13 PM	11/02/2017, 8:08:14 PM	10.31.183.69

Note

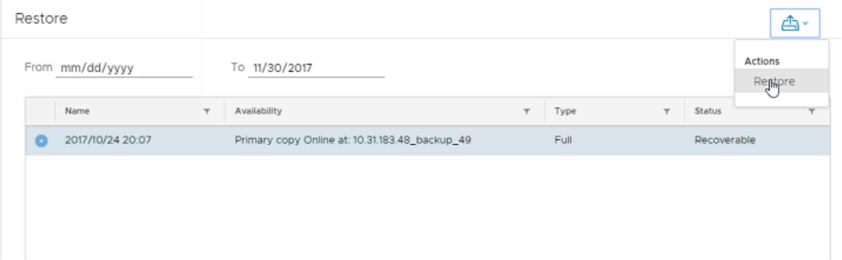
If this list does not contain a virtual machine that was recently backed up, refresh the window.

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 86 Select Restore from the Action drop-down

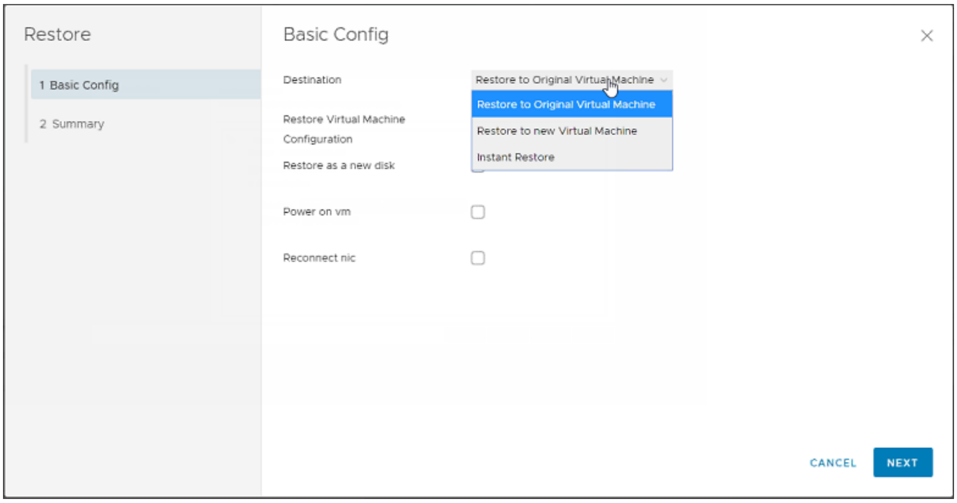
   From mm/dd/yyyy To 11/30/2017

	Name	Availability	Type	Status
●	2017/10/24 20:07	Primary copy Online at: 10.31.183.48_backup_49	Full	Recoverable

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

6. From the **Destination** drop-down, select **Instant Restore**.

Figure 87 Instant Restore



Restore
1 Basic Config
2 Summary
Basic Config
Destination
Restore to Original Virtual Machine
Restore to Original Virtual Machine
Restore to new Virtual Machine
Instant Restore
Restore Virtual Machine Configuration
Restore as a new disk
Power on vm
Reconnect nic
CANCEL
NEXT

7. Click **Next**.

   The **Advanced Config** page displays.

8. Specify a name for the new virtual machine, and then click **Next**.

   The **Location** page displays.

9. Expand the vCenter server tree and select a destination for recovery within the vCenter server, and then click **Next**.

   The **Host/Cluster** page displays.

10. Select a host within the destination datacenter, and then click **Next**.

    The **Resource Pool** page displays.

11. Select a resource pool, and then click **Next**.

12. In the **Summary** page, review the information and then click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Recent Tasks** pane. Once the instant restore completes, use storage vMotion to save the virtual machine, and then cancel the vSphere **NetWorker Recovery** task to delete the datastore. Power ON the virtual machine to validate the recovery.

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

If using a vSphere version prior to 6.5, you can still use the vSphere Web Client's flash-based **VM Backup and Recovery** interface to perform image-level recoveries to the original virtual machine or to a new virtual machine.

In the **vSphere Web Client**, click **VM Backup and Recovery** in the left navigation pane. Once you establish a connection to the required NetWorker server, click the **Restore** tab to open the **Restore** pane.

Connect to the NetWorker server in the vSphere Web Client

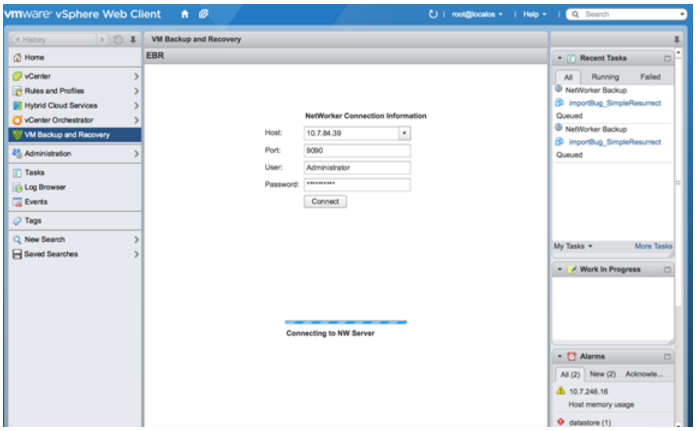
After installing the vCenter plug-in, you must establish a connection to the NetWorker server before performing any vProxy operations in the vSphere Web Client.

Procedure

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

   The required NetWorker connection information appears in the right pane.

   Figure 88 NetWorker connection information in the vSphere Web Client



NetWorker Connection Information

Host: 10.7.84.39

Port: 9090

User: Administrator

Password: **********

Connect

Connecting to NW Server

3. Enter the following information for the NetWorker server:

   a. In the **Host** field, type the IP address of the NetWorker server.

   b. In the **Port** field, type **9090**.

   c. In the **User** field, type the NetWorker administrator username.

   d. In the **Password** field, type the NetWorker administrator password.
4. Click **Connect**.

Results

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

Accessing the vCenter plug-in as a non-administrator Active Directory user

You can only access the vCenter plug-in (the VM Backup and Recovery interface) in the vSphere Web Client if you are an NetWorker administrator or a non-administrator Active Directory user associated with appropriate privileges in NetWorker . The following procedure describes how to access the plug-in as a non-administrator Active Directory user.

Before you begin

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

Procedure

1. Create a **vmwareAdmin** group in NetWorker that contains the following privileges at a minimum:

- View Security Settings
- View Application Settings
- Remote Access All Clients
- Operate NetWorker
- Monitor NetWorker
- Operate Devices and Jukeboxes
- Recover Local Data
- Recover Remote Data
- Backup Local Data

2. Create an Active Directory user within your desired security group.
3. Add the user and group to the NetWorker Management Console's **External Roles** attribute. For example:

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

   ```
   default\vproxy\VMwareUser
   ```

Results

The Active Directory user that you create using these steps will only have access to the **vSphere Web Client VM Backup and Recovery** interface, and cannot be used to log in to NetWorker Management Console. If you also need to provide access to NMC, then add those required privileges accordingly.

Recovery to the original virtual machine

In the vSphere Web Client's **VM Backup and Recovery** interface, use the following procedure to perform an image-level recovery to the original virtual machine.

Before you begin

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

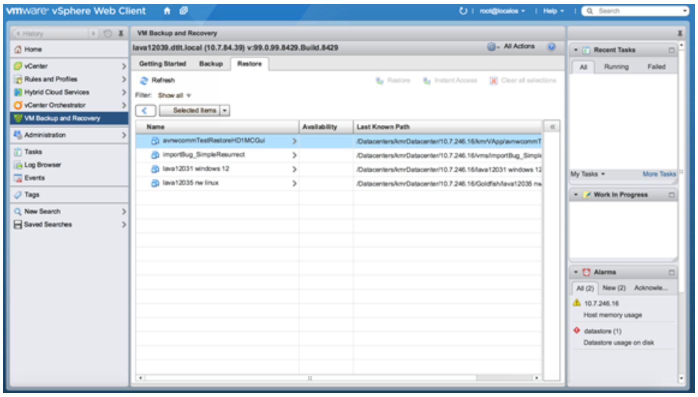
Procedure

1. Login to the **vSphere Web Client** as an administrator.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

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

   A list of virtual machines available for recovery displays.

Figure 89 Virtual machines for recovery in the Restore pane



VM Backup and Recovery

lava12039.dtlt.local (10.7.84.39) v:99.0.99.8429.Build.8429

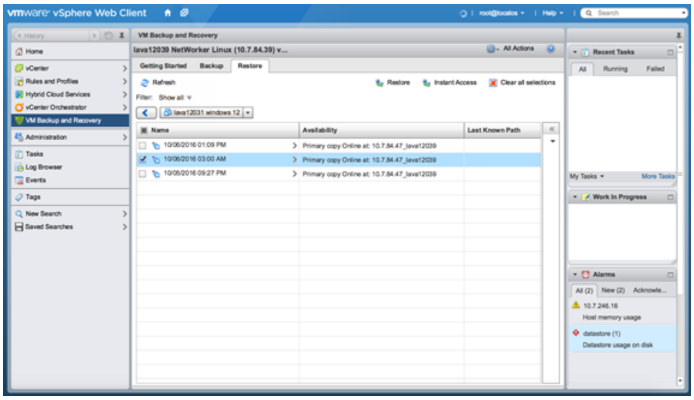
Filter: Show all

Name	Availability	Last Known Path
avnwcommTestRestoreHD1MCGui		/Datacenters/kmrDatacenter/10.7.246.16/kmrVApp/avnwcommT
importBug_SimpleResurrect		/Datacenters/kmrDatacenter/10.7.246.16/vms/importBug_Simple
lava12031 windows 12		/Datacenters/kmrDatacenter/10.7.246.16/lava12031 windows 12
lava12035 nw linux		/Datacenters/kmrDatacenter/10.7.246.16/Goldfish/lava12035 nw

If you do not see the virtual machine backup listed, refresh the window.

4. Browse the list of virtual machines and select the virtual machine backup you want to recover. You can expand the virtual machine backup to view a list of restore points from which to select.

Figure 90 Select a restore point



VM Backup and Recovery

lava12039 NetWorker Linux (10.7.84.39) v...

Filter: Show all

lava12031 windows 12

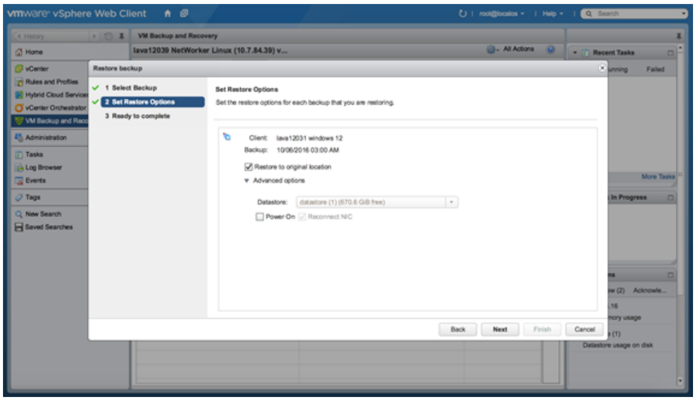
Name	Availability	Last Known Path
□ 10/06/2016 01:09 PM	Primary copy Online at: 10.7.84.47_lava12039	
☑ 10/06/2016 03:00 AM	Primary copy Online at: 10.7.84.47_lava12039	
□ 10/05/2016 09:27 PM	Primary copy Online at: 10.7.84.47_lava12039	

5. Select one of the restore points by clicking the checkbox next to the backup time, and then click **Restore**.

   The **Restore Backup** wizard launches.

6. In the **Set Restore Options** page of the **Restore Backup** wizard, leave the default **Restore to original location** selected and click **Next**.

Figure 91 Restore to original location



Restore backup

1 Select Backup
2 Set Restore Options
3 Ready to complete

Set Restore Options

Set the restore options for each backup that you are restoring.

Client: lava12031 windows 12
Backup: 10/06/2016 03:00 AM

☑ Restore to original location

Advanced options

Datastore: datastore (1) (670.6 GiB free)

□ Power On ☑ Reconnect NIC

7. In the **Ready to Complete** page, click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Running** tab of the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Recovery to a new virtual machine

In the vSphere Web Client's **VM Backup and Recovery** interface, use the following procedure to perform an image-level recovery to a new virtual machine.

Procedure

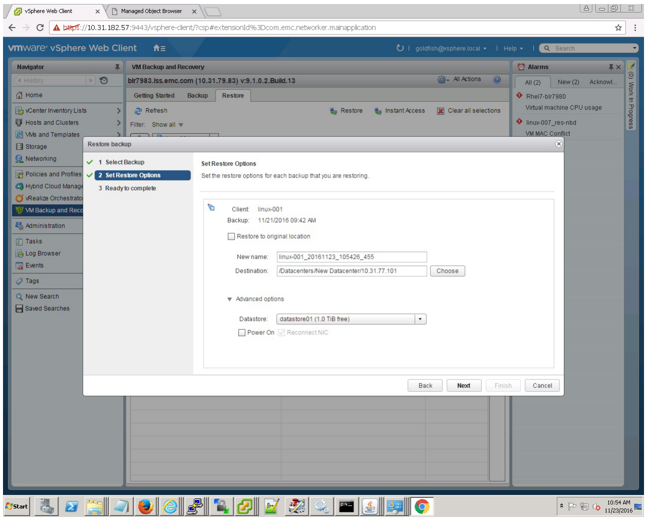
1. Login to the **vSphere Web Client** as an administrator.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   When a connection to the NetWorker server is established, the **Getting Started** pane appears.
3. Click the **Restore** tab to open the **Restore** pane.

   If you do not see the virtual machine backup listed, refresh the window.
4. Browse the list of virtual machines and select the virtual machine backup you want to recover. You can expand the virtual machine backup to view a list of restore points from which to select.
5. Select one of the restore points by clicking the checkbox next to the backup time, and then click **Restore**.

   The **Restore Backup** wizard launches.
6. In the **Set Restore Options** page of the **Restore Backup** wizard, uncheck the default **Restore to original location**.
7. Specify a name for the new virtual machine, and select a destination for recovery in the vCenter server. You are not required to select the **Choose** button and can ignore the text New or Existing.

   Figure 92 Restore options for the new virtual machine recovery



blr7983.lss.emc.com (10.31.79.83) v:9.1.0.2.Build.13

Restore backup

1 Select Backup
2 Set Restore Options
3 Ready to complete

Set Restore Options

Set the restore options for each backup that you are restoring.

Client: linux-001
Backup: 11/21/2016 09:42 AM

□ Restore to original location

New name: linux-001_20161123_105426_455
Destination: /Datacenters/New Datacenter/10.31.77.101

Advanced options

Datastore: datastore01 (1.0 TiB free)

□ Power On ☑ Reconnect NIC

8. Specify a datastore for the virtual machine, and then click **Next**.
9. In the **Ready to Complete** page, click **Finish** to start the recovery.

Results

You can monitor the progress of the recovery in the **Running** tab of the **Recent Tasks** pane. Once the recovery completes successfully, power ON the virtual machine to validate the recovery.

Virtual disk recovery

In the vSphere Web Client's **VM Backup and Recovery** interface, use the following procedure to perform a VMDK recovery to an existing virtual machine.

Procedure

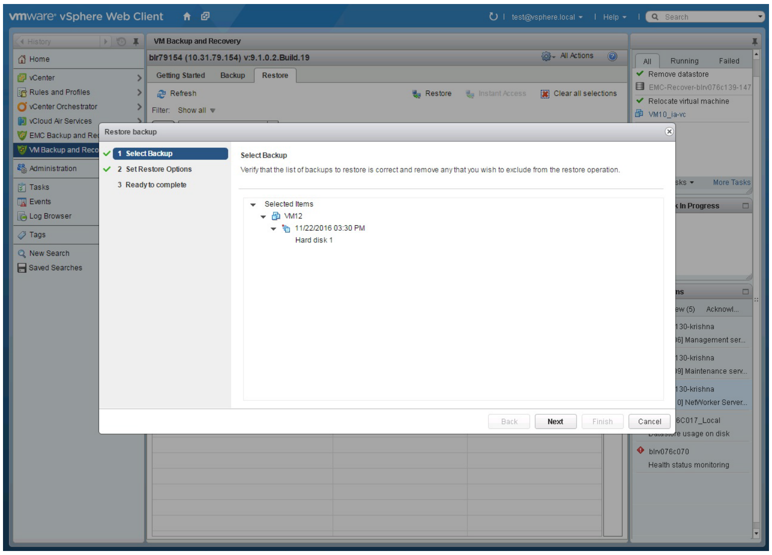
1. Log in to the **vSphere Web Client** as an administrator.
2. In the **vSphere Web Client**, click **VM Backup and Recovery** in the left pane.

   When a connection to the NetWorker server is established, the **Getting Started** pane displays.
3. Click the **Restore** tab to open the **Restore** pane.

   If you do not see the virtual machine backup listed, refresh the window.
4. Browse the list of virtual machines and select the virtual machine backup that contains the VMDK you want to recover. You can expand the virtual machine backup to view a list of restore points from which to select.
5. Double-click one of the restore points to view the list of available VMDKs for the virtual machine.
6. Select the VMDK you want to restore by selecting the checkbox next to the VMDK, and then click **Restore**.

   The **Restore Backup** wizard launches.

Figure 93 Select VMDK backup to restore



Restore backup

1 Select Backup
2 Set Restore Options
3 Ready to complete

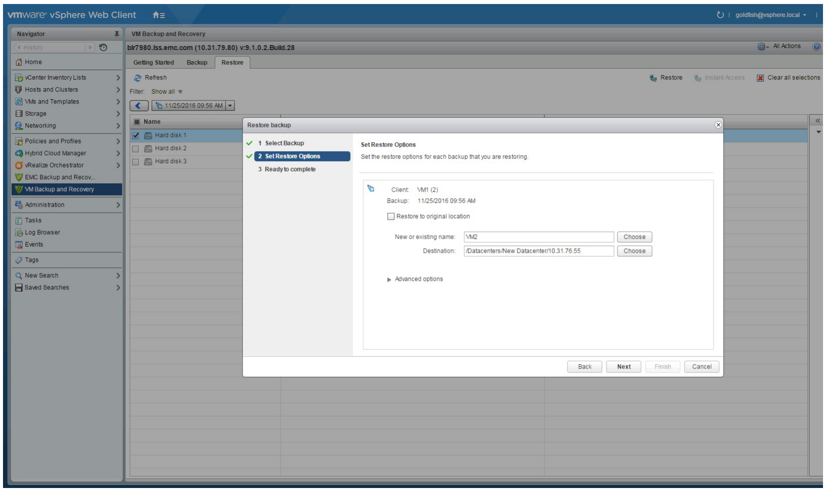
Select Backup

Verify that the list of backups to restore is correct and remove any that you wish to exclude from the restore operation.

- Selected Items
  - VM12
    - 11/22/2016 03:30 PM
      - Hard disk 1

7. In the **Select Backup** page, verify that the correct VMDK is selected and click **Next**.
8. In the **Set Restore Options** page, uncheck the default **Restore to original location** and then click **Next**.
9. Click **Choose** to browse the existing virtual machine where the VMDK needs to be restored in the vCenter.

Figure 94 Set Restore Options for VMDK recovery



Restore backup

1 Select Backup
2 Set Restore Options
3 Ready to complete

Set Restore Options

Set the restore options for each backup that you are restoring.

Client: VM1 (2)
Backup: 11/25/2016 09:56 AM

□ Restore to original location

New or existing name: VM2
Destination: /Datacenters/New Datacenter/10.31.76.55

▶ Advanced options

10. Specify a datastore for the VMDK, and then click **Next**.
11. In the **Ready to Complete** page, click **Finish** to start the recovery.

Results

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

Note

When you start a VMDK recovery, the virtual machine will be powered off automatically without issuing a warning message.

Instant recovery of a virtual machine

In the vSphere Web Client's **VM Backup and Recovery** interface, use the following procedure to perform an instant access recovery to a new virtual machine.

Before you begin

Note the following before performing an instant access recovery in the **VM Backup and Recovery** plug-in:

- Ensure that you provide the management credentials for the Data Domain resource before you initiate the recovery. If you do not configure the management credentials in NMC prior to the recovery, the recovery will fail silent without an error message. The section Entering management credentials for the Data Domain resource (instant recovery and User mode file-level restore only) provides instructions.
- Ensure that you do not perform an instant recovery of virtual machines in resource pools and other similar containers that are part of a currently running protection group.
- Ensure that the free space on the Data Domain system is equal to or greater than the total disk size of the virtual machine being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target virtual machine fails.

Procedure

1. Log in to the **vSphere Web Client** as an administrator.

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

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

3. Click the **Restore** tab to open the **Restore** pane.

   If you do not see the virtual machine backup listed, refresh the window.

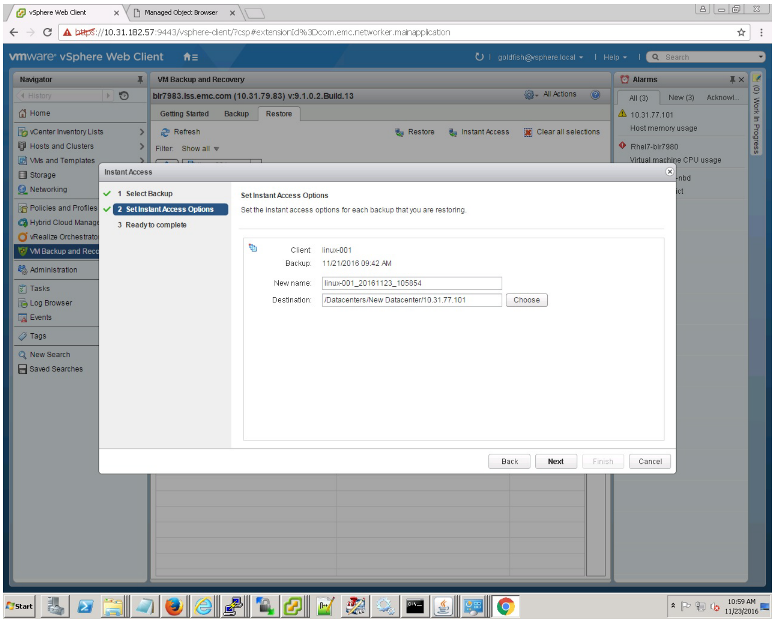
4. Browse the list of virtual machines and select the virtual machine backup you want to recover. You can expand the virtual machine backup to view a list of restore points from which to select.

5. Select one of the restore points by selecting the checkbox next to the backup time, and then click **Instant Access**.

   The **Restore Backup** wizard launches.

6. In the **Set Instant Access Options** page, specify a name for the new virtual machine, and select a destination for recovery in the vCenter server, and then click **Next**. You can ignore the text New or Existing.

   Figure 95 Set Instant Access restore options



VM Backup and Recovery

blr7983.lss.emc.com (10.31.79.83) v:9.1.0.2.Build.13

Instant Access

1 Select Backup
2 Set Instant Access Options
3 Ready to complete

Set Instant Access Options

Set the instant access options for each backup that you are restoring.

Client: linux-001

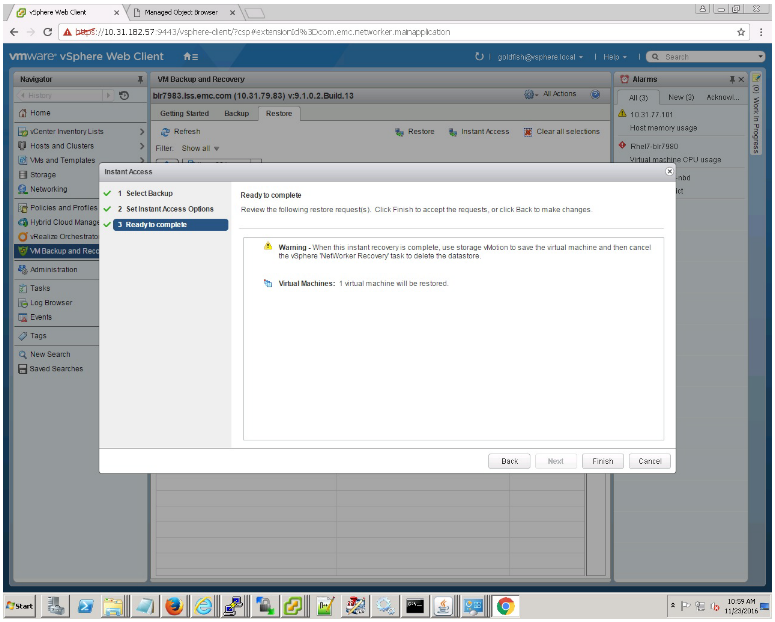
Backup: 11/21/2016 09:42 AM

New name: linux-001_20161123_105854

Destination: /Datacenters/New Datacenter/10.31.77.101

7. In the **Ready to Complete** page, click **Finish** to start the recovery.

Figure 96 Finish Instant Access recovery



Instant Access

1 Select Backup

2 Set Instant Access Options

3 Ready to complete

Ready to complete

Review the following restore request(s). Click Finish to accept the requests, or click Back to make changes.

Warning - When this instant recovery is complete, use storage vMotion to save the virtual machine and then cancel the vSphere 'NetWorker Recovery' task to delete the datastore.

Virtual Machines: 1 virtual machine will be restored.

Results

You can monitor the progress of the recovery in the **Running** tab of the **Recent Tasks** pane. Once the instant access recovery completes, use storage vMotion to save the virtual machine, and cancel the vSphere **NetWorker Recovery** task to delete the datastore. Power ON the virtual machine to validate the recovery.

vProxy recovery log files

The vProxy appliance contains log files, which you can configure to display debug information.

The following table provides information about the vProxy recovery log files and how to enable debugging.

Table 15 Recovery log files

Log file	Log location and name	Logging levels
Primary recovery log	For image level recoveries, `/opt/emc/vrproxy/runtime/logs/vrecoverd/vrecoverd-engine.log`. For file-level recoveries or SQL application-consistent recoveries, `/opt/emc/vrproxy/runtime/logs/vflrd/vflrd-engine.log`.	To modify the logging level: 1. Edit the `/usr/lib/systemd/system/vrecoverd.service` file. 2. Search for the for the *ExecStart=* string. 3. Edit the *--program-log-level=* argument with one of the following values: • warn • info • trace • debug 4. Reload the unit config file into systemd: **`systemctl daemon-reload`**

Table 15 Recovery log files (continued)

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

CHAPTER 5

NetWorker VMware Protection with the VMware Backup Appliance (legacy)

This chapter contains the following topics:

Introduction to NetWorker VMware Protection with the VMware Backup appliance (legacy)

NetWorker VMware Protection with the VMware Backup appliance is a NetWorker-integrated VMware backup, monitoring and recovery solution introduced in NetWorker 8.x. This solution allows you to assign backup and cloning policies for a VMware Backup appliance to Datacenters, Clusters, virtual machines and VMDKs within NMC's **NetWorker Administration** window. You can also perform image-level, VMDK, or file-level recoveries of those backups.

This solution becomes available when you deploy the VMware Backup appliance in the vSphere server and register the appliance with NetWorker and vCenter. After running policy workflows, you can then perform full recoveries or VMDK-level recoveries of these backups from the **vSphere Web Client EMC Backup and Recovery** plug-in, or file-level recoveries from the **Dell EMC Data Protection Restore Client** user interface.

Note

NetWorker 18.1 does not support the creation of new VMware Backup appliance policies. After upgrading to NetWorker 18.1, you can only schedule a backup of existing VMware Backup appliance policies created in NetWorker 9.0.x releases, or modify what contents are included in the existing policies. For the creation of new policies, use the vProxy appliance.

It is strongly recommended to upgrade both the NetWorker server and storage node to the latest NetWorker release, and use the latest available VMware Backup appliance. NetWorker 18.1 does not feature a new version of the VMware Backup appliance, but supports the OVA and proxy version compatible with Networker 9.0 and 9.0.1 for running existing VMware Backup appliance policies.

NetWorker VMware Protection tasks for the VMware Backup appliance

The following table compares tasks in NMC's **NetWorker Administration** window with tasks in the **vSphere Web Client** and the **Dell EMC Data Protection Restore client** for NetWorker VMware Protection with the VMware Backup appliance.

Table 16 NetWorker VMware Data Protection tasks

Program/Role	Task
NMC NetWorker Administration window	• Modify Data Protection policies to perform actions such as backup, clone, and checkpoint backup for disaster recovery. • Assign a checkpoint discover policy to the VMware Backup appliance. • Assign virtual machines/VMDKs to the policy.

Table 16 NetWorker VMware Data Protection tasks (continued)

Program/Role	Task
	• Start or schedule a group/policy to run any backup and clone actions associated with the group/policy. When you start a policy from the **NetWorker Administration** window, you can perform both backups and clones, based on the actions defined in the policy.
EMC Backup and Recovery user interface in the VMware vSphere Web Client	• Assign VMs/VMDKs to a VMware Backup appliance policy workflow. • Start an on-demand (ad-hoc) backup using **Backup Now**, which runs the entire workflow with associated backup and clone actions, and **Backup only out of date sources** options. • Restore a FULL virtual machine (image-level) backup. • Restore a VMDK backup. • Instant restore from a Data Domain system.
Dell EMC Data Protection Restore Client	• Perform file-level restores.
CLI	• Perform FULL VM and VMDK-level backup and restore. • Perform file-level restores. • Perform external proxy deployment.

System requirements

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

After upgrading to NetWorker 18.1, in order to continue using the VMware Backup appliance to run or modify existing policies, ensure that the NetWorker server and storage node are at the same version, and that you install or upgrade to the latest OVA version of the VMware Backup appliance, which is version 1.5.1.7.

Note

The VMware Backup appliance is available in two capacities — a 0.5 TB and 4 TB OVA. You only need to download one of these appliances, based on your system requirements.

Table 17 NetWorker VMware Protection requirements

Component	Requirements
NetWorker	NetWorker 18.1 server software with NMC. NetWorker VMware Protection only supports the following NetWorker server architectures: • Windows 64-bit • Linux x86_64
VMware Backup appliance (0.5 TB OVA)	• Version 1.5.1.7 • CPU: 4 * 2 GHz • Memory: 8GB • Disks: 3* 250 GB • Backup storage capacity: 0.5 TB • OS: 250 GB • Internet Protocol: IPv4 only, IPv6 only, or dual stack
VMware Backup appliance (4 TB OVA)	• Version 1.5.1.7 • CPU: 4 * 2 GHz • Memory: Refer to Table 20 on page 216 • Disks: 6 * 1 TB • Backup storage capacity: 4 TB • OS: 250 GB • Internet Protocol: IPv4 only, IPv6 only, or dual stack
Proxy appliance	• Version 1.5.1.7 • CPU: 4 * 2 GHz • Memory: 4 GB • Disks: 2 disks (16 GB and 1 GB) • Internet Protocol: IPv4 only, IPv6 only, or dual stack
vCenter server	• Version 5.5.x and 6.0.x • Linux or Windows platform, or VC appliance • vSphere Web Client (the VMware website provides information for supported web browsers). In order to access the EMC Backup and Recovery user interface in the vSphere Web Client, you must enable web browsers with Adobe Flash Player version 11.5 or later. Since Linux platforms only support up to Adobe Flash Player version 11.2, only Windows platforms can

Table 17 NetWorker VMware Protection requirements (continued)

Component	Requirements
	access the EMC Backup and Recovery user interface.
ESX/ESXi server	• Version 5.5.x and 6.0.x • Changed Block Tracking (CBT) enabled Note Adding containers or virtual machines to a policy will automatically enable CBT.
Data Domain	• Data Domain system OS at DDOS 5.7 and later Note The compatibility guide, available at http://compatibilityguide.emc.com:8080/CompGuideApp/, provides detailed information on NetWorker and DD Boost version compatibility. • DDBoost user requires administrator privileges

Port requirements

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

Table 18 Incoming port requirements

From	To	Port	Purpose
Data Domain	VMware Backup appliance	161	SNMP traps
NetWorker server	VMware Backup appliance	8543	NetWorker VMware Protection web service calls to initiate and monitor backups
NetWorker server	VMware Backup appliance	7937-9936 (RPC)	Checkpoint backups
ESX server	VMware Backup appliance and external proxy	902	NBD backups
Dell EMC Data Protection Restore Client	VMware Backup appliance	8543	File-level restore (FLR)

Table 18 Incoming port requirements (continued)

From	To	Port	Purpose
EMC Backup and Recovery Configuration Utility	VMware Backup appliance	8580, 8543	VMware Backup appliance configuration
vCenter server	VMware Backup appliance	7778, 7779, 8509, 9443	EMC Backup and Recovery user interface in the vSphere Web Client

The following diagram shows the incoming firewall port configuration with the VMware Backup appliance.

Figure 97 Firewall configuration (VMware Backup appliance with internal proxy)

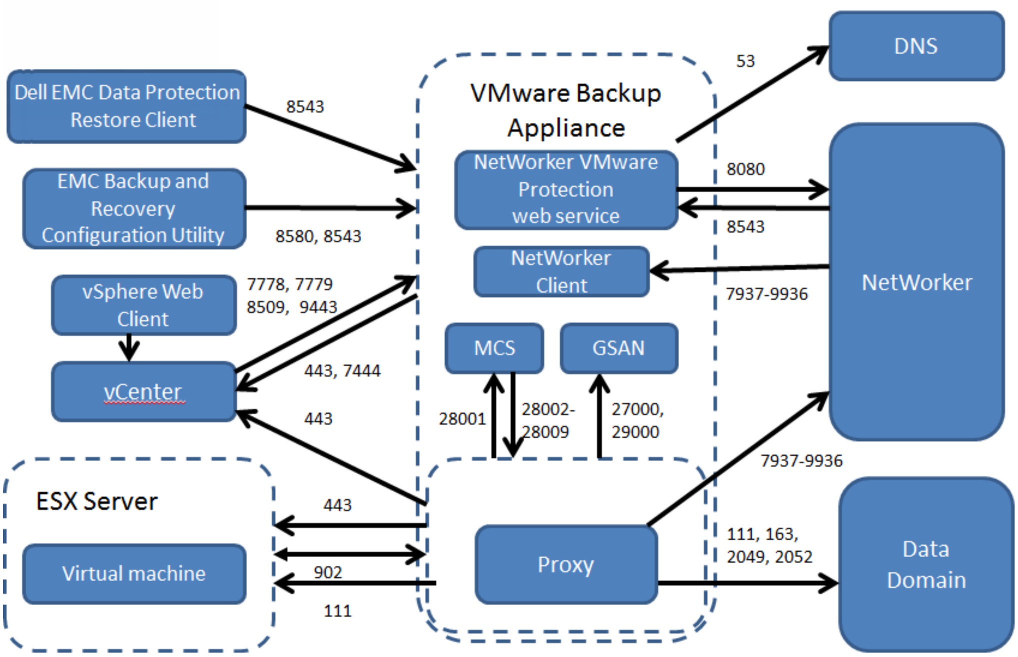


Table 19 Outgoing port requirements — with external proxies

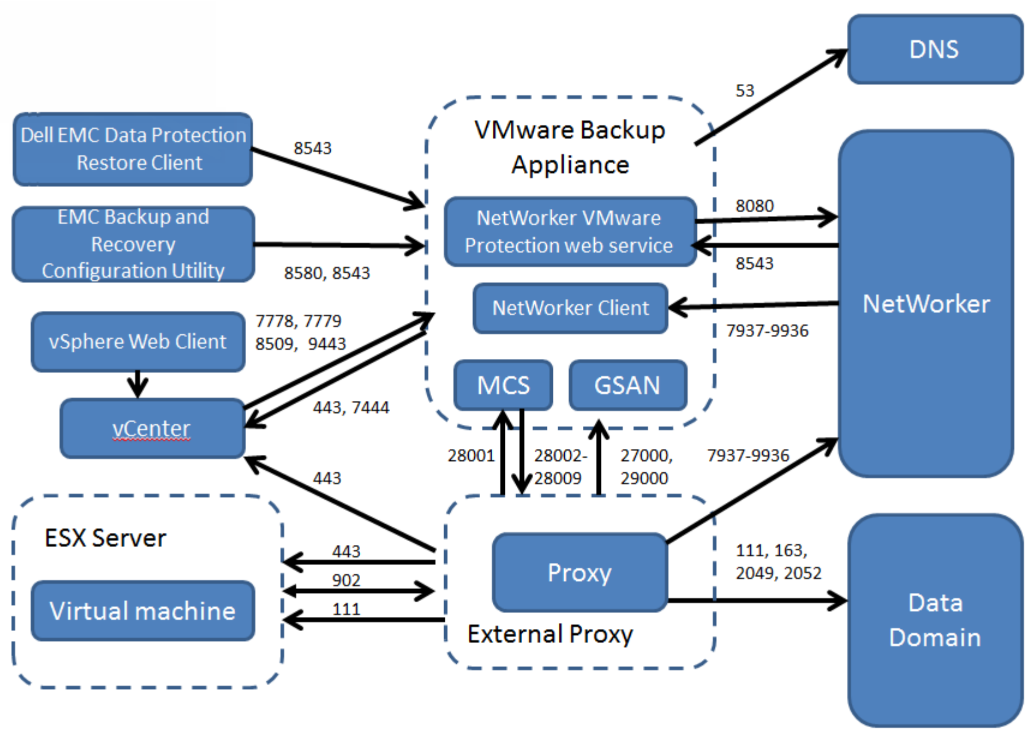
From	To	Port	Purpose
VMware Backup appliance	DNS	53	Name resolution
VMware Backup appliance	NetWorker server	8080	Initiate operations in NetWorker
VMware Backup appliance and external proxy	NetWorker server	7937-9936 (RPC)	NetWorker client communications
VMware Backup appliance and external proxy	Data Domain	7, 22, 80, 111, 131, 163, 2049, 2052	Data Domain management

Table 19 Outgoing port requirements — with external proxies (continued)

From	To	Port	Purpose
VMware Backup appliance and external proxy	vCenter	443	vCenter integration
VMware Backup appliance and External Proxy	ESX servers	443, 111, 902	Backup and recovery operations
VMware Backup appliance	External proxy	28002-28009 (pre-NetWorker 8.2); 28009 (NetWorker 8.2 and later)	MCS to proxy communications
External proxy	VMware Backup appliance	28001, 27000, 29000	External proxy to MCS and GSAN

The following diagram shows the outgoing firewall port configuration with the VMware Backup appliance.

Figure 98 Firewall configuration (VMware Backup appliance with external proxy)



To communicate with the VMware Backup appliance, the NetWorker server VM web services (nsrvmwsd) listen on port 8080 by default. Ensure that no other services, such as HBA, use port 8080. To check port usage for 8080 outside of NetWorker:

- On Windows, run `netstat -anbo | findstr 8080`
- On Linux, run `netstat -anp | grep 8080`
- On Solaris, run `lsof -i :8080`

If any software other than NetWorker listens on this port, you can change the NetWorker web services port in NMC's **NetWorker Administration** window.

To change the port, right-click the server in the **Server** window and select **Properties**. The **VMWS port** field is located under the **Miscellaneous** tab.

Download and deploy the VMware Backup appliance

The NetWorker 18.1 release does not provide a new version of the VMware Backup appliance. NetWorker 18.1 supports the most recent OVA and proxy version compatible with NetWorker 9.0.x.

If you plan to continue using Networker VMware Protection with the VMware Backup appliance in Networker 18.1, ensure that you have upgraded the VMware Backup appliance to the NetWorker 9.0.1 version, which 1.5.1.7.

Pre-installation requirements

Before you upgrade to NetWorker 18.1, review the pre-installation requirements in this section.

VMware Backup appliance requirements

Review the following requirements specific to using NetWorker with the VMware Backup appliance before you install or upgrade to NetWorker 18.1.

- Ensure that the NetWorker server and storage node are at the same version, and that you use the latest VMware Backup appliance. For example, for NetWorker 18.1, install or upgrade to the latest OVA version, 1.5.1.7.
  When you upgrade NetWorker and the VMware Backup appliance, upgrade in the following order:
  - NetWorker server to NetWorker 18.1.
  - NetWorker storage node to NetWorker 18.1.
  - VMware Backup appliance along with external proxies to version 1.5.1.7.
- Note that you cannot create new policies and workflows with the VMware Backup appliance in NetWorker 18.1. For new policies and workflows, you must use the vProxy appliance.
- Ensure that the DDOS version is compatible with the NetWorker server and VMware Backup appliance version. The VMware Backup appliance version 1.5.1.7 supports DDOS 5.7 and later.
  The Data Domain Boost Compatibility Guide, available at http://compatibilityguide.emc.com:8080/CompGuideApp/DataDomainBoost.jsp, provides detailed information on NetWorker and DD Boost version compatibility.
- You must provide an unused IP for the VMware Backup appliance server so that it does not conflict with the IP for another virtual machine in the environment, even if these hosts are not physically connected.
- For registration of the VMware Backup appliance with the vCenter server, it is recommended to use a Service account.
- Deploy the VMware Backup appliance on shared VMFS5 or higher to avoid block size limitations.
- For better performance, it is recommended to use a dedicated datastore for the VMware Backup appliance.

- Keep the default values for annotations for the VMware Backup appliance node and external proxy.

DNS Configuration

The DNS server plays a very important role during the VMware Backup Appliance configuration and backup/restore operations. You must add an entry to the DNS Server for the VMware Backup Appliance IP address and Fully Qualified Domain Names (FQDNs).

The DNS server must support both forward and reverse lookup for the following:

- VMware Backup Appliance
- External Proxy
- NetWorker server
- Data Domain device
- vCenter and ESXi hosts

NOTICE

Failure to set up DNS properly can cause many runtime or configuration issues. Do not manually change entries in the /etc/hosts file on the VMware Backup appliance.

You can set details for the DNS server and network IP during deployment of the VMware Backup Appliance in the **Deploy OVF Template** window, as described in the section Deploy the VMware Backup Appliance.

To confirm your DNS configuration, open a command prompt and run the following commands from the vCenter Server.

Procedure

1. To verify DNS configuration, type the following:

   ```
   nslookup VMware_Backup_Appliance_IP_address DNS_IP_address
   ```

2. To verify that the FQDN of the VMware Backup appliance resolves to the correct IP address, type the following:

   ```
   nslookup VMware_Backup_Appliance_FQDN DNS_IP_address
   ```

   Ensure this is the same IP as the previous command.

3. To verify that the FQDN of the vCenter Server resolves to the correct IP address, type the following:

   ```
   nslookup vCenter_FQDN DNS_IP_address
   ```

   If the `nslookup` commands return the proper information, then close the command prompt; if not, correct the DNS configuration. If you configure short names for the DNS entries, then perform additional look-ups for the short names.

   NOTICE

   After deployment, check for DNS resolution (forward and reverse) from the VMware Backup appliances and proxies for vCenter and the NetWorker hosts.

NTP Configuration

The VMware Backup Appliance leverages VMware Tools to synchronize time through NTP by using the **Sync guest OS time with host** option by default.

On ESXi hosts, the vCenter server, and the NetWorker server, you must configure NTP properly. Since the VMware Backup Appliance obtains the correct time through VMware Tools, the appliance does not require configuration with NTP. However, you must ensure that the time on the vCenter server and the ESX that hosts the VMware Backup Appliance are as close as possible, for example, within 30 seconds of each other. This will occur when the vCenter server is on same host as the ESX that hosts the VMware Backup Appliance, but when this is not the case, you should configure NTP on the VMware Backup Appliance in order to keep host times in sync.

Note

If you configure NTP directly in the **EMC Backup and Recovery Configuration Utility** window, then time synchronization errors occur.

ESXi and vCenter Server documentation provides more information about configuring NTP.

Downloading the OVAs for the VMware Backup appliance

You can obtain the VMware Backup appliance by downloading the VMware bundles, which appear as OVAs. The OVAs are available from the same location you download the NetWorker software.

Note

It is not recommended to configure a NetWorker 9.0.1 VMware Backup appliance with a VMware Backup appliance earlier than NetWorker 9.0.1 in the same vCenter.

Three VMware bundles and one ISO update are available. Each fulfills a specific requirement:

- 0.5 TB OVA
- 4 TB OVA
- EBR-Proxy OVA — download the external proxy appliance when performing more than eight concurrent backups, or to improve performance in certain situations. For example, you may need to deploy an external proxy to an ESX server in order to perform `hotadd` backups of VMs on that server. The section Deploy an external proxy appliance in vCenter provides the steps required to deploy an external proxy.
- EBRUpgrade — download this ISO if you need to update the deployed VMware Backup appliance to the latest version.

The following table provides recommendations on provisioning memory and swap space based on the storage space in use.

Table 20 Recommended memory and swap space based on storage space utilization

Utilization	Physical Memory	Swap Space
less than 25% (1.0 TB)	12 GB	16 GB
less than 65% (2.5 TB)	18 GB	16 GB

Table 20 Recommended memory and swap space based on storage space utilization (continued)

Utilization	Physical Memory	Swap Space
up to 100% (4.0 TB)	24 GB	16 GB

Other system requirements for the appliances are provided in System requirements. Download the desired OVA and place in shared storage.

Proxy assignment for backup and recovery

When you have more than 8 virtual machines to protect, backup and recover operations require the deployment of proxy virtual machines.

The OVA described in the following section has 8 internal proxies that allow you to backup 8 virtual machines concurrently. To back up more than 8 virtual machines concurrently, you must deploy an external proxy virtual machine that encompasses 8 internal proxies. The section Deploy external proxy appliance in vCenter describes how to deploy the external proxy OVA.

A proxy is selected from the proxy pool based on its availability and periodically refreshes the Proxy to datastore association.

Deploy the VMware Backup appliance

These deployment steps apply to each OVA, including the proxy OVA. Once you download the .ova files to shared storage, open the **vSphere Web Client**.

Before you begin

Note

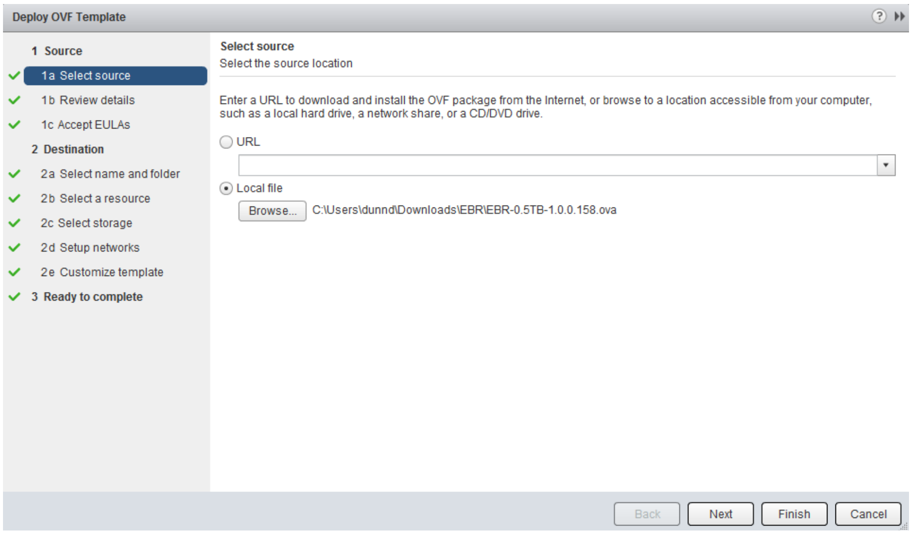
The VMware Backup appliance does not include security roll-ups. As a result, you may also be required to manually install a security roll-up after you complete the appliance deployment. You can access the latest version of the ESA for the security roll-up, titled "EMC Avamar and NetWorker Security Update for Multiple Components", from the NetWorker advisories page at https://support.emc.com/products/1095_NetWorker/Advisories/. Scroll to the bottom of the page to view Security Advisories. The **Link to remedies** section of the ESA provides instructions on how to install the roll-up on the appliance.

To deploy the .ova:

Procedure

1. In the **vSphere Web Client**, navigate to **Home** > **vCenter** > **Hosts and Clusters**.
2. Right-click the vCenter server and select **Deploy OVF template**.
3. In the Select source window, select Local file and then click **Browse**, as shown in the following figure.

Figure 99 Selecting the OVA to deploy in vCenter/vSphere Web Client



Select source

Select the source location

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

● Local file

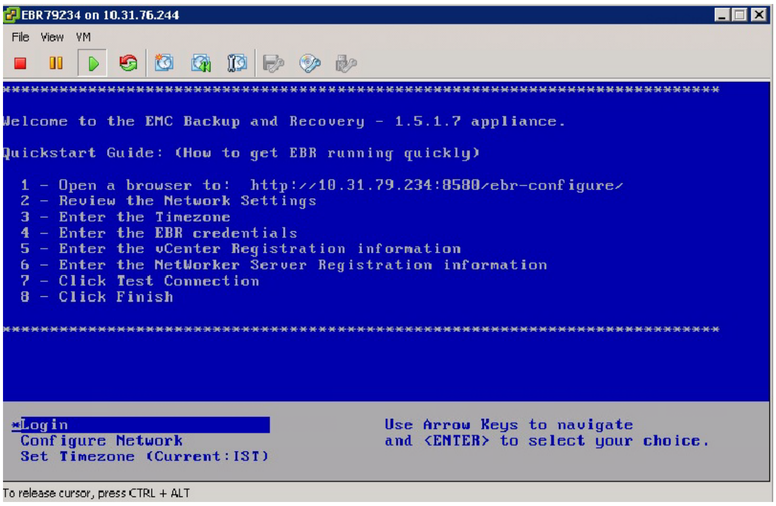
Browse... C:\Users\dunnd\Downloads\EBR\EBR-0.5TB-1.0.0.158.ova

4. In the **filetype** drop-down, select OVA Packages then navigate to the directory that contains the ova files. Select the file and then click **Open**.
5. On the **Deploy OVF Template** window, click **Next**.
6. On the **Review Details** window, click **Next**.
7. Accept the EULA and click **Next**.
8. Specify a name for the VMware Backup appliance, and then select the folder or datacenter to which you want to deploy the appliance. Click **Next**.
9. Select the resource where you want to deploy the VMware Backup appliance, then click **Next**.
10. Select **Storage**, then select the virtual disk format and click **Next**. It is recommended to use thin provisioning disk format.
11. On **Setup Networks**, select the destination network from the drop-down, then click **Next**.
12. Provide the networking properties, including the correct IP (static IP), DNS, and so on. Verify this information is correct, otherwise the appliance will not work. Click **Next**.
13. In the **Ready to Complete** window, ensure that the **Power-on after deployment** option is selected, then click **Finish**.

Results

After a few minutes a screen similar to the following figure appears in the console of the VMware Backup Appliance in vCenter.

Figure 100 EMC Backup and Recovery registration



```
****************************************************************************

Welcome to the EMC Backup and Recovery - 1.5.1.7 appliance.

Quickstart Guide: (How to get EBR running quickly)

  1 - Open a browser to:  http://10.31.79.234:8580/ebr-configure/
  2 - Review the Network Settings
  3 - Enter the Timezone
  4 - Enter the EBR credentials
  5 - Enter the vCenter Registration information
  6 - Enter the NetWorker Server Registration information
  7 - Click Test Connection
  8 - Click Finish

****************************************************************************


 *Login                                     Use Arrow Keys to navigate
  Configure Network                         and <ENTER> to select your choice.
  Set Timezone (Current:IST)
```

Note

The VMware Backup appliance version 1.5.1.7 supports vCenter server versions 5.5 Update 3e, 5.5 Update 3g, 6.0 Update 2a, 6.0 Update 3b, and vCenter 6.0 Update 3d, but only with the workaround described at https://support.emc.com/kb/489490.

Deploy external proxy appliance in vCenter

This topic describes how to deploy the proxy appliance in the vCenter.

Before you begin

Note

The external proxy appliance does not include security roll-ups. As a result, you may also be required to manually install a security roll-up after you complete the external proxy appliance deployment. You can access the latest version of the ESA for the security roll-up, titled "EMC Avamar and NetWorker Security Update for Multiple Components", from the NetWorker advisories page at https://support.emc.com/products/1095_NetWorker/Advisories/. Scroll to the bottom of the page to view Security Advisories. The **Link to remedies** section of the ESA provides instructions on how to install the roll-up on the proxies.

Procedure

1. Launch the vSphere client and log in to the vCenter server.

   The **vSphere Client** window appears.

2. Select **File** > **Deploy OVF Template**.

   The **Deploy OVF Template** wizard appears.

3. In the **Source** screen, complete the following.

   a. Select **Deploy from file or URL** and click **Browse**.

      The **Open** dialog box appears.

b. Select **Ova files (*.ova)** from the **Files of Type** list.

c. Browse to the proxy OVA file that was previously downloaded in Downloading the OVAs for the VMware Backup appliance on page 216.

d. Select the proxy appliance template file and click **Open**.

The **Open** dialog box closes.

The full path to the appliance template file appears in the **Deploy from file** field.

e. Click **Next**.

The **OVF Template Details** screen appears.

4. In the **OVF Template Details** screen, complete the following.

a. Ensure that the template information is correct.

b. Click **Next**.

The **End User License agreement** appears.

5. Accept the agreement, and then click **Next**.

The **Name and Location** screen appears.

6. In the **Name and Location** screen, complete the following.

a. Type a unique fully-qualified hostname in the **Name** field.

A Proxy can potentially have three different names:

- The name of the ESX on which the proxy runs. This is also the name managed and visible within vCenter.
- The DNS name assigned to the proxy VM.
- The VMware Backup appliance hostname after the proxy registers and activates with the server.
  As a best practice, EMC strongly recommends that you consistently use the same fully-qualified hostname for this proxy in all contexts.

b. Select a datacenter and folder location for this proxy in the Inventory tree.

c. Click **Next**.

The **Host / Cluster** screen appears.

7. In the **Host / Cluster** screen, complete the following.

a. Select an ESX server or cluster.

b. Click **Next**.

If you selected a cluster, the **Specific Host** screen appears.

8. In the **Specific Host** screen, complete the following.

a. Select a specific ESX server from the **Host Name** list.

b. Click **Next**.

The **Resource pool** screen appears.

9. In the **Resource pool** screen, complete the following.

   a. Select a resource pool for this proxy.

   b. Click **Next**.

   The **Storage** screen appears.

10. In the **Storage** screen, complete the following.

    a. Select a storage location for this proxy.

    b. Click **Next**.

    The **Disk Format** screen appears.

11. In the **Disk Format**screen, complete the following.

    a. Accept the suggested default setting for **Available Space (GB)**.

    b. Accept the suggested default provisioning setting (**Thin Provision**).

    c. Click **Next**.

    The **Network Mapping** screen appears.

12. In the **Network Mapping** screen, complete the following.

    a. Select a destination network from list.

    b. Click **Next**.

    The **Networking Properties** screen appears.

    NOTICE

    Proxy network settings are difficult to change after you register and activate the Proxy. Therefore, ensure that you type the correct settings in this screen.

13. In the **Networking Properties** screen, complete the following.

    a. In the **Default Gateway** field, type the default gateway IP address for your network.

    b. Enter one or more Domain Name Server (DNS) hostnames or IP addresses in the **DNS** field. Separate multiple entries with commas.

    c. Enter a valid routable IP address on your network in the **Network IP Address** field.

    d. Type the correct netmask/prefix for your network in the **Network Netmask** field.

14. Click **Next**.

    The **Ready To Complete** screen appears.

15. Ensure that the information is correct.

16. Click **Finish**.

    The **Deploy OVF Template** wizard closes.

17. Wait for the deployment operation to complete.

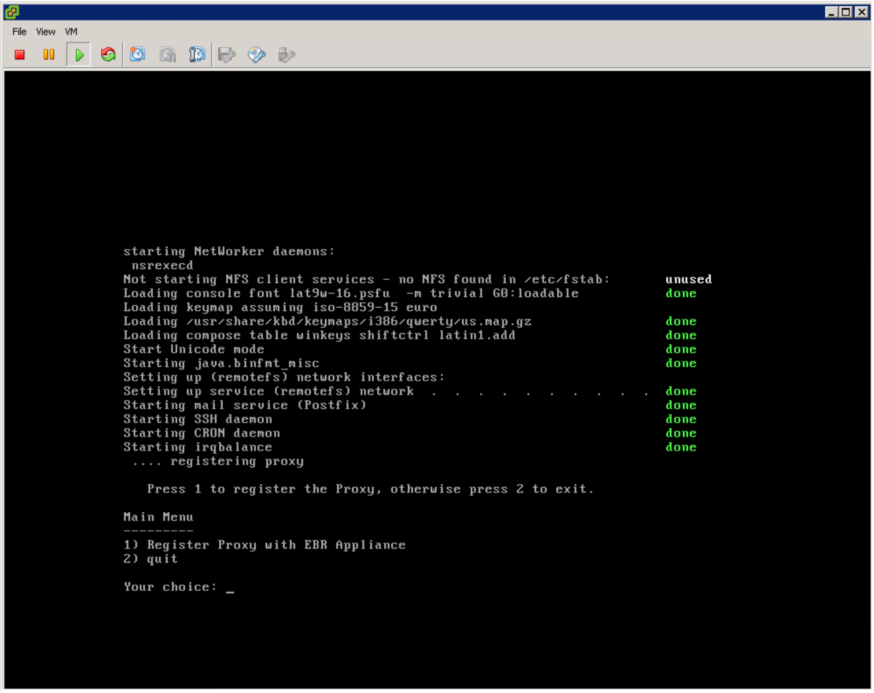
    This might take several minutes.

A confirmation message appears.

18. Click **Close** to dismiss the confirmation message.

    Once you deploy the proxy, navigate to the console of the VM in the vSphere client.

    Figure 101 Registering proxy with the VMware Backup appliance

```
starting NetWorker daemons:
 nsrexecd
Not starting NFS client services - no NFS found in /etc/fstab:       unused
Loading console font lat9w-16.psfu  -m trivial G0:loadable           done
Loading keymap assuming iso-8859-15 euro
Loading /usr/share/kbd/keymaps/i386/qwerty/us.map.gz                 done
Loading compose table winkeys shiftctrl latin1.add                   done
Start Unicode mode                                                   done
Starting java.binfmt_misc                                            done
Setting up (remotefs) network interfaces:
Setting up service (remotefs) network  . . . . . . . . . .           done
Starting mail service (Postfix)                                      done
Starting SSH daemon                                                  done
Starting CRON daemon                                                 done
Starting irqbalance                                                  done
 .... registering proxy

   Press 1 to register the Proxy, otherwise press 2 to exit.

Main Menu
---------
1) Register Proxy with EBR Appliance
2) quit

Your choice: _
```

19. Follow the prompts to register the proxy, as shown in the figure above.

    a. Press **1** to register the proxy.

    b. At the **Enter the EMC Backup and Recovery Appliance address** prompt, type the FQDN of the VMware Backup appliance server name.

    c. At the **Enter the server domain [clients]**: prompt, press **enter** and do not modify.

    d. Provide the VMware Backup appliance password if using a non-default password.

    e. Wait for the **Attempting to connect to the appliance...Connection successful** message.

20. Validate the registration in the NMC **Devices** tab by ensuring that the external proxy host appears under the **External Proxy Hosts** column of the VMware Backup appliance that it is registered to.

    Note

    When you upgrade the VMware Backup appliance, you need to deploy a new proxy appliance. After rebooting the VMware Backup Appliance, you do not need to re-register the external proxy.

After you deploy external Proxy hosts, each Proxy provides all of the following capabilities:

- Backup of Microsoft Windows and Linux VMs. This includes entire images or specific drives.
- Restore of Microsoft Windows and Linux VMs. This includes entire images or specific drives.
- Selective restore of individual folders and files to Microsoft Windows and Linux VMs.

Although you can restore data across datacenters by using a proxy deployed in one datacenter to restore files to a VM in another datacenter, the restores will take noticeably longer than if the proxy and the target VM are both located in the same datacenter. Therefore, for best performance, deploy at least one proxy in each datacenter you are protecting.

Add DNS Entries

When you deploy a Proxy appliance, as described in Deploy external proxy appliance in vCenter on page 219, you must specify a unique IP address and name to each proxy VM. The vCenter server performs name resolution lookups to ensure that the host can resolve the name and IP address. For best results, configure all required DNS entries for the proxies you plan to deploy before performing the following steps.

Re-registering the proxy with a different server

After deploying the external proxy appliance in vCenter, if you need to re-register the proxy with a different server perform the following.

Procedure

1. Launch the **EMC Backup and Recovery** Console in the **vSphere Client**, then log in to the proxy.
2. Run the following command:

   ```
   /usr/local/avamarclient/etc/initproxyappliance.sh start
   ```

3. Provide details for the new VMware Backup Appliance/server to re-register the proxy.

Upgrade the VMware Backup Appliance and vCenter

The following section provides considerations and instructions for upgrading the VMware Backup Appliance and the vCenter server to the latest version.

Upgrade the vCenter server software

NetWorker VMware Protection in NetWorker requires a minimum version of vCenter 5.5, and supports up to vCenter 6.0. The following sections provide considerations and instructions when upgrading to a supported vCenter version.

Upgrading vCenter from version 5.1 to 5.5

The following considerations apply if upgraded your vCenter version from vCenter 5.1 to vCenter 5.5.

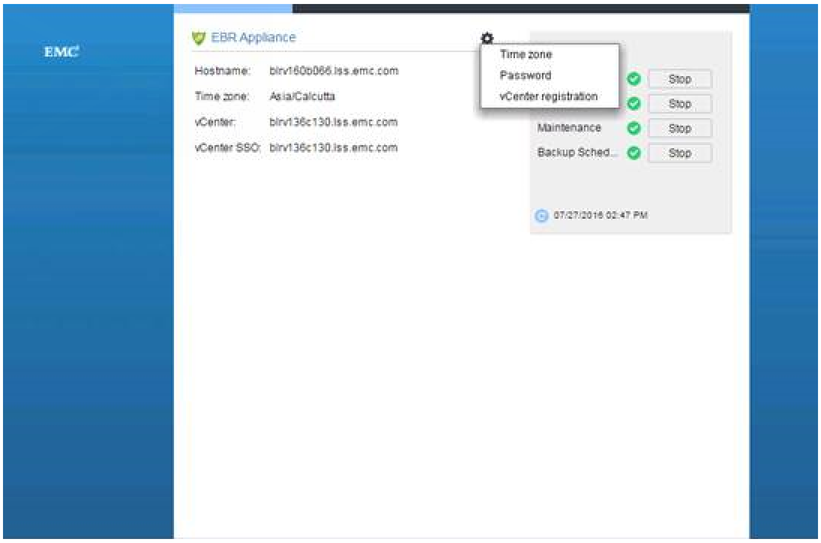
- If you created a non-root user (for example, `test`) in vCenter 5.1 using the minimum required privileges, this user cannot log in to vCenter after you upgrade to vCenter 5.5 because the username must now contain the full domain/path, in the form DOMAIN\test. Use the domain that was assigned during the creation of the user in vCenter 5.1.

- If you deployed and configured a VMware Backup Appliance with this non-root user `test` in vCenter 5.1, you must perform the following steps in order to connect to the VMware Backup Appliance after upgrading to vCenter 5.5:

  1. From a web browser, type the following URL:
     `https://<IP_address_VMware_Backup_appliance>:8543/ebr-configure`

     The **EMC Backup and Recovery Configuration Utility** window appears with a tool icon from which you can select three options—Time zone, password, and vCenter registration.

     Figure 102 Select vCenter registration in the EMC Backup and Recovery Configuration Utility

     EBR Appliance

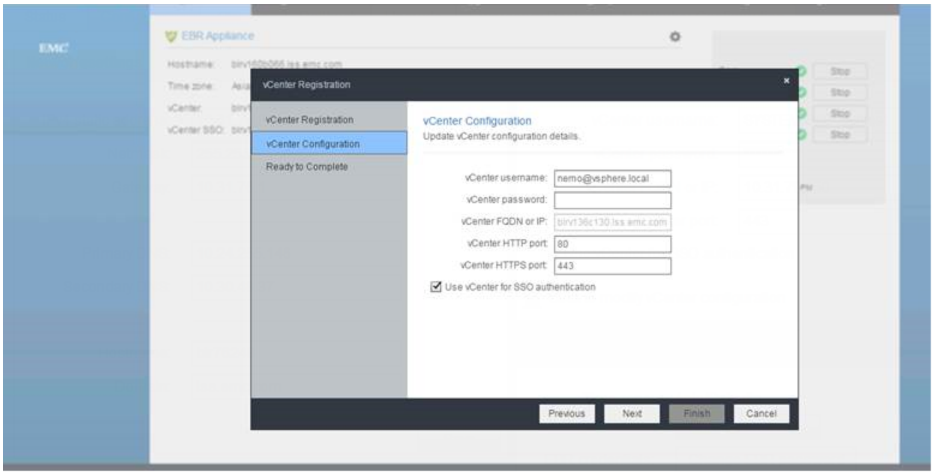
     Hostname: blrv160b066.lss.emc.com
     Time zone: Asia/Calcutta
     vCenter: blrv136c130.lss.emc.com
     vCenter SSO: blrv136c130.lss.emc.com

     07/27/2016 02:47 PM

  2. From the tool drop-down, select **vCenter registration** to unlock the vCenter registration.
     The **vCenter Registration** window opens

  3. From the **vCenter Registration** window, select **vCenter Configuration**.

     Figure 103 vCenter Configuration in the EMC Backup and Recovery Configuration Utility

     vCenter Configuration
     Update vCenter configuration details.

     vCenter username: nemo@vsphere.local
     vCenter password:
     vCenter FQDN or IP: blrv136c130.lss.emc.com
     vCenter HTTP port: 80
     vCenter HTTPS port: 443
     ☑ Use vCenter for SSO authentication

  4. Change the username to `DOMAIN\test`, and then click **Next**.

  5. In the **Ready to Complete** tab, click **Finish** and then reboot the appliance.

Upgrading vCenter to version 6.0

If using vCenter version 5.1 or 5.5 and a VMware Backup Appliance previous to NetWorker 9.0.1, perform the following steps to upgrade the vCenter server to version 6.0 and the VMware Backup Appliance to the latest available version, which is version 1.5.1.7 for NetWorker 9.0.1.

Note

In the example provided, a dedicated non-root user `test` has been set up with the domain name `system-domain` and configured with a VMware Backup Appliance previous to NetWorker 9.0.1. You will need to change the domain of the dedicated non-root user from `system-domain` to `vsphere.local` by using the **vSphere Web Client**, and change the vCenter username in the **EMC Backup and Recovery Configuration Utility** window from `test@system-domain` to `test1@vsphere.local` to re-register the VMware backup Appliance with vCenter.

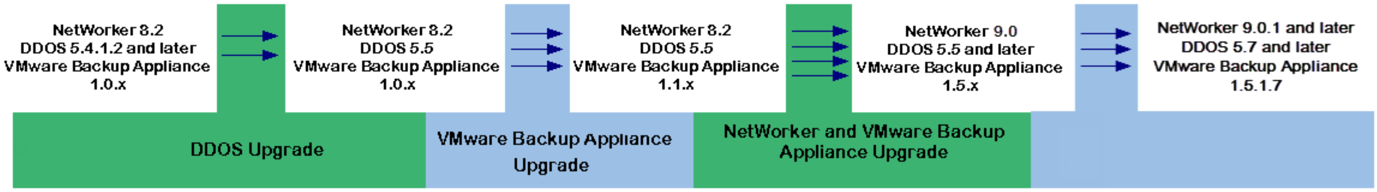
Procedure

1. Upgrade vCenter 5.1 or vCenter 5.5 to vCenter version 6.0.
2. Open the **vSphere Web Client** for vCenter 6.0 with `administrator@vsphere.local` as the username and use the password you set during the vCenter upgrade procedure, and perform the following:
   a. In the left pane, select **Administration** > **Users and Groups**, and then click the **+** sign to create a new user, `test1`.
   b. In the **Administration** pane, select **Roles**.
   c. Right-click on the role which you assigned to the user `test` and select **Clone** to create a new role, `test1role`.
   d. Select **vCenter** > **Hosts and Clusters** > **Manage** > **Permissions**, and then click the **+** sign.
   e. In the **Users and Groups** pane, click **Add** and select the user `test1` with the domain `vsphere.local`. Assign the role as `test1Role` and click **Add**.
3. Open the **EMC Backup and Recovery Configuration Utility** window as shown in the figure above, and change the vCenter username from `test@system-domain` to `test1@vsphere.local` to re-register the VMware backup Appliance with vCenter, and then restart the appliance to apply the changes.
4. Upgrade the VMware Backup Appliance to version 1.5.1.7.

Considerations prior to upgrading

When you upgrade the VMware Backup appliance, first upgrade the NetWorker version, then upgrade the Data Domain operating system (DDOS), and then upgrade the appliance.

Figure 104 Upgrading order for NetWorker components when upgrading the VMware Backup appliance



Before upgrading, also review the following considerations:

- VMware Backup appliance version 1.5.1.7 is only compatible with NetWorker 9.0.1 and later.

  Note

  When you upgrade to NetWorker 9.0.1 and later, you must also upgrade the VMware Backup appliance to version 1.5.1.7.

- If the internal proxy is disabled before you upgrade the Virtual Backup appliance, the proxy is reset to enabled when you reboot the appliance. However, NMC still shows the internal proxy's state as disabled. If this happens, run the following command on the NetWorker server:

  ```
  nsrim -X -S -h <VBA hostname> -f
  ```

  Note

  Do not attempt to enable the proxy manually, because it could result in NetWorker server connection issues with the appliance.

- You only need to upgrade to DDOS 5.7 or later if you upgrade the VMware Backup appliance to version 1.5.1.7 and plan to use Networker 18.1.
- You cannot run backup and recovery operations during an appliance upgrade. Before performing the upgrade, ensure that you complete any policies running or disable active policies.
- You cannot upgrade external proxies. If using a previous version of the external proxy and you want to upgrade, you must redeploy the external proxy.

Upgrade the VMware Backup appliance

Use the following procedure to upgrade the VMware Backup appliance.

Procedure

1. Verify that the account connecting to vCenter has the required level of permissions, particularly if a non-admin user. The section Create a customized role provides a list of permissions.

   If the permissions are not correct before the upgrade, then the upgrade process may fail or leave the system in an inconsistent state.

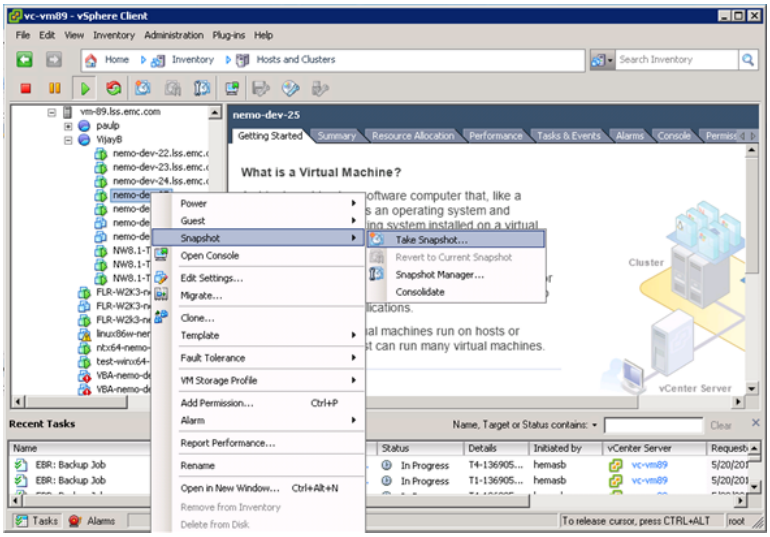
2. If you made any changes to the `/etc/hosts` file, remove these changes. It is not recommended to manually change entries in the `/etc/hosts` file on the VMware Backup appliance.
3. Create and validate a checkpoint of the existing VMware Backup appliance by running an integrity check.

   a. Select the **Configuration** tab.

   b. Select the **Run integrity Check** option, as shown in Running an integrity check on page 273.

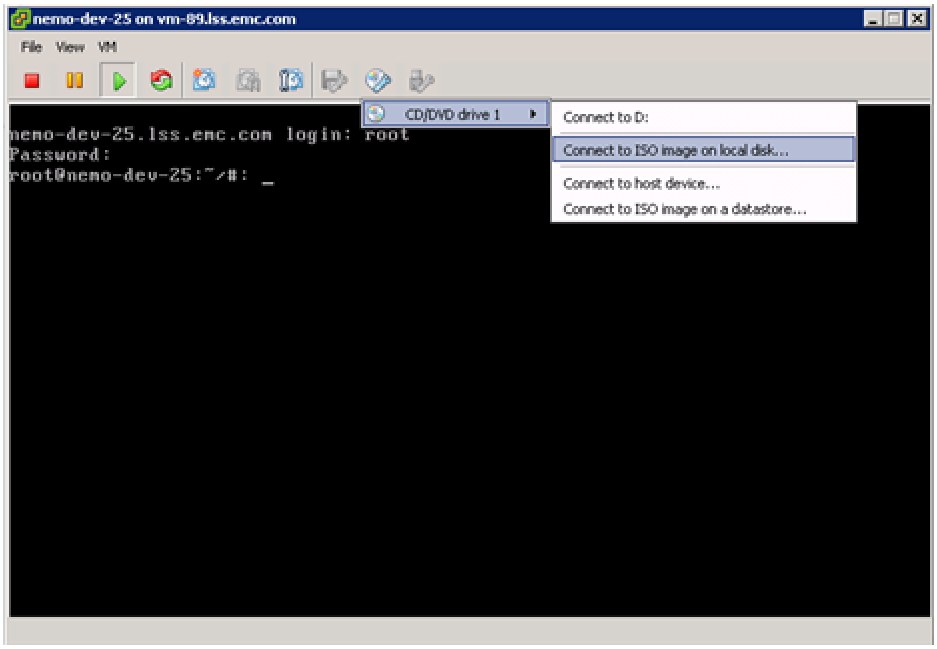
   c. Make sure that the integrity check passes successfully.
4. Shut down the VMware Backup appliance, and then create a snapshot of the EMC Backup and Recovery virtual machine by right-clicking the virtual machine in the **vSphere Client** and selecting **Snapshot** > **Take Snapshot...**, as shown in the following figure.

   Figure 105 Take Snapshot in vSphere Client



5. Restart the appliance.
6. Verify the md5 checksum of the upgrade package.
7. Attach the ISO to the VMware Backup appliance by selecting **Connect to ISO image on local disk** in the **vSphere Client** and selecting the ISO, as shown in the following figure.

Figure 106 Connect to ISO in vSphere Client


nemo-dev-25 on vm-89.lss.emc.com
File View VM
CD/DVD drive 1
Connect to D:
Connect to ISO image on local disk...
Connect to host device...
Connect to ISO image on a datastore...

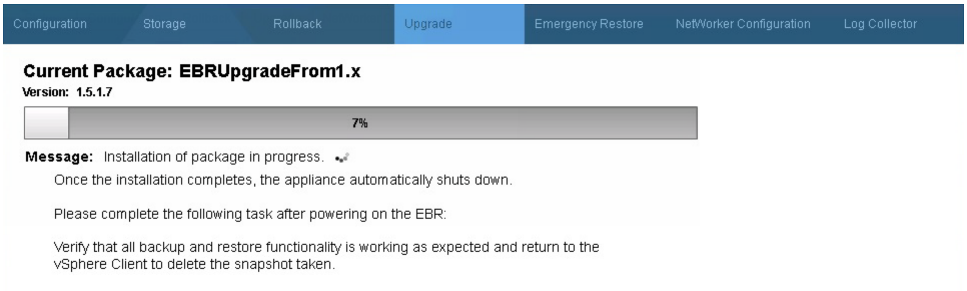
```
nemo-dev-25.lss.emc.com login: root
Password:
root@nemo-dev-25:~/#: _
```

8. Open the **EMC Backup and Recovery Configuration Utility** window. Post-installation configuration on page 240 provides more information.
9. Navigate to the **Upgrade** tab and click **Check Upgrades**. The available upgrade package appears.
10. Navigate to the **Status** tab to ensure all services are running.
11. Return to the **Upgrade** tab and click **Upgrade EBR**.

Note

If you want to access the **EMC Backup and Recovery Configuration Utility** online help, click the **Help Documentation** link located on the **Upgrade** tab.

Figure 107 Accessing online help during upgrade



Current Package: EBRUpgradeFrom1.x
Version: 1.5.1.7

Message: Installation of package in progress.
Once the installation completes, the appliance automatically shuts down.

Please complete the following task after powering on the EBR:

Verify that all backup and restore functionality is working as expected and return to the vSphere Client to delete the snapshot taken.

When the upgrade completes, the VMware Backup appliance shuts down automatically.

12. Power on the VMware Backup appliance.

When you launch the **EMC Backup and Recovery** user interface in the **vSphere Web Client**, and then connect to the upgraded appliance and navigate to the **Configuration** tab, the new version appears.

Note

To see the new version of the appliance in the VMware console, log out and then log back in. The previous version is shown in the console until you do this.

13. When you complete a successful upgrade and verify that all backup and restore functionality is working as expected, return to the **vSphere Client** and delete the snapshot taken in step 4.
14. Disconnect from the ISO image used for the upgrade by unmounting or removing the image.

Note

To upgrade a 8.2.x/9.0 VMware Backup appliance to the 9.0.1 VMware Backup appliance version 1.5.1.7 with vCenter server versions 5.5 Update 3e, 5.5 Update 3g, 6.0 Update 2a, 6.0 Update 3b and vCenter 6.0 Update 3d, refer to the knowledgebase article at https://support.emc.com/kb/493777.

Enable VMware View in NMC's Administration window after upgrading by creating a NSR Hypervisor resource

When you upgrade the NetWorker server to NetWorker 18.1 and upgrade to the latest VMware Backup appliance(s), VMware View may not appear in NMC's **Administration** window until you create a NSR Hypervisor resource.

To create the NSR Hypervisor resource, download and deploy a NetWorker 9.0.1 VMware Backup Appliance (version 1.5.1.7) from vCenter, following the registration steps described in EMC Backup and Recovery Configuration Utility on page 235, or perform the following to manually create a NSR Hypervisor resource by using the `nsradmin` program.

1. Start the NetWorker administration program by running `nsradmin`. Use the `help` command for help, or the `visual` command to enter full-screen mode.
2. Type the following:

```
nsradmin> create type:NSR Hypervisor;name:vCenter_FQDN_or_IP
nsradmin> vi
Select type: NSR hypervisor;
name: esx3-vc1.lss.emc.com;
comment: ;
service: [VMware VirtualCenter];
endpoint: "https://esx3-vc1.lss.emc.com/sdk";
username: "ajayads\\nemo"; ======================> vCenter info
password: *******;
command: nsrvim;
proxy: nemo220-3.lss.emc.com; ============> NW Server
```

Note

If using NetWorker VMware Protection with the VMware Backup Appliance, ensure that the vCenter FQDN or IP for the NSR Hypervisor resource matches what you specified in the vCenter Registration page of the **EMC Backup and Recovery Configure** window. You must use only FQDN or only IP in both instances, not a combination of the two.

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

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

Create vCenter user account

Procedure

1. From a web browser, type the following:

   ```
   https://<IP_address_vCenter_Server>:5480
   ```

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

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

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

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

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

Create a customized role

Procedure

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

   The Create Role dialog appears.

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

Table 21 Minimum required vCenter user account privileges

Setting	vCenter 5.5 and later required privileges
Alarms	• Create alarm • Modify alarm
Datastore	• Allocate space • Browse datastore • Configure datastore • Low level file operations • Move datastore • Remove datastore • Remove file • Rename datastore
Extension	• Register extension • Unregister extension • Update extension
Folder	• Create folder
Global	• Cancel task • Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Settings • Set custom attribute
Host	• Configuration > Storage partition configuration

Table 21 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 and later required privileges
	Note Not applicable to vCenter 5.5.
Network	• Assign network • Configure
Resource	• Assign virtual machine to resource pool • Migrate powered off virtual machine • Migrate powered on virtual machine
Sessions	• Validate session
Tasks	• Create task • Update task
vApp	• Export • Import • vApp application configuration
Virtual Machine	
Configuration	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Configure managed by • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Set annotation

Table 21 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 and later required privileges
	• Settings • Swapfile placement • Upgrade virtual machine compatibility
Guest Operations	• Guest operation modifications • Guest operation program execution • Guest operation queries
Interactions	• Configure CD media • Console interaction • Device Connection • Guest operating system management by VIX API • Power off • Power on • Reset • VMware Tools install
Inventory	• Create new • Register • Remove • Unregister
Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Mark as Template
Snapshot Management	• Create snapshot • Remove Snapshot • Revert to snapshot

vSphere Client user accounts

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

Note

In high-security environments, you can restrict the vCenter user account permissions required to configure and administer the vProxy appliance. Table 9 on page 60 provides the account permission categories.

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

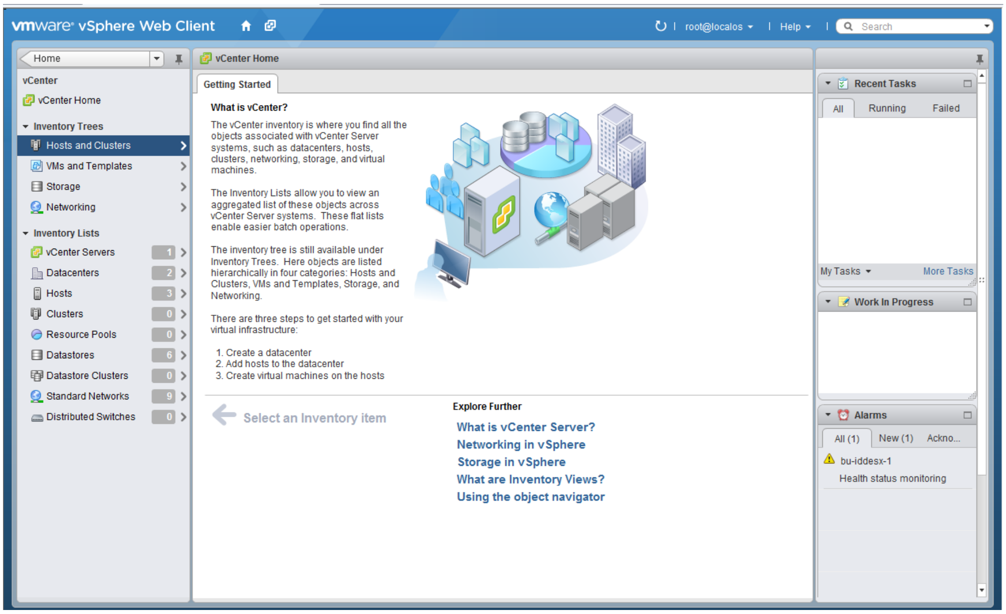
Procedure

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

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

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

   Figure 108 Hosts and Clusters in the vSphere Web Client

   What is vCenter?

   The vCenter inventory is where you find all the objects associated with vCenter Server systems, such as datacenters, hosts, clusters, networking, storage, and virtual machines.

   The Inventory Lists allow you to view an aggregated list of these objects across vCenter Server systems. These flat lists enable easier batch operations.

   The inventory tree is still available under Inventory Trees. Here objects are listed hierarchically in four categories: Hosts and Clusters, VMs and Templates, Storage, and Networking.

   There are three steps to get started with your virtual infrastructure:

   1. Create a datacenter
   2. Add hosts to the datacenter
   3. Create virtual machines on the hosts

   Explore Further

   What is vCenter Server?
   Networking in vSphere
   Storage in vSphere
   What are Inventory Views?
   Using the object navigator

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

   Note

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

   ---

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

   The **Add Permission** dialog box opens.

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

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

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

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

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

Restrict mapping of datastores

You can perform VM backups by using one of two methods:

- Hotadd—The VMware Backup Appliance or External proxy directly mounts the VM's hard disk to read the backup data. This mode requires that the proxy has direct access to the datastore of the VM that you want to back up.
- NBD—The VMware Backup Appliance or External proxy will connect to the ESX server that the VM is running on over the IP network, and data will be transferred over the IP network to the proxy. As a result, NBD mode is typically slower than hotadd mode.

By default, hotadd mode is used. If the proxy does not have direct access to the datastore that the VM is running on, it will fall back to using NBD mode to improve the chances of obtaining a successful backup.

In certain environments, you may want to prevent fallback to NBD backups to ensure no backup traffic occurs across the IP network. In such cases, you can configure your system to use an alternate mode where backup jobs will only be given to proxies that have the ability to perform a hotadd backup of the VM. When configuring this mode, you must deploy an external proxy on an ESX server that has access to the datastore that the VM resides on. Failure to do so results in the backup failing with the error "No Proxy."

To configure this mode of operation, you can select the option in the NSR VBA Server Properties window, described in the section VMware Backup Appliance monitoring and properties on page 251.

EMC Backup and Recovery Configuration Utility

Complete the VMware Backup Appliance registration and configuration by using the **EMC Backup and Recovery Configuration Utility** window.

Procedure

1. Open an internet browser and type the URL to connect to the VMware Backup Appliance. The URL will be similar to the following:

```
http://VMware Backup appliance IP:8580/ebr-configure
```

The **EMC Backup and Recovery Configuration Utility** window opens.

Note

The **EMC Backup and Recovery Configuration Utility** requires Adobe Flash Player version 11.5 or later. If you do not have the appropriate version of Adobe Flash Player installed, a message appears with a link to download it. If you are still unable to connect after installing Adobe Flash Player, then check the network configuration (IP address, DNS, and so on) by logging into the VMware Backup Appliance registration screen. If any of the network information was incorrectly entered, you must re-deploy.

---

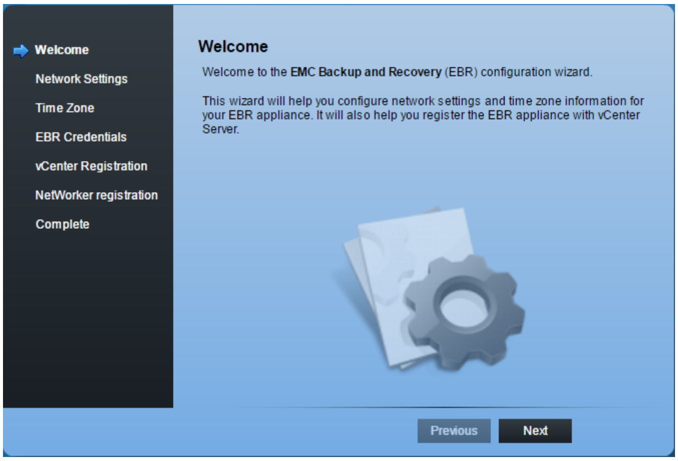
2. Log in with the userid `root`, and create a password that is a minimum of 9 characters long and contains a combination of one more more upper and lower-case letters, one or more numbers from 0-9, and at least one special character.

Note

You can use the previous default password `8RttoTriz` or a password without special characters only if you apply a hotfix to the OVA version 1.5.1.7 prior to running the **EMC Backup and Recovery Configuration Utility**. The hotfix is available in the same download location as the OVA.

The **Welcome** page displays.

Figure 109 Welcome configuration page



Welcome

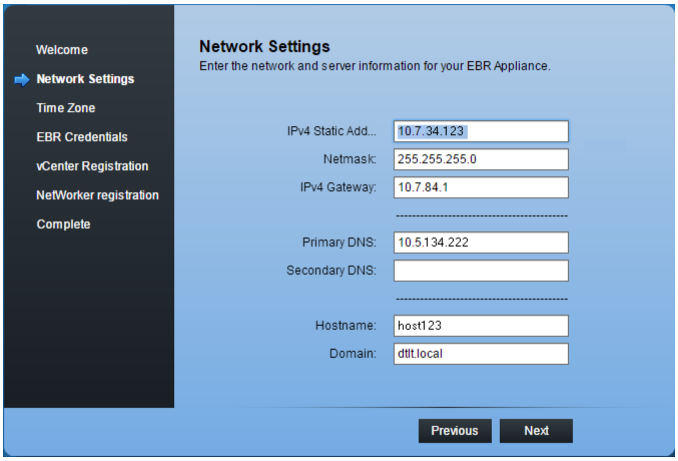
Welcome to the **EMC Backup and Recovery** (EBR) configuration wizard.

This wizard will help you configure network settings and time zone information for your EBR appliance. It will also help you register the EBR appliance with vCenter Server.

3. Click **Next**.

   The **Network Settings** page displays.

Figure 110 Network Settings configuration page



Network Settings

Enter the network and server information for your EBR Appliance.

IPv4 Static Add...: 10.7.34.123

Netmask: 255.255.255.0

IPv4 Gateway: 10.7.84.1

Primary DNS: 10.5.134.222

Secondary DNS:

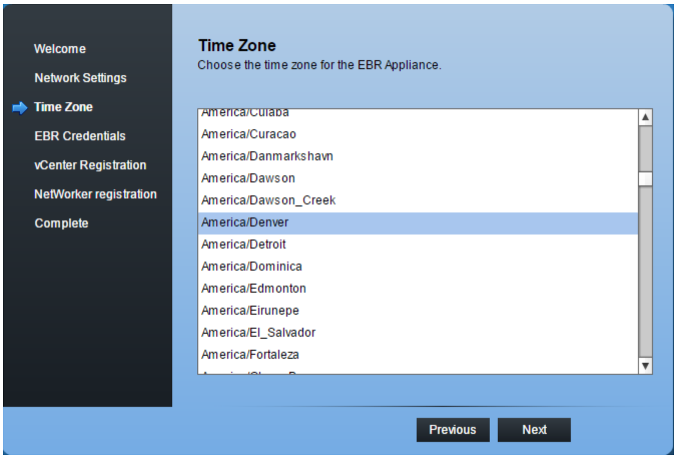
Hostname: host123

Domain: dtlt.local

4. Verify the network settings, and click **Next**.

   The **Time Zone** page displays.

   Figure 111 Time Zone configuration page



Time Zone

Choose the time zone for the EBR Appliance.

America/Cuiaba
America/Curacao
America/Danmarkshavn
America/Dawson
America/Dawson_Creek
America/Denver
America/Detroit
America/Dominica
America/Edmonton
America/Eirunepe
America/El_Salvador
America/Fortaleza

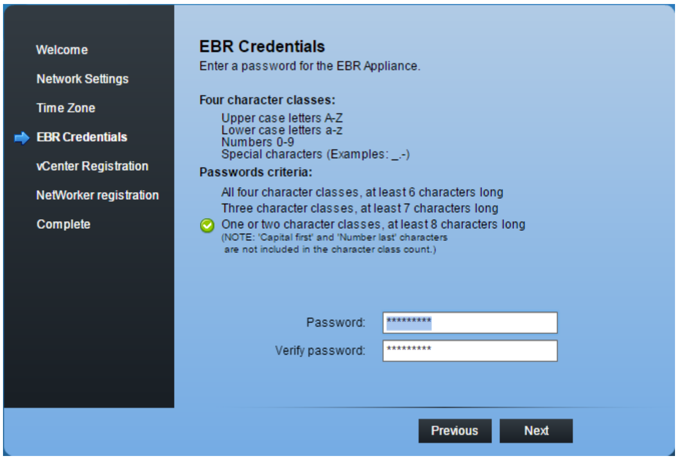
5. Set the time zone to match that of the vCenter appliance, and click **Next**.

   Note

   If the time zone does not match that of the appliance, you may encounter issues connecting with EMC Backup and Recovery from the vCenter. The default time zone for vCenter is UTC.

   The **EBR Credentials** page displays.

Figure 112 EBR Credentials configuration page



EBR Credentials

Enter a password for the EBR Appliance.

Four character classes:

Upper case letters A-Z
Lower case letters a-z
Numbers 0-9
Special characters (Examples: _.-)

Passwords criteria:

All four character classes, at least 6 characters long
Three character classes, at least 7 characters long
✓ One or two character classes, at least 8 characters long
(NOTE: 'Capital first' and 'Number last' characters
are not included in the character class count.)

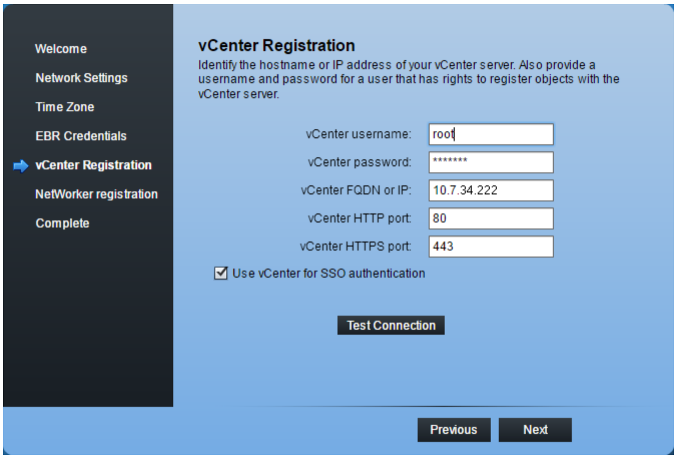
Password: *********

Verify password: *********

6. Specify a new EMC Backup and Recovery password for the root account, and click **Next**.

   The **vCenter Registration** page displays.

Figure 113 vCenter Registration configuration page



vCenter Registration

Identify the hostname or IP address of your vCenter server. Also provide a username and password for a user that has rights to register objects with the vCenter server.

vCenter username: root

vCenter password: *******

vCenter FQDN or IP: 10.7.34.222

vCenter HTTP port: 80

vCenter HTTPS port: 443

☑ Use vCenter for SSO authentication

7. Type the details required to connect to the appliance.

   Note

   When you use the FQDN or IP to register the vCenter server in this window and with the NetWorker server, ensure that you specify *only* the FQDN or *only* the IP in both instances, not a combination of the two.

8. Click **Test connection**.

   You should see a message that the connection test completed successfully.

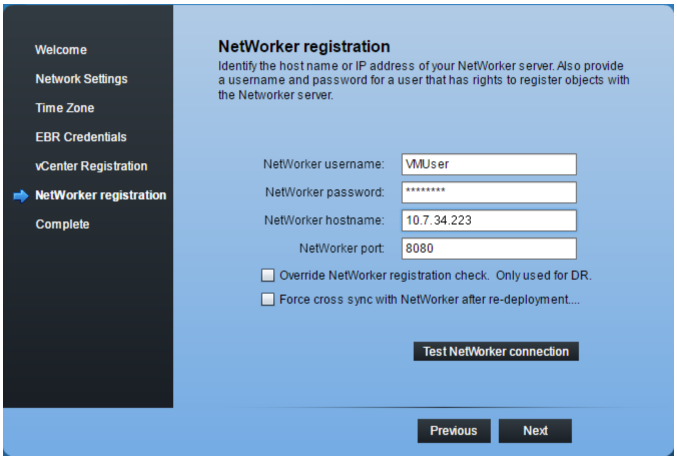
9. Ensure that **Use vCenter for SSO authentication** remains selected , and click **Next**.

   Note

   If the vCenter server host is different from the vSphere web server host, use admin@system/domain as the user name along with the appropriate password.

The **NetWorker registration** page displays.

Figure 114 NetWorker registration configuration page



NetWorker registration

Identify the host name or IP address of your NetWorker server. Also provide a username and password for a user that has rights to register objects with the Networker server.

NetWorker username: VMUser

NetWorker password: ********

NetWorker hostname: 10.7.34.223

NetWorker port: 8080

□ Override NetWorker registration check. Only used for DR.

□ Force cross sync with NetWorker after re-deployment....

10. Type the details required to connect to the NetWorker server:
    - **NetWorker username** = VMUser (default).
    - **NetWorker password** = changeme (default)
    - **NetWorker hostname**: type the IP address or FQDN of the NetWorker server
    - **NetWorker port** = 8080 (default)

    Note

    To change the default name **VMUser**, in NMC go to **NetWorker Administration** > **NetWorker server properties** > **Miscellaneous**, and change both the user name and password. Ensure that when you change the user name and password in NMC that you specify the new values in the **NetWorker registration** page.

Note

If you are performing a disaster recover, select the **Override NetWorker registration check** option if the VMware Backup Appliance has registered to the NetWorker server.

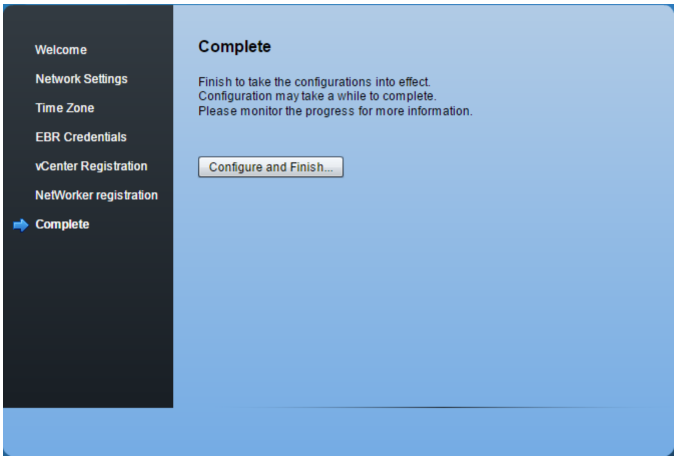
11. Click **Test NetWorker connection**.

    You should see a message that the connection test completed successfully.

12. Click **Next**.

    The **Complete** page appears.

Figure 115 Complete configuration page



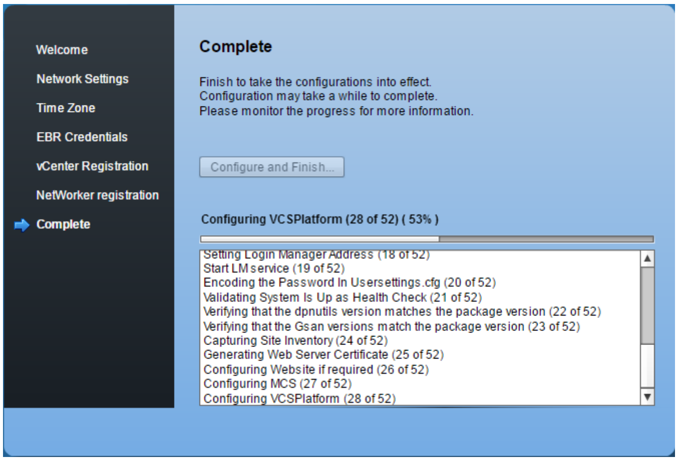
Complete

Finish to take the configurations into effect.
Configuration may take a while to complete.
Please monitor the progress for more information.

13. **Click Complete and Finish.**

    Configuration begins, and the progress is shown.

    Figure 116 Complete progress page



Complete

Finish to take the configurations into effect.
Configuration may take a while to complete.
Please monitor the progress for more information.

Configuring VCSPlatform (28 of 52) (53%)

```
Setting Login Manager Address (18 of 52)
Start LM service (19 of 52)
Encoding the Password In Usersettings.cfg (20 of 52)
Validating System Is Up as Health Check (21 of 52)
Verifying that the dpnutils version matches the package version (22 of 52)
Verifying that the Gsan versions match the package version (23 of 52)
Capturing Site Inventory (24 of 52)
Generating Web Server Certificate (25 of 52)
Configuring Website if required (26 of 52)
Configuring MCS (27 of 52)
Configuring VCSPlatform (28 of 52)
```

Post-installation configuration

You can confirm that the installation process successfully registered and configured the VMware Backup Appliance in NetWorker.

Procedure

1. Ensure that the **Log** window in NMC's **Administration** window displays the following information:

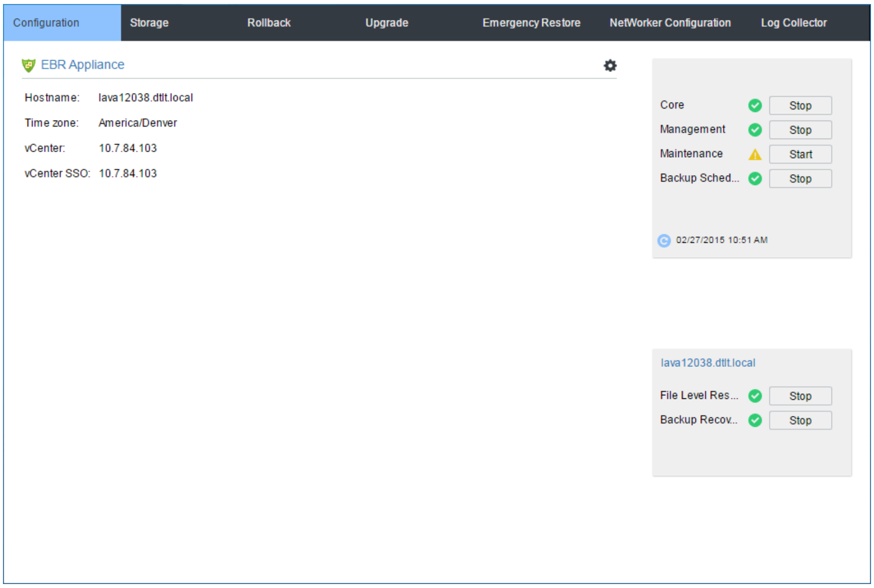
   ```
   NetWorker server, 'server_name' registration succeeded for
   VMware Backup Appliance VBA_hostname
   ```

2. Log in to the **EMC Backup and Recovery Configuration Utility** window at the following URL by using the new EMC Backup and Recovery password that you defined during configuration:

   ```
   http://VMware_Backup_appliance_IP:8580/ebr-configure
   ```

   You should see the following window, in which you can verify information about your configuration and ensure that required services are running. You can also see a summary of storage and capacity usage, and perform tasks such as rolling back the VMware Backup appliance to a known validated checkpoint, upgrading the appliance, executing emergency restore, editing Networker configuration, and downloading client and VMware Backup appliance logs.

Figure 117 Post VMware Backup Appliance configuration



Hostname: lava12038.dtlt.local
Time zone: America/Denver
vCenter: 10.7.84.103
vCenter SSO: 10.7.84.103

Core ✓
Management ✓
Maintenance ⚠
Backup Sched... ✓

02/27/2015 10:51 AM

lava12038.dtlt.local
File Level Res... ✓
Backup Recov... ✓

Starting and stopping services

The **Configuration** tab lists all of the services required by EMC Backup and Recovery and the current status of each service. The following table describes these services.

Table 22 Description of services running on the VMware Backup Appliance

Service	Description
Core	Comprise the backup engine of the appliance. If these services are disabled no backup jobs (either scheduled or “on demand”) will run, and no restore activities can be initiated.
Management	Stop these services only under the direction of technical support.
Maintenance services	Perform maintenance tasks (for example, evaluating whether retention periods of backups have expired). Services will start up at the Start Time for the first maintenance window after 24 hours have elapsed. For example, if the system was deployed at 10.20am on Thursday, then 24 hours after this would be 10.20am on Friday. The next maintenance window would then start at 8am on Saturday. The maintenance window is scheduled by default to start at 8am each day. You can make changes to the default maintenance window by using the command line.

Table 22 Description of services running on the VMware Backup Appliance (continued)

Service	Description
Backup Scheduler	Allow mounting of backups for file-level restore operations.
File level restore	Support the management of file-level restore operations.
Backup Recovery	Support the management of backup and recovery operations.

To stop a service, click **Stop** next to the service on the **Configuration** tab of **EMC Backup and Recovery Configuration Utility** window. In general, you should only stop running services under the direction of Technical Support.

If you stop a service, you can attempt to restart it by clicking **Start**. In some cases, additional troubleshooting steps may be required for the service to work properly.

Note

When any service stops running, the action triggers an alarm on the vCenter server. When the service restarts, vCenter clears the alarm. A delay of up to 10 minutes can occur before vCenter clears or triggers an alarm.

Click the refresh icon to update the status display.

If all services are stopped, then start the services in the following order:

1. Core
2. Management
3. Maintenance
4. Backup Scheduler
5. File Level Restore
6. Backup Recovery

Changing the maintenance window

Use the following procedure if you want to change the backup schedule (maintenance window) settings. This example demonstrates how to change the maintenance window from the default (8 PM to 8 AM the following day) to a custom value (6 PM to 2 PM the following day):

Procedure

1. Check the current schedule by running the following from the command line:

   ```
   admin@ebr169:/usr/local/avamar/bin/>: status.dpn
   ```

   The end of the output indicates the current settings for backup window and maintenance window start times.

   ```
   Next backup window start time: Sat Sep 28 20:00:00 2013
   IST
   Next maintenance window start time: Sat Sep 28 08:00:00
   2013 IST
   ```

2. Change the backup start time (in format HHMM) and duration (in format HHMM) by running:

   ```
   admin@ebr169:/usr/local/avamar/bin/>: avmaint sched window --
   backup-start=1800 --backup-duration=2000 --ava
   ```

3. Verify the change by running:

   ```
   admin@ebr169:/usr/local/avamar/bin/>: status.dpn
   ```

   The end of the output indicates the new backup window and maintenance window start times:

   ```
   Next backup window start time: Sat Sep 28 18:00:00 2013
   IST
   Next maintenance window start time: Sat Sep 28 14:00:00
   2013 IST
   ```

Adding or swapping a NIC for VMXNET 3 on the VMware Backup appliance or external proxy

The following section describes how to set up a virtual network interface card (vNIC) of type VMXNET 3 for the VMware Backup appliance and/or external proxy appliance.

Before you begin

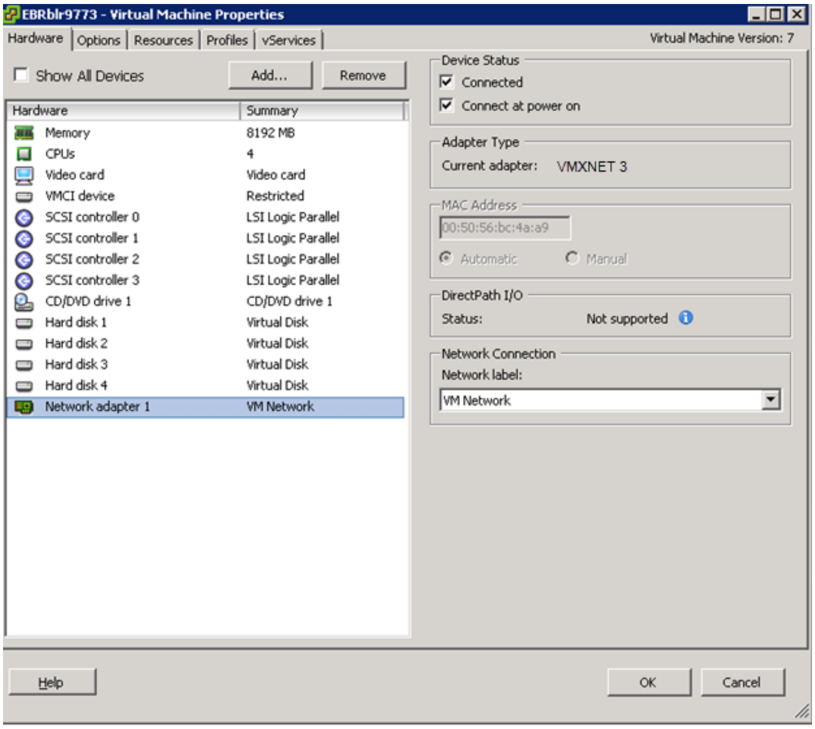
This procedure is required for custom setup using dual NIC as described in the section Dual vNIC Setup and configuration requirements, but is otherwise optional for most VMware Backup appliances and external proxy appliances.

Performing this setup requires that you download and deploy the VMware Backup appliance or external proxy appliance, and then use the following steps to configure the appliance before the steps outlined in the section EMC Backup and Recovery Configure window setup. When you deploy the VMware Backup Appliance, configure the vNIC, or eth0, with an IP address from the production subnet/VLAN.

Procedure

1. Log in to the VMware Backup appliance console in the **vSphere Client**.
2. Right-click the VMware Backup appliance and select **Power** > **Shutdown Guest**.
3. Add the second NIC to the VMware Backup Appliance:
   a. Right click the VMware Backup appliance, and then select **Edit Settings**. The **Virtual Machine Properties** window appears.

Figure 118 Swap network for NICs in the Virtual Machine Properties window



Virtual Machine Version: 7

□ Show All Devices

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
SCSI controller 1	LSI Logic Parallel
SCSI controller 2	LSI Logic Parallel
SCSI controller 3	LSI Logic Parallel
CD/DVD drive 1	CD/DVD drive 1
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Hard disk 4	Virtual Disk
Network adapter 1	VM Network

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: VMXNET 3

MAC Address
00:50:56:bc:4a:a9
● Automatic ○ Manual

DirectPath I/O
Status: Not supported

Network Connection
Network label: VM Network

b. (Optional when swapping NIC) In the **Hardware** tab, select **Network adapter 1** in the list, and then click **Remove**.

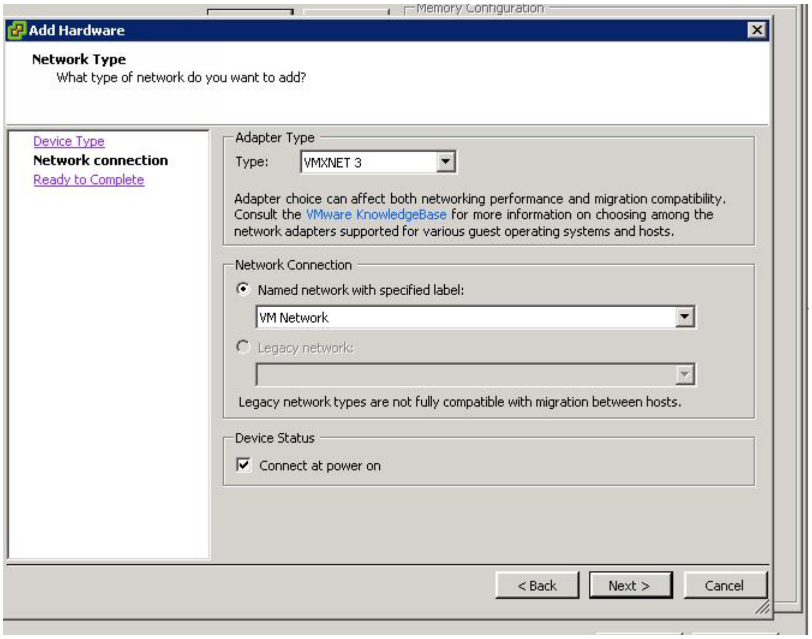
c. In the **Hardware** tab, click **Add**.

The **Add Hardware** wizard opens.

d. In the **Device Type** page, select **Ethernet Adapter** and click **Next**.

e. In the **NetWork Type** page, change the value in the **Adapter Type** field to **VMXNET 3**, and assign this vNIC to the appropriate virtual machine port group. Select the **Connect at power on** checkbox if it is not selected.

Figure 119 Change Adapter Type



Network Type

What type of network do you want to add?

Adapter Type

Type: VMXNET 3

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

Network Connection

● Named network with specified label:

VM Network

○ Legacy network:

Legacy network types are not fully compatible with migration between hosts.

Device Status

☑ Connect at power on

f. Select the appropriate virtual machine port group for the production network/VLAN, and then click **Next**.

g. In the **Ready to Complete** page, verify the information and then click **Finish**.

4. Right click the VMware Backup appliance and select **Power > Power On**.
5. Configure the second NIC on the VMware Backup Appliance:

a. After you power on the VMware Backup appliance, log in as root to the VMware Backup appliance Console by using the **vSphere Client**.

b. Type `yast2` to invoke the YaST configuration tool.

c. Select **Network Devices** and press **Enter**.

The **Network Devices** dialog appears.

d. Select **Network Settings** and press **Enter**.

The **Network Settings** dialog appears.

e. In the **Overview** tab, select the Second Ethernet Adapter labeled **eth1**.

f. Use the tab key to select **Edit** and press **Enter**.

g. From the Network Card Setup, use the tab key to access **Statically assigned IP Address** and select using the spacebar. Use the tab key to select **IP Address** and enter the IP Address, the Subnet Mask, and the host name of the VMware Backup appliance for the backup network.

h. Use the tab key to select **Edit**, and then press **Enter**.

i. (Optional when setting up second NIC) From **Network Settings**, use the tab key to select **Overview**. Use the right-arrow key to select **Hostname/DNS**. Use the tab key to select and then specify the following fields:

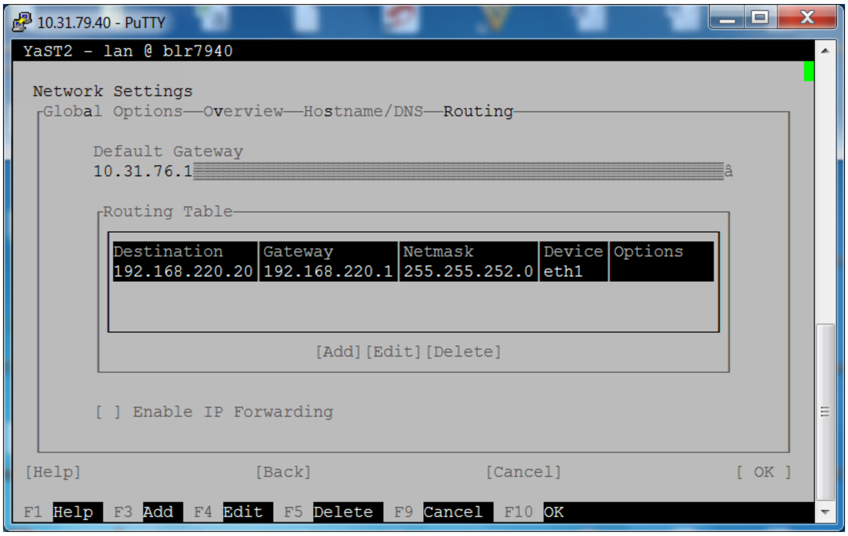
- Host name
- Domain name for the production network

- Policy for DNS configuration
- Name Server 1 for production network
- Name Server 2 for backup network
- Domain Search for both production and backup network.

When setting up a second NIC, carefully review the following sections including operating system routes since you may need to be define these routes as custom routes.

j. From **Network Settings**, use the tab key to select **Hostname/DNS**.Use the right-arrow key to select **Routing**, and update the routing table by setting the Default Gateway to the gateway/address for the production network, if not already set, as shown in the following figure.

Figure 120 Routing table with production network gateway



```
YaST2 - lan @ blr7940

Network Settings
┌Global Options──Overview──Hostname/DNS──Routing──────────────────────┐
│                                                                     │
│     Default Gateway                                                 │
│     10.31.76.1▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒â        │
│                                                                     │
│     ┌Routing Table────────────────────────────────────────────┐     │
│     │┌───────────────────────────────────────────────────────┐│     │
│     ││Destination  │Gateway      │Netmask      │Device│Options ││     │
│     ││192.168.220.20│192.168.220.1│255.255.252.0│eth1  │        ││     │
│     ││                                                        ││     │
│     │└───────────────────────────────────────────────────────┘│     │
│     │                [Add] [Edit] [Delete]                    │     │
│     └─────────────────────────────────────────────────────────┘     │
│                                                                     │
│     [ ] Enable IP Forwarding                                        │
│                                                                     │
└─────────────────────────────────────────────────────────────────────┘
[Help]                [Back]                [Cancel]               [ OK ]
F1 Help  F3 Add  F4 Edit  F5 Delete  F9 Cancel  F10 OK
```

k. Use the tab key to select **OK**, and then press **Enter**.

l. Use the tab key to select **Quit**, and then press **Enter**.

6. (Optional) If setting up vNIC on the external proxy, follow the instructions in the section Re-registering the proxy with a different server.

Dual NIC support

This section outlines NetWorker support for enabling the VMware Backup appliance and external proxy appliance to support dual vNIC.

Enabling a second vNIC on the VMware Backup appliance and the external proxy appliance can provide the following benefits:

- You can separate the backup data traffic going to the back-end from the production network so that backups do not negatively impact performance in your environment.
- You can use a separate private or isolated physical network infrastructure for your backup network and send the backup data in this isolated network unencrypted, leading to performance gains.

- You can dedicate a NIC to backup traffic so as not to impact production performance if using an older host with a slower physical NIC.

Dual vNIC setup and configuration requirements

Along with the requirements specified in the sections Pre-installation requirements and Download and deploy the VMware Backup Appliances, the VMware Backup Appliance and external proxy appliance require the following:

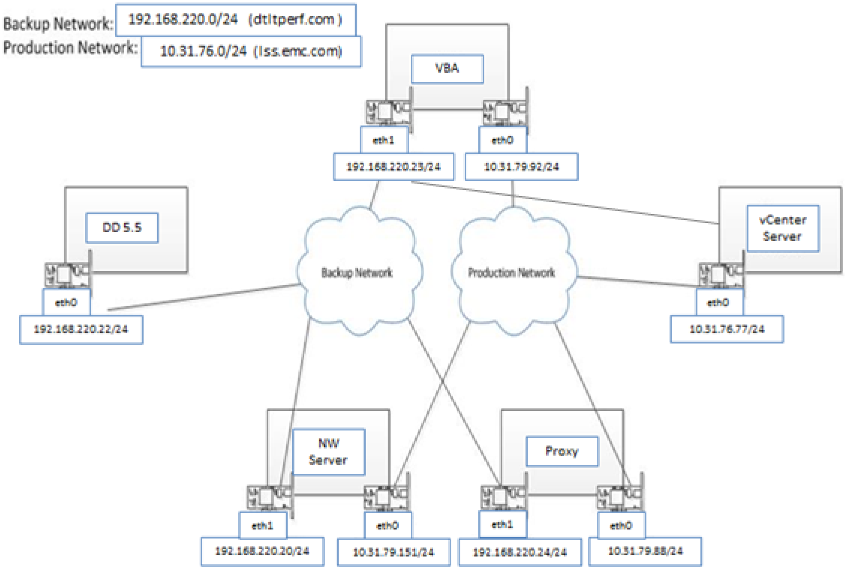
- Manually add a new vNIC of type **VMXNET 3** according to the instruction in step 3b of the section "Adding or swapping a NIC on the VMware Backup appliance or external proxy."
- Configure the two vNICs with two separate and unique subnets in order to facilitate the direction of production traffic (which includes vCenter Server traffic, VMTools requests used by file-level restore, and so on) on the first vNIC. All backup traffic will flow out of the second vNIC on the backup network. Further details for VMware Backup appliance NIC connectivity are provided in the bullets below.
- Internal proxies must be disabled.
- In order to use Instant Access restore, which will mount a NFS Data-store on the ESX, the backup network on the ESX may require a VMkernel port configured.
- Proxies with multiple NICs rely on the operating system routes and require reliable bi-directional communications with the respective subnets on which the NICs are configured with Data Domain systems.

  Note

  You may be required to define operating system routes as custom routes.

- The VMware Backup Appliance and external proxy appliance must have eth0 belong to the production network and contained within the same subnet which includes your vCenter Server eth0. Also, for the VMware Backup Appliance and external proxy appliance, eth1 must belong to the backup network and contained within the same subnet as the Data Domain device.

Figure 121 Sample backup and production network traffic flow



You can use a non-routable private address space for the subnet used for the backup traffic/data, providing that:

- All devices/vNICs using a private IP address exist on the same physical switch, and
- There is a DNS server on the non-routed private network so that the proxies can perform a reverse lookup for its host name.

Note

A private address space-based network is an optional example and not a requirement.

Verify vNIC connectivity

You can verify that the vNIC is associated to the correct network by running a test using ping or traceroute against the IP of the NetWorker server and/or vCenter and other required componenets. If the IP is not reachable, you may need to swap the network for NICs.

1. Right-click the VMware Backup appliance and select **Edit Settings**.
2. in the Hardware tab of the **Virtual Machine Properties** window, select **Network adaptor** and **Network connection** on the right of the screen.
3. In the **Network connection** page, select the correct network label.
4. Click **OK** to complete the configuration change.

For systems with swapped NICs or dual vNIC configurations, you can use the `proxycp.jar` command line utility on the VMware Backup appliance to test connectivity.

To download the `proxycp.jar` command line utility:

1. Log into the VMware Backup appliance by using the **vSphere Client** or a putty session.
2. If required, run **`sudo su -`** to switch to the root user.
3. In a command prompt, cd to **`usr/local/avamar/bin/`**.
4. Run the following command:

   ```
   curl -O ftp://avamar_ftp:anonymous@ftp.avamar.com/software/scripts/
   proxycp.jar
   ```

   For sites where direct download using `curl` is unavailable, use `WinSCP` to transfer the script to the VMware Backup appliance or external proxy.
5. Change the permissions on `proxycp.jar`:

   ```
   chmod 755 /usr/local/avamar/bin/proxycp.jar
   ```

After downloading `proxycp.jar`, you can use the following command tools to test connectivity:

- `proxycp.jar --vctest --dryrun`—Tests connectivity to vCenter and returns many details of the vCenter.
- `proxycp.jar --testconn`—connects to vCenter to perform tests at set intervals, similar to "ping tests".
- `proxycp.jar --testwebservice`—Tests connectivity to the Avamar MC SDK.

- `proxycp.jar --portcheck [--timeout <Num> ]` - Tests proxy connectivity to vCenter by discovering all nodes and hosts in the environment and then checking connectivity of each proxy to every single ESX host. Also checks for Data Domain in the environment and checks connectivity from the proxy. If running in a slower environment you can change the timeout value from the default of 10 seconds to 60 seconds.

Dual NIC configuration, and particularly operating system routes, can be very complex and require careful planning by the administrator. When complete the setup and verified working functionality of the configuration, make note of the configuration details including NIC Type, IPs, operating system routes and any other custom setttings since these may be required if he has to re-create the OVA for situations like proxy upgrades, storage failures, etc

Backing up the VMware environment using NMC

Once the OVA for the VMware Backup appliance has been successfully deployed, you can run an existing VMware protection policy with a workflow for VMware backup within the NMC **NetWorker Administration** window, and assign virtual machines and VMDKs to the workflows for backup and recovery.

Setting user privileges for the root user in the NetWorker server

Before you access the VMware Protection solution in NMC to create and assign policies, you must assign the appropriate user privileges to the root user in a user group of the NetWorker server.

Procedure

1. Run **nsradmin** from a Windows command line or UNIX terminal.
2. Type the following command:

   ```
   create type:NSR usergroup; name:user defined user group
   ```

3. When prompted with the question "Create?", type **Y**, and then exit from **nsradmin**.
4. From NMC, navigate to **NetWorker Administration** > **Server** > **User Groups**.
5. Select the created user group for the root user and type the following in the **Users** field:

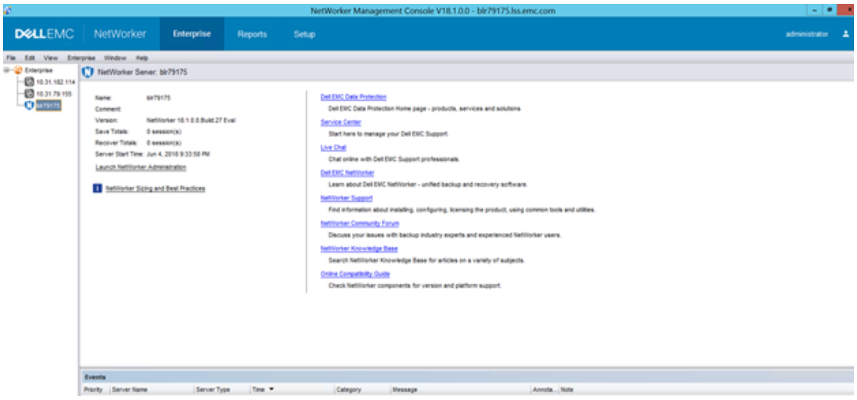
   username@VBA node
   where username is the name of a user with root privileges.

6. Assign the following privileges in the Privileges field:
   - Monitor NetWorker
   - View Application Settings.

Accessing VMware Protection in NMC

When you connect to the NMC server, the NMC GUI's **Enterprise** window appears.

Figure 122 NMC Enterprise window



NetWorker Server: blr79175

Name: blr79175
Comment:
Version: NetWorker 18.1.0.0.Build.27 Eval
Save Totals: 0 session(s)
Recover Totals: 0 session(s)
Server Start Time: Jun 4, 2018 9:33:58 PM
Launch NetWorker Administration

NetWorker Sizing and Best Practices

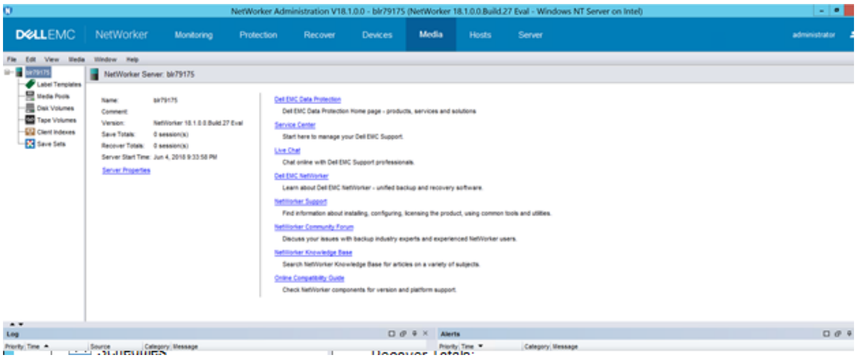
Dell EMC Data Protection
Dell EMC Data Protection Home page - products, services and solutions
Service Center
Start here to manage your Dell EMC Support.
Live Chat
Chat online with Dell EMC Support professionals.
Dell EMC NetWorker
Learn about Dell EMC NetWorker - unified backup and recovery software.
NetWorker Support
Find information about installing, configuring, licensing the product, using common tools and utilities.
NetWorker Community Forum
Discuss your issues with backup industry experts and experienced NetWorker users.
NetWorker Knowledge Base
Search NetWorker Knowledge Base for articles on a variety of subjects.
Online Compatibility Guide
Check NetWorker components for version and platform support.

Procedure

1. In the left panel of the **Enterprise** window, select the appropriate server.
2. Right-click the server, and select **Launch Application**.

   The **Administration** window opens.

   Figure 123 Protection window in the Administration window

   NetWorker Server: blr79175

   Name: blr79175
   Comment:
   Version: NetWorker 18.1.0.0.Build.27 Eval
   Save Totals: 0 session(s)
   Recover Totals: 0 session(s)
   Server Start Time: Jun 4, 2018 9:33:58 PM
   Server Properties

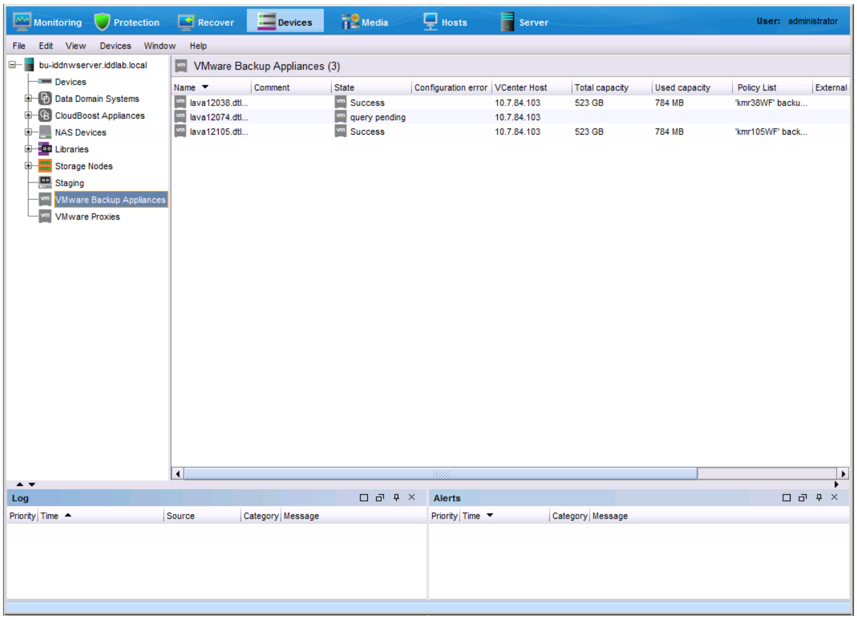
   Dell EMC Data Protection
   Dell EMC Data Protection Home page - products, services and solutions
   Service Center
   Start here to manage your Dell EMC Support.
   Live Chat
   Chat online with Dell EMC Support professionals.
   Dell EMC NetWorker
   Learn about Dell EMC NetWorker - unified backup and recovery software.
   NetWorker Support
   Find information about installing, configuring, licensing the product, using common tools and utilities.
   NetWorker Community Forum
   Discuss your issues with backup industry experts and experienced NetWorker users.
   NetWorker Knowledge Base
   Search NetWorker Knowledge Base for articles on a variety of subjects.
   Online Compatibility Guide
   Check NetWorker components for version and platform support.

   You can access many of the options for the VMware Protection solution in the **Protection** window.

VMware Backup Appliance monitoring and properties

In the **Devices** window, select **VMware Backup Appliances** and the available VMware Backup Appliances appear in the right pane. From the right pane, you can monitor the state of the VMware Backup appliance, as shown in the following figure.

Figure 124 VMware Backup appliance health monitoring in the Devices window

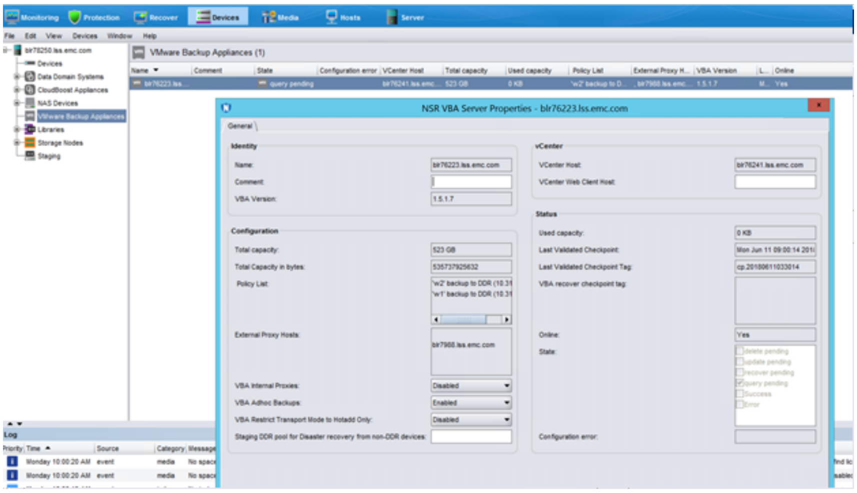


VMware Backup Appliances (3)

Name	Comment	State	Configuration error	VCenter Host	Total capacity	Used capacity	Policy List	External
lava12038.dtl...		Success		10.7.84.103	523 GB	784 MB	'kmr38WF' backu...	
lava12074.dtl...		query pending		10.7.84.103				
lava12105.dtl...		Success		10.7.84.103	523 GB	784 MB	'kmr105WF' back...	

To view more VMware Backup Appliance related properties, right-click an appliance resource and select **Properties**, or double-click an appliance. The **NSR VBA Server Properties** window displays.

Figure 125 NSR VBA Server Properties window


Monitoring
Protection
Recover
Devices
Media
Hosts
Server
File Edit View Devices Window Help
blr78250.lss.emc.com
Devices
Data Domain Systems
CloudBoost Appliances
NAS Devices
VMware Backup Appliances
Libraries
Storage Nodes
Staging
VMware Backup Appliances (1)
Name Comment State Configuration error VCenter Host Total capacity Used capacity Policy List External Proxy H... VBA Version L... Online
Log
Priority Time Source Category Message
General

NSR VBA Server Properties - blr76223.lss.emc.com

Identity

Name: blr76223.lss.emc.com

Comment:

VBA Version: 1.5.1.7

Configuration

Total capacity: 523 GB

Total Capacity in bytes: 535737925632

Policy List: 'w2' backup to DDR (10.31
'w1' backup to DDR (10.31

External Proxy Hosts: blr7968.lss.emc.com

VBA Internal Proxies: Disabled

VBA Adhoc Backups: Enabled

VBA Restrict Transport Mode to Hotadd Only: Disabled

Staging DDR pool for Disaster recovery from non-DDR devices:

vCenter

VCenter Host: blr76241.lss.emc.com

VCenter Web Client Host:

Status

Used capacity: 0 KB

Last Validated Checkpoint: Mon Jun 11 09:00:14 201

Last Validated Checkpoint Tag: cp.20180611033014

VBA recover checkpoint tag:

Online: Yes

State: ☐ delete pending ☐ update pending ☐ recover pending ☑ query pending ☐ Success ☐ Error

Configuration error:

NetWorker automatically retrieves information about the VMware Backup Appliance, including the following details and health information:

- vCenter host
- Policies pushed to the VMware Backup Appliance
- List of External proxy hosts

- Total internal storage capacity
- Used internal storage capacity
- Last Validated checkpoint
- Online/Offline
- Configuration Error
- State

In addition to the fields that NetWorker populates automatically based on the current settings, the **NSR VBA Server Properties** window includes the following fields that you can edit:

- **VBA Internal Proxies**—When set to **Enabled**, the internal proxy is active and available. Setting to **Disabled** shuts down the internal proxies and limits proxy availability to the external proxy, which is required for EXT4 and LVM support. This is set to **Enabled** by default.
- **VBA Adhoc Backups**—When set to **Enabled**, this setting allows you to run a workflow that includes any associated backup and clone actions immediately from the **Administration** window or the **vSphere Web Client**. When set to **Disabled**, you can only perform adhoc backups from the **Administration** window, and the **Backup Now** functionality in the **vSphere Web Client** is not available. This is set to **Enabled** by default.
- **VBA Restrict Transport Mode to Hotadd Only**—When set to **Enabled**, NetWorker will use only Hotadd transport mode for policy backups, and fallback to NBD mode (backups over IP) will not occur, even if Hotadd mode is not available. When set to **Disabled**, NetWorker will use Hotadd mode, and fallback to NBD mode if Hotadd mode is not available. This is set to **Disabled** by default.

Note

When you restrict the transport mode to Hotadd only, backups will fail for any VM that does not meet the Hotadd criteria as outlined in the VMware knowledgebase article 2048138. When such a failure occurs, the backup policy only reports that the backup was "Interrupted." The correct status displays when you run the following command:

```
mccli activity show | grep Eligible
```

Output similar to the following displays:

```
9139905687058209 No Eligible Proxies 0 2014-05-03 00:24 IST
00h:00m:00s 2014-05-03 00:24 IST On-Demand Backup 0 bytes 0%
VM-Local
```

VMware data protection policies for the VMware Backup appliance in NMC

You can use the NMC **NetWorker Administration** window to schedule a backup of existing VMware protection policies for the VMware Backup appliance that were created in NetWorker 9.0.x releases, or to modify what contents are included in the existing policies.

Note

NetWorker 18.1 does not support the creation of new VMware Backup appliance policies. For the creation of new policies, use the vProxy appliance.

The sections Overview of data protection policies and Default data protection policies provide more information about protection policies in NMC.

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.

Procedure

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

   A confirmation message appears.

   Note

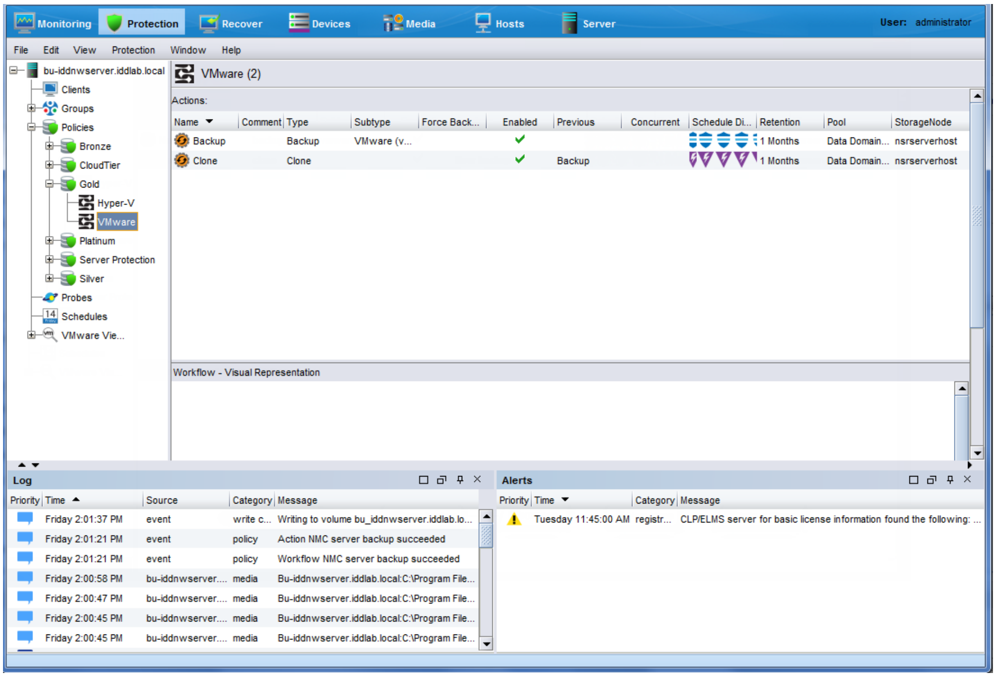
   You cannot stop, restart, or start individual actions.

   ---
3. Click **Yes**.

Visual representation of VMware policy and associated actions

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

Figure 126 VMware protection policy in the Protection window



VMware (2)

Actions:

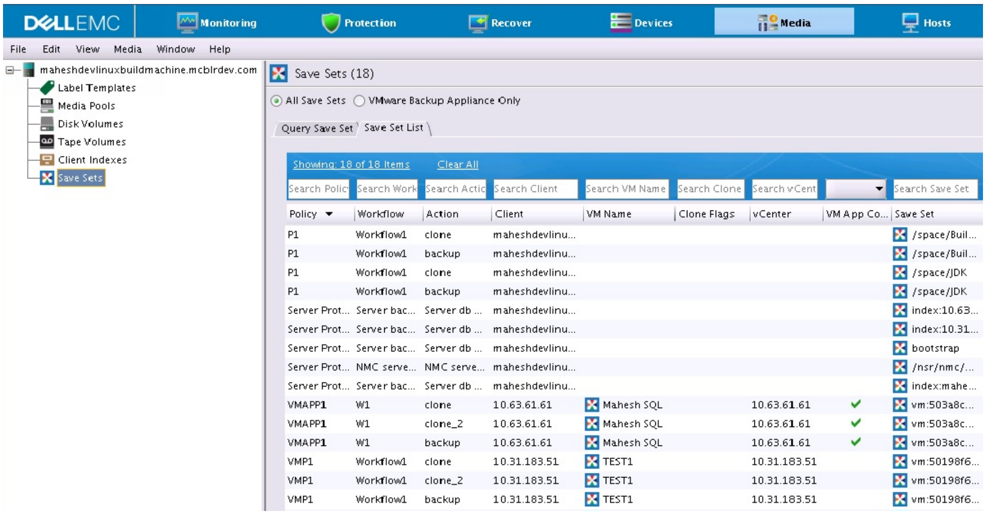
Name	Comment	Type	Subtype	Force Back...	Enabled	Previous	Concurrent	Schedule Di...	Retention	Pool	StorageNode
Backup		Backup	VMware (v...		✓				1 Months	Data Domain...	nsrserverhost
Clone		Clone			✓	Backup			1 Months	Data Domain...	nsrserverhost

Priority	Time	Source	Category	Message
	Friday 2:01:37 PM	event	write c...	Writing to volume bu_iddnwserver.iddlab.lo...
	Friday 2:01:21 PM	event	policy	Action NMC server backup succeeded
	Friday 2:01:21 PM	event	policy	Workflow NMC server backup succeeded
	Friday 2:00:58 PM	bu-iddnwserver....	media	Bu-iddnwserver.iddlab.local:C:\Program File...
	Friday 2:00:47 PM	bu-iddnwserver....	media	Bu-iddnwserver.iddlab.local:C:\Program File...
	Friday 2:00:45 PM	bu-iddnwserver....	media	Bu-iddnwserver.iddlab.local:C:\Program File...
	Friday 2:00:45 PM	bu-iddnwserver....	media	Bu-iddnwserver.iddlab.local:C:\Program File...

Priority	Time	Category	Message
⚠	Tuesday 11:45:00 AM	registr...	CLP/ELMS server for basic license information found the following: ...

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 127 VMware protection policy save sets in Media window



Save Sets (18)

● All Save Sets ○ VMware Backup Appliance Only

Policy	Workflow	Action	Client	VM Name	Clone Flags	vCenter	VM App Co...	Save Set
P1	Workflow1	clone	maheshdevlinu...					/space/Buil...
P1	Workflow1	backup	maheshdevlinu...					/space/Buil...
P1	Workflow1	clone	maheshdevlinu...					/space/JDK
P1	Workflow1	backup	maheshdevlinu...					/space/JDK
Server Prot...	Server bac...	Server db ...	maheshdevlinu...					index:10.63...
Server Prot...	Server bac...	Server db ...	maheshdevlinu...					index:10.31...
Server Prot...	Server bac...	Server db ...	maheshdevlinu...					bootstrap
Server Prot...	NMC serve...	NMC serve...	maheshdevlinu...					/nsr/nmc/...
Server Prot...	Server bac...	Server db ...	maheshdevlinu...					index:mahe...
VMAPP1	W1	clone	10.63.61.61	Mahesh SQL		10.63.61.61	✓	vm:503a8c...
VMAPP1	W1	clone_2	10.63.61.61	Mahesh SQL		10.63.61.61	✓	vm:503a8c...
VMAPP1	W1	backup	10.63.61.61	Mahesh SQL		10.63.61.61	✓	vm:503a8c...
VMP1	Workflow1	clone	10.31.183.51	TEST1		10.31.183.51		vm:50198f6...
VMP1	Workflow1	clone_2	10.31.183.51	TEST1		10.31.183.51		vm:50198f6...
VMP1	Workflow1	backup	10.31.183.51	TEST1		10.31.183.51		vm:50198f6...

VMware View in NMC

The VMware view provides an overview of the vCenter environment.

After detecting VMware environments, the **Administration** window provides a visual representation of these environments when you select **VMware View** in the left pane of the **Protection** window. Using **VMware View**, you can also assign policies.

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

Note

After upgrading to NetWorker 18.1, **VMware View** may not be visible.

Map view of the VMware environment

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

- vCenters
- DataCenters within the vCenter
- Clusters within the DataCenter
- ESX servers
- vApps
- Resource Pools
- Folders

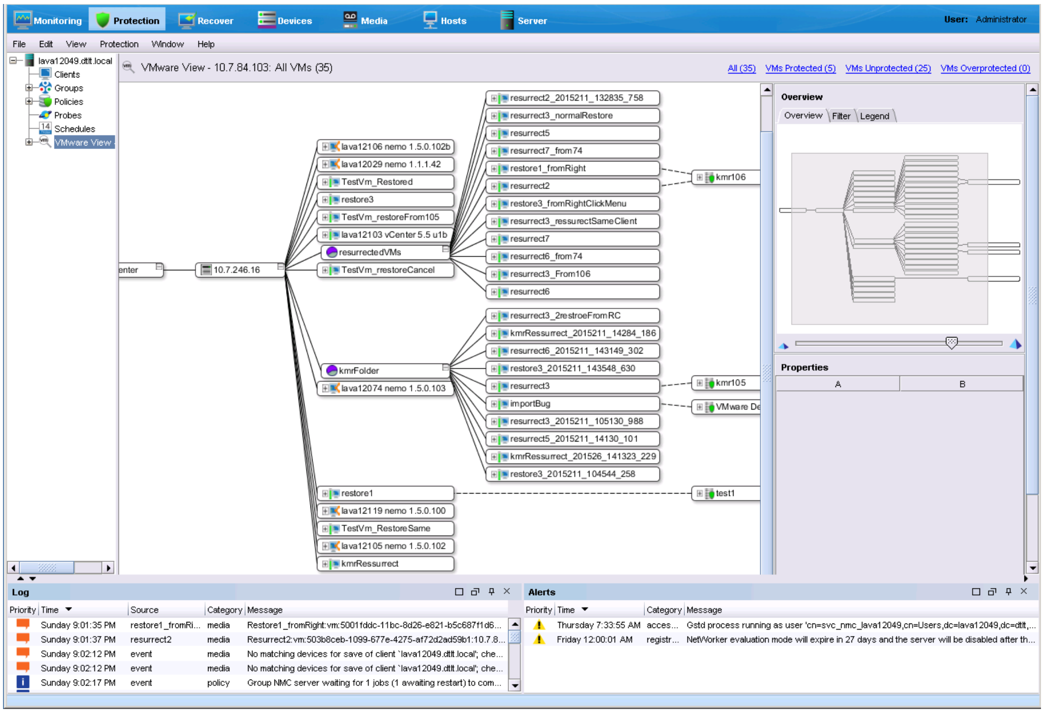
You can use several operations to navigate within the map view:

- 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, VMware Backup Appliances, external proxies, along with 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 128 Map view of VMware environment in NMC



Log

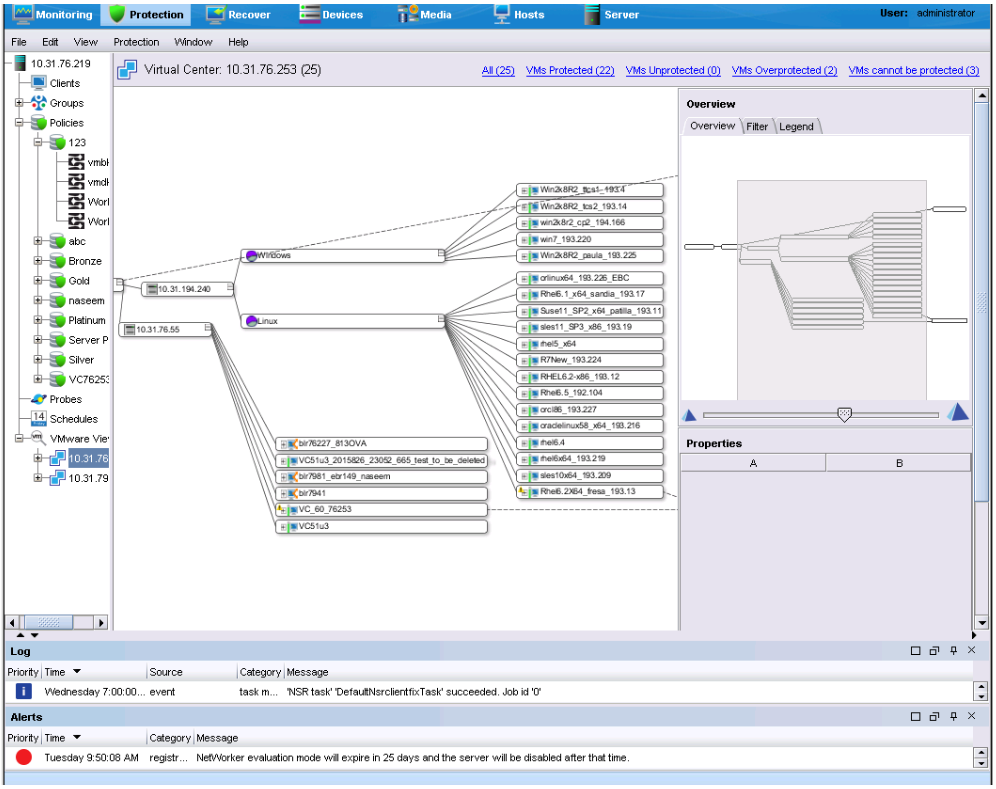
Priority	Time	Source	Category	Message
	Sunday 9:01:35 PM	restore1_fromRi...	media	Restore1_fromRight:vm:5001fddc-11bc-8d26-e821-b5c687f1d6...
	Sunday 9:01:37 PM	resurrect2	media	Resurrect2:vm:503b8ceb-1099-677e-4275-af72d2ad59b1:10.7.8...
	Sunday 9:02:12 PM	event	media	No matching devices for save of client `lava12049.dtlt.local'; che...
	Sunday 9:02:12 PM	event	media	No matching devices for save of client `lava12049.dtlt.local'; che...
i	Sunday 9:02:17 PM	event	policy	Group NMC server waiting for 1 jobs (1 awaiting restart) to com...

Alerts

Priority	Time	Category	Message
⚠	Thursday 7:33:55 AM	acces...	Gstd process running as user 'cn=svc_nmc_lava12049,cn=Users,dc=lava12049,dc=dtlt,...
⚠	Friday 12:00:01 AM	registr...	NetWorker evaluation mode will expire in 27 days and the server will be disabled after th...

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 129 Cluster with child elements in VMware View



Wednesday 7:00:00... event task m... 'NSR task' 'DefaultNsrclientfixTask' succeeded. Job id '0'

Tuesday 9:50:08 AM registr... NetWorker evaluation mode will expire in 25 days and the server will be disabled after that time.

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.

Figure 130 Filtering results in VMware View

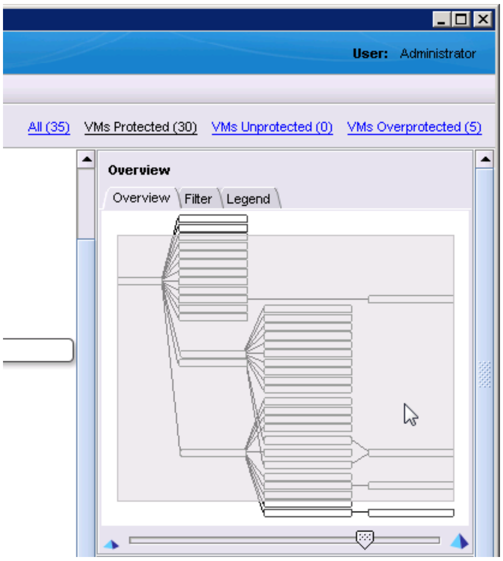


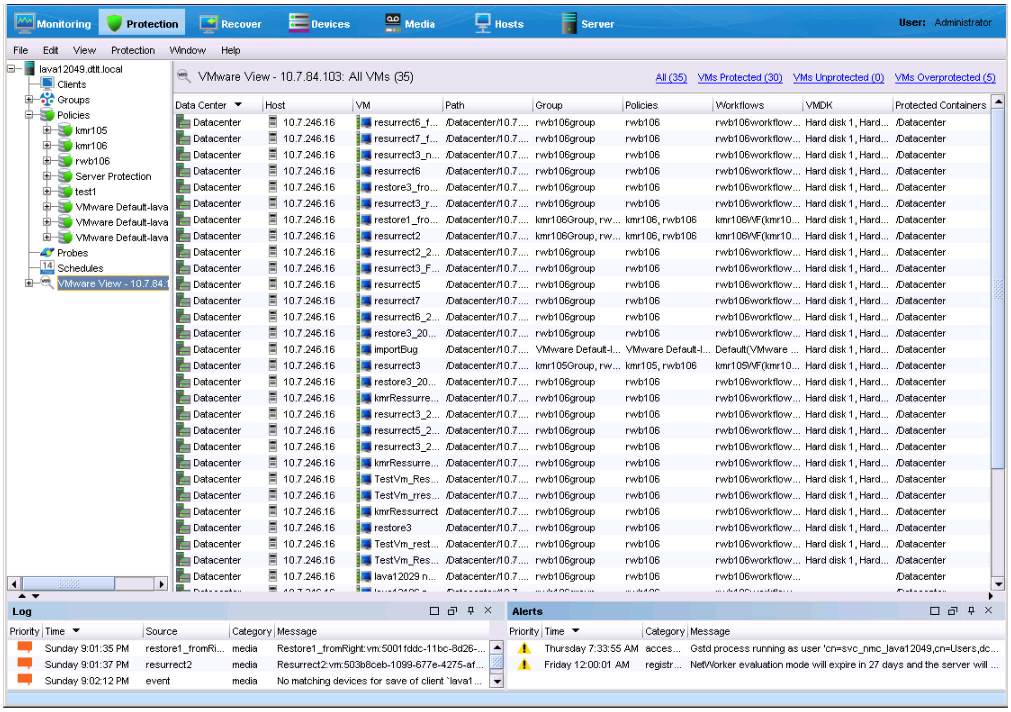
Table view of the VMware environment

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 131 VMware table view



VMware View - 10.7.84.103: All VMs (35)

All (35) VMs Protected (30) VMs Unprotected (0) VMs Overprotected (5)

Data Center	Host	VM	Path	Group	Policies	Workflows	VMDK	Protected Containers
Datacenter	10.7.246.16	resurrect6_f...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect7_f...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_n...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect6	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore3_fro...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_r...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore1_fro...	/Datacenter/10.7....	kmr106Group, rw...	kmr106, rwb106	kmr106WF(kmr10...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect2	/Datacenter/10.7....	kmr106Group, rw...	kmr106, rwb106	kmr106WF(kmr10...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect2_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_F...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect5	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect7	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect6_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore3_20...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	importBug	/Datacenter/10.7....	VMware Default-l...	VMware Default-l...	Default(VMware ...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3	/Datacenter/10.7....	kmr105Group, rw...	kmr105, rwb106	kmr105WF(kmr10...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore3_20...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	kmrRessurre...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect5_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	resurrect3_2...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	kmrRessurre...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	TestVm_Res...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	TestVm_rres...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	kmrRessurrect	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	restore3	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	TestVm_rest...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	TestVm_Res...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...	Hard disk 1, Hard...	/Datacenter
Datacenter	10.7.246.16	lava12029 n...	/Datacenter/10.7....	rwb106group	rwb106	rwb106workflow...		/Datacenter

Log

Priority	Time	Source	Category	Message
	Sunday 9:01:35 PM	restore1_fromRi...	media	Restore1_fromRight:vm:5001fddc-11bc-8d26-...
	Sunday 9:01:37 PM	resurrect2	media	Resurrect2:vm:503b8ceb-1099-677e-4275-af...
	Sunday 9:02:12 PM	event	media	No matching devices for save of client `lava1...

Alerts

Priority	Time	Category	Message
⚠	Thursday 7:33:55 AM	acces...	Gstd process running as user 'cn=svc_nmc_lava12049,cn=Users,dc...
⚠	Friday 12:00:01 AM	registr...	NetWorker evaluation mode will expire in 27 days and the server will ...

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 groups within VMware View

You can assign groups at any level, for example, you can assign a group to the entire datacenter, a cluster, a resource pool, a virtual machine, or even a VMDK by using VMware View.

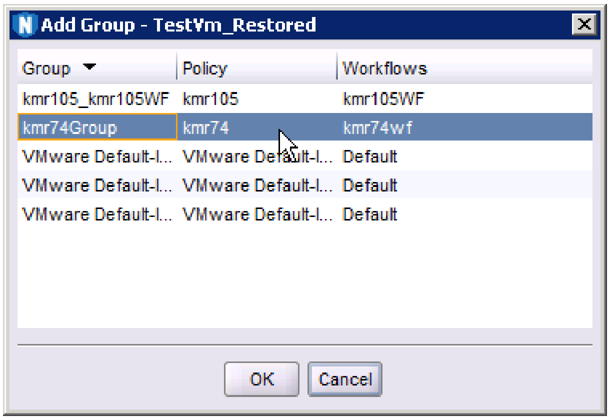
Procedure

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

2. Select **Add to Group**.

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

   Figure 132 Add group in VMware View



Add Group - TestVm_Restored

Group	Policy	Workflows
kmr105_kmr105WF	kmr105	kmr105WF
kmr74Group	kmr74	kmr74wf
VMware Default-I...	VMware Default-I...	Default
VMware Default-I...	VMware Default-I...	Default
VMware Default-I...	VMware Default-I...	Default

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**.

Overprotected and unprotected virtual machines in VMware View

NMC uses a warning icon within VMware View to show virtual machines that are overprotected (when a particular virtual machine is protected by two different groups, or two different VMware Backup appliances) or unprotected (when there are no groups assigned to protect a particular virtual machine or container).

Overprotection can only occur when you use the EMC Backup and Recovery user interface in the vSphere Web Client and NMC to assign groups to virtual machines/ VMDKs. When overprotection occurs, you can remove a group. Right-click the object and select **Remove Group**. When you unselect the additional group in the resulting dialog, the warning sign disappears.

You can use the filter links, as shown in Figure 130 on page 257, to narrow your view to only overprotected or only unprotected virtual machines.

Assigning a group to a disconnected ESXi server in VMware View

When you disconnect an ESXi host from the vCenter server, the ESXi is removed from the **EMC Backup and Recovery** user interface in the **vSphere Web Client**, but still appears in NMC's **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 connect the disconnected ESXi back to the vCenter server and run the group again.

Note

Disconnecting an ESXi server from a vCenter server only temporarily disconnects the server and does not remove the server. To permanently remove the ESXi server from the vCenter inventory, use the `Remove` option from vCenter.

Decommissioning the VMware Backup Appliance in NMC

Decommissioning should be done only with the help of EMC Support.

Managing the VMware environment using the vSphere Web Client

The vSphere Web Client provides access to the EMC Backup and Recovery user interface. The EMC Backup and Recovery user interface functions as a plug-in within the vSphere Web Client that connects to the VMware Backup Appliance, allowing you to perform several operations including:

- Assign VMs/VMDKs to policies created in NMC

  Note

  Since this same functionality, described in the section Assigning groups within VMware View on page 258, is available within NMC, EMC recommends that you only use NMC to assign VMs/VMDKs to policies.

- Backups (Ad-hoc VM backups, also known as **Backup Now** and **Backup only out of date sources**)
- Recoveries (FULLVM image-level recoveries, VMDK recoveries, and instant access recovery)
- View reports and log files for policies run
- Configuration options such as email notifications

Note

You cannot use the VMware Backup Appliance without a vCenter Server. In linked mode, the appliance works only with the associated vCenter server.

Benefits of EMC Backup and Recovery user interface in the vSphere Web Client

The **EMC Backup and Recovery** user interface provides the following benefits:

- Provides fast and efficient data protection for all of your virtual machines/VMDKs, even those migrated between ESX hosts.
- Significantly reduces disk space consumed by backup data by using patented variable-length deduplication with every backup operation. The section Deduplication store benefits on page 261 provides more information.
- Reduces the cost of backing up virtual machines and minimizes the backup window by using Changed Block Tracking (CBT) and virtual machine snapshots.
- Allows for easy backups without the need for third-party agents installed in each virtual machine.
- Uses a simple, straight-forward installation as an integrated component within EMC Backup and Recovery, which is managed by a web portal.
- Provides direct access to EMC Backup and Recovery configuration integrated into the **vSphere Web Client**.

- Protects backups with checkpoint and rollback mechanisms.
- Provides simplified recovery of Windows and Linux files with end-user initiated file level recoveries from a web-based interface.

Deduplication store benefits

Enterprise data is highly redundant, with identical files or data stored within and across systems. For example, OS files or documents sent to multiple recipients. Edited files also have tremendous redundancy with previous versions. Traditional backup methods magnify this by storing all of the redundant data repeatedly. EMC Backup and Recovery uses a patented deduplication technology to eliminate redundancy at both the file and the subfile data segment level.

Variable vs. Fixed-Length Data Segments

A key factor in eliminating redundant data at a segment (or subfile) level is the method used to determine the segment size. Snapshots and some deduplication technologies commonly use fixed-block or fixed-length segments to determine the segment size. Unfortunately, even small changes to a dataset, for example, inserting data at the beginning of a file, can change all fixed-length segments in a dataset, despite the fact that very little of the dataset has been changed. EMC Backup and Recovery uses an intelligent variable-length method to determine the segment size, which examines the data to determine logical boundary points and increases efficiency.

Logical Segment Determination

EMC Backup and Recovery uses a patented method to determine the segment size that yields optimal efficiency across all systems. The algorithm analyzes the binary structure of a data set to determine the context-dependent segment boundaries. Variable-length segments average 24 KB in size and EMC Backup and Recovery further compresses the segments to an average size of 12 KB.

EMC Backup and Recovery works for all file types and sizes and intelligently deduplicates the data by analyzing the binary structure within the VMDK files.

Image-level Backup and Restore

EMC Backup and Recovery creates VADP-integrated image-level backups. This integration offloads the backup processing overhead from the virtual machine to the EMC Backup and Recovery appliance. The EMC Backup and Recovery appliance communicates with the vCenter Server to make a snapshot of a virtual machine’s .vmdk files. Deduplication takes place within the appliance using a patented variable-length deduplication technology.

To support the large scale and continually expanding size of many environments, each EMC Backup and Recovery appliance can simultaneously back up to eight virtual machines. All virtual machines must belong to the vCenter that is dedicated to EMC Backup and Recovery.

To increase the efficiency of image-level backups, EMC Backup and Recovery utilizes the VMware Changed Block Tracking (CBT) feature. CBT enables EMC Backup and Recovery to only back up disk blocks that have changed since the last backup. This greatly reduces the backup time of a given virtual machine image and provides the ability to process a large number of virtual machines within a particular backup window.

By leveraging CBT during restores, EMC Backup and Recovery offers fast and efficient recoveries when you restore virtual machines to their original location. During a restore process, EMC Backup and Recovery queries VADP to determine which blocks have changed since the last backup, and then only recovers or replaces those blocks during a recovery. This reduces data transfer within the EMC Backup and Recovery environment during a recovery operation and reduces the recovery time.

Additionally, EMC Backup and Recovery automatically evaluates the workload between both restore methods (full image restore or a recovery leveraging CBT) and performs the method that results in the fastest restore time. This is useful in scenarios where the change rate since the last backup in a virtual machine being restored is very high and the overhead of a CBT analysis operation would be more costly than a direct full-image recovery.

The advantages of image-level backups are:

- Provides full image backups of virtual machines, regardless of the guest operating system
- Utilizes the efficient transport method SCSI hotadd when available and properly licensed, which avoids copying the entire VMDK image over the network
- Provides file-level recovery from image-level backups
- Deduplicates within and across all .vmdk files protected by the EMC Backup and Recovery appliance
- Uses CBT for faster backups and recoveries
- Eliminates the need to manage backup agents in each virtual machine
- Supports simultaneous backup and recovery for superior throughput

Connecting to the EMC Backup and Recovery user interface in the vSphere Web Client

Perform the following to connect to the **EMC Backup and Recovery** user interface within the **vSphere Web Client**.

Procedure

1. From a web browser, open the **vSphere Web Client**:

   https://*IP_address_vCenter_Server*:9443/vsphere-client/

   Note

   If you receive an SSL certificate error in your web browser, refer to the VMware knowledgebase article 1021514 at the following link:

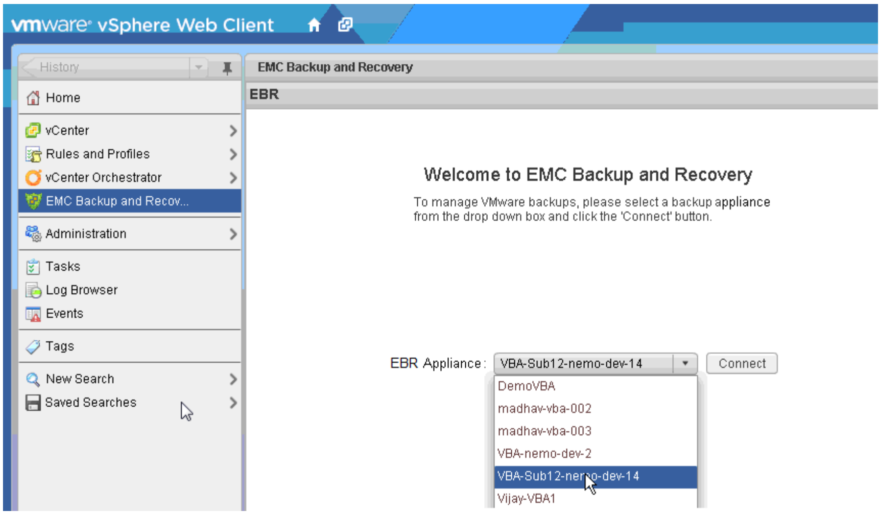
   http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021514

   ---

2. In the **Credentials** window, type the vCenter user name and password for the dedicated EMC Backup and Recovery user you created and then click **Login**.
3. In the vSphere Web Client, select **EMC Backup and Recovery**.
4. In the **Welcome to EMC Backup and Recovery** window, select an appliance from the drop-down. This drop-down lists all the VMware Backup appliances registered in the vCenter.

   Each vCenter Server supports up to 10 appliances. The EBR Appliance field, as shown in the following figure, displays the appliance names alphabetically in a drop-down list. In the EMC Backup and Recovery user interface, the name of the active appliance displays on the left pane, and the appliance name in the drop-down list is the first in the list of available appliances.

Figure 133 Selecting the Backup Appliance



Welcome to EMC Backup and Recovery

To manage VMware backups, please select a backup appliance from the drop down box and click the 'Connect' button.

EBR Appliance : VBA-Sub12-nemo-dev-14

5. Click **Connect**.

Note

The maximum retry attempts for the VMware Backup appliance to connect to the vCenter is two. Further attempts to connect to the vCenter requires restarting the EMC Backup and Recovery server by typing the command

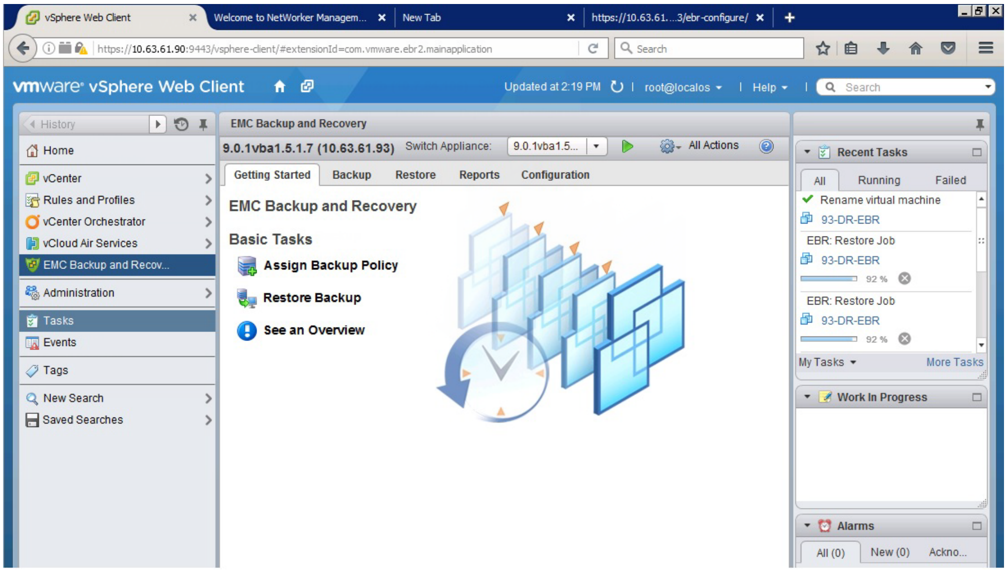
```
ebrserver.pl --restart.
```

Available tasks in the EMC Backup and Recovery user interface (VMware Backup Appliance only)

The **EMC Backup and Recovery** user interface in the **vSphere Web Client** allows you to configure and manage the VMware Backup Appliance.

When you connect to the **vSphere Web Client** and then click **EMC Backup and Recovery** in the left pane, the following page displays.

Figure 134 EMC Backup and Recovery user interface in the vSphere Web Client



The **EMC Backup and Recovery** user interface consists of five tabs:

- **Getting Started**—Provides an overview of functionality within the **EMC Backup and Recovery** user interface along with quick links to assign virtual machines to a workflow and to perform restores.
- **Backup**—Provides a list of scheduled backup workflows and details about each workflow created in NMC. This window enables you to add the virtual machines/ VMDKs that you want protected to the workflows, and to run workflows on demand.
- **Restore**—Provides a list of successful backups that you can restore.
- **Reports**—Provides backup status reports for the virtual machines on the vCenter Server that you added to the workflow.
- **Configuration**—Displays EMC Backup and Recovery configuration information and allows you to edit email settings. It also allows you to run integrity checks (for example, checkpoint creation and validation).

Backup

The **Backup** tab displays information about available backup policies.

Table 23 Backup tab column descriptions

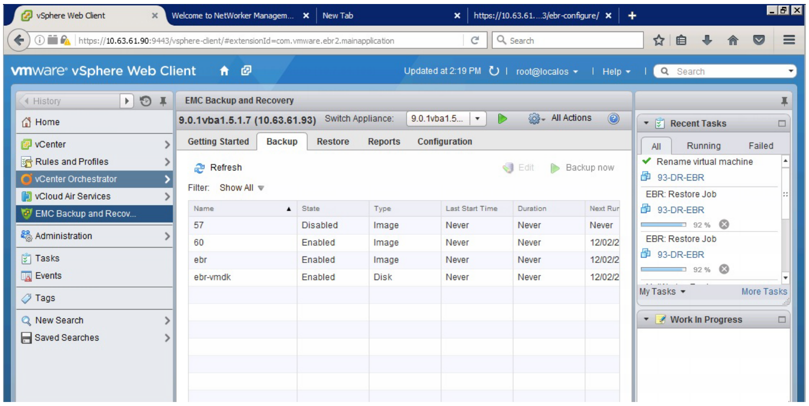
Column	Description
Name	The name of the backup policy.
State	Whether the policy is enabled or disabled. Disabled backup policies will not run. Also, a “No Schedule” state displays when you disable **Autostart** in NMC for a policy.
Type	The type of backup specified in the policy; for example, Image.
Last Start Time	The last time the policy was started.
Duration	The length of time the policy took to complete the last time it ran.
Next Run Time	The next time the policy is scheduled to run.

Table 23 Backup tab column descriptions (continued)

Column	Description
Success Count	The number of virtual machines that were backed up successfully the last time the policy ran. This number updates after each backup. Changes to a policy between backups will not be reflected in this number until after the policy runs again. For example, if a backup reports that 10 virtual machines successfully backed up, and then you edit the policy so that only one virtual machine remains, this number remains at 10 until the policy runs again and, if successful, the number changes to one.
Failure Count	The number of virtual machines that did not back up successfully the last time the policy ran. This number updates after each backup. Changes to a policy between backups will not be reflected in this number until after the policy runs again. For example, if a backup reports that 10 virtual machines failed to back up, and then you edit the policy so that only one virtual machine remains, this number remains at 10 until the policy runs again and, if the backup fails, the number changes to one.
Destination	The location specified in the policy for the backup.

The following figure displays three example backup policies.

Figure 135 VMware Backup Appliance Backup tab

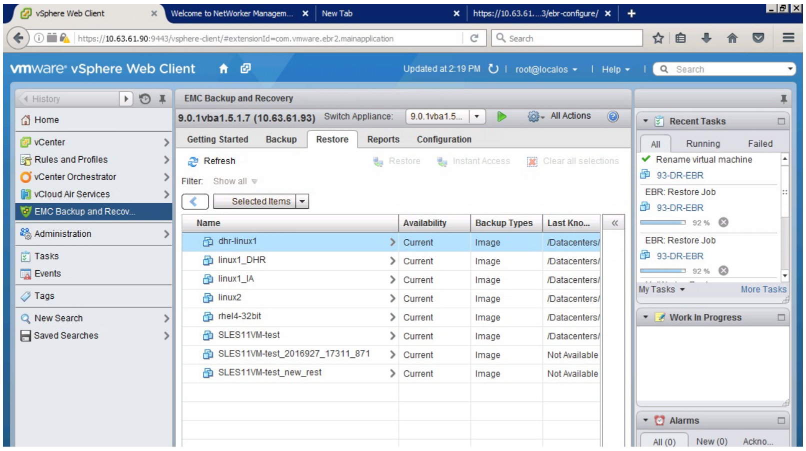


Name	State	Type	Last Start Time	Duration	Next Rur
57	Disabled	Image	Never	Never	Never
60	Enabled	Image	Never	Never	12/02/2
ebr	Enabled	Image	Never	Never	12/02/2
ebr-vmdk	Enabled	Disk	Never	Never	12/02/2

Restore

The **Restore** tab displays a list of virtual machines that were backed up using the VMware Backup Appliance. By navigating through the list of backups, you can select and restore specific backups.

Figure 136 VMware Backup Appliance Restore tab



Name	Availability	Backup Types	Last Kno...
dhr-linux1	Current	Image	/Datacenters/
linux1_DHR	Current	Image	/Datacenters/
linux1_IA	Current	Image	/Datacenters/
linux2	Current	Image	/Datacenters/
rhel4-32bit	Current	Image	/Datacenters/
SLES11VM-test	Current	Image	/Datacenters/
SLES11VM-test_2016927_17311_871	Current	Image	Not Available
SLES11VM-test_new_rest	Current	Image	Not Available

Over time, the information displayed on the **Restore** tab may become out of date. To view the most up-to-date information on backups available for restore, click **Refresh**.

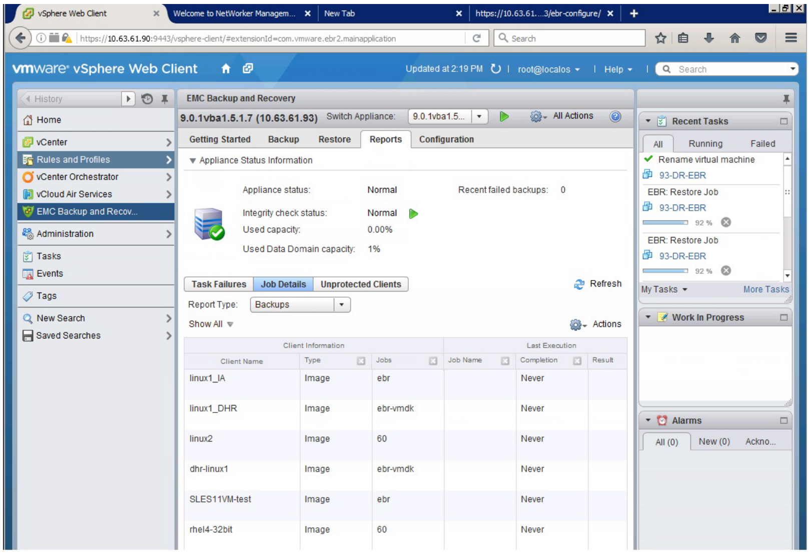
More information on restore is provided in the section Restoring the VMware environment on page 276.

Reports

On the **Reports** tab, you can view lists of task failures, job details, and unprotected clients. You can also export report information to a CSV file by selecting **Actions** > **Export to CSV**.

The following figure shows the **Reports** tab with the **Job Details** report selected.

Figure 137 VMware Backup appliance Reports tab



Appliance status: Normal

Recent failed backups: 0

Integrity check status: Normal

Used capacity: 0.00%

Used Data Domain capacity: 1%

Report Type: Backups

Client Information			Last Execution		
Client Name	Type	Jobs	Job Name	Completion	Result
linux1_IA	Image	ebr		Never	
linux1_DHR	Image	ebr-vmdk		Never	
linux2	Image	60		Never	
dhr-linux1	Image	ebr-vmdk		Never	
SLES11VM-test	Image	ebr		Never	
rhel4-32bit	Image	60		Never	

Task Failures

The **Task Failures** tab lets you list all of the tasks that have failed, or filter the failed tasks by **Error**, **Job**, or **Client**. When filtering task failures, select the options that display depending on the type of failure you select.

You can rerun a failed task by selecting the task, and clicking **Actions** > **Rerun Task**.

The information displayed on the **Task Failure** tab is described in the following table.

Table 24 Task Failure column descriptions

Column	Description
Failure Time	The date and time that the task failed.
Reason	The reason the task failed.
Client/Source Name	The name of the client for which the task failed.
Job Name	The name of the job that failed.
Job Type	The type of job that failed.
Next Run Time	The next time the job is scheduled to run.

Job Details

The **Job Details** tab lets you display information about backup and restore jobs that have occurred and that are scheduled. You can view information about all backup or restore jobs, or filter the jobs by **Client**, **Last Execution**, and **Next Execution**. When filtering jobs, select the options that display depending on the type of job you select.

The information displayed on the **Job Details** tab is described in the following table.

Table 25 Job Details column descriptions

Column	Description
Client Information	
Client Name	The name of the client on which the job ran.
Type	The type of job: Image, MS SQL, MS Exchange, MS SharePoint
Jobs	The name of the job.
Last Execution	
Job Name	The name of the job that ran.
Completion	The date and time the job completed. If the job has not run, this column contains **Never**.
Result	The result of the job: Success or Failure.
Next Execution	
Job Name	The name of the job that is scheduled to run.
Scheduled	The date and time the job is scheduled to run again.

Unprotected Clients

The **Unprotected Clients** tab lets you display information about the clients the are currently unprotected by the VMware Backup Appliance. You can list all unprotected clients, or you can filter by **Name**, **IP Address**, or **VM Path**. When filtering clients, select the options that display, and type the filter criteria in the text box.

The information displayed on the **Unprotected Clients** tab is described in the following table.

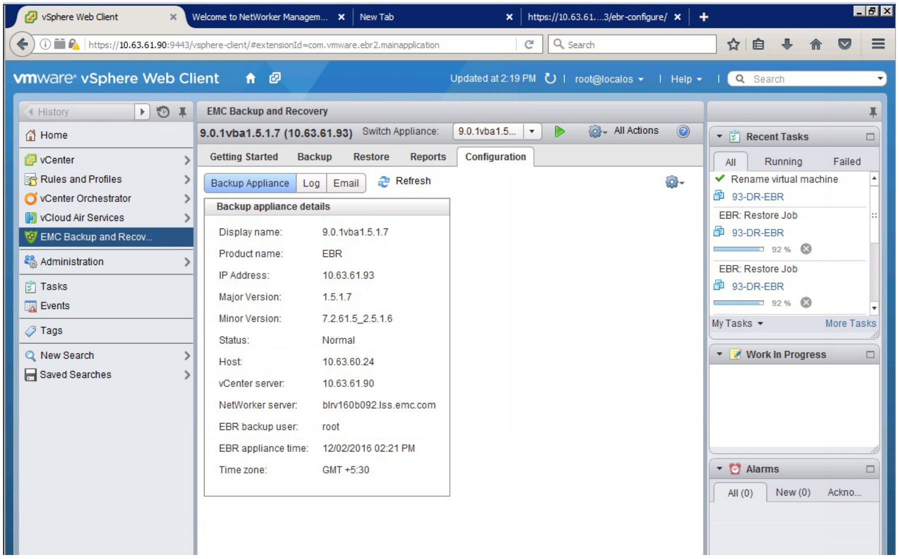
Table 26 Unprotected Clients column descriptions

Column	Description
Client Name	The name of the client on which the job ran.
IP Address	The client's IP address.
VM Path	The client's VM path.

Configuration

The **Configuration** tab allows you to manage the maintenance tasks for the VMware Backup Appliance.

Figure 138 VMware Backup Appliance Configuration tab



Backup appliance details

Display name: 9.0.1vba1.5.1.7

Product name: EBR

IP Address: 10.63.61.93

Major Version: 1.5.1.7

Minor Version: 7.2.61.5_2.5.1.6

Status: Normal

Host: 10.63.60.24

vCenter server: 10.63.61.90

NetWorker server: blrv160b092.lss.emc.com

EBR backup user: root

EBR appliance time: 12/02/2016 02:21 PM

Time zone: GMT +5:30

Viewing VMware Backup Appliance details

The **Backup Appliance** view on the **Configuration** tab shows you how the VMware Backup Appliance is configured.

The details that are displayed are described in the following table.

Table 27 Backup appliance detail descriptions

Detail	Description
Display name	The name of the VMware Backup Appliance in the vCenter.

Table 27 Backup appliance detail descriptions (continued)

Detail	Description
Product name	The name of the product.
IP Address	The IP address of the VMware Backup Appliance.
Major Version	The main version number of the VMware Backup Appliance.
Minor Version	The build version of the VMware Backup Appliance.
Status	The status of the VMware Backup Appliance.
Host	The hostname of the VMware Backup Appliance.
vCenter server	The IP address of the vCenter managing the VMware Backup Appliance.
NetWorker server	The IP address of the NetWorker server on which the VMware Backup Appliance is managed.
EBR backup user	The user name used to log in to the vSphere Web Client.
EBR appliance time	The current time in the time zone set on the VMware Backup Appliance.
Time zone	The time zone in which the VMware Backup Appliance is running.

You can configure these options during the VMware Backup Appliance installation. You can also edit these options by using the **EMC Backup and Recovery Configuration** utility as described in Post-installation configuration on page 240.

Viewing and exporting logs

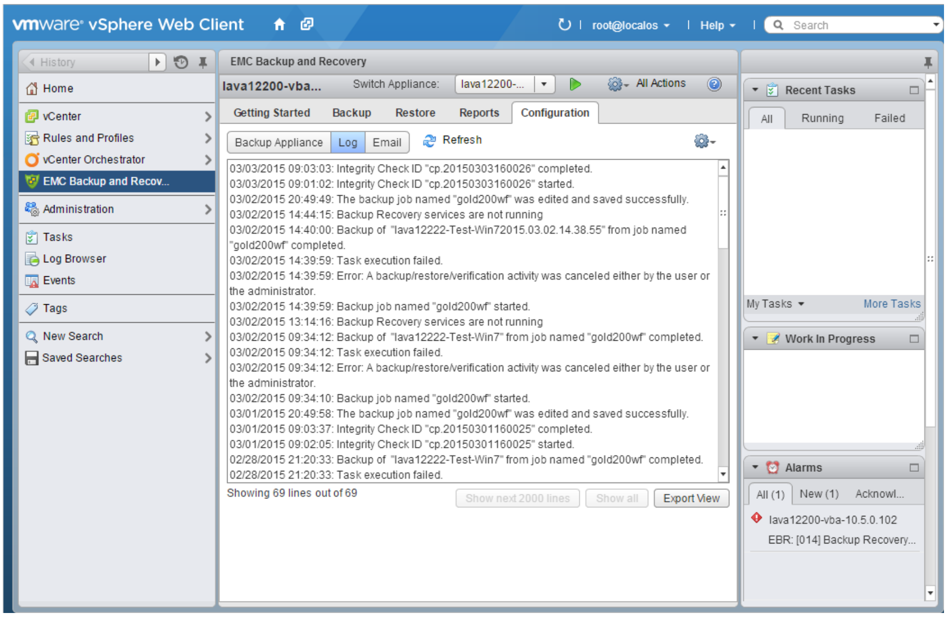
The **Log** view on the **Configuration** tab displays a log that lists the activities that have been initiated with the user interface and that identifies some key status items. You can export the log information as a .log file if needed.

Procedure

1. On the **Configuration** tab, click **Log**.

   A high-level log is displayed.

Figure 139 Log view



```
03/03/2015 09:03:03: Integrity Check ID "cp.20150303160026" completed.
03/03/2015 09:01:02: Integrity Check ID "cp.20150303160026" started.
03/02/2015 20:49:49: The backup job named "gold200wf" was edited and saved successfully.
03/02/2015 14:44:15: Backup Recovery services are not running
03/02/2015 14:40:00: Backup of  "lava12222-Test-Win72015.03.02.14.38.55" from job named
"gold200wf" completed.
03/02/2015 14:39:59: Task execution failed.
03/02/2015 14:39:59: Error: A backup/restore/verification activity was canceled either by the user or
the administrator.
03/02/2015 14:39:59: Backup job named "gold200wf" started.
03/02/2015 13:14:16: Backup Recovery services are not running
03/02/2015 09:34:12: Backup of  "lava12222-Test-Win7" from job named "gold200wf" completed.
03/02/2015 09:34:12: Task execution failed.
03/02/2015 09:34:12: Error: A backup/restore/verification activity was canceled either by the user or
the administrator.
03/02/2015 09:34:10: Backup job named "gold200wf" started.
03/01/2015 20:49:58: The backup job named "gold200wf" was edited and saved successfully.
03/01/2015 09:03:37: Integrity Check ID "cp.20150301160025" completed.
03/01/2015 09:02:05: Integrity Check ID "cp.20150301160025" started.
02/28/2015 21:20:33: Backup of  "lava12222-Test-Win7" from job named "gold200wf" completed.
02/28/2015 21:20:33: Task execution failed.
```

Showing 69 lines out of 69

2. Scroll through the log information, using the scroll bar and the **Show next 2000 lines** and **Show all** navigation buttons as needed.
3. Click **Export View** if you want to save the details that are displayed on the screen to a file on the machine where your browser is running.

   The **Save As** dialog box opens, and you can select where to save the file.

Configuring email

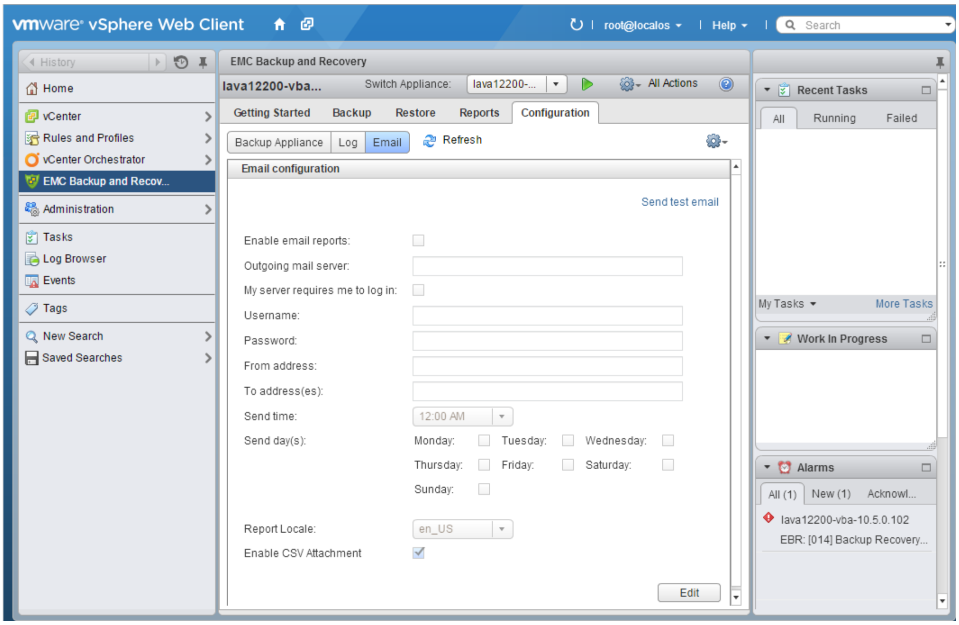
The **Email** view on the **Configuration** tab lets you configure EMC Backup and Recovery to send SMTP email reports to specified recipients.

Procedure

1. On the **Configuration** tab, click **Email**.

   The **Email configuration** screen displays.

Figure 140 Email configuration view



Enable email reports: ☐

Outgoing mail server:

My server requires me to log in: ☐

Username:

Password:

From address:

To address(es):

Send time: 12:00 AM

Send day(s): Monday: ☐ Tuesday: ☐ Wednesday: ☐ Thursday: ☐ Friday: ☐ Saturday: ☐ Sunday: ☐

Report Locale: en_US

Enable CSV Attachment: ☑

2. Click **Edit**.
3. Select the **Enable email reports** checkbox.

   The configuration fields are enabled so that you can enter information.
4. Supply information in the fields using the definitions shown in the following table.

   Red asterisks indicate required information.

Table 28 Email configuration field descriptions

Field name	Description
Outgoing mail server	Enter the name of the SMTP server that want to use to send email. This name can be entered as an IP address, a host name, or a fully qualified domain name. The EMC Backup and Recovery appliance needs to be able to resolve the name entered. The default port for non-authenticated email servers is 25. The default port of authenticated mail servers is 587. You can specify a different port by appending a port number to the server name. For example, to specify the use of port 8025 on server "emailserver" enter: ***`emailserver`***`:8025`
My server requires me to log in	Check this box if your SMTP server requires authentication.
Username	Enter the username you want to authenticate with.
Password	Enter the password associated with the username. (EMC Backup and Recovery does not validate the password in any way; the password entered is passed directly to the email server.)
From address	Enter the email address you would like the email report to be from. This can only be a single address.
To address(es)	Enter a comma separated list of up to 10 email addresses.

Table 28 Email configuration field descriptions (continued)

Field name	Description
Send time	From the drop-down list choose the time you want EMC Backup and Recovery to email reports.
Send day(s)	Check the days you want the reports sent.
Report Locale	From the drop-down list choose the locale for the email reports.
Enable CSV Attachment	Select this option to enable the email to attach a CSV file.

5. To test the email configuration, click **Send test email**.

Results

EMC Backup and Recovery reports sent by email will contain information similar to that shown below.

```
Example-6.2.30.40 - (10.5.123.45)
--------------------------------------------------------------------
-
Report Date:                            February 27, 2012 - 15:12
Last Report Date:                       February 27, 2012 - 14:45

Appliance Status:                       Normal
Byte Capacity:                          498.945 GiB
Bytes Free:                             498.196 GiB
Used Capacity:                          0.50%
Bytes Protected:                        8 GiB
Bytes Deduped:                          0.748 GiB
Integrity Check Status:                 Normal
Recent Successful Backups:                  1
Recent Failed Backups:                  1

Backup Jobs Summary
--------------------------------------------------------------------
Backup Job: another-one-with-vm-315
  Backup Sources:                       VM-315
  Last Start Time:                      February 27, 2012 - 15:07
  Next Run Time:                        February 27, 2012 - 20:00
 Last Successful Backups:              0
 Last Failed Backups:                  1
 Backup Job: VM-315
  Backup Sources:                       VM-315
  Last Start Time:                      February 27, 2012 - 15:01
  Next Run Time:                        February 27, 2012 - 20:00
  Last Successful Backups:              1
  Last Failed Backups:                  0

Virtual Machines Summary
------------------------------------------------------------------
Virtual Machine: @#_+-&<>.
  State:                                poweredOff
  Backup Jobs:
  Last Backup Job:
  Last Successful Backup:               Never
  Last Backup Job Date:                 Never

Virtual Machine: VM-315
State:                                 poweredOff
Backup Jobs:                           VM-315, another-one-with-
vm-315
Last Backup Job:                       another-one-with-vm-315
Last Successful Backup:                        February 27, 2012 - 15:03
Last Backup Job Date:                          February 27, 2012 - 15:09
```

Running an integrity check

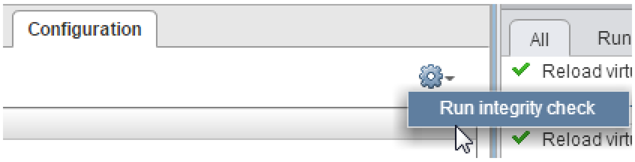
When EMC Backup and Recovery performs an integrity check, the appliance evaluates whether the contents are internally consistent. You can run an integrity check from any view on the Configuration tab.

Procedure

1. Select the EMC Backup and Recovery appliance's **Configuration** tab.
2. Click the gear icon, and select **Run integrity check**.

   The following figure shows how to run an integrity check.

   Figure 141 Run Integrity Check option

3. In the **Confirm** dialog box, click **Yes**.

   A message displays that inform you that the integrity check was successfully initiated.
4. Click **OK**.

Assigning virtual machines/VMDKs to a backup

Note

Even though you can use the **EMC Backup and Recovery** user interface in the **vSphere Web Client** to assign virtual machines or VMDKs to a workflow that you created in NMC, EMC recommends that you use NMC for this functionality.

You can assign collections of virtual machines (such as all virtual machines in a datacenter), individual virtual machines, and VMDKs to be included in a policy's workflow that you created in NMC using the **EMC Backup and Recovery** user interface in the **vSphere Web Client**. If you select an entire resource pool, host, datacenter, or folder, then subsequent backups will include any new virtual machines in the container. If you select a virtual machine, then NetWorker includes any disk added to the virtual machine in the backup. If you move the virtual machine from the selected container to another unselected container, then the virtual machine is no longer part of the backup.

You can also manually select a virtual machine for back up, which ensures that NetWorker will back up the virtual machine, even when you move the virtual machine.

EMC Backup and Recovery will not back up the following specialized virtual machines:

- VMware Backup Appliances
- VMware Data Protection (VDP) Appliances
- Templates
- Secondary fault tolerant nodes
- Proxies

- Avamar Virtual Edition (AVE) Servers

The wizard allows you to select these virtual machines; however, when you click **Finish**, the wizard displays a warning that the job does not contain these special virtual machines.

Procedure

1. Select **EMC Backup and Recovery** in the vSphere Web Client.
2. On the **Getting Started** tab, select **Assign Backup Policy**.

   The **Backup** tab displays, which shows the available policy workflows in the upper half of the window, and the workflow details in the lower half.

   The description matches the description of the policy workflow in NMC.

3. Select the workflow to which you want to add a virtual machine or VMDK, and then click **Edit**.

   The **Editing backup policy** wizard opens, and displays all of the virtual machines in the vCenter.

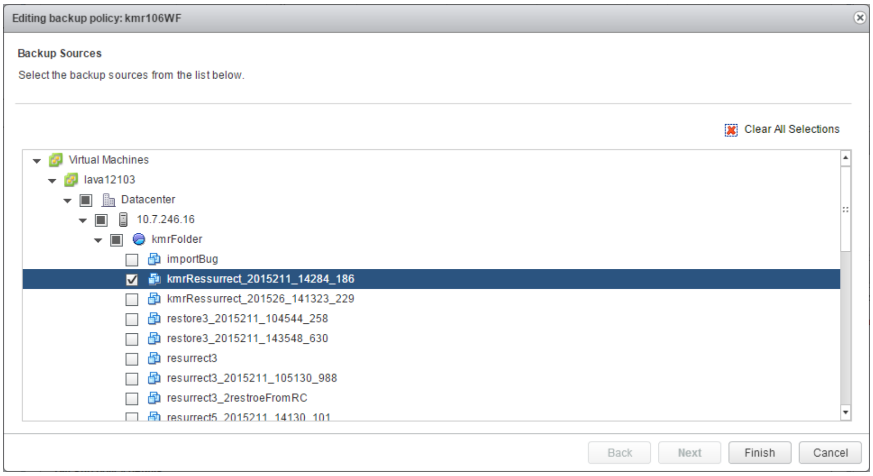
4. Click the checkboxes to select the virtual machines that you want to include in the selected workflow, as shown in the following figure, or expand the virtual machines to select VMDKs. You can also select other inventory objects, for example, Resource Pools or Clusters in addition to specific virtual machines.

   #### Note

   You can only assign virtual machines and VMDKs to the workflows that you create in NMC.

   The following figure provides an example of how to select virtual machines in the wizard.

   Figure 142 Selecting virtual machines in the Editing backup policy wizard



Editing backup policy: kmr106WF

Backup Sources

Select the backup sources from the list below.

Clear All Selections
Virtual Machines
lava12103
Datacenter
10.7.246.16
kmrFolder
□ importBug
☑ kmrRessurrect_2015211_14284_186
□ kmrRessurrect_201526_141323_229
□ restore3_2015211_104544_258
□ restore3_2015211_143548_630
□ resurrect3
□ resurrect3_2015211_105130_988
□ resurrect3_2restroeFromRC
□ resurrect5_2015211_14130_101
Back
Next
Finish
Cancel

5. Click **Finish**.

   A message indicates that the policy workflow was saved successfully.

6. Click the **Refresh** button to refresh your screen.

   You may have to click **Refresh** more than once. When the editing process has completed, the **Backup** and **Edit** buttons become active again.

Results

To see which backup sources are protected by a policy workflow, click **Show items** next to **Sources** in the **Backup policy details** panel.

Manually starting a workflow by using Backup Now

Within the **EMC Backup and Recovery** user interface in the **vSphere Web Client**, you can manually start the policy workflow that you created in NetWorker by using the **Backup** tab.

Procedure

1. On the **Backup** tab, select the policy that you want to run.
2. Click **Backup now**, and select one of the following options:
   - **Backup all sources**
   - **Backup only out of date sources**

   When you start the workflow, any clone actions associated with the workflow will also run.

   Note

   If you disabled the **Backup Now** functionality in the **NSR VBA Server Properties** window in NetWorker, as described in the section VMware Backup Appliance monitoring and properties on page 251, a message displays when you click this button indicating that Backup Now is locked and not available.

   Otherwise, you can wait for NetWorker to start the workflow based on the scheduled start time.

Stopping a workflow

Procedure

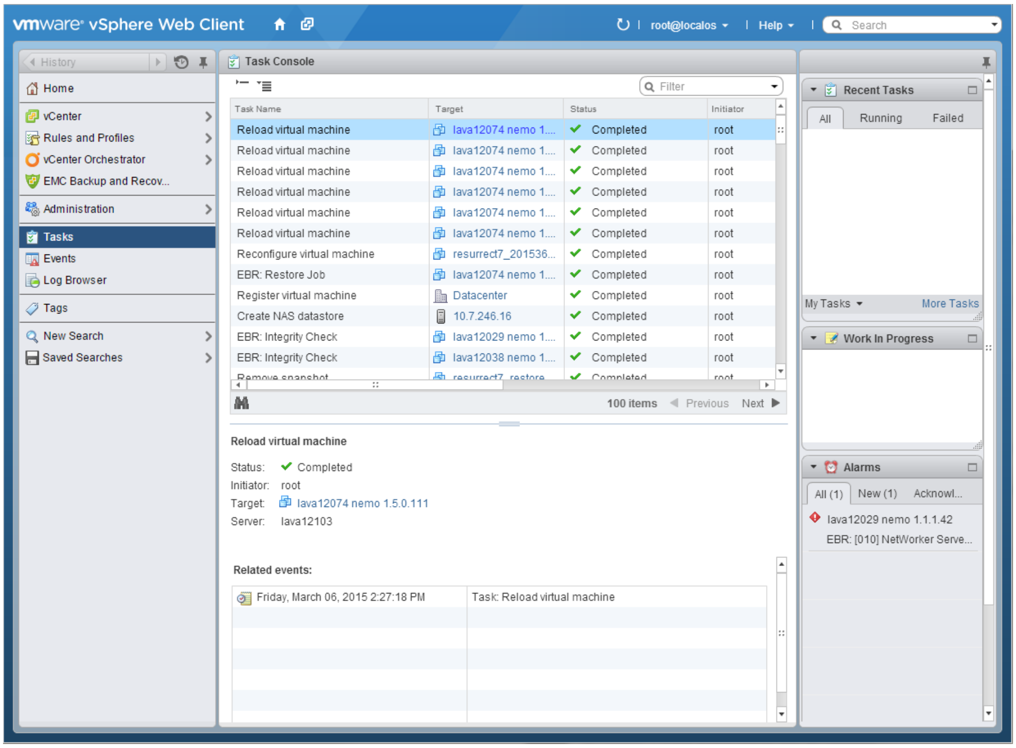
1. Select the **Backup** tab.
2. in the **Recent Tasks** pane, click the circular **x** symbol associated with the workflow.

Viewing workflow progress

To view the progress for a policy's workflow, select **Tasks** in the left pane of the **vSphere Web Client**.

The **Task Console** displays, as shown in the following figure.

Figure 143 Viewing workflow progress in the Task Console



Task Name	Target	Status	Initiator
Reload virtual machine	lava12074 nemo 1....	✓ Completed	root
Reload virtual machine	lava12074 nemo 1....	✓ Completed	root
Reload virtual machine	lava12074 nemo 1....	✓ Completed	root
Reload virtual machine	lava12074 nemo 1....	✓ Completed	root
Reload virtual machine	lava12074 nemo 1....	✓ Completed	root
Reload virtual machine	lava12074 nemo 1....	✓ Completed	root
Reconfigure virtual machine	resurrect7_201536...	✓ Completed	root
EBR: Restore Job	lava12074 nemo 1....	✓ Completed	root
Register virtual machine	Datacenter	✓ Completed	root
Create NAS datastore	10.7.246.16	✓ Completed	root
EBR: Integrity Check	lava12029 nemo 1....	✓ Completed	root
EBR: Integrity Check	lava12038 nemo 1....	✓ Completed	root
Remove snapshot	resurrect7_restore...	✓ Completed	root

100 items Previous Next

Reload virtual machine

Status: ✓ Completed
Initiator: root
Target: lava12074 nemo 1.5.0.111
Server: lava12103

Related events:

Friday, March 06, 2015 2:27:18 PM	Task: Reload virtual machine

After the backup completes, you can recover the virtual machine in the **vSphere Web Client** or use the **EMC Data Protection Restore Client** to perform a file-level restore.

Restoring the VMware environment

The NetWorker VMware Protection solution provides two levels of restore functionality:

- A FULLVM (image-level) restore will restore an entire backup image or selected drives to the original VM, another existing VM, or a new VM. These restores are less resource intensive and are best used for restoring large amounts of data quickly.
- File-level restores will restore specific folders or files from an image backup. These restores are more resource intensive and are best used to restore a relatively small amounts of data.

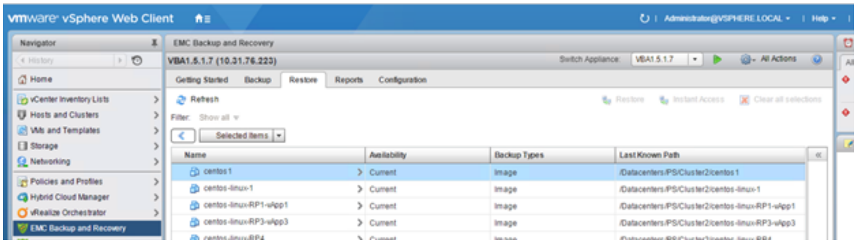
FULLVM (Image-level) Restore

When the backup completes, you can perform an image-level restore of full virtual machines by selecting either of the following options in the EMC Backup and Recovery user interface:

- Click **Restore Backup** on the **Getting Started** tab.
- Select the **Restore** tab.

When you select the **Restore** tab, available virtual machines for the selected appliance display. Additionally, you can select a different appliance from the **Restore points from** drop-down, as described in the section Recovering from a secondary site. For every clone, a backup appears under the restore point.

Figure 144 Restore tab in EMC Backup and Recovery user interface



Name	Availability	Backup Types	Last Known Path
centos1	Current	Image	/Datacenters/PS/Cluster2/centos1
centos-linux-1	Current	Image	/Datacenters/PS/Cluster2/centos-linux-1
centos-linux-RP1-vApp1	Current	Image	/Datacenters/PS/Cluster2/centos-linux-RP1-vApp1
centos-linux-RP3-vApp3	Current	Image	/Datacenters/PS/Cluster2/centos-linux-RP3-vApp3
centos-linux-RP4	Current	Image	/Datacenters/PS/Cluster2/centos-linux-RP4

Image-level restore with resurrection

Restores from devices will be slow if resurrection is required. Resurrection is a type of recovery in which the primary backup (or snapup) in the VMware Backup Appliance is no longer available. Resurrection is not supported for VMDK-level backups, and you can only perform resurrection when you associate a client with the policy.

For Data Domain devices, resurrection only occurs when restoring a cloned backup. For AFTD and tape devices, resurrection requires a local Data Domain device on the NetWorker server. For a Cloud Boost device, a resurrection restore can take more than an hour depending on the virtual machine size, during which time the only progress that displays is message within ebrserver.log showing a save set copy is in progress.

Note

If there is no staging pool available when resurrecting from an AFTD, the restore does not fail automatically after timing out. You must manually cancel the restore operation.

Performing a FULLVM restore

Procedure

1. If restoring the VM to its original location, power off each virtual machine that you want to restore.

   Note

   Power off is not required if restoring the VM to a new location.

   ---

2. In **EMC Backup and Recovery**, on the **Restore** tab, use the **Restore points from** drop-down to select the appliance from which you want to restore.

   EMC Backup and Recovery displays the virtual machines that are available to restore.

3. Click the virtual machine that you want to restore to expand its backups.

   Use the **Filter** drop-down to display a specific VM and related items. You can also click a backup to display the VMDK level and select a single VMDK for restore, if you only want to restore that disk.

4. Select a backup, and then click **Restore**.

   The **Restore Backup** wizard launches.

5. On the **Select Backup** page, verify that the list of backups is correct. Remove any backup that you want to exclude, and click **Next**.

6. On the**Set Restore Options** page, perform one of the following tasks:

- Select the **Restore to original location** option to restore the backup to its original location. If the VMDK file still exists at the original location, the restore process overwrites the file.
- Unselect the **Restore to original location** option, and specify a new name and destination where the virtual machine or VMDK will be restored.

7. Optionally, select **Advanced options** to set the VM to **Power On** and **Reconnect NIC** after the restore process completes.

   Note

   Reconnect NIC is enabled by default and greyed out. Only when you select **Power On** are you given the option to clear the **Reconnect NIC** option.

8. Click **Next**.
9. On the **Ready to complete** page, verify the selections. The wizard displays a summary of the number of machines that will be replaced (restore to the original location) and the number of machines that will be created (restore to a new location).
10. To change any of the settings for your restore request, either use the **Back** button to return to the appropriate screen, or click the appropriate numbered step title to the left of the wizard. If the settings are correct, then click **Finish**.

    The **Restore Backup** wizard displays a message that the restore process initiated successfully.

11. Click **OK**.

    You can monitor the restore progress by using the **Recent Tasks** pane.

    Note

    If you selected **Reconnect NIC** during the restore process, then confirm the network configuration for the newly-created virtual machine. Once the restore completes, the new virtual machine NIC might use the same IP address as the original virtual machine, which will cause conflicts.

Results

When the recovery starts, a recovery session also displays in NMC. Any activities that occur on the vCenter side are visible on the NMC side.

Canceling a FULLVM restore

To cancel a restore at any time during setup, click the circular **x** symbol associated with the restore job in the **Recent Tasks** pane.

Instant Access restore (for Data Domain systems only)

If your primary backup is located on a Data Domain system, clicking the **Instant Access** button on the **Restore** tab allows you to perform a quick restore of these backups, the same as you would perform a typical FULLVM restore. No further configuration is required to use this feature.

The Instant Access restore operation has the following limitations:

- The free space on the Data Domain system must be equal to or greater than the total disk size of the VM being restored, as the restore does not take into account the actual space required after deduplication occurs. If there is insufficient disk space, an error appears indicating "Insufficient disk space on datastore," and creation of the target VM fails.

- You cannot use the **Instant Access** button when you select more than one different Data Domain system backup for multiple VMs.
- You can perform only one Instant Access restore at a time. Ensure that you `vMotion` the VM to a different datastore and that you unmount the datastore before performing another instant access restore for the Data Domain system.
- You cannot recover multiple save sets concurrently using Instant Access restore.

Procedure

1. In the **EMC Backup and Recovery** user interface, select the **Restore** tab.

   EMC Backup and Recovery displays the virtual machines that are available to restore.

2. Click a virtual machine to expand the list of available backups, from which to restore.

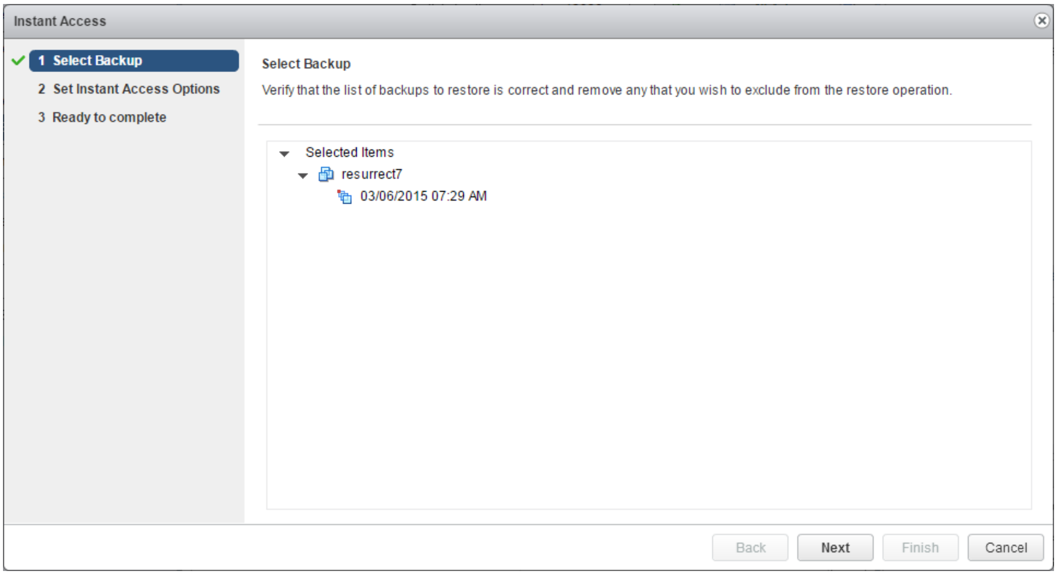
   Note

   You cannot browse and select backup data at the disk level.

3. Select the backup that you want to restore, and click **Instant Access**.

   The **Instant Access** wizard opens to the **Select Backup** page.

   Figure 145 Select a backup



Instant Access

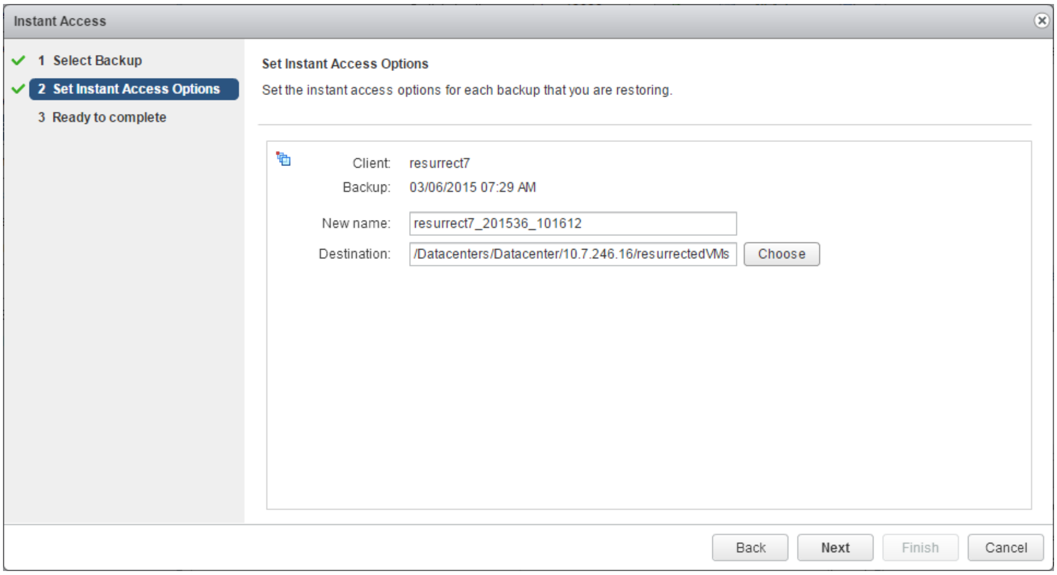
Select Backup

Verify that the list of backups to restore is correct and remove any that you wish to exclude from the restore operation.

4. Verify that the list of backups is correct, remove any backups that you want to exclude from the restore, and click **Next**.

   The **Set Instant Access Options** page displays.

Figure 146 Set instant access options



Set Instant Access Options

Set the instant access options for each backup that you are restoring.

Client: resurrect7

Backup: 03/06/2015 07:29 AM

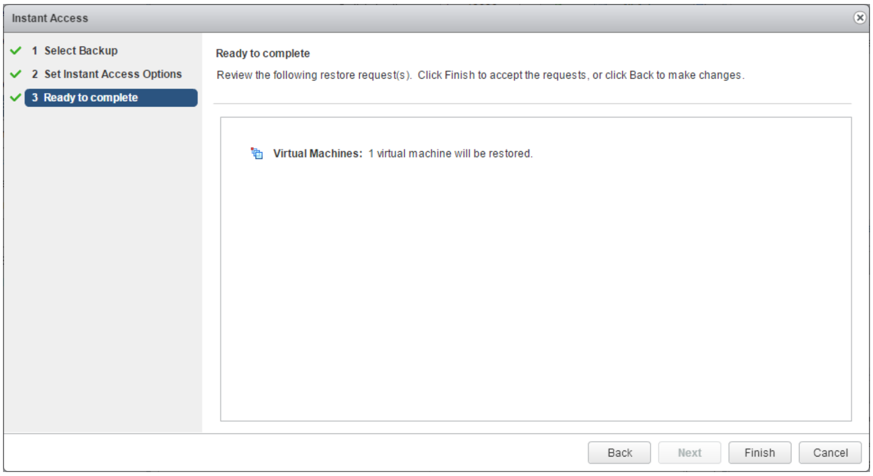
New name: resurrect7_201536_101612

Destination: /Datacenters/Datacenter/10.7.246.16/resurrectedVMs

5. Specify a new name and destination for the restore, and click **Next**.

   The **Ready to complete** page displays.

Figure 147 Ready to complete



Ready to complete

Review the following restore request(s). Click Finish to accept the requests, or click Back to make changes.

Virtual Machines: 1 virtual machine will be restored.

6. Review the restore request, and click **Finish**.

   You should see a message that indicates that the instant access operation was successfully completed.

Restore from last backup

The vSphere Web Client also provides an option to perform a VMware Backup Appliance restore from the last successful backup. This option is available when you right-click the VM and select **All EBR actions** > **Restore from last backup**.

Note

Before you use this option, make sure that you establish a connection to the VMware Backup Appliance by selecting the EMC Backup and Recovery user interface in the vSphere Web Client.

Direct to host recovery

You can recover image-level backups directly to an ESX host without requiring a vCenter server by using the **Emergency Restore** tab **EMC Backup and Recovery Configure** window. Direct to host recovery is available only for VMs that you back up to a VMware Backup appliance.

Before performing an emergency restore, ensure that you meet the following requirements:

- The VM you want to restore must have a VMware Hardware version that is supported by the ESX host running the VMware Backup Appliance (VMware Hardware version 7 or later).
- A vSphere host that is currently managed by the vCenter Server must be temporarily disassociated from the vCenter Server to perform the emergency restore. To disassociate the vCenter Server, use the vSphere Client (not the vSphere Web Client) connected directly to the vSphere host.
- You must have adequate free space in the target datastore to accommodate the entire VM. The target VMFS datastore to which the VM is being restored must support the VMDK file size.
- Network connectivity must be available for the restored VMs from the ESX host running the VMware Backup Appliance.
- You must have at least one local account with administrator privileges on the ESX host running the VMware Backup Appliance.

Note

You can only perform an emergency restore from a primary backup; you cannot use a cloned backup.

Procedure

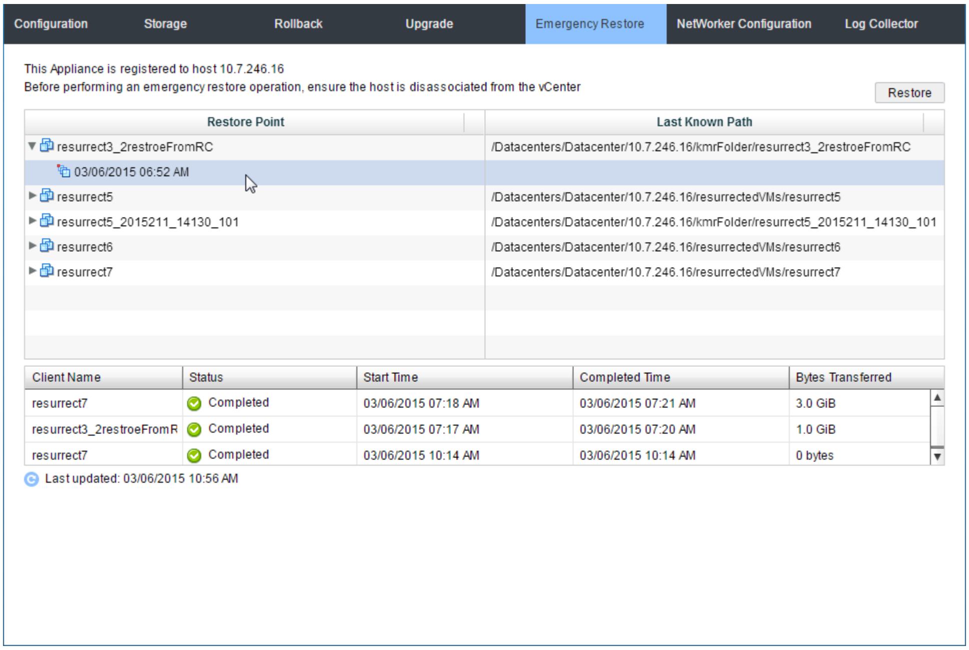
1. Log in to the **EMC Backup and Recovery Configure** window at the following URL using the EMC Backup and Recovery username and password credentials that you defined during configuration:

   `http://`*`VMware_Backup_appliance_IP`*`:8580/ebr-configure`

2. Select the **Emergency Restore** tab.
3. Click **Refresh** to view the most recent available VM backups.
4. Click the arrow beside a restore point to display its backups.
5. Select the backup that you want to restore, and then click **Restore**.

   The following figure provides an example of the **Emergency Restore** window.

Figure 148 Emergency Restore window



This Appliance is registered to host 10.7.246.16
Before performing an emergency restore operation, ensure the host is disassociated from the vCenter

Restore Point	Last Known Path
▼ resurrect3_2restroeFromRC	/Datacenters/Datacenter/10.7.246.16/kmrFolder/resurrect3_2restroeFromRC
03/06/2015 06:52 AM	
▶ resurrect5	/Datacenters/Datacenter/10.7.246.16/resurrectedVMs/resurrect5
▶ resurrect5_2015211_14130_101	/Datacenters/Datacenter/10.7.246.16/kmrFolder/resurrect5_2015211_14130_101
▶ resurrect6	/Datacenters/Datacenter/10.7.246.16/resurrectedVMs/resurrect6
▶ resurrect7	/Datacenters/Datacenter/10.7.246.16/resurrectedVMs/resurrect7

Client Name	Status	Start Time	Completed Time	Bytes Transferred
resurrect7	✓ Completed	03/06/2015 07:18 AM	03/06/2015 07:21 AM	3.0 GiB
resurrect3_2restroeFromR	✓ Completed	03/06/2015 07:17 AM	03/06/2015 07:20 AM	1.0 GiB
resurrect7	✓ Completed	03/06/2015 10:14 AM	03/06/2015 10:14 AM	0 bytes

Last updated: 03/06/2015 10:56 AM

File-level restore

Where FULLVM restore allows you to restore backups in their entirety using the **EMC Backup and Recovery** user interface in the **vSphere Web Client**, file-level restore (FLR) allows you to restore specific files and folders from virtual machines by using the **EMC Data Protection Restore Client**, or from a command prompt by using the `nsrvbaflr` command, which is part of the base NetWorker client install.

The following text is an example of how to use the `nsrvbaflr` command:

```
nsrvbaflr --vba 10.7.77.200 --adminuser administrator@vsphere.local --
adminpass pw123 --sourceclient /10.7.84.219/VirtualMachines/jinTest4
--targetclient /10.7.77.227/VirtualMachines/lava12204-win --targetpath
C: --targetuser Administrator --targetpass pw456 --recover [Disk#1]
```

Note

If you plan to use the `nsrvbaflr` command, you must copy the `nsrvbaflr` java script (nsrvbaflr.exe on Windows) to the virtual machine you want to restore from. The *NetWorker Command Reference Guide* provides information about how to use the `nsrvbaflr` command.

The **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 Restore Client operates in one of two modes:

- User—A local user account with administrative privileges that can restore folders or files to the original virtual. The section Restoring specific folders or files to the original virtual machine (User mode) provides more information.
- Admin—A vCenter administrator account that can restore folders or files from a different VM to any available destination client. The section Restoring specific folders or files from a different virtual machine (Admin mode) provides more information.

Note

Before you start a file-level restore, review the limitations specified in the section FLR limitations to ensure that you can perform FLR in your configuration.

File-level restore limitations

This section provides a list of limitations that apply to file-level restore.

Note

Before performing a file-level restore, make sure that your browser is updated to the latest version.

- In a large environment where many virtual machines appear in the **EMC Data Protection Restore Client**, the navigation buttons (**Back**, **Next**, **Finish**) may appear very small, requiring you to zoom in to see the options. If this occurs, it is recommended that you use the latest versions of the Chrome or Firefox browsers to avoid the issue.
- 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.
- You must install VMware Tools to use file-level restore. 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 the file-level restore operation.
- You can perform file-level restore across vCenter servers as long as the vCenter servers 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 does not support the following virtual disk configurations:
  - Dynamic disks
  - Unformatted disks
  - FAT16 file systems
  - FAT32 file systems
  - Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)
  - Two or more virtual disks mapped to single partition
  - Encrypted partitions
  - Compressed partitions
  - Btrfs
  - XFS
- File-level restore does not restore or browse symbolic links.
- When you create partitions, fill the lower ordered indices first. For example, you cannot create a single partition and place it in the partition index 2, 3, or 4. You must place the single partition in partition index 1.
- File-level restore of Windows 8 and Windows Server 2012 virtual machines is not supported on the following file systems:
  - Windows Dynamic Disks

  - Deduplicated NTFS
  - Resilient File System (ReFS)
  - EFI bootloader
- File-level restore of ext4 file systems is supported only with external proxies. To perform FLR of ext4 file systems, you must disable the internal proxies from the **NSR VBA Server Properties** window in NMC. VMware Backup Appliance monitoring and properties on page 251 provides more information.
- File-level restore does not support a direct restore from a cloned backup. To recover individual files from a clone, you must first perform an image-level recovery of the clone. This creates a primary copy on the VMware Backup appliance, from which you can then perform file-level restore.
- File-level restore does not restore ACLs.
- File-level restore cannot restore more than 5,000 folders or files in the same restore operation.
- File-level restore cannot browse more than 14,498 folders or files in the same restore operation.

Restoring specific folders or files to the original virtual machine in User mode

Select the User tab in the **EMC Data Protection Restore Client** login page to restore specific folders and files to the original virtual machine on Windows and Linux virtual machines. In this mode, you connect to the Restore Client from a virtual machine that has been backed up by NetWorker VMware Protection.

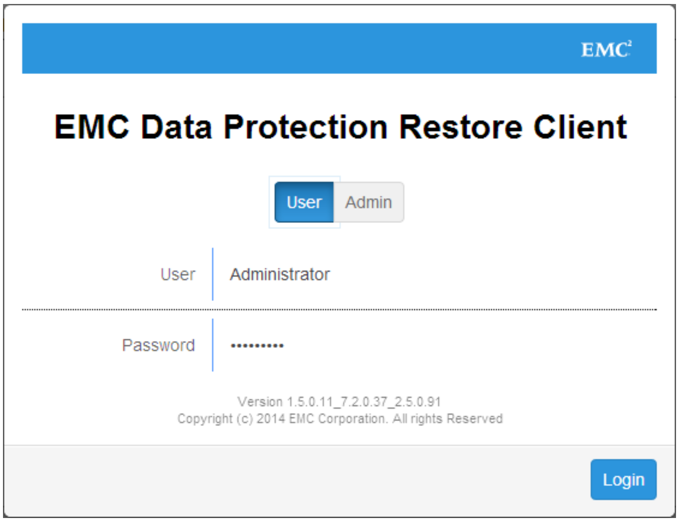
Procedure

1. Connect to the host that will receive the file-level restore with a user that is a member of the administrations group.
2. Open a browser and enter a URL that points to the VMware Backup Appliance and indicates file-level restore. For example:

   ```
   http://VMware_Backup_Appliance_host:8580/flr
   ```

   The following figure provides an example of the user login window.

   Figure 149 EMC Data Protection Restore Client User Login



EMC Data Protection Restore Client

User Administrator

Password ••••••••••

Version 1.5.0.11_7.2.0.37_2.5.0.91
Copyright (c) 2014 EMC Corporation. All rights Reserved

Note

You must connect to the VMware Backup Appliance from a web browser on the virtual machine that the files will be restored to.

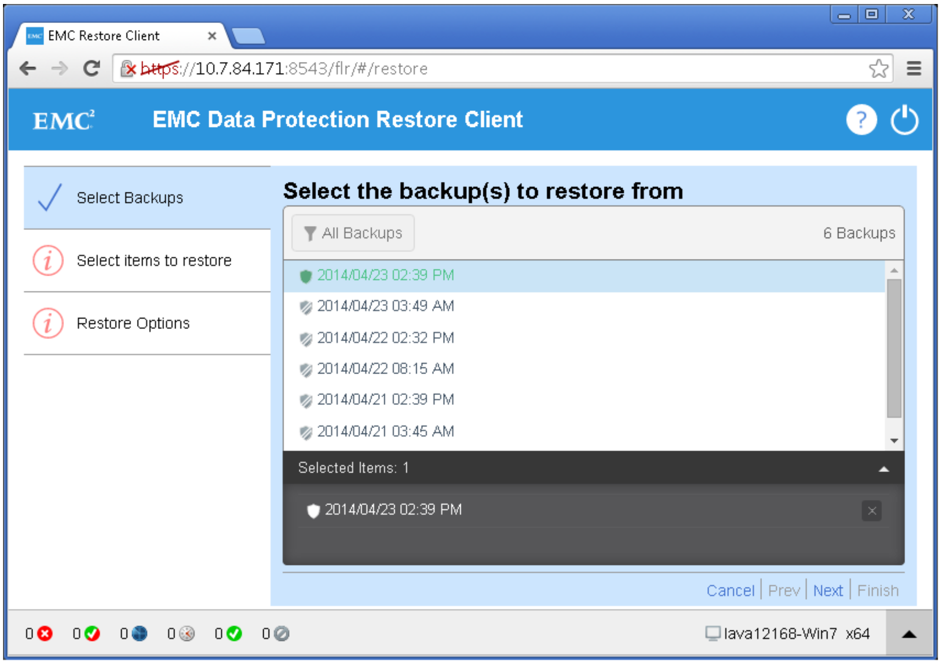
3. Select the **User** tab, and then log in to the Restore Client with the local administrative credentials of the virtual machine to which you are logged in.

   When you log in, the **Select the backup(s) to restore from** page displays with a list of backups for the local virtual machine.

4. Use the drop-down list to view the available backups. You can view all backups, or only backups on a specific date or within a specific range. Highlight a backup and double-click or drag and drop to move the backup to the **Select Items** pane. Click **Next**.

   The following figure provides an example of the **Select the backups to restore from** page.

   Figure 150 Select the backups to restore from page

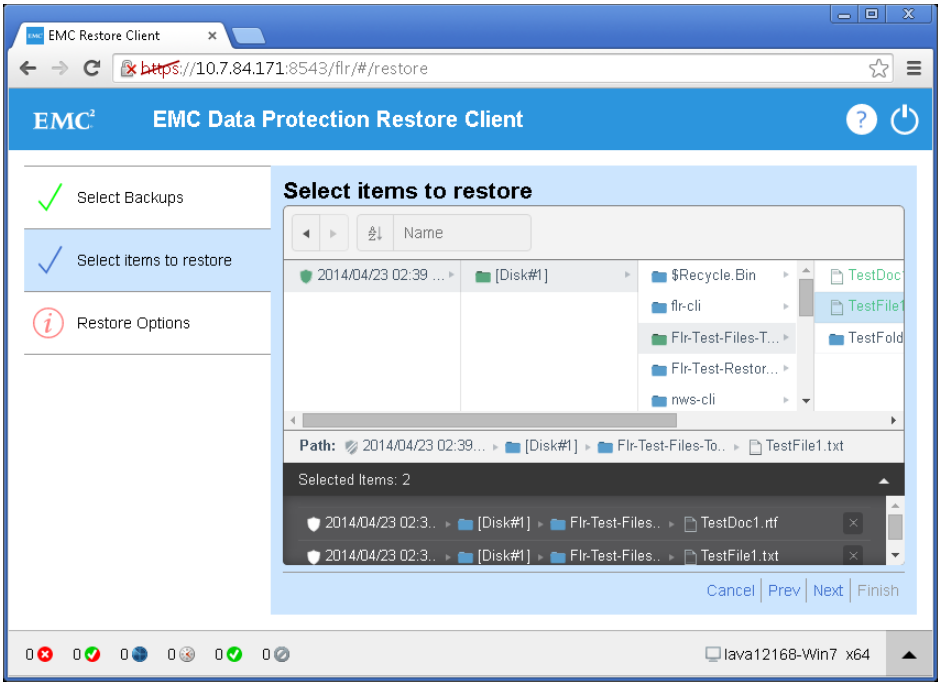


Note

When you click **Next**, if a folder hierarchy does not appear, the file system in use on the virtual machine may not support file-level restore. The section File-level restore limitations on page 283 provides more information.

5. On the **Select items to restore** page, browse and select the files and folders available for recovery. You can sort items by Name, Date, and so on. Items marked for restore appear in the **Selected Items** pane. To mark an item for recovery, double-click the item, or drag and drop the item into the **Selected Items** pane.

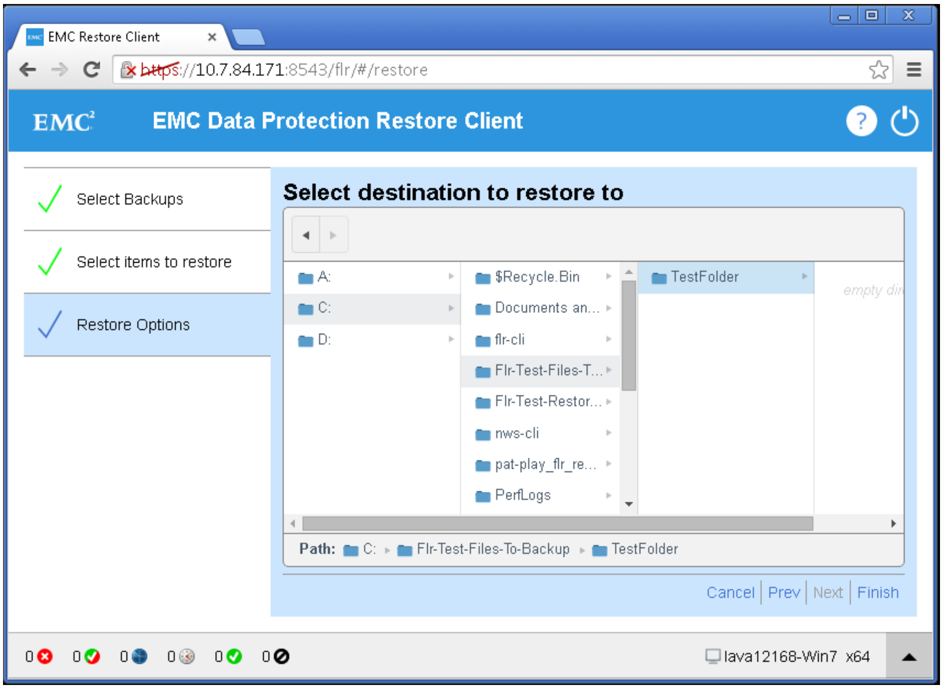
Figure 151 Select items to restore page



6. On the **Select destination to restore to** page, select the folder to which you want to restore the items, and then click **Finish**.

   The following figure provides an example of the **Select destination to restore to** page.

Figure 152 Select destination to restore to page



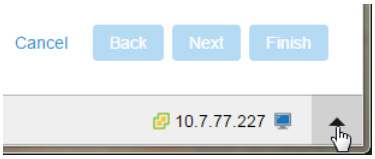
7. Click **Yes** when you are prompted to continue the restore.

   The restore begins.

8. To monitor the progress of the restore operation, click the arrow button located at the lower right-hand corner of the restore client screen.

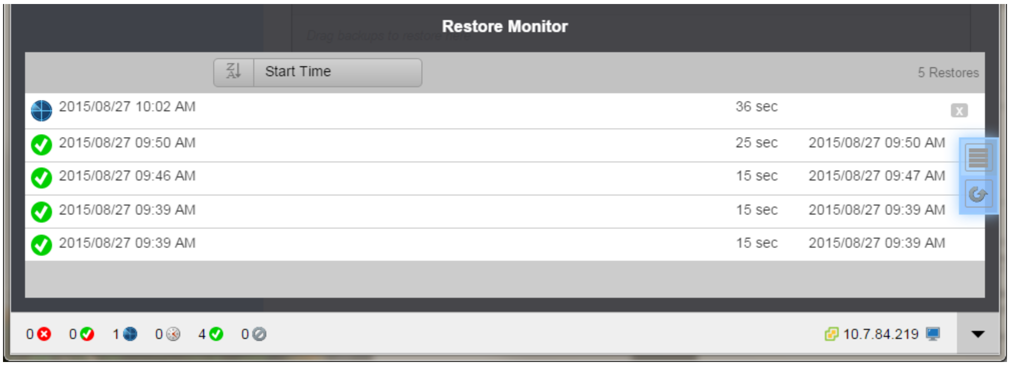
The following figure provides an example of the arrow button.

Figure 153 Accessing the restore monitor



When you select the arrow button, the **Restore Monitor** panel slides up. The following figure provides an example of the **Restore Monitor** panel.

Figure 154 Restore Monitor panel


Restore Monitor

	Start Time		5 Restores
●	2015/08/27 10:02 AM	36 sec	
✓	2015/08/27 09:50 AM	25 sec	2015/08/27 09:50 AM
✓	2015/08/27 09:46 AM	15 sec	2015/08/27 09:47 AM
✓	2015/08/27 09:39 AM	15 sec	2015/08/27 09:39 AM
✓	2015/08/27 09:39 AM	15 sec	2015/08/27 09:39 AM

Click the **Refresh** button on the right-hand side of the panel to refresh the contents as the restore occurs.

Restoring specific folders or files from a different virtual machine in Admin mode

To restore specific folders or files from a different virtual machine, use **Admin** mode in the **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 by using NetWorker VMware Protection. You can then restore items to the virtual machine on which you are currently logged in, or to any available destination virtual machine.

Procedure

1. Open a browser and specify the URL that points to the EMC Backup and Recovery appliance and indicates file-level restore (FLR), as in the following example:

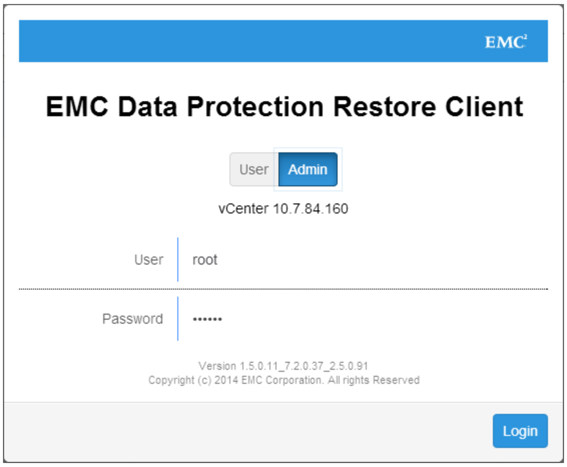
   ```
   http://VMware_Backup_Appliance_host:8580/flr
   ```

   Ensure that you launch the **EMC Data Protection Restore Client** from a virtual machine that you backed up using the NetWorker VMware Protection solution.

2. Click **Admin**, and then log in to the Restore Client with the vCenter administrative credentials that you used to register the VMware Backup appliance to the vCenter Server.

   The following figure provides an example of the Admin login window.

Figure 155 EMC Data Protection Restore Client Admin Login



EMC Data Protection Restore Client

User Admin

vCenter 10.7.84.160

User root

Password ••••••

Version 1.5.0.11_7.2.0.37_2.5.0.91
Copyright (c) 2014 EMC Corporation. All rights Reserved

Note

When you use **Admin** mode, ensure that the user you specify for the vCenter login has the correct privileges to use this option.

When you log in, the **Select the backup(s) to restore from** page appears with a list of all the virtual machines that were backed up by using NetWorker VMware Protection. The available backups appear under each virtual machine.

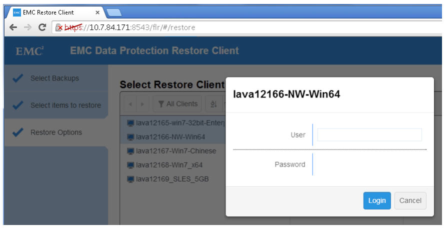
3. Use the drop-down list to view the available backups. You can view all backups, or only backups on a specific date or within a specific range. Highlight a backup and double-click or drag and drop to move the backup to the **Select Items** pane. Click **Next**.

4. On the **Select items to restore** page, browse and select the files and folders available for restore. You can sort items by Name, Date, and so on. Items marked for restore appear in the **Selected Items** pane. To mark an item for recovery, double-click the item, or drag and drop the item into the **Selected Items** pane.

5. In the **Select Restore Client** page, select a destination virtual machine.

   A login dialog box similar to the following figure appears for the destination client.

Figure 156 Select and log in to the destination client



https://10.7.84.171:8543/flr/#/restore

EMC Data Protection Restore Client

Select Restore Client

lava12165-win7-32bit-Enter
lava12166-NW-Win64
lava12167-Win7-Chinese
lava12168-Win7_x64
lava12169_SLES_5GB

lava12166-NW-Win64

User

Password

6. Log in to the client.

7. Select the destination location where you want to restore the file.

8. Click **Finish**.

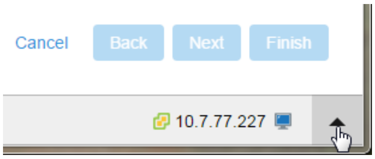
9. Click **Yes** when you are prompted to continue with the restore.

   The restore begins.

10. To monitor the progress of the restore operation, click the arrow button located at the lower right-hand corner of the restore client screen.

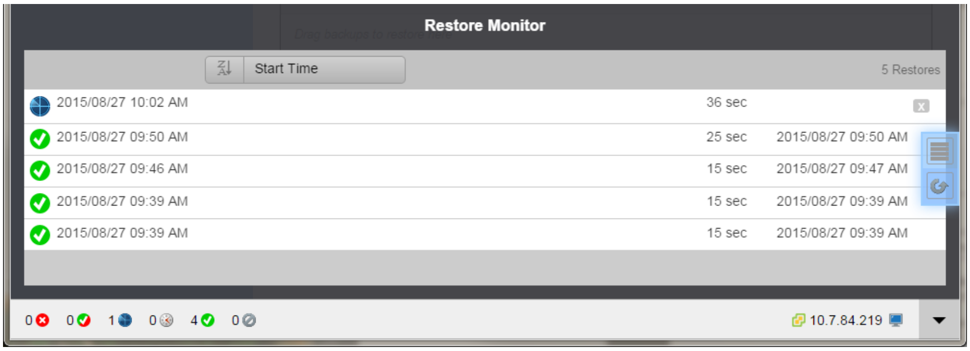
    The following figure provides an example of the arrow button.

    Figure 157 Accessing the restore monitor

    When you select the arrow button, the **Restore Monitor** panel slides up. The following figure provides an example of the **Restore Monitor** panel.

    Figure 158 Restore Monitor panel

    Restore Monitor

Start Time			5 Restores
2015/08/27 10:02 AM	36 sec		
✓ 2015/08/27 09:50 AM	25 sec	2015/08/27 09:50 AM	
✓ 2015/08/27 09:46 AM	15 sec	2015/08/27 09:47 AM	
✓ 2015/08/27 09:39 AM	15 sec	2015/08/27 09:39 AM	
✓ 2015/08/27 09:39 AM	15 sec	2015/08/27 09:39 AM	

    Click the **Refresh** button on the right-hand side of the panel to refresh the contents as the restore occurs.

Monitoring EMC Backup and Recovery activity

You can monitor backup and recovery activities from the **EMC Backup and Recovery** user interface in the **vSphere Web Client**, with the **EMC Data Protection Restore Client** and from the command line.

Most EMC Backup and Recovery tasks, events, and alarms are prefaced by “EBR:” Note that some of the tasks and events that occur as part of EMC Backup and Recovery processes are performed by the vCenter Server and do not have this prefix.

For example, if EMC Backup and Recovery runs a scheduled backup job for a running virtual machine, the following task entries are created:

- Create a VM snapshot (vCenter acting on the VM to be backed up).
- EMC Backup and Recovery: Scheduled Backup Job (EMC Backup and Recovery starting the backup job).
- Reconfigure the VM (the VMware Backup appliance requesting services from vCenter).
- Remove snapshot (vCenter acting on the VM that has completed backing up).

To see only EMC Backup and Recovery-generated tasks or events in the **Tasks** or **Event** console, click **Event** in the left pane, and type `EMC Backup and Recovery:` in the **Filter** field.

Viewing Recent Tasks in the vSphere Web Client

The EMC Backup and Recovery user interface in the vSphere Web Client displays task entries in the **Recent Tasks** window when you perform the following operations:

- Backups
- Restores
- Integrity Checks

Click on a task entry in the **Recent Tasks** window to display task details in the pane at the bottom of the window. You can also display task details by clicking the link next to the VM icon on the **Running** tab in the **Recent Tasks** section.

To cancel tasks from the **Running tasks** pane, click the **Delete** icon.

Viewing Alarms

EMC Backup and Recovery can trigger the following alarms:

Table 29 EMC Backup and Recovery alarms

Alarm Name	Alarm Description
EBR: [001] The most recent checkpoint for the VMware Backup appliance is outdated.	From the **Configuration** tab of the EMC Backup and Recovery user interface, click the **All Actions** icon, and then select **Run integrity check**.
EBR: [002] The VMware Backup appliance is nearly full.	The VMware Backup Appliance is nearly out of disk space for additional backups. You can free disk space on the appliance by manually deleting unnecessary or older backups and by changing retention policies on backup jobs, to shorten the backup retention time.
EBR: [003] The VMware Backup appliance is full.	The VMware Backup Appliance does not have any disk space for additional backups. The appliance will run in read-only (or restore-only) mode until you make additional space available. You can free space on the appliance by manually deleting unnecessary or older backups and by changing retention policies on backup jobs to shorten the backup retention time.
EBR: [004] The VMware Backup appliance datastore is approaching maximum capacity.	The datastore that contains the disks provisioned for the VMware Backup Appliance is approaching maximum capacity. When datastore reaches the maximum capacity, the VMware Backup Appliance will be suspended. The appliance cannot be resumed until additional space is made available on the datastore.
EBR: [005] Core services are not running.	The Core services are not running. Start the Core services by using the EMC Backup and Recovery **Configure** window.

Table 29 EMC Backup and Recovery alarms (continued)

Alarm Name	Alarm Description
EBR: [006] Management services are not running.	The Management services are not running. Start Management services by using the EMC Backup and Recovery **Configure** window.
EBR: [007] File system services are not running. **Note** This alarm does not apply to EBR version 1.5.1.7.	The File system services are not started. Start the File system services by using the EMC Backup and Recovery **Configure** window.
EBR: [008] File level restore services are not running. **Note** This alarm does not apply to EBR version 1.5.1.7.	The File level restore services are not started. Start the File level restore services by using the EMC Backup and Recovery **Configure** window.
EBR: [009] Maintenance services are not running.	The Maintenance services are not running. Start Maintenance services by using the EMC Backup and Recovery **Configure** window.
EBR: [010] Backup scheduler is not running.	The Backup scheduler is not running. Start Backup scheduler by using the EMC Backup and Recovery **Configure** window.

Viewing the Event Console

EMC Backup and Recovery can generate info, error, and warning events. For example:

- Info— “EMC Backup and Recovery: Critical VMs Backup Job created.”
- Warning— “EMC Backup and Recovery: Unable to add Host123 client to backup job Critical VMs because . . .”
- Error— “EMC Backup and Recovery: Appliance has changed from Full Access to Read Only.”

EMC Backup and Recovery generates events on all state changes in the appliance. As a general rule, state changes that degrade the capabilities of the appliance are labeled errors, and state changes that improve the capabilities are labeled informational. For example, when starting an integrity check, EMC Backup and Recovery generates an event that is labeled an error because the appliance is set to read-only before performing the integrity check. After the integrity check, EMC Backup and Recovery generates an informational event because the appliance changes from read-only to full access.

Select an event entry to display the details of that event, which includes a link to Show related events.

Shutdown and Startup Procedures

If you need to shut down the VMware Backup Appliance, use the Shut Down Guest OS action. This action automatically performs a clean shutdown of the appliance. If you power off the appliance without using the **Shut Down Guest OS** action, corruption might occur. It can take up to 30 minutes to shut down and restart the VMware Backup Appliance. You can monitor the status through the EMC Backup and Recovery Console in the vSphere Client. After vSphere shuts down the appliance, use the **Power On** action to restart the appliance.

If the appliance does not shutdown properly, then a rollback to the last validated checkpoint action occurs during the restart. This means that any changes to backup policies or backups that occur between the checkpoint and the unexpected shutdown will be lost. This is expected behavior and is used to ensure system corruption does not occur from unexpected shutdowns.

The VMware Backup Appliance is designed to run 24x7, to support maintenance operations and to provide the ability to perform restore operations. EMC does not recommend that you shutdown the appliance, unless there is a specific reason for the shutdown.

EMC Backup and Recovery Capacity Management

This section focuses on EMC Backup and Recovery capacity management and includes the following topics:

- Impact of selecting thin or thick provisioned disks on page 292
- Save set lifecycle on page 293

Impact of selecting thin or thick provisioned disks

This section describes the advantages and disadvantages of selecting a thin or thick disk partitioning for the EMC Backup and Recovery datastore.

Thin provisioning uses virtualization technology to allow the appearance of more disk resources than what might be physically available. Use thin provisioning when an administrator actively monitors disk space and can allocate additional physical disk space as the thin disk grows. If you do not monitor and manage disk space and the EMC Backup and Recovery datastore is on a thin provisioned disk that cannot allocate space, the VMware Backup appliance fails. When this occurs, you can rollback to a validated checkpoint. Any backups and configuration changes that occurred after the checkpoint will be lost.

Thick provisioning allocates all of the required storage when the disk is created. The best practice for the EMC Backup and Recovery datastore is to create a thin provisioned disk when the EMC Backup and Recovery appliance is deployed (this allows for rapid deployment), and then convert the disk from thin provisioning to thick provisioning after deployment.

Note

See the VMware documentation for details on inflating thin provisioned disks to thick provisioned disks. This procedure requires that you shut down the VMware Backup appliance. This may take several hours to complete.

Save set lifecycle

The NetWorker server exclusively manages the lifecycle of save sets created by VMware Backup Appliance nodes.

Deletion and expiration of save sets and metadata

The following sections describe how to delete and expire save sets and metadata on the NetWorker server.

Expiring save sets from NetWorker

NetWorker manages the retention period for the VMware Backup Appliance backups. When a save set for the appliance expires in NetWorker, NetWorker deletes the corresponding backup data from the storage on the appliance.

Manual deletion of save sets from NetWorker

Use the `nsrmm` command to delete EMC Backup and Recovery Appliance backups from the media database on the NetWorker server.

For example:

```
nsrmm -d -S ssid/cloneid
```

where *ssid/cloneid* is the SSID and cloneID of the save set that you want to delete.

When you delete a save set from NetWorker server, NetWorker will also remove the corresponding backup from the EMC Backup and Recovery Appliance.

Data Domain backup

If a Data Domain backup has multiple clones, then deleting the primary clone only deletes the copy on the EMC Backup and Recovery appliance.

Deleting a Data Domain volume
You can delete a user-defined Data Domain device volume that contains VMware Backup Appliance backups after you unmount the devices. If NetWorker cannot delete the backups from the VMware Backup appliance, then the volume deletion operation fails.

Relabeling a Data Domain volume
You can relabel a user-defined Data Domain volume that the VMware Backup Appliance uses in the same method as any other volume. The relabel operation deletes all the VMware Backup Appliance backups that belong to the volume associated with the device from both NetWorker and the VMware Backup Appliance server. If NetWorker cannot delete the backups from the VMware Backup Appliance, then the device relabel operation fails.

Checkpoints and VMware Backup Appliance rollback

The maintenance services for EMC Backup and Recovery start between 24 to 48 hours after booting up, and maintenance services are responsible for creating checkpoints. A checkpoint is initiated within the vSphere Web Client and captures a point in time snapshot of the VMware Backup Appliance for disaster recovery purposes. In the event that you need to recover the VMware Backup Appliance, a rollback setting within the EMC Backup and Recovery **Configure** window allows the VMware administrator to automatically roll back to the last validated checkpoint.

By default, checkpoints are automatically scheduled during the maintenance window. In addition to the twice daily checkpoints, you can also create and validate additional EMC Backup and Recovery server checkpoints at any time.

Checkpoint validation might take several hours, depending on the amount of data in the NetWorker server. You can configure each validation operation individually to perform all checks (full validation) or perform a partial “rolling” check, which fully validates all new and modified stripes, then partially checks a subset of unmodified stripes. You can also delete checkpoints to reclaim server storage capacity.

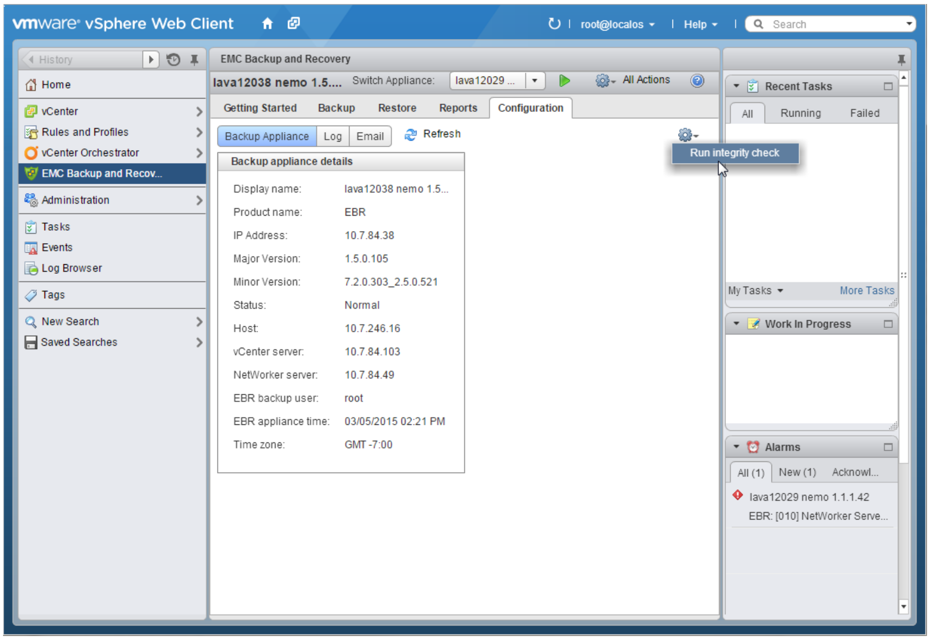
Creating a checkpoint using the EMC Backup and Recovery user interface

You can create a validated checkpoint by using the command line or the EMC Backup and Recovery user interface in the vSphere Web Client. The section Preparing the VMware Backup appliance for disaster recovery on page 298 provides information on creating and validating checkpoints from the command line.

Procedure

1. In the EMC Backup and Recovery user interface, select the **Configuration** tab.
2. Click the gear icon, and then select **Run integrity Check** as shown in the following figure.

Figure 159 Running an integrity check



Backup appliance details

Display name:	lava12038 nemo 1.5...
Product name:	EBR
IP Address:	10.7.84.38
Major Version:	1.5.0.105
Minor Version:	7.2.0.303_2.5.0.521
Status:	Normal
Host:	10.7.246.16
vCenter server:	10.7.84.103
NetWorker server:	10.7.84.49
EBR backup user:	root
EBR appliance time:	03/05/2015 02:21 PM
Time zone:	GMT -7:00

Rolling back to a checkpoint

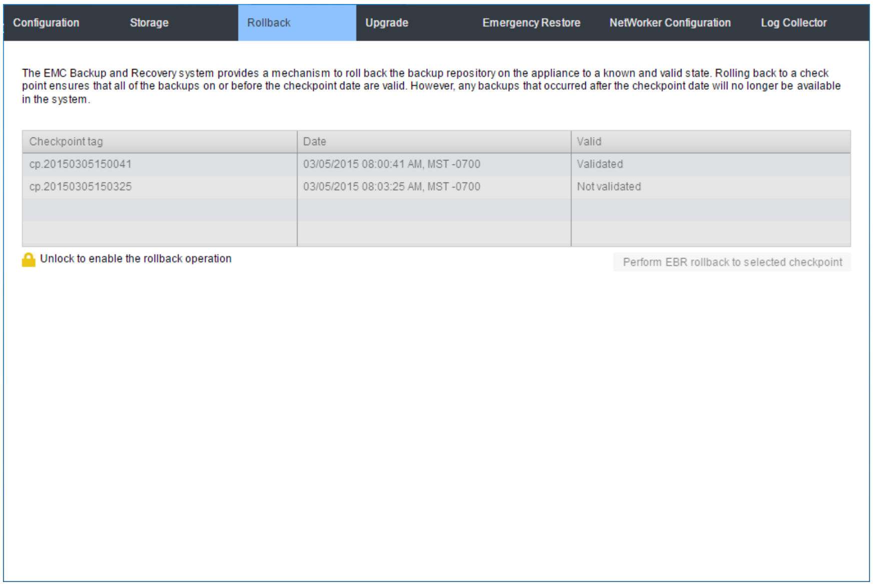
Rollback is a setting in the EMC Backup and Recovery **Configure** window that allows you to automatically roll back to the last validated checkpoint when performing a disaster recovery.

Procedure

1. Log in to the appliance at `http://`***`VMware Backup appliance FQDN`***`:8580/ebr-configure`.
2. Select the **Rollback** tab.

   The following figure provides an example of the **Rollback** tab.

Figure 160 Roll back to checkpoint



The EMC Backup and Recovery system provides a mechanism to roll back the backup repository on the appliance to a known and valid state. Rolling back to a check point ensures that all of the backups on or before the checkpoint date are valid. However, any backups that occurred after the checkpoint date will no longer be available in the system.

Checkpoint tag	Date	Valid
cp.20150305150041	03/05/2015 08:00:41 AM, MST -0700	Validated
cp.20150305150325	03/05/2015 08:03:25 AM, MST -0700	Not validated

Unlock to enable the rollback operation
Perform EBR rollback to selected checkpoint

Note

NetWorker does not support disaster recovery from a checkpoint backup that was performed with a VMware Backup Appliance version earlier than the currently installed version. For example, if you upgrade to a NetWorker 18.1 server and VMware Backup Appliance version 1.5.1.7 from NetWorker 8.2 SP1 and VMware Backup Appliance version 1.1.1.50, you cannot perform a disaster recovery from a checkpoint backup created with OVA 1.1.1.50. Backup and restore operations will hang in "Waiting: Queued" state.

3. Click **Unlock to enable the rollback operation**.
4. When prompted, type the appliance password, and then click **OK**.
5. Select a validated checkpoint, and then click **Perform EBR rollback to selected checkpoint**.
6. On the **EBR Rollback window**, click **OK**.

Protecting checkpoints for the VMware Backup appliance

To protect the appliance with checkpoints, add the VBA checkpoint discover and VBA checkpoint backup actions to a data protection policy.

You should run backups once or twice daily that occur a couple hours after checkpoint creation, to secure the checkpoint files on the NetWorker media. Preparing the VMware Backup appliance for disaster recovery on page 298 provides a list of checkpoint locations.

Cross Sync

A cross sync operation synchronizes the VMware Backup Appliance and NetWorker databases for backups and configurations. A VMware Backup Appliance rollback automatically starts a cross sync operation on the NetWorker server. You can also perform a cross sync manually from the command line to check the consistency of the

NetWorker metadata. Before you perform a cross sync, ensure that the VMware Backup Appliance is online.

Use the following command to manually perform cross sync from the command line of the NetWorker server:

```
nsrim -X -S -h EMC_Backup_and_Recovery_appliance_hostname -t last
checkpoint time -f
```

where:

- `-S` initiates the VMware Backup appliance cross sync.
- `-h` specifies the VMware Backup appliance server name.
- `-t` is an optional parameter that specifies the last checkpoint time. EMC Backup and Recovery performs a cross sync for the backups that occur only after the specified time. Specify the time in a format that NetWorker accepts. The `nsr_getdate` man page provides information on acceptable formats.
- `-f` synchronizes the entire database and deletes out of sync backups. If the backups exist only on the VMware Backup appliance, then you can only delete the backups by using this option.
  To cross sync the entire database, specify `-f` without specifying the time.

If you do not specify a time when you perform a manual cross sync, NetWorker retrieves the most recent validated checkpoint from the VMware Backup appliance and performs a cross-sync starting from that time.

If you perform a cross sync on an entire database and the database is very large, the synchronization process may take longer than normal.

Cross sync generates the following NMC events:

- "`Cross sync with` *`appliance name`* `VMware Backup Appliance is started.`"
- "`Cross sync with` *`appliance name`* `VMware Backups Appliance is successful for configuration and backups.`"

Disaster Recovery

In the event of failure, as a first course of action, NetWorker VMware Protection will perform a rollback to a known validated checkpoint. To recover from a VMware Backup Appliance failure, refer to the following disaster recovery guidelines.

Disaster Recovery Guidelines

Review these guidelines before performing a disaster recovery:

- When you set the save set retention policy, ensure that the save sets in the media database are active and *not* expired and recycled.
- Ensure that the checkpoint backup that you plan to use was created with the same VMware Backup Appliance version as the version currently installed. NetWorker does not support disaster recovery from a checkpoint backup created using a previously installed VMware Backup Appliance version. For example, if you upgrade to a NetWorker 18.1 server and VMware Backup Appliance version 1.5.1.7 from NetWorker 8.2 and VMware Backup Appliance version 1.1.0.149, you cannot perform a disaster recovery from a checkpoint backup created with OVA 1.1.0.149. Backup and restore operations will hang in the "Waiting: Queued" state.

- Although the 0.5TB appliance contains 3 * 256 GB disks and the 4TB appliance contains 6 * 1TB disks, NetWorker only creates one checkpoint save set for all the disks. Ensure that you know which VMware Backup Appliance (0.5 or 4TB) that you deployed before you perform a disaster recovery. This information is not required when performing the checkpoint backup, but you will require this information during the re-deployment of the appliance. To help identify the deployed appliance and verify the checkpoint backup, you can review the log messages that appear in the `daemon.raw` file on the NetWorker server, and within the policy logs. The location of the logs files differ on a Windows and Linux NetWorker server.
  - Linux—By default the `daemon.raw` file appears in the `/nsr/logs` directory. The policy log files appear in the `/nsr/logs/policy` directory.
  - Windows—By default the `daemon.raw` file appears in the `C:\Program Files\EMC NetWorker\nsr\logs` folder. The policy log files appear in the `C:\Program Files\EMC NetWorker\nsr\logs\policy` folder.
- Before you shut down the VMware Backup Appliance, verify that there are not any backup or maintenance tasks running. Depending on the backup method used and how long it takes, schedule your checkpoint backup during a time when no tasks are scheduled. For example, if your backup window is eight hours and backups only take one hour to complete, you have an additional seven hours before maintenance tasks are scheduled. This is an ideal time to shut down and backup the appliance.
- To shutdown the appliance, use the vSphere Client to perform a **Shut Down Guest OS** task on the virtual machine. Do not use a **Power Off** task, which is the equivalent to unplugging the power cord on a physical server and may not result in a clean shut down process. Shutdown and Startup Procedures on page 292 provides more information.

Disaster recovery without checkpoint

Use the following procedure to perform a disaster recovery of the VMware Backup Appliance without using checkpoints.

Note

When you perform a disaster recovery for a VMware Backup Appliance without using checkpoints, you can only perform a FULL VM (image-level) restore. VMDK, FLR, and instant access restores are not supported in this case. You can, however, perform these types of restore after a resurrection restore.

Procedure

1. Deploy a new VMware Backup Appliance and specify the same IP address that was used at the time of the backup, from which you are recovering.

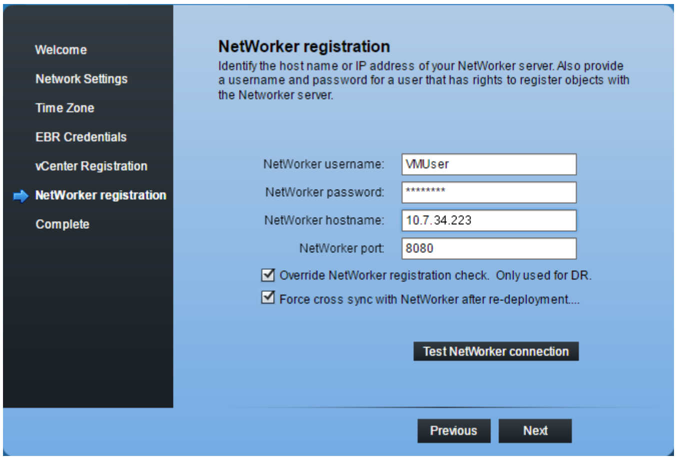
   EMC Backup and Recovery Configuration Utility on page 235 provides instructions.

2. Configure the new VMware Backup Appliance.

   During the **NetWorker Registration** step, select the **Override NetWorker registration check** and the **Force cross sync with NetWorker after re-deployment** options.

   The following figure provides an example of the **NetWorker Registration** page.

Figure 161 Networker registration during new appliance configuration



NetWorker registration

Identify the host name or IP address of your NetWorker server. Also provide a username and password for a user that has rights to register objects with the Networker server.

NetWorker username: VMUser

NetWorker password: ********

NetWorker hostname: 10.7.34.223

NetWorker port: 8080

☑ Override NetWorker registration check. Only used for DR.

☑ Force cross sync with NetWorker after re-deployment....

3. Click **Next**, and finish the configuration.

Results

Once the VMware Backup Appliance configuration completes, the following events appear in NMC:

```
Cross sync with appliance name VMware Backup Appliance is
started.
Cross sync with appliance name VMware Backups Appliance is
successful for configuration and backups.
```

You can then perform a resurrection restore of previous backups.

Preparing the VMware Backup appliance for disaster recovery

Perform the following steps to prepare for a disaster recovery of the VMware Backup appliance.

Note

When you use `ssh` to connect to or log in to the EMC Backup and Recovery console, ensure that you log in with admin account instead of the root account. Log in to the EMC Backup and Recovery Console as admin instead of root on page 312 provides more information.

Procedure

1. If you do not have a recent checkpoint or want to create a new checkpoint backup, create the checkpoint by running the following command:

   ```
   # mccli checkpoint create --override_maintenance_scheduler
   ```

2. Use the `mccli` command to verify that you have created a successful checkpoint by running:

   ```
   mccli checkpoint show
   ```

   An output similar to the following displays:

   ```
   Tag Time Validated Deletable
   ----------------- ----------------------- ---------
   ---------
   cp.20130206170045 2013-02-06 09:00:45 PST Validated Yes
   ```

3. Use the `mccli` command to validate the checkpoint:

   ```
   mccli checkpoint validate --cptag=cp.20130206170045 --
   override_maintenance_scheduler
   ```

   Validation takes some time to complete. Keep checking the status by running **`mccli checkpoint show`**.

4. Use the NetWorker Administration GUI to add two actions to a workflow for the VMware Protection Policy, in the following order:

   a. VMware checkpoint discover action.

   b. VMware checkpoint backup action.

   Note

   Checkpoint backup is a traditional NetWorker backup that you can perform to any NetWorker-supported pool. The pool can include Data Domain devices and AFTDs.

   Optionally, add a clone action after the checkpoint backup action to clone the checkpoint backup to a Data Domain system, AFTD, or tape.

5. Start or schedule the policy.

Performing a disaster recovery of the VMware Backup Appliance

Note

For any disaster recovery, you must repeat any changes previously made to the configuration files. For example, the changes performed in the section Restrict mapping of datastores on page 235.

Procedure

1. Redeploy the VMware Backup Appliance with the same network configuration that was used at the time of the checkpoint. Use the **Override** button within the **EMC Backup and Recovery Configure** window.

   Note

   Ensure that the password for the system that you plan to recover to matches the password that was defined for the system when the checkpoint was taken.

2. Re-register the proxies with the redeployed VMware Backup Appliance by running the following command from each external proxy, or reboot the external proxy:

   ```
   /usr/local/avamarclient/etc/initproxyappliance.sh start
   ```

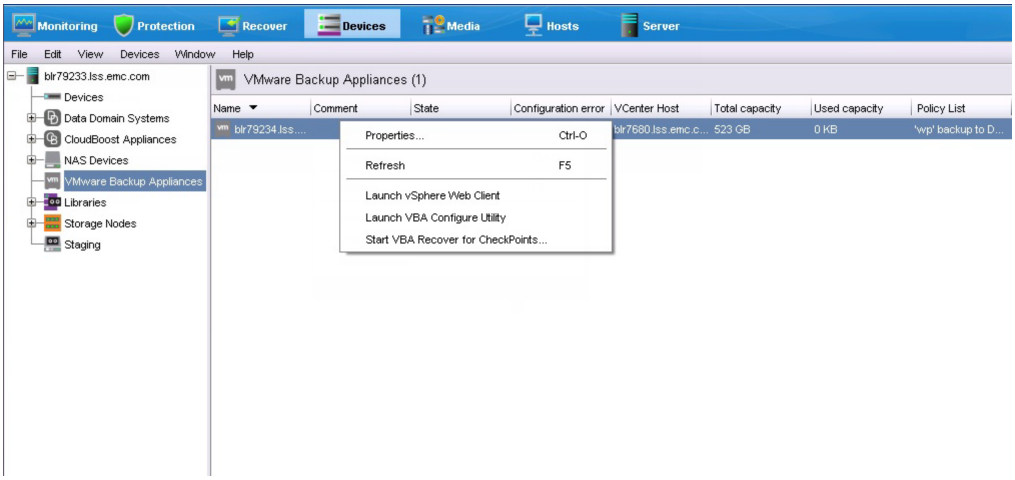
3. Use NMC to connect to the NetWorker server, and then select the **Devices** tab in **Administration** GUI.

4. In the left pane, select **VMware Backup Appliance**.

   The backup appliances display in the right pane.

5. In the right pane, right-click the VMware Backup Appliance that you want to recover, and then select **Start VBA Recover for Checkpoints**, as shown in the following figure.

Figure 162 Starting a VMware Backup Appliance disaster recovery



Name	Comment	State	Configuration error	VCenter Host	Total capacity	Used capacity	Policy List
blr79234.lss....				blr7680.lss.emc.c...	523 GB	0 KB	'wp' backup to D...

A list of checkpoint backups displays.

6. Select the checkpoint backup to which you want to roll back, and then click **OK**. After you click **OK**, the following events occur:
   - The status of the VMware Backup Appliance changes to **recover pending**, and the recovery takes 10-15 minutes to complete.
   - Upon successful recovery, the status of the VMware Backup Appliance changes to **query pending**.
   - After 10 minutes, Cross sync generates the following events in NMC:

     ```
     Cross sync with appliance name VMware Backup Appliance
     is started.
     Cross sync with appliance name VMware Backups Appliance
     is successful for configuration and backups.
     ```

   - The status of the VMware Backup Appliance changes to **Success**.
7. Check for restores of old backups and that the policies are intact as per the checkpoint.

Complete disaster recovery of the VMware Backup Appliance and the Data Domain or tape device

The following sections describe the steps that are required to a complete disaster recovery, where you need to restore both the connection to the VMware Backup Appliance, and the Data Domain or tape device that has completely failed.

Prerequisites for performing a complete disaster recovery

You can only run a complete disaster recovery after performing the following prerequisites:

- Create regular checkpoint backups of the VMware Backup Appliance, as described in the section Preparing the VMware Backup appliance for disaster recovery on page 298.
- Clone the backups to a secondary Data Domain or tape device.

Performing a complete disaster recovery

The following steps describe how to perform a complete disaster recovery of the VMware Backup Appliance.

Procedure

1. Redeploy the VMware Backup Appliance with the same network configuration that was used at the time of the checkpoint. Use the **Override** button within the **EMC Backup and Recovery Configure** window.

   Note

   Ensure that the password for the system that you plan to recover to matches the password that was defined for the system when the checkpoint was taken.

2. Re-register the proxies with the redeployed VMware Backup Appliance by running the following command from each external proxy, or reboot the external proxy:

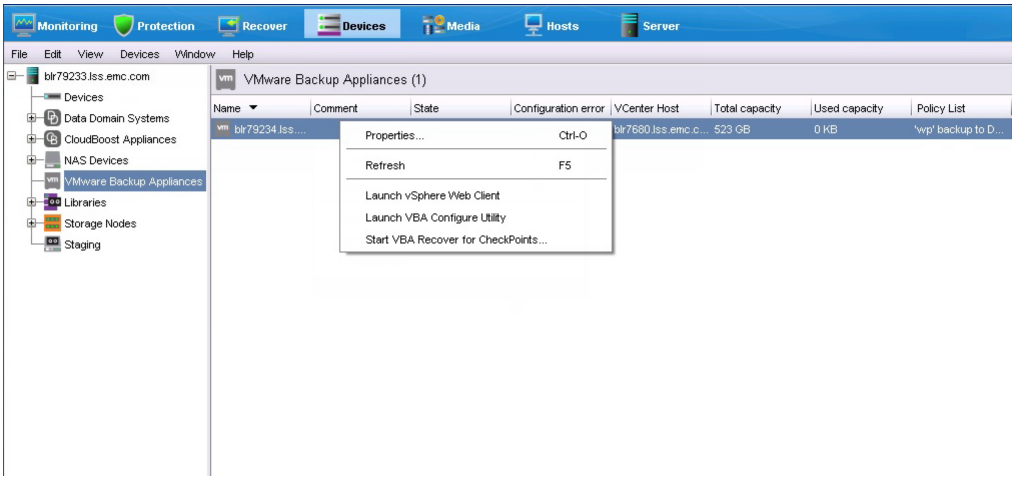
   ```
   /usr/local/avamarclient/etc/initproxyappliance.sh start
   ```

3. Use NMC to connect to the NetWorker server, and then select the **Devices** tab in **Administration** GUI.
4. In the left pane, select **VMware Backup Appliance**.

   The backup appliances display in the right pane.

5. In the right pane, right-click the VMware Backup Appliance that you want to recover, and then select **Start VBA Recover for Checkpoints**, as shown in the following figure.

   Figure 163 Starting a VMware Backup Appliance disaster recovery



Name	Comment	State	Configuration error	VCenter Host	Total capacity	Used capacity	Policy List
blr79234.lss....				blr7680.lss.emc.c...	523 GB	0 KB	'wp' backup to D...

   A list of checkpoint backups displays.

6. Select the checkpoint backup that you want to rollback to, and click **OK**.
7. Unmount the volumes pointing to the primary Data Domain device that has failed.

Results

After performing these steps, you can now replace the primary Data Domain device and either configure NetWorker Data Domain Boost devices the same way you set up the devices prior to the failure, or create new Data Domain Boost devices and adapt your VMware policy and pools accordingly.

Recovery from a secondary site

When you clone a VM or VMDK backup to a secondary site with its own vCenter and VMware Backup appliance, and the secondary site shares the same NetWorker server as the primary site, you can recover data from the secondary site. This procedure is particularly useful to recover data to a different vCenter when the primary site becomes unavailable, or when restoring backups on the same vCenter using a different VMware Backup Appliance.

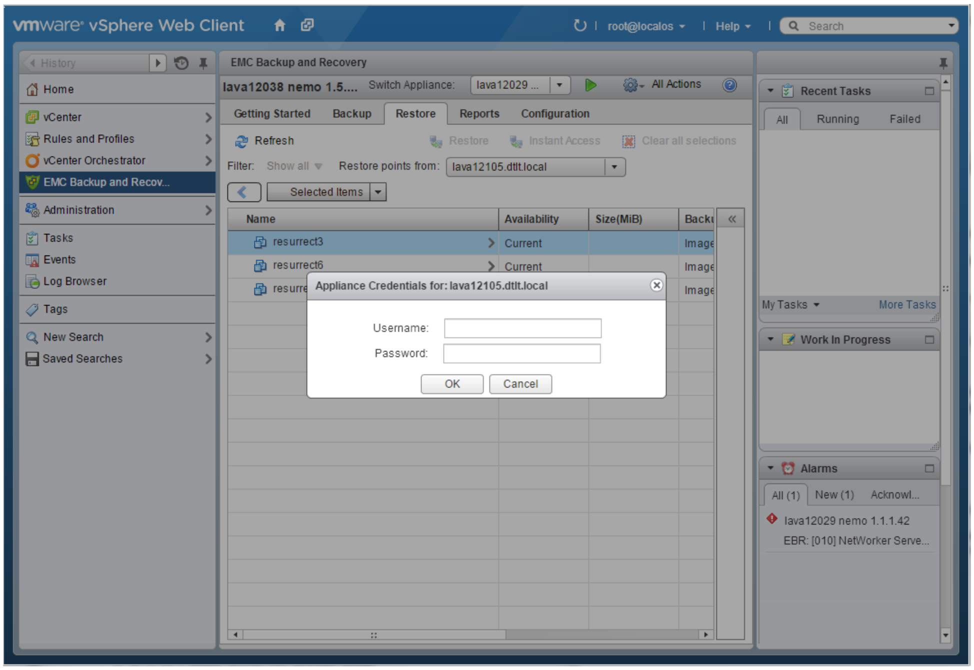
This feature allows you to perform restores for all backups using any available VMware Backup Appliance on any available vCenter as long as they are connected to the same NetWorker server where the backup was performed.

Procedure

1. Select the **Restore** tab in the EMC Backup and Recovery user interface in the vSphere Web Client.
2. From the **Restore points from** list, select the VMware Backup Appliance that contains the required backup(s).

   The **Appliance Credentials** dialog displays.

   Figure 164 Entering appliance credentials

3. Type the username and password for the VMware Backup Appliance, and click **OK**.
4. Browse restores from the VMware Backup Appliance and select the VMs/VMDKs that you want to restore to the new location. Performing a FULLVM restore on page 277 provides more information.

Best practices and troubleshooting

This section provides best practices and troubleshooting information for the NetWorker VMware Protection solution.

Performance and scalability

Performance and scalability of the NetWorker VMware Protection solution depends on several factors, including which VMware Backup Appliance you deploy, the number of vCenter servers and proxies, and whether you perform a large number of concurrent Virtual Machine backups. The following table provides these scalability factors.

Table 30 Scalability Factors

Component	Recommended count	Notes
VMs per VMware Backup appliance (Data Domain backup, no external proxy)	800-1000 VMs	Given an average size of 20-30 GB per Virtual Machine, the 0.5 TB OVA can accommodate a maximum of 800-1000 Virtual Machines, when you back up to a Data Domain device. One VMware Backup Appliance can run 8 sessions in parallel. Considering the Virtual Machine size and data change rate, a VMware Backup Appliance can complete a backup of 800-1000 Virtual Machines within 24 hours.
VMs per VMware Backup appliance (Data Domain backup + 5 external proxies, 48 concurrent sessions		VMware Backup Appliance + 5 external proxies can backup 1000 Virtual Machines in approximately 8 hours.
VMware Backup appliance per vCenter	3 or lower	Better performance is observed with a single vCenter processing 48 concurrent sessions. When you perform backups from multiple VMware Backup Appliances, EMC recommends that you stagger the backup to reduce the load on vCenter.
Proxies per vCenter	5	Each VMware Backup Appliance has one internal proxy that can handle 8 concurrent sessions, and the external proxy adds 8 more concurrent sessions.

Table 30 Scalability Factors (continued)

Component	Recommended count	Notes
		Therefore, use 1 VMware Backup Appliance and 5 external proxies. Note EMC recommends that you disable the internal proxy for the VMware Backup Appliance if you will back up more than 100 Virtual Machines.
VMs per policy	200 or lower	A single policy can scale up to 200 Virtual Machines. If more than 48 Virtual Machines per policy, the remaining Virtual Machines will be queued during backup.
VMs per restore	16	More than 16 Virtual Machines may result in NBD based restore due to VMware API limitations.
Files/directories per FLR	Maximum of 5000	FLR restore may be significantly impacted when there are more than 5000 files to be restored.

A VMware Backup Appliance can backup up to 8 Virtual Machines in parallel. If you want to run up to 48 Virtual Machines backups in parallel, then add up to 5 external proxies. Each external proxy can backup up to 8 Virtual Machines.

To achieve the best concurrent backup performance in a setup that requires additional vCenters, VMware Backup Appliances or proxies, EMC recommends using 1 VMware Backup Appliance + 5 External proxies per vCenter. The following tables provide information on expected performance for different setups.

Table 31 Maximum concurrent sessions per VMware Backup Appliance

Deployed per vCenter	Maximum concurrent sessions
1 VMware Backup Appliance	8
1 VMware Backup Appliance (internal proxy disabled) + 1 External Proxy	8
1 VMware Backup Appliance (internal proxy disabled) + 2 External proxies	16
1 VMware Backup Appliance (internal proxy disabled) + 3 External proxies	24
1 VMware Backup Appliance (internal proxy disabled) + 4 External proxies	32

Table 31 Maximum concurrent sessions per VMware Backup Appliance (continued)

Deployed per vCenter	Maximum concurrent sessions
1 VMware Backup Appliance (internal proxy disabled) + 5 External proxies	40
2 VMware Backup Appliance (internal proxy disabled) +1 External proxy	16

Backups from the VMware Backup Appliance and external proxy create sessions with NetWorker devices. The count of sessions is driven by the number of appliances, external proxies, clone jobs and other backups running through this server. Every VMware Backup Appliance and external proxy can run up to 8 sessions. If using external proxies, EMC recommends that you disable the internal proxy on the VMware Backup Appliance. The values calculated in the table above reflects a disabled internal storage.

Table 32 Concurrency/parallelism recommendations

Component	Concurrency count	Notes
vCenter	50 concurrent sessions	EMC recommends a maximum of 50 concurrent virtual machine backups per vCenter.
External proxy	8 concurrent hotadd sessions of VMDKs	External proxy has one SCSI controller which limits the concurrent hotadd sessions to 8 per external proxy.
Proxies per vCenter	6	vCenter achieves good performance with 50 concurrent sessions as indicated in the recommendation above. Each external proxy adds 8 concurrent sessions. Therefore, using one VMware Backup appliance (with internal proxies disabled) and 6 external proxies will enable you to reach 48 concurrent sessions.

VMware Backup Appliance best practices

Observe the following best practices when using NetWorker with the VMware Backup Appliance.

Note

For more best practices related specifically to the deployment of the VMware Backup Appliance in new or upgraded installations of NetWorker, review the section VMware Backup Appliance requirements.

- Ensure that the NetWorker server and storage node are at the same version, and that the VMware Backup Appliance you deploy is compatible with this version, for example, NetWorker 18.1 with OVA 1.5.1.7.
- Use Hotadd transport mode for faster backups and restores and less exposure to network routing, firewall, and SSL certificate issues. To support Hotadd mode, deploy the VMware Backup Appliance on an ESXi host that has a path to the storage that holds the target virtual disk(s) for backup. In environments that use the older VMFSv3 format datastore, deploy the proxy on the datastore with the largest block size.

  Note

  Hotadd mode requires VMware hardware version 7 or later. Ensure all Virtual Machines that you want to back up are using Virtual Machine hardware version 7 or later.

  For sites that contain a large number of Virtual Machines that do not support Hotadd requirements, NBD backups will be used. This can cause congestion on the ESXi host management network. Plan your backup network carefully for large scale NBD installs. You may consider configuring one of the following options:

  - Set up Management network redundancy.
  - Set up backup network to ESXi for NBD.
  - Set up storage heartbeats. http://www.vmware.com/files/pdf/techpaper/vmw-vsphere-high-availability.pdf provides more information.
- Avoid deploying VMs with IDE virtual disks; using IDE virtual disks degrades backup performance. Use SCSI virtual disks instead whenever possible.

  Note

  You cannot use hotadd mode with IDE Virtual disks and therefore backup of these disks will be performed using NBD mode.
- During policy configuration, assign clients to a policy based on logical grouping to allow for better scheduling of backups that will help you avoid resource contention and create more organized logs for review.
- It is recommended that you perform regular checkpoint backups to protect the VMware metadata in your environment. You can schedule daily checkpoint discover and checkpoint backup actions for a VMware Protection Policy, within NetWorker.
- When you plan the backups, ensure that NetWorker VMware Protection supports the disk types that you use in the environment. Currently, NetWorker VMware Protection does not support the following disk types:
  - Independent (persistent and non-persistent)
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode
- When you enable Change Block Tracking (CBT) NetWorker can achieve faster incremental backup performance. The default VMware Backup Appliance configuration has a threshold of 25% change per client, which means that if the particular Virtual Machine has changed more than 25% since the last backup, NetWorker will perform a level full backup. In order to support Changed Block Tracking (CBT):
  - Ensure that all Virtual Machines run VMware hardware version 7 or higher.

  - If you add a disk or dynamically expand a disk on a Virtual Machine, you must take a new full backup for CBT to function.

  For Incremental backups with CBT, remove any existing snapshots of a Virtual Machine before you add the VMware Backup Appliance.

  Note

  Adding containers or Virtual Machines to a policy will automatically enable CBT.

- 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 1035096 at http://kb.vmware.com/kb/1035096 provides more information.

- Install VMware Tools on each Virtual Machine that you want to back up by using the EMC Backup and Recovery user interface in the vSphere Web Client. VMware Tools adds additional backup capability that quiesces certain processes on the guest OS prior to backup. Some features in File Level Restore also require VMware Tools.

- Conflicting vSphere Web Client plug-ins can cause unexpected behavior with the EMC Backup and Recovery user interface in the vSphere Web Client. Examples include the VDP plug-in, and the HP Insight Manager plug-in. VMware knowledge base article 1025360 at http://kb.vmware.com/kb/1025360 provides the instructions to remove conflicting plugins.

- EMC recommends that you set an appropriate NetWorker server/storage parallelism value, according to the available resources, to reduce queuing. For example, a VMware Backup Appliance with 5 external proxies and clones requires more than 64 parallel sessions. Therefore, setting the parallelism for the NetWorker server to 128 or higher (while also setting the server with 32+ GB memory and 8+ CPUs) will suit such an environment. The *NetWorker Performance Optimization Planning Guide* provides more details.
  If you require a larger number of parallel image backups, also consider setting the maximum number of vCenter SOAP sessions to larger value. Note that this requires careful planning and additional resources on the vCenter Server You can configure this by modifying the following line in the vCenter `vpxd.cfg` file:

  ```
  <vmacore><soap><maxSessionCount> N </maxSessionCount></soap></vmacore>
  ```

  This applies specifically to SDK sessions as opposed to VI client sessions:

- Each Virtual Machine backup to a Data Domain system consumes more than one session on the Data Domain device. The default device configuration is `target sessions=6` and `max session=60`, however EMC recommends that you configure additional devices for more than 10 parallel backups.

- Virtual Machines with extremely high IO may face hangs during consolidation due to the ESXi forced operation called synchronous consolidate. Plan your backups of such Virtual Machines according to the amount of workload on the Virtual Machine.

- When you work with the vCenter database either directly or by using scripts, do not change the name attribute for the `vmfolder` object. VMware knowledge base article at https://support.emc.com/kb/190755 provides more information.

- When you set up multiple devices locally on the NetWorker server, this can lead to resource contention. Large VMware environments will have more stability when most backup devices are set up on a remote storage node.

When you mount a backup or clone pool volume on a remote storage node, then modify the client properties for the VMware Backup Appliance resource in NetWorker to add the remote storage node names to the **Storage nodes** attribute on the **Globals (2 of 2)** tab.

- Resource contention can occur at various points during the backup cycle. When NetWorker runs larger policies issues due to contention of resources can occur, which impact all running operations. Adjust your resources and times for other larger policies to avoid overlaps, and avoid resource contention.
  For example, you configure one pool named Bronze, with one device. If you set up a policy where every day at 10 pm two policies called 'Bronze1' and 'Bronze2' with 400 clients 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.

Limitations and unsupported features

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

Note

Review the VMware limitations:

- vSphere 5.5—https://www.vmware.com/pdf/vsphere5/r55/vsphere-55-configuration-maximums.pdf
- vSphere 6.0—https://www.vmware.com/pdf/vsphere6/r60/vsphere-60-configuration-maximums.pdf

VMware Backup appliance versions must be the same when deploying multiple VMware Backup appliances in same vCenter
When you deploy more than one VMware Backup appliance in your environment and the appliances are registered to the same vCenter, then these VMware Backup appliance versions must be the same.

Incremental backups across Data Domain systems not supported
Performing incremental backups across Data Domain systems is not supported for VMware Backup appliance policies.

Recovery of virtual machine configured with EFI firmware fails to find operating system during virtual machine startup
When a virtual machine is configured with EFI firmware, backup and recovery completes successfully. However, when the restore is performed and the virtual machine is powered on, the virtual machine fails to find an operating system during startup. To work around this issue, perform an Instant Access recovery of the virtual machine.

Cannot add Actions to workflows that have the same name in different policies
For traditional workflows, VMware allows you to use the same workflow name in different policies. However, if you add such a workflow to a policy, you cannot add actions to the workflow.

Datastore names cannot contain special characters
Using special characters in datastore names can cause problems with the Virtual Backup appliance, such as failed backups and restores. Special characters include the following: `% & * $ # @ ! \ / : * ? " < > | ;`, etc.

External proxy appliance must be at same version as VMware Backup appliance

Performing an image level recovery in the vSphere Web Client fails with error code 10002 when the external proxy is running an older awncomm version than the VMware Backup appliance, due to the addition of the *NW_VBA_NAME* flag in later versions.

Ensure that the external proxy appliance is at the same version as the VMware Backup appliance and if not, upgrade the external proxy. If you require an immediate recovery in an environment with mixed versions, temporarily shut down all of the external proxies while you start the Virtual Machine restore. This will ensure that the recovery gets assigned to the VMware Backup appliance internal proxy. Knowledge base article 457952 available at http://support.emc.com provides more information.

Avamar image backups to Data Domain fail if proxies not added to DD Boost Access list

Avamar VMware image backups to Data Domain fail with errors when you do not add the proxies to the DD Boost access list.

To add the proxies to the DD Boost access list, run the following command: `ddboost access add clients` *client-list*. Knowledge base article 453486 available at http://support.emc.com provides more information.

FLR browse in EMC Data Protection Restore Client may not display second of three disks

When you use the EMC Data Protection Restore Client to browse disks for FLR, the second of three disks may not display due to partition detection failing for this specific disk. The disk will display properly from the command line.

Knowledge base article 457783 at http://support.emc.com provides possible workarounds and more information on this issue.

Data Domain SMT not supported

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

Backups to Data Domain device over WAN may fail if TLS used

Backups to a DDBoost device over WAN occasionally fail when you use TLS. DDBoost fails to establish a TLS connection to the Data Domain device due to an SSL Handshake Failure. DDBoost can successfully connect to the same Data Domain device when TLS is not used.

Do not use combination of FQDN and IP when registering vCenter server

When you register the vCenter server with the VMware Backup appliance and the NetWorker server, ensure that you specify only the FQDN or only the IP in all instances. Do not use a combination of the two.

VMware Backup appliance must be deployed to an ESX host managed by the same vCenter you register the appliance to when using multiple vCenters

When you have multiple vCenters, you must deploy the VMware Backup appliance to an ESX host that is managed by the same vCenter you register the appliance to. Otherwise, a connection error message similar to the following appears: “`Unable to find this EBR in the vCenter inventory.`”

Only hotadd and NBD transport modes supported

The NetWorker VMware Protection solution supports only the hotadd and NBD transport modes. The hotadd mode is the default transport mode.

Higher default target session and max session values for VMware Backup appliance
NetWorker creates the default VMware Backup appliance with the values target session=50 and max session=200. These values are higher than normal default values for a device created in NetWorker because each appliance or external proxy comes with 8 proxy agents.

Backup of individual folders within a Virtual Machine is not supported
The NetWorker VMware Protection solution only supports image-level backup and disk-level backup. You cannot perform backups of individual folders within the Virtual Machine.

VMware View in the NetWorker Administration map view does not display when configuration for Virtual Machines within the vCenter is incomplete
When you use VMware View, the map view does not appear when the configuration for one or more Virtual Machines in the vCenter is incomplete. To avoid this issue, remove the incomplete Virtual Machine configurations from vCenter.

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

No automatic migration tool to move from previous solution to NetWorker VMware Protection
An automatic migration tool to move from the previous Virtual Machine backup solution to the NetWorker VMware Protection solution does not exist.

Only English keyboards supported in vSphere Web Client's EMC Backup and Recovery user interface
The EMC Backup and Recovery user interface in the vSphere Web Client only supports English language keyboards.

Configuration checklist

The following configuration checklist provides best practices and troubleshooting tips that may 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

- Upgrade all Data Domain systems to use DDOS version 5.6 and later.
- 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.

NetWorker configuration

- Ensure that the relevant devices are mounted
- Wait until you successfully configure a policy before you run the policy.
- A message appears after successful registration in NMC.

VMware Backup Appliance configuration

- Supports configuration on thin disks.
- Use the **EMC Backup and Recovery Configuration Utility** to confirm that all services on the VMware Backup Appliance except the backup scheduler are running. Note that maintenance services will start between 24 to 48 hours after booting up, or you can start maintenance services manually.
- To avoid slower recovery times , do not add more than 500 VMs to a VMware Backup Appliance.
- Ensure that the VMware Backup Appliance still has space left for backups.
- VMware snapshot for backup is not supported for independent disks.

IPv6 considerations

The following considerations apply when using IPv6 instead of IPv4 for NetWorker VMware Protection.

Register with FQDN instead of IP in EMC Backup and Recovery Configuration Utility
During registration of the VMware Backup Appliance in the **EMC Backup and Recovery Configuration Utility** window, if using IPv6 do not specify the IPv6 address. Use the FQDN of the vCenter server to register the appliance instead.

Additional zeros display in IPv6 address in EMC Backup and Recovery Configuration Utility
The IPv6 static address tab in the **EMC Backup and Recovery Configuration Utility** window displays additional zeros in the address.

Remove the extra zeros, or re-type the correct IPv6 address prior to clicking **Next**.

Emergency restore (Direct to host recovery) unavailable
Emergency restore, also referred to as Direct to host recovery, is currently unavailable in an IPv6 environment.

VMware Backup Appliance installation

If you have problems with the VMware Backup Appliance installation:

- Confirm that all of the software applications meet the minimum software requirements. System requirements on page 209 provides more information.
- Confirm that the hardware meets the minimum hardware requirements (see System requirements on page 209 provides more information.
- Confirm that DNS is properly configured for the VMware Backup Appliance (see Pre-installation requirements on page 214 provides more information.

AV-NetWorker Communicator (avnwcomm) timeout

The default timeout for avnwcomm communication between the proxy and the NetWorker server is two minutes.

During the backup window, the following issues may cause a delayed response from NetWorker, leading to failures during backup and restore operations:

- Devices unavailable
- Low server parallelism
- Peer information issues
- DNS problems
- Offsite deployments where the VMware Backup appliance node or proxy are on a different site from the NetWorker server

For sites experiencing delays, you can tune the *avnwcomm.cmd* inactivity timeout to allow for longer wait times, for example 5 minutes, using the following procedure.

1. Run the following command to verify the version. `/usr/local/avamarclient/bin/avnwcomm --version`
2. Create a file on the VMware Backup appliance node and external proxy called *avnwcomm.cmd* under `/usr/local/avamarclient/var/`.
3. Edit *avnwcomm.cmd* to add the following: `--nw_init_timeout=300`
4. Ensure you have the correct permissions by running: `chmod 755 /usr/local/avamarclient/var/avnwcomm.cmd`

Log in to the EMC Backup and Recovery Console as admin instead of root

When you use `ssh` to connect or login to the EMC Backup and Recovery Console, ensure that you login as the admin user instead of root. Direct login as the root user is not permitted.

EMC does not recommend that you modify the `ssh` configuration file in `/etc/ssh` so that a user can `ssh` into the appliance directly as root. Changes this file can result in future upgrade failures.

After you `ssh` to the Console as admin, you can then switch to the root user, as shown in the following example:

```
# ssh <VBA-host> -l admin
Password:
#su
Password:
```

If you use the vSphere Client to connect to the EMC Backup and Recovery Console, you can log in as the root user.

Note

The password for the admin user is the same as the password that you specified in the **EMC Backup and Recovery Configure** window during the initial installation of the VMware Backup Appliance.

Launching the Dell EMC Data Protection Restore Client after upgrade on Mozilla Firefox browser

After upgrading the VMware Backup Appliance from a NetWorker 8.2 release to NetWorker 9.0 and later, the **Dell EMC Data Protection Restore Client** window might not launch when using the Mozilla Firefox browser.

If you cannot launch the **Dell EMC Data Protection Restore Client** window, run the following commands on the VMware Backup Appliance as the root user:

- `/usr/java/latest/bin/keytool -delete -alias tomcat -storepass changeit`
- `/usr/java/latest/bin/keytool -genkeypair -v -alias tomcat -keyalg RSA -sigalg SHA256withRSA -keystore /root/.keystore -storepass changeit -keypass changeit -validity 3650 -dname "CN=localhost.localdom, OU=Avamar, O=EMC, L=Irvine, S=California, C=US"`
- `emwebapp.sh --restart`

If you use the Mozilla Firefox browser on a Linux machine and are unable to browse the backups even after you upgrade the browser to the latest version, an error message similar to the following might appear: `sec_error_ca_cert_invalid issue`

To resolve this issue, perform the following steps:

1. Open the Mozilla Firefox browser.
2. In the **Location** bar, type `about:config` and press **Enter**.
   You may see a warning that says `This might void your warranty!`

   Click **I'll be careful, I promise!** to continue to the **about:config** page.
3. Set **security.use_mozillapkix_verification** to **True**, if the value is set to **False**.

Launching the EMC Backup and Recovery Configuration Utility after upgrade on Mozilla Firefox browser

After upgrading the VMware Backup Appliance from a NetWorker 8.2 release to NetWorker 9.0.1 and later, the **EMC Backup and Recovery Configuration Utility** window may not launch when using the Mozilla Firefox browser.

If you cannot launch the **EMC Backup and Recovery Configuration Utility** window, perform the following:

1. Login via SSH to the VMware Backup Appliance Console as the admin user.
2. Switch to the root user by running the following command:

   ```
   su -
   Password:
   ```

3. Run the following commands on the VMware Backup Appliance:

   ```
   /usr/java/latest/bin/keytool -delete -alias tomcat -storepass
   changeit /usr/java/latest/bin/keytool -genkeypair -v -alias tomcat
   -keyalg RSA -sigalg
   SHA256withRSA -keystore /root/.keystore -storepass changeit -
   keypass changeit -validity 3650 -dname "CN=localhost.localdom,
   ```

```
OU=Avamar, O=EMC, L=Irvine, S=California, C=US"emwebapp.sh --
restart
```

Restart the Enterprise Manager Web Application (emwebapp)

Use the following steps to restart `emwebapp`.

1. Log into the Console, and then type:

   ```
   emwebapp.sh --stop
   emwebapp.sh --start
   ```

2. Restart the EMC Backup and Recovery database by running:

   ```
   emwebapp.sh --stop
   su - admin
   ebrdbmaint.pl --startdb
   exit
   emwebapp.sh --start
   ```

3. Patch the EMC Backup and Recovery server by running:

   ```
   emwebapp.sh --stop
   cd /usr/local/avamar/lib/ebr
   mv ebr-server.war ebr-server.war.orig
   ```

4. Use SFTP to upload the new war file to this location:

   ```
   emwebapp.sh --start*
   ```

Note

When you use `ssh` to connect or log in to the EMC Backup and Recovery Console in the vSphere Client, ensure that you login as admin instead of root. Log in to the EMC Backup and Recovery Console as admin instead of root on page 312 provides more information.

VMware Backup Appliance Log file locations

Review the following VMware Backup Appliance log file locations:

- Tomcat logs—`/usr/local/avamar-tomcat/logs catalina.out` for HTTP request and respond at high level
- EMC Backup and Recovery server logs—`/usr/local/avamar/var/ebr/server_log/ebr-server.log` for specific EMC Backup and Recovery activities
- MC logs—`/usr/local/avamar/var/mc/server_log`
- MC Soap service logs—`/usr/local/avamar/var/mc/server_log/axis2.log`
- Boot logs—`/usr/local/avamar/var/av_boot.log`
  `/usr/local/avamar/var/av_boot_err.log`
- EMC Backup and Recovery configure or registration with EMC Backup and Recovery appliance logs—`/usr/local/avamar/var/ebr/server_log/ebr-configure.log`
- File Level Recovery logs—`/usr/local/avamar/var/flr/server_log`
- NetWorker log file location—`/nsr/logs/`

Collecting log files

To collect all log files on the EMC Backup and Recovery appliance:

1. Connect to the **EMC Backup and Recovery Configure** window, as shown in Post-installation configuration on page 240.
2. Open the **Log Collector** tab.
   Three sections appear:
   - All EBR appliance logs
   - Client logs
   - Configurations
3. On the **Status** tab, click **Collect Logs**.
4. Click **Download** to save the log files to the local machine that you used to open the **EMC Backup and Recovery Configure** window.

Enabling low-level logging of NetWorker web server on Windows systems

To enable low-level logging, log into the NetWorker server and perform the following steps:

1. Open a command prompt and run **cmd.exe**.
2. Use Task Manager to get the pid of **nsrvmwsd**.
3. CD to **networker-install-dir** > **\nsr\bin**.
4. Run **dbgcommand -p** > **<nsrvmwsd-pid** > > **Debug=11**.

NetWorker operations

The following troubleshooting items provide some direction on how to identify and resolve common issues with NetWorker and VMware Protection Policies.

VMware Protection Policy fails for manually created client resource with DataDomain backup attribute enabled

When you manually create a client resource and enable the DataDomain backup attribute (using nsradmin or the NMC Client Properties window), the default VMware Protection Policy fails with the following error:

```
NWP_LOG_OUTPUT: NW Client Plugin: ABORT session operation
successful. Reason for abort: nwp_start_backup_session_helper: no
matching IP interface data domain devices for save of client
clientname; check storage nodes, devices or pools
```

If this occurs, unselect/disable the DataDomain backup attribute on the manually created client resource.

“No proxies running on VBA {appliance name} for backing up VM {VM name}”

When the avagent is not running, or no proxies are running, this error appears in the VMware Protection Policy details window in NMC.

If you see this error, log in as root from the EMC Backup and Recovery Console in the vSphere Client and invoke service avagent restart:

```
/etc/init.d/avagent restart
```

NetWorker web services timeout

Due to the extended time required to perform larger operations such as cross-sync, NetWorker web services may time out.

For example, web services may request a clean-up of a large amount of data on the VMware Backup Appliance, for which the time required to complete the operation exceeds the timeout setting. When a VMware Backup Appliance communication timeout occurs, an "operation timed out" error message appears.

To fix VMware Backup Appliance communication timeouts, you can set two environment variables on the NetWorker server -- one for connection attempts to the VMware Backup Appliance, and the other for requests.

```
NSR_VBA_CONNECT_TIMEOUT=900
```

```
NSR_VBA_REQUEST_TIMEOUT=2400
```

If your timeout values are lower than these numbers, it is recommended to these values.

Note

Values are in seconds. The maximum value permitted for *NSR_VBA_CONNECT_TIMEOUT* is 1200 and the maximum value permitted for NSR_VBA_REQUEST_TIMEOUT is 3600.

Changes to these values may depend on the operating system of the NetWorker server. The sections "Setting environment variables on UNIX" and "Setting environment variables on Windows systems" in the *NetWorker Administration Guide* provide more information. If VMware Backup Appliance registration fails with the Networker server after the initial deployment and registration, you can also set *NSR_VBA_CONNECT_TIMEOUT* at the operating system level for successful registration.

On Linux, login to the NetWorker server and perform the following:

1. Run `# printenv | grep NSR_VBA_CONNECT_TIMEOUT export NSR_VBA_CONNECT_TIMEOUT=900`.
2. Restart NetWorker services by using the command `/etc/init.d/networker restart`.
3. Run `emwebapp.sh --restart` on the VMware Backup Appliance.

To re-register the VMware Backup Appliance on Windows:

1. Right-click **My Computer** > **Select Environment Variables**.
2. Add a new variable *NSR_VBA_CONNECT_TIMEOUT* with the value 900.
3. Restart NetWorker services on the NetWorker server and run `emwebapp.sh --restart` on the VMware Backup Appliance.

vCenter server operations

The following troubleshooting items provide some direction on how to identify and resolve common issues from the vCenter server.

Clear All EMC Backup and Recovery plug-ins

1. Log into vCenter Server's MOB at http://*vcenter-server*/mob.

2. Click on the **content** link.
3. Click on **ExtensionManager** link.
4. Click on the **UnregisterExtension** link.
5. Enter the value **com.emc.networker.ebr** and click the **Invoke Method** link.

Enable HTTP access from EMC Backup and Recovery

1. Log in to the vCenter server console, then type:
   `vi /var/lib/vmware/vsphere-client/webclient.properties`
2. Ensure that the output contains a line similar to **allowHttp=true**.

vSphere Client operations

The following troubleshooting items describe how to identify and resolve common issues that occur with EMC Backup and Recovery Console from the vSphere Client, or the EMC Backup and Recovery user interface in the vSphere Web Client.

Time synchronization error

A time synchronization error can occur when launching the EMC Backup and Recovery user interface in the vSphere Web Client in the following scenarios:

- When you configure the EMC Backup and Recovery appliance to synchronize its time with the ESX server on which the appliance runs.
- When the vCenter server is a VM, and runs on an ESX server that differs from the ESX server that hosts the EMC Backup and Recovery appliance.

In such environments, if the times differ on the two ESX servers, and the vCenter server is not set up to synchronize with the ESX server it runs on, then the following errors appear in the vSphere Web Client interface:

```
The most recent request has been rejected by the server.
The most common cause for this error is that the times on the EMC
Backup and Recovery appliance and your SSO server are not in sync
```

To fix this issue:

1. Verify that the times match on all the ESX servers in your environment. You can configure the time settings in the vCenter UI. EMC recommends that you configure the time settings to use NTP. The VMware knowledgebase article 2012069 provides details on configuring NTP on ESX/ESXi hosts using the vSphere Client.
2. On your vCenter system, ensure that it is configured to synchronize its time with the ESX server it is running on by running the following:
   `vmware-toolbox-cmd timesync enable`
3. Verify that the time on your EMC Backup and Recovery appliance and your vCenter server are the same by running the **date** command on each.

   Note

   Allow a couple of minutes after making the changes for times to merge.

4. Log in to the vSphere Web Client. If the time synchronization message does not appear when you launch the **EMC Backup and Recovery** user interface, the times have been synchronized successfully.

Restart vSphere Web Client Server

To restart the vSphere Web Client server:

1. Log into the vCenter server console, then type:
   `cd /usr/lib/vmware-vsphere-client`
2. Run `./vsphere-client stop`.
3. Run `./vsphere-client start`.

Start user interface does not display as available in vSphere Web Client

If the user interface does not display as available in the vSphere Web Client, log into vCenter and restart the vSphere Client Services by running the following from a command prompt:

```
cd /usr/lib/vmware-vsphere-client
./vsphere-client stop
./vsphere-client start
```

When you deploy a VM, do not change the default network (VM Network) provided by the wizard. After the deployment completes and prior to powering on the VM, reconfigure the VM to use the appropriate network if VM Network is not correct. If you change the network in the wizard, EMC Backup and Recovery looks for eth1 instead of eth0, and network connectivity fails.

Launching the Console in the vSphere Web Client to reboot the VM

When you log into the vSphere Web client and launch the Console for the EMC Backup and Recovery appliance, a delay of several minutes may occur while the VM reboots. A message similar to the following appears in the output:

```
Identity added: /home/dpn/.ssh/dpnid (/home/dpn/.ssh/dpnid)
```

If you see this message, do not shutdown the VM, and allow time for the reboot to complete.

The EMC Backup and Recovery appliance is not responding. Please try your request again

If you were previously able to connect to EMC Backup and Recovery and this message appears, check the following:

- Confirm that the user name or password used to validate EMC Backup and Recovery to the vCenter Server has not changed. Only one user account and password are used for EMC Backup and Recovery validation. This is configured through the EMC Backup and Recovery Configure window.
- Confirm that the name and IP address of the appliance have not changed since the initial EMC Backup and Recovery installation. DNS Configuration on page 215 provides additional information.

Integrity Check

After you start an integrity check, a delay of several seconds may occur before the “EBR: Integrity Check” task shows up in the Recent Tasks pane of the EMC Backup and Recovery user interface in the vSphere Web Client. Similarly, when you cancel an integrity check, a delay of several seconds may occur before the task is cancelled.

In some cases (for example, when the integrity check progress is above 90%), the integrity check may actually complete before the cancel operation completes. Even when the integrity check completes successfully, the Task Console may still show an error indicating that the integrity check was cancelled.

If you knew that the Integrity Check Status of the appliance (shown on the Reports tab) was “Out of Date” before you started the integrity check, then you can look at the status immediately after you cancel the job to see if the cancel operation succeeded. If the Integrity Check Status is “Normal,” then the check was successful. If the status is “Out of Date,” then the check was cancelled.

Backup operations

The following troubleshooting items provide some direction on how to identify and resolve common issues with NetWorker VMware Protection backups for the VMware Backup Appliance (VBA).

Backups fail with external proxy after upgrading from NetWorker 8.1.*x* to 18.1

Backups may fail with the external proxy after an upgrade from NetWorker 8.1.*x* to version 18.1 has occurred.

If this happens, delete the peer information for the external proxy from the NetWorker server.

Backups fail when EMC Backup and Recovery plug-in registers with an incorrect version string in vCenter

Backups may fail when the EMC Backup and Recovery plug-in registers with an incorrect version string in vCenter. Additionally, EMC Backup and Recovery cannot co-exist with VMware VDP or any third-party backup plug-in in the same vCenter. If a conflict occurs, then unregister the EMC Backup and Recovery plug-in extension from the managed object browser (MOB):

1. Navigate to http://*vcenter-ip*/mob.
2. In the **Properties** table, select the content link.
3. Select **Extension Manager** and verify that the Properties table lists “**com.vmware.ebr2**”.
4. From the Methods table, select **UnregisterExtension**.
5. Type **com.vmware.ebr2** and select **Invoke Method**.

   Note

   This name will be different if removing VDP or a third party backup plug-in.

6. Verify in **Extension Manager** that the plug-in is no longer listed in the **Properties** table, and then restart vCenter services or the vCenter server.
7. Restart emwebapp on the EMC Backup and Recovery appliance by using the command **emwebapp.sh --restart**.

“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.

“Unable to add client {client name} to the EMC Backup and Recovery appliance while creating backup job {backupjob name}.”

This error can appear when there is a duplicate client name on the vApp container or the ESX/ESXi host. In this case only one backup job is added. Resolve any duplicate client names.

“The following items could not be located and were not selected {client name}.”

This error can occur when the backed up VM(s) cannot be located during Edit of a backup job. This is a known issue.

Windows 2008 R2 VMs may fail to backup with “disk.EnableUUID” configured to “true.”

Windows 2008 R2 backups may fail if the VM is configured with the *disk.EnableUUID* parameter set to *true*. To correct this problem, manually update the vmx configuration parameter *disk.EnableUUID* to *false* by using the vSphere Web Client:

1. Shut down the VM by right clicking the VM and selecting **Shut Down Guest OS**.
2. Right click the VM and select **Edit Settings**.
3. Click **VM Options**.
4. Expand the **Advanced** section and click **Edit Configuration**.
5. Locate the name *disk.EnableUUId* and set the value to *false*.
6. Click **OK** on the next two pages.
7. Right click the VM and select **Power On**.

After you update the configuration parameter, the backups of the Windows 2008 R2 VM should succeed.

Backup fails if EMC Backup and Recovery does not have sufficient datastore capacity

Scheduled backups fail at 92% complete if there is insufficient datastore capacity. If you configured the EMC Backup and Recovery datastore with thin provisioning and maximum capacity has not been reached, then add additional storage resources. If you configured the EMC Backup and Recovery datastore with thick provisioning and it is at full capacity, see EMC Backup and Recovery Capacity Management on page 292.

Backup fails if VM is enabled with VMware Fault Tolerance

When you enable Fault Tolerance for a VM, the backup fails. This is expected behavior; EMC Backup and Recovery does not support backing up VMs with Fault Tolerance enabled.

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.

After an unexpected shutdown, recent backup jobs and backups are lost

When an unexpected shutdown occurs, the VMware Backup appliance performs a rollback to the last validated checkpoint. This is expected behavior.

vMotion operations are not allowed during active backup operations

The vSphere vMotion feature enables the live migration of running virtual machines from one physical server to another. You cannot run vMotion operations on the vProxy appliance or VMware Backup appliance during active backup operations. This is expected behavior. Wait until all backup operations have completed prior to performing a vMotion operation.

Backups fail if certain characters are used in the virtual machine name, datastore, folder, or datacenter names

When you use spaces or special characters in the virtual machine name, datastore, folder, or datacenter names, the .vmx file is not included in the backup. The vProxy appliance and VMware Backup appliance do not back up objects that include the following special characters, in the format of character/escape sequence:

- & %26
- + %2B
- / %2F
- = %3D
- ? %3F
- % %25
- \ %5C
- ~ %7E
-] %5D

Restore operations

The following troubleshooting items describe how to identify and resolve some common issues with restores.

Restore to new virtual machine not available for backups that included physical RDM disks

When you back up a virtual machine that contains both virtual disks and physical Raw Device Mapping (RDM) disks, the backup successfully processes the virtual disks and bypasses the RDM disks, which are not supported for backup. However, when you restore data from one of these backups, you cannot restore the data to a new virtual machine because data residing on the physical RDM disks that were bypassed during the backup cannot be restored.

If you need to restore the data to a new virtual machine, perform the following:

1. Manually create a new virtual machine in vCenter. This new virtual machine must contain the same number of virtual disks as the original virtual machine from which the backup was taken.
2. Manually add the new virtual machine to NetWorker.

3. Restore the data to this virtual machine.

Restore tab shows backups taken after checkpoint backup as "not available"

When you complete a successful disaster recovery of the VMware Backup appliance, and then attempt to restore a backup performed after the last checkpoint backup, the **Restore** tab in the **EMC Backup and Recovery user interface** in the **vSphere Web Client** displays these backups as "not available." This occurs because no account for these backups exists, since the client or VM was added to the policy after the checkpoint backup.

When you add the client or VM back into a policy, backups display correctly with a valid path in the **Restore** tab.

Message appears during FLR indicating “error finding vm by ipAddr” when you do not install VMware Tools

You must install VMware Tools to perform FLR. When you do not install VMware Tools, a message appears indicating the restore client is unable to find a backup of a VM by IP.

Message appears indicating “Login failed. Cannot locate vm in vCenter.”

This error can occur when you attempt to connect to the EMC Data Protection Restore Client from a host that has not been backed up by the VMware Backup appliance

Log into a virtual machine that has been backed up by the VMware Backup appliance, and then connect to the restore client.

Restore tab shows a “Loading backups” message and is slow to load

It typically takes two seconds per VM backup to load each of the backups on the Restore tab. This is expected behavior.

Restore tab is slow to load or refresh

If there is a large number of VMs, then the Restore tab may be slow to load or refresh. For example, when you have approximately 100 VMs, the Restore tab can take up to four and a half minutes to load.

Adding external proxies

The VMware Backup appliance has 8 internal proxies. A proxy can only do one backup or restore at a time.

If you need more proxies, then deploy an external proxy OVA. The section Proxy assignment for backup and recovery on page 217 provides information.

Creating and analyzing crashes on Windows 2008 R2

1. Update the registry with the new key provided at http://msdn.microsoft.com/en-us/library/bb787181(VS.85).aspx.
   Using the recommended values, the dump file gets created in `C:\Users\Administrator\AppData\Local\CrashDumps`
2. Enable full crash dumps.

3. File an Open dump file in **windbg**.
4. To retrieve the full information, type **analyze --v** in the bottom command window.

Changing the Data Domain Boost password

When you change the password of the Data Domain Boost user, perform the following steps to ensure you also make the change on the VMware Backup appliance.

1. Update the password in the **NMC Device Properties** window, or in the **Device Configuration** wizard, for all devices belonging to the Data Domain host for which the password was changed.
2. Run the following command on the EMC Backup and Recovery Console in the **vSphere Client**:

```
mccli dd edit --name=fqdn --password=newpassword --password-
confirm=newpassword --user-name=boostuser
```

Accessing Knowledge Base Articles

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

CHAPTER 6

VADP Recovery (legacy)

Note

NetWorker 18.1 releases do not feature a new version of the VADP proxy. For VADP, NetWorker 18.1 only supports recoveries that were configured in a previous release. The NetWorker Online Compatibility Guide available on the Dell EMC Online Support site at https://support.emc.com/products/1095_NetWorker provides the most up-to-date compatibility information.

This chapter contains the following topics:

Software and hardware requirements

The software and hardware requirements for VADP include the following.

- One or more VADP proxy systems running any of the following 64-bit operating systems (English versions only):
  - Windows 2008 R2
  - Windows 2012
- One or more vCenter servers running any of the following versions:
  - vSphere 5.5 with ESX 5.5 and vCenter 5.5
  - vSphere 6.0 with ESX 6.0 and vCenter 6.0

  Note

  NetWorker supports VMware vCenter appliance versions 5.5 and 6.0.
- You must perform the following prerequisites on the NetWorker server/proxy machine in order to run vSphere version 5.5 and 6.0:
  1. Since the registry key for SSL verification is not set by default, add the following keypath in the registry:

     ```
     'HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/VMware, Inc./VMware
     Virtual Disk Development Kit'
     ```

     Add a DWORD VerifySSLCertificates and set it to zero ('VerifySSLCertificates=0'). This will disable SSL verification for all VDDK Hotadd operations.
  2. Install .NET framework 3.5.1 or later on the proxy. In Windows 2008 R2, even though the .NET framework is bundled with the operating system, ensure that you enable the framework under **Server Manager-** > **features**.
  3. Install VC++ runtime 9.0 (VC++2008 SP1) on the proxy. The following link provides more details: http://www.microsoft.com/en-us/download/details.aspx?id=2092
- Network connectivity must be available between the VADP proxy server and the vCenter Server managing the ESX server cluster. It also requires connection to the ESX server system.
- To connect to a Fibre Channel (FC) SAN, the VADP proxy requires a FC host bus adapter (HBA).
- You must install the NetWorker 9.0.x or later client software on the VADP Proxy host.
- The NetWorker server requires NetWorker 18.1 software.
- The VADP proxy host must have access to the LUNs required for supported VMs. Considerations vary depending on the environment, for example, physical and virtual Compatibility RDMs are not supported and therefore do not require proxy access. The section VADP proxy access to LUNs on page 347 provides more information.

Limitations and unsupported features

The following limitations apply to the VADP solution with NetWorker:

- NetWorker supports the recovery of non-English versions of guest operating systems for virtual machines. However, if using non-English versions of the Windows operating system for the vCenter or VADP proxy host, note the limitations in the sections Limitations to vCenter on non-English versions of Windows on page 327 and Limitation for VADP proxy host on non-English versions of Windows on page 327.
- Global directives (both encryption and compression directives) are not supported by NetWorker for VADP recovery.
- Image-level recovery from a CBT-based incremental backup is not supported.

Limitations to vCenter on non-English versions of Windows

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

- The following names should always contain only English characters:
  - Backup VM display name in the left pane of vCenter
  - Backup VM hostname/FQDN
  - vCenter Datacenter name
  - vCenter Resource pool name
  - ESX datastore names containing the VM configuration files and virtual disks.
- You can only restore VMs to the same language OS vCenter that you perform the backup from. For example, you cannot recover a VM backed up from a Japanese OS vCenter onto an English OS vCenter.
- You can only perform VADP recovery using the NetWorker User program. A command line recovery of the entire image will not work for backups from a non-English vCenter.

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

The following limitation applies to non-English versions of the Windows operating system for the VADP proxy host:

On the machine where you launch the VADP recovery, install the NetWorker package in English only without any language packages. You must unselect all the other language packages explicitly during the NetWorker installation.

Note

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

Transport modes

The VADP proxy host supports advanced transport modes for image-level recovery. You can set the configured network transport mode to the following values during recovery:

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

  SAN mode requires a physical proxy with SAN access, and the VMs need to be hosted on either Fibre Channel or iSCSI-based storage. The corresponding VMFS volumes must be visible in the Microsoft Windows Disk Management snap-in of the VADP proxy host.
- Hotadd—In this mode, the I/O happens internally through the ESX I/O stack using SCSI hot-add technology. This provides better I/O rates than NBD/NBDSSL. However, selecting this mode places CPU, memory and I/O load on the ESX hosting the VADP proxy.

  Hotadd mode requires a virtual proxy, and the ESX hosting the virtual proxy should have access to all the datastores where the VMs are hosted So, if the datastores are SAN/iSCSI/NFS and if the ESX server where the VADP proxy resides is separate from the ESX server where the VMs are hosted, then:
  - In the case of SAN LUNs the ESX hosting the proxy and the ESX hosting the VMs should be part of the same fabric zones.
  - In the case of iSCSI LUNs the ESX hosting the proxy and the ESX hosting the VMs should be configured for the same iSCSI-based storage targets.
  - In the case of NFS datastores, the ESX hosting the proxy and the ESX hosting the VMs should be configured for the same NFS mount points.
- NBD (Network Block Device): in this mode, the CPU, memory and I/O load gets directly placed on the ESX hosting the production VMs, because the data has to move through the same ESX and reach the proxy over the network. NBD mode can be used either for physical or virtual proxy, and also supports all storage types.
- NBDSSL (Network Block Device with SSL): NBDSSL transport mode is the same as NBD except that the data transferred over the network is encrypted. Data transfer in NBDSSL mode can therefore be slower and use more CPU due to the additional load on the VADP host from SLL encryption/decryption.

You can set multiple transport modes to be used by the VADP proxy host using the pipe symbol "|" (for example, san|nbd|nbdssl).

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

More information on configuring transport modes is provided in Configuring the VADP proxy host and Hypervisor resource. The transport modes are outlined in the table Table 33 on page 330.

Independent persistent disks cannot be recovered

VADP does not support the recovery of independent persistent disks. If NetWorker detects these disks, they are skipped and a message is logged that indicates the disks were skipped. If using independent persistent disks, you must use traditional NetWorker recovery.

Configuring the VADP proxy host and Hypervisor resource

A NetWorker client must be created for the VADP proxy host when configuring the virtual clients for recovery. The VADP proxy NetWorker client will be referred to by VM clients during VADP recovery operations.

You can create a NetWorker client for the VADP proxy host manually by using the `nsradmin` command.

Note

If multiple client instances of the same VADP proxy host exist in the NetWorker server, ensure that all the instances have the same application information attributes related to VADP. Manually copy the application information attributes into all the VADP proxy client instances. Note, however, that when a virtual proxy is used, it cannot be created by copying the template of other VMs that are being protected.

If vCenter is configured in the environment, there must be a Hypervisor resource for the vCenter server hosting the VMs that use VADP. You may also need to create a Hypervisor resource if you cannot use VMware View in the NetWorker VMware Protection solution, as indicated in the section Enable VMware View in NMC's Administration window after upgrading by creating a NSR Hypervisor resource on page 229.

If vCenter is not configured in the environment, there must be a Hypervisor resource created for each server in the environment.

You must create the corresponding Hypervisor resource in the NetWorker server prior to starting the VADP recovery.

Creating a Hypervisor resource from the NetWorker server

Procedure

1. Start the NetWorker administration program by running **nsradmin**. Use the **help** command for help, or the **visual** command to enter full-screen mode.
2. Type the following:

```
nsradmin> create type:NSR Hypervisor;name:vCenter_FQDN_or_IP
nsradmin> vi
Select type: NSR hypervisor;
name: esx3-vc1.lss.emc.com;
comment: ;
service: [VMware VirtualCenter];
endpoint: "https://esx3-vc1.lss.emc.com/sdk";
username: "ajayads\\nemo";  =======================> vCenter
info
password: *******;
command: nsrvim;
proxy: nemo220-3.lss.emc.com;  ============> NW Server
```

Creating a NetWorker client for the VADP Proxy host by using the Client properties windows

Table 33 Application information values

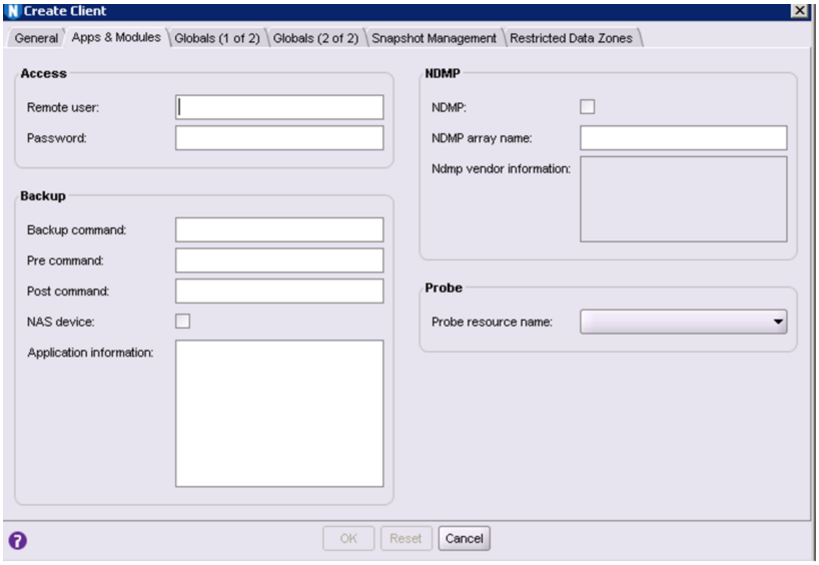
Attribute name	Description	Default value
VADP_HYPERVISOR This attribute is mandatory.	Specify the hostname of the VC server configured as part of the NSR Hypervisor resource. If there are multiple VC servers configured as part of the NSR hypervisor resource, specify their hostnames here. For example: *VADP_HYPERVISOR=any.vc* *VADP_HYPERVISOR=another.vc*	
VADP_TRANSPORT_MODE	Specify the transport mode to transfer data from a VMFS data store to a VADP proxy server. The following options are supported: • SAN – Virtual disk data is read directly off a shared storage device that the virtual disk resides on. This requires VMFS storage on SAN or iSCSI and the storage device has to be accessible from both ESX and the VADP proxy. • Hotadd – This mode can be used when VADP is used in a virtual proxy. Because it uses the ESX I/O stack to move data, Hotadd is more efficient than the transport mode NBD. • NBDSSL – This mode is the same as nbd except that the data transferred over the network is encrypted. The data transfer in nbdssl mode can be slower and use more CPU than in the nbd transport mode. • NBD – VADP will use an over-the-network protocol to access the virtual disk. Data is read from the storage device by the ESX host and then sent across an unencrypted network channel to the VADP proxy. Please note that this mode does not provide the offload capabilities of the san mode (because data is still transferred from the ESX host across the network). However, nbd does not require shared storage and also enables VADP to be run inside a VM.	Blank. If left blank, the default values are selected in the order of the description list. You can specify multiple modes by inserting a pipe (|) symbol between each value as shown in the following example: *VADP_TRANSPORT_MODE= san | Hotadd | nbdssl | nbd*. The order in which modes are specified dictate the priority in which they are attempted. In the above example, the san mode is attempted first; if that fails the Hotadd mode is attempted, and so on.

Procedure

1. In the NMC **NetWorker Administration Protection** window, right-click **Clients**, and select **New**.

   The **Create Client** dialog box displays.
2. Select the **General** tab.
3. In the **Name attribute** field, type the name of the proxy.
4. Select the **Apps and Modules** tab, shown in the following figure.

   Figure 165 Apps and Modules tab in NMC

5. In the **Application Information** field, type the following:

```
VADP_HYPERVISOR=any.vc
VADP_HYPERVISOR=another.vc
VADP_BACKUPROOT=G:\mnt
VADP_TRANSPORT_MODE=Hotadd
```

6. Click **OK**.

Creating a VADP User role in vCenter

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

Creating a VADP Proxy role

The section Minimum vCenter permissions needed to recover using VADP on page 332 provides more information.

Procedure

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

2. From the vCenter Server, select **View** > **Administration** > **Roles**.
3. Click **Add Role**.
4. Name the role **VADP User**.
5. Assign the required permissions to the **VADP User** role and click **OK**.

Assigning the VADP User role to the user specified in the NetWorker Hypervisor resource

Note

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

VMware documentation can be found at http://www.vmware.com/support/pubs/

Procedure

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

Minimum vCenter permissions needed to recover using VADP

It is recommended to create a single VADP User role with the recovery privileges specified in the following tables. You can then use the associated user for VADP recovery operations.

The following table provides VADP recovery privileges.

Table 34 VADP recovery privileges

Setting	Privileges
Global	• Cancel task • Licenses • Log Event • Settings
Resource	• Assign virtual machine to resource pool
Datastore	• Allocate space • Browse datastore • Low level file operations • Remove file • Update virtual machine files (only found in 4.1 and later)

Table 34 VADP recovery privileges (continued)

Setting	Privileges
Virtual machine > Inventory	• Create new • Register • Remove • Unregister
Virtual machine > Configuration	• Add existing disk • Add new disk • Add or Remove device • Advanced • Change CPU count • Change Resource • Disk change Tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility
Virtual machine > Interaction	• Power Off • Power On • Reset
Virtual machine > Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download
Virtual machine > State	• Create snapshot • Remove snapshot • Revert to snapshot
Network	• Assign network

Table 34 VADP recovery privileges (continued)

Setting	Privileges
	• Configure
Session	• Validate session
Tasks	• Create task • Update task

Recovering VADP Backups

This section covers these topics:

- File based recovery of a VM on page 334
- Image level (single step) recovery of a full VM on page 336

File based recovery of a VM

File-level recovery (FLR) is supported only on VMs that have a Windows operating system with the NTFS file system. FLR is not supported in the following configurations:

- Windows 8 and Windows Server 2012 VMs with Resilient File System (ReFS)
- VM operating system containing GPT or dynamic disks
- VM operating system containing uninitialized disks
- VM operating system containing unformatted partitions
- VM operating system containing partitions without drive letters
- VM configuration with Virtual IDE Disk Devices (only SCSI)
- VM configuration with independent disk mode

Performing a file based recovery on the local host

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

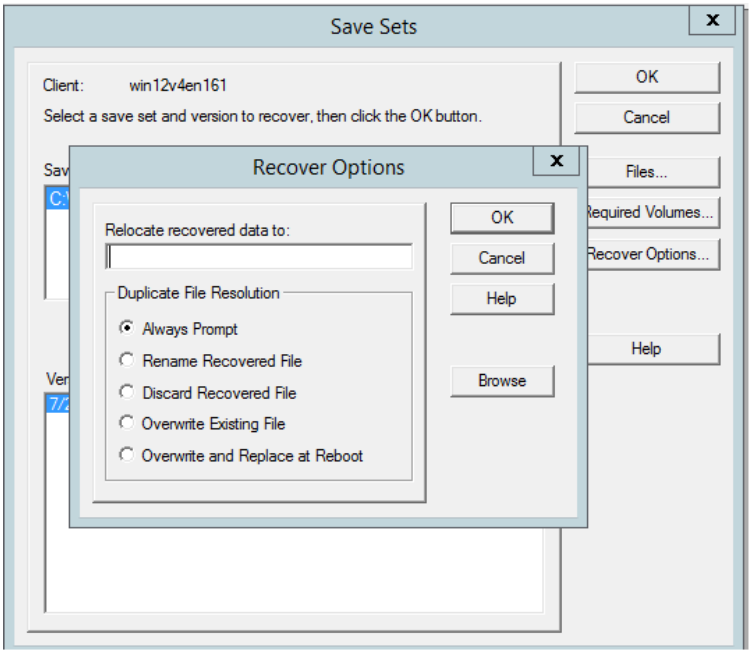
To perform a file based recovery on the local host:

Procedure

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

   If you click OK without specifying a restore path in the Recover Options dialog, a warning message displays, indicating that restoring data to the proxy storage node from the VM image can result in overwriting system files. To ensure overwriting of files does not occur, enter a restore path prior to clicking OK.

Figure 166 Recover Options dialog



Client: win12v4en161

Select a save set and version to recover, then click the OK button.

Relocate recovered data to:

Duplicate File Resolution

● Always Prompt

○ Rename Recovered File

○ Discard Recovered File

○ Overwrite Existing File

○ Overwrite and Replace at Reboot

Performing a file based recovery using CIFS share

Before you begin

Ensure that the remote access list of the VM client includes either user@server or user@proxy and that you add the proxies to the DD Boost access list. To add a client to the DDBoost access list, run the following command from the DDBoost command line:

```
 ddboost access add clients (- Add clients to a DD Boost access
list)
ddboost access add clients client-list
```

Procedure

1. Launch the NetWorker User program on the NetWorker server or VADP proxy.
2. Browse the file system for the VM client and select file to recover, as outlined in the NetWorker Administration Guide’s Recovery chapter.
3. Set the destination directory to the CIFS share of the VM client.
4. Recover the files onto the CIFS share.
5. At the VM client, move the files from the CIFS share to the appropriate directory.

Performing a file based recovery using directed recovery

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

Procedure

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

Note

The user must have the Remote Access All Clients privilege.

2. Select the VM client as the source client.
3. Select the target client as VM-client.
4. Select a destination folder.
5. Follow the procedure in the NetWorker Administration Guide’s Recovery chapter to select files for recovery and perform the recovery.

Image level (single step) recovery of a full VM

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

- Performing an image level recovery from the NetWorker User program on page 337
- Performing an image level recovery from the command line on page 338

Recommendations and considerations

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

- For a remote VADP proxy client, image level recovery requires the members of the VADP proxy client’s administrator group to be part of the remote access list of the VM clients or the member should have the “Remote access all clients” privilege.
- The user must have VMware privileges to register or create VMs.
- Recovery of the full VM is only supported using save set recovery.
- Only level FULL of FULLVM save sets are supported for VM image recovery.
- The VADP proxy system must be running one of the following:
  - Microsoft Windows 2008 R2
  - Microsoft Windows 2012
- If any hardware level changes such as a new disk partition, are made to the VM, you must perform a level full backup before you can perform an image level recovery of the full VM.
- The VM can recover to the same VMware ESX server or VMware vCenter (VC) taken at the time of backup or to a different ESX or VC. Recovery to different resource pools and different datastores are also supported. A different datastore can be specified for each disk and a configuration datastore can be specified to restore the configuration files.
- During the recovery of a full VM (FULLVM save set), the recovered VM will start in forceful powered off state because of a VADP snapshot limitation.
- For non-Windows VMs: If using traditional NetWorker client-based backups along with VADP image based backups for the same VM client, ensure that the browse policy for the client-based backups does not exceed the frequency of VADP image based backups. This practice is recommended because the indices of client-based backups may have to be removed prior to image-level recovery.

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

- If the image level backup of the VM being recovered was performed with the Encryption directive, the current Datazone pass phrase by default is automatically used to recover the VM image. If the current Datazone pass phrase was created after a password-protected backup was performed, you must provide the password that was in effect when the VM image was originally backed up.

Performing an image level recovery from the NetWorker User program

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

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

Procedure

1. Launch the **NetWorker User** program on the NetWorker client or VADP proxy.
2. From the **Operation** menu, select **Save Set Recover**.
3. In the **Source Client** dialog box, select the VM client from where the save set originated and click **OK.**
4. In the **Save Sets** dialog box, select the Save Set name for the full VM backup client (FULLVM) and select a level **FULL** backup. Click **OK**.

   Note

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

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

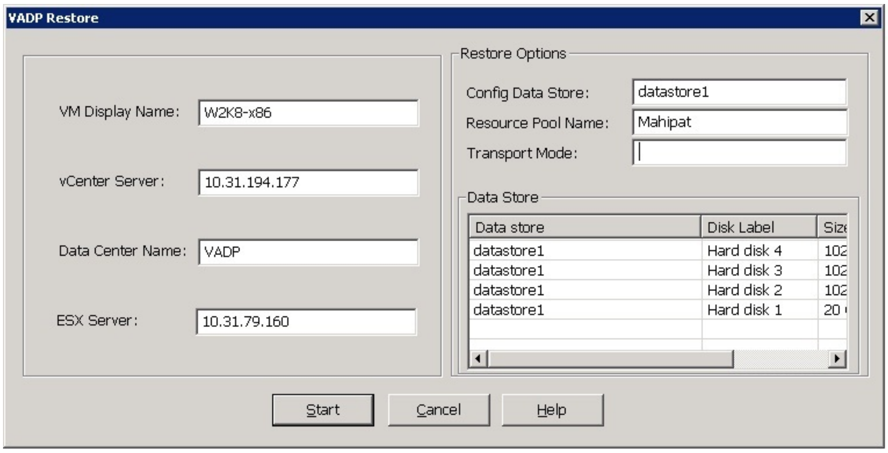
   Restore to VMware vCenter (VC):

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

Results

The following figure depicts a VADP Restore dialog box that is set up for a VMware vCenter restore.

Figure 167 VMware vCenter restore



VM Display Name: W2K8-x86

vCenter Server: 10.31.194.177

Data Center Name: VADP

ESX Server: 10.31.79.160

Config Data Store: datastore1

Resource Pool Name: Mahipat

Transport Mode:

Data store	Disk Label	Size
datastore1	Hard disk 4	102
datastore1	Hard disk 3	102
datastore1	Hard disk 2	102
datastore1	Hard disk 1	20

Performing an image level recovery from the command line

The following describes how to perform a command line recover of a full VM to the VMware ESX server or VMware vCenter (VC) server.

Procedure

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

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

   Note

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

2. Recover the full VM using the **recover** command, for example:

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

   where

   - *ssid* is the save set identifier of the FULLVM.
   - *staging-location* is the staging location path to recover the FULLVM image to the proxy. This value is needed only for a recovery to staging location and applies only to backups taken before NetWorker 7.6 SP2.
   - *VC hostname* is the VMware VC name that is used to perform the restore.
   - *port* is the port used to log in to the web server of the VC host. If no value is entered, the default port number is used.
   - *transport mode* is the transport mode to use for recovery. For example,SAN.
   - *datacenter name* is the data center name where the VM is restored to.
   - r*esource pool name* is the resource pool that the restored VM is connected to.
   - *ESX hostname* is the VMware ESX server machine name where the VMware VM needs to be restored.

- *datastores* is the list of datastores that need to be associated with the configuration and the disks of the VM that is being restored. They are name / value pairs separated with hash (#) symbols. For example:

  ```
  VADP:datastore=”config=stor1#disk1=stor2#disk2=stor3”
  ```

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

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

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

If your VMs have a mix of both VADP image level backups and traditional guest based (also known as client based) backups, you may have to use the following recovery procedure.

Unable to browse guest based backups on non NTFS file systems

Traditional guest based (client based) backups are not browsable in the recovery GUI for VMs that are running a non NTFS file system and that have a mix of VADP and guest based backups. This issue does not apply to Windows VMs that are using NTFS. Additionally, save set recoveries are not affected and can be performed in the usual way.

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

To find the backup time:

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

To perform the recovery:

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

Example

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

```
C:\mminfo -av -s jupiter -q "client=mars"
volume type client date time size ssid fl lvl name
kuma-1 Data Domain mars 5/24/2011 10:38:39 PM 281 MB 1658578527 cb
full /root
kuma-1.RO Data Domain mars 5/24/2011 10:38:39 PM 281 MB 1658578527 cb
full /root
kuma-6 Data Domain mars 5/24/2011 10:59:22 PM 5243 MB 1440475890 cb
```

```
full FULLVM
kuma-6.RO Data Domain mars 5/24/2011 10:59:22 PM 5243 MB 1440475890
cb full FULLVM
C:\recover -t "5/24/2011 10:38:39 PM" -s jupiter -c mars
```

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

Image level recovery to a different FARM or vCenter

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

Recovering a VM using SAN or Hotadd transport mode on Windows 2008

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

Procedure

1. Open a command prompt on the proxy host.
2. Run the following command:

   ```
   DISKPART
   ```

3. Enter **SAN** and check for the SAN policy.
4. If the policy indicates **offline**, enable the policy by entering the following:

   ```
   SAN POLICY=OnlineALL
   ```

   Note

   After the recovery is successful, **SAN POLICY** can be changed back to the default value (SAN POLICY=offline or SAN POLICY=offlineshared).

5. Restart the proxy for the change to take effect.

Results

You can now initiate the VM recovery using SAN or Hotadd mode.

Note

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

VADP Planning and Best Practices

This section covers topics related to best practices when using VADP.

Recommendations and considerations for VADP recovery

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

- Ensure that VC and ESX/ESXi are updated to the latest released update.
- VADP supports recovery via VMware VirtualCenter or vCenter. The section Software and hardware requirements on page 326 provides more information on supported vCenter versions.

  Note

  Recovery directly to a standalone ESX/ESXi host is not supported. The ESX/ESXi must be connected to either VirtualCenter or vCenter.

- VADP does not support IPv6. Instructions for disabling IPv6 and using IPv4 are provided in the section Network and Firewall port requirements on page 343.
- It is recommended to keep the vCenter and VADP proxy as separate machines to avoid contention of CPU and memory resources.
- The vSphere Client does not need to be installed on the NetWorker server.
- Ensure the path specified in VixDisklib and VixMountAPI config files are enclosed in double quotes as below:

  ```
  tempDirectory="C:\Program Files\EMC NetWorker\nsr\plugins\VDDK
  \tmp"
  ```

  These files are stored in the following location by default:

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

  Note

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

- It is recommended to use the VADP proxy host as the storage node. This provides the optimal configuration for any given transport mode as data transfer occurs directly from the ESX/ESXi datastore to the storage node.
- If reattaching RDM disks after recovery, make note of all LUNs that are zoned to the protected VMs.

Selection of physical vs. virtual proxy

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

Proxy node sizing and performance considerations

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

Note that there are no observed performance differences between physical and virtual proxies when running on similar hardware.

- The maximum number of concurrent sessions when using a physical proxy is higher than that of a virtual proxy. The section Recommendations and considerations for transport modes on page 345 provides more information on concurrent sessions for specific transport modes.
- Recommendations for a physical proxy is 4 CPU cores with 8GB of RAM. Recommendations for a virtual proxy is 4 vCPUs and 8GB vRAM per proxy, where each vCPU is equal to or greater than 2.66 GHz.
- Number of virtual proxies per ESX host depends only on the type of hardware on which the ESX has been installed.
- For lower-end ESX hosts, it is recommended not to mix I/O load on ESX (with the virtual proxy and VMs residing on a single ESX), but to have a separate ESX for the virtual proxy.
- For high-end ESX hosts, it is recommended to have a maximum of 5 virtual proxies concurrently running on a single ESX host.

Recommendations for Data Domain systems

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

- When using DD VTLs, SAN transport mode is required; as a result, the proxy host cannot be a virtual machine.
- For DD Boost enabled VADP backups:
  - The best CPU load and performance is observed with 4 concurrent backups per device. However, a NetWorker 8.x DD Boost library supports a greater number of concurrent backups (target sessions).
  - Setting a lower number of parallel sessions to a single device does not result in optimal performance.
  - Setting a higher number of parallel sessions to a single device increases the CPU load without any improvements to performance.
  - It is recommended to have at least 400MB to 500MB of RAM for each virtual machine being backed up if small to medium sized virtual machines are in use (virtual machines with less than 100GB virtual disks attached). If the largest virtual machine being backed up has more than 100GB of virtual disks attached, the RAM can be further increased.
- Better throughput is observed with DD Boost when there is less commonality between the virtual machines being backed up. As a best practice, it is recommended that virtual machines related to the same parent virtual machine template/clone should be part of different backup groups, and these backup groups should have different start times.
- In the case of both Hotadd and SAN modes, a 20-40% improvement is observed in the backup throughput for every additional proxy, provided the back-end storage where the virtual machines reside is not a bottleneck.

- If using Hotadd mode:
  - Refer to the section Recommendations and considerations for transport modes on page 345 for memory requirements. These requirements may increase depending on the size of the virtual machine's virtual disks, as described in the RAM recommendation above.
  - Virtual proxy parallelism should not be set to a value greater than 12. This limit can further be decreased if the virtual machines have more than one disk attached. More information related to best practices when using Hotadd mode is provided in the section Recommendations and considerations for transport modes on page 345.
  - In the case of multiple virtual proxies, it is recommended to consolidate all virtual proxies under dedicated ESX/ESXi host(s) in the environment to minimize the impact on production VMs during the backup window. These ESX/ESXi hosts should not be running any other VMs.
  - A maximum of 5 virtual proxies per one standalone ESX is recommended.
  - A maximum of 3 virtual proxies per ESX is recommended in a DRS cluster for proxies.

Network and Firewall port requirements

Be aware of the following firewall and network requirements:

- If there is a firewall between the VADP proxy host and the servers that run VMs that you plan to back up from the VADP proxy host, ensure that bi-directional TCP/IP connections can be established on port 902 between the VADP proxy host and the servers.
- If the Virtual Center or vCenter server uses a port other than the default port of 443, specify the port in the endpoint attribute of NSRhypervisor field. Configuring the VADP proxy host and Hypervisor resource on page 329 provides more information.
- VADP does not support IPv6. If vCenter is installed in a Windows 2008 system with IPv6 enabled (IPv6 is enabled by default) and the same system is also used as the VADP proxy, VADP backups will hang.
  Ensure that IPv6 is disabled on the following:
  - vCenter
  - ESX/ESXi
  - VADP-Proxy

  Note

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

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

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

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

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

Support for tape drives in a virtual machine

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

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

The following section requires a working knowledge of VMware vSphere ESX/ESXi and virtual machine configuration.

VMDirectPath requirements and recommendations

The following requirements and recommendations apply when using VMDirectPath:

- VMDirectPath requires Intel Virtualization Technology for Directed I/O (VT-d) or AMD IP Virtualization Technology (IOMMU). You may need to enable this option in the BIOS of the ESX/ESXi system.
- The VM should be Hardware version 7. For example, vmx-07.
- The optimal VMDirectPath PCI/PCIe devices per ESX/ESXi host is 8.
- The optimal VMDirectPath PCI/PCIe devices per VM is 4.

VMDirectPath restrictions

The following restrictions apply during the configuration of VMDirectPath:

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

The VMware knowledge base article http://kb.vmware.com/kb/1010789 provides information on configuring VMDirectPath.

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

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

Note

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

The following technical note provides additional information on VMDirectPath:

http://www.vmware.com/pdf/vsp_4_vmdirectpath_host.pdf

Considerations for VMDirectPath with NetWorker

The following are considerations apply when using VMDirectPath with NetWorker:

- For virtual environments that must run backups to Fibre Channel connected tape devices where there is a large amount of data in the VM, VMDirectPath can be used with NetWorker.
- 1 vCPU is sufficient to process 500 GB of data as long as the other VMs are not sharing the physical core on the underlying ESX/ESXi hardware, and the vCPU has exclusive access to the single core.
- If other VMs that reside on the same ESX/ESXi are sharing the underlying hardware (physical CPU), it may be required to add more vCPU and dedicating underlying hardware by using CPU affinity settings.
- To achieve optimal performance, it is recommended that the guest VM acting as the DSN has a minimum of 4 GB of memory available with 2 vCPUs allocated.
- If multiple target sessions are needed in each device and 4 or more vCPUs are assigned to the VM, ensure that there are enough devices available for backup operations. An insufficient amount of devices can result in less throughput due to CPU scheduling overhead of the Hypervisor.
- Ensure that the device drivers for the HBA are updated on the guest operating system.

Recommendations and considerations for transport modes

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

SAN transport mode considerations

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

- Prior to connecting the VADP proxy host to the SAN fabric, perform the steps in the section Diskpart utility for SAN and Hotadd transport modes on page 348.
- Memory usage per DD BOOST device should be approximately 500 MB.

Hotadd transport mode considerations

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

- Prior to running VADP backups using the virtual proxy host, perform the steps in the section Diskpart utility for SAN and Hotadd transport modes on page 348.
- A minimum of 4 vCPUs must be allocated per virtual proxy, with 8GB vRAM per proxy and each vCPU equal to or greater than 2.66 GHz.
- Memory usage per DD BOOST device should be approximately 300MB.
- The ESX server must be running ESX 3.5 update 4 or later.
- If there are multiple virtual proxies, it is recommended to host all the virtual proxies in a dedicated ESX/ESXi server. This would keep the virtual proxy resource consumption of CPU and memory isolated within that ESX/ESXi environment without impacting the production VMs.

- VMs having IDE virtual disks are not supported for Hotadd mode. Instead, nbd mode is recommended for these.
- The VM to restore and the VM where the restore is initiated must reside in the same VMware datacenter.
- The virtual proxy might fail to unmount Hotadd disks. In such cases, you must manually unmount the Hotadd disks from the virtual proxy. If any of the client VM disks are still attached to the virtual proxy, perform the following:
  1. Right-click the virtual proxy and go to **Edit Settings**.
  2. Select each of the Hotadd disks and choose **Remove**.

     Note

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

NBD/NBDSSL transport mode considerations

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

- You can only run a concurrent backup of 20 virtual disks against a given ESX/ESXi. The limit refers to the maximum number of virtual disks and is per ESX/ESXi host, irrespective of the number of proxies being used in the environment.
  Due to this limitation, it is recommended to apply the following best practices:
  - If the ESX is not part of a VMware cluster or is part of a DRS-disabled VMware cluster, then apply one of the following:
    - When using a single proxy to backup a given ESX via NBD/NBDSSL, set the client parallelism of the VADP proxy Client resource such that the limit of 20 concurrent disk connections per ESX host is not exceeded.
    - When using multiple proxies to backup a given ESX via NBD/NBDSSL, then the client parallelism on each VADP proxy should be calibrated such that the total concurrent disk connections per ESX host does not exceed 20.
  - If ESX is part of a DRS-enabled VMware cluster, then apply one of the following best practices:
    - When using a single proxy to backup via NBD/NBDSSL, set the client parallelism of the VADP proxy Client resource such that the limit of 20 concurrent disk connections per cluster is not exceeded.
    - When using multiple proxies to backup via NBD/NBDSSL, then the client parallelism on each VADP proxy should be calibrated such that the total concurrent disk connections per cluster does not exceed 20.

      Note

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

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

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

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

Use one of the following best practices:

- Set the client parallelism of the proxy to 8.
- Create a single backup group containing all 11 VMs from the given ESX and set the group parallelism to 8.

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

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

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

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

Use one of the following best practices:

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

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

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

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

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

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

Use one of the following best practices:

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

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

VADP proxy access to LUNs

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

SAN transport mode

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

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

Hotadd transport mode

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

NBD/NBDSSL transport modes

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

Diskpart utility for SAN and Hotadd transport modes

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

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

Note

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

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

APPENDIX A

NetWorker VMware Protection in VMware Cloud on Amazon Web Services

This appendix includes the following topics:

Introduction to NetWorker VMware Protection in VMware Cloud on AWS

NetWorker 18.1 supports NetWorker VMware Protection in VMware Cloud on Amazon Web Services (AWS).

Using NetWorker to protect virtual machines running in VMware Cloud on AWS is similar to how you protect the virtual machines in an on-premises datacenter. This appendix provides information on network configuration prerequisites, VMware Cloud on AWS best practices for NetWorker, and NetWorker operations that are currently unsupported for VMware Cloud on AWS

A NetWorker with CloudBoost environment can be useful for storing backups in Amazon S3 cloud object storage, including short term backups for operational recovery and long term retention backups for compliance. This capability is currently available with both in-guest filesystem agents as well as a broad range of application modules for NetWorker. NetWorker vProxy backups are currently not supported with CloudBoost, however cloning of vProxy backups to cloud object storage is supported via the CloudBoost appliance.

Additional information on NetWorker VMware Protection in VMware Cloud on AWS, including setup and configuration instructions, is provided in the whitepaper on https://support.emc.com/products/1095_NetWorker/Documentation/.

Prerequisites

Domain Name System (DNS) resolution is critical for NetWorker deployment and configuration. All infrastructure components should be resolvable through a fully qualified domain name (FQDN). This is especially important for the NetWorker Server, NetWorker vProxy, Data Domain appliance, and CloudBoost appliance. Resolvable means that components are accessible through both forward (A) and reverse (PTR) look-ups.

Review the following prerequisites prior to configuring NetWorker in a VMware Cloud on AWS. Also, ensure that you plan your firewall according to these prerequisites.

VMware Cloud on AWS web portal console
In the VMware Cloud on AWS web portal console, note the following requirements:

- If using NSX-T, configure the DNS to resolve to the internal IP address of the vCenter server. Navigate to **SDDC Management** > **Settings** > **vCenter FQDN** and select the **Private vCenter IP address** so that you can directly access the management network over the built-in firewall. Additionally, ensure that you open TCP port 443 of the vCenter server in both the management gateway and the compute gateway.
- By default, there is no external access to the vCenter Server system in your SDDC (Software Defined Data Center). You can open access to your vCenter Server system by configuring a firewall rule. Set the firewall rule in the compute gateway of VMware Cloud on AWS to enable communication to the vCenter public IP address from the desired logical network of your SDDC. The NetWorker server will not allow you to add the vCenter Server if this firewall rule is not configured in the SDDC.
- The default compute gateway firewall rules prevent all virtual machine traffic from reaching the internet. To allow your NetWorker Server virtual machine to connect to the internet, you need to create a compute gateway firewall rule to allow

outbound traffic on the logical network that your NetWorker Server virtual machine is connected to.

- Configure DNS to allow machines in your SDDC to resolve fully-qualified domain names (FQDNs) to IP addresses belonging to the internet. The NetWorker Server will not allow you to add the vCenter Server using the server's public FQDN or IP address if the DNS server is not configured in your SDDC.
- It is recommended that you deploy the Data Domain system as a virtual appliance in the Amazon VPC (Virtual Private Cloud) of your choice. During the SDDC creation, ensure that you connect your SDDC to an AWS account, and select a VPC and subnet within that account.
- The Data Domain system running in your Amazon VPC must be connected to your VMware SDDC by using the VMware Cloud Elastic Network Interfaces (ENIs), allowing your SDDC and services in the AWS VPC and subnet in your AWS account to communicate without requiring the routing of traffic through the internet gateway. The same ENI channel is recommended for access to Data Domain systems (for the vProxy solution) and access to cloud object storage (for the CloudBoost solution). Detailed steps on configuring ENI are provided by VMware at https://vmc.vmware.com/console/aws-link.
- Ensure that you configure the inbound and outbound firewall rules of your compute gateway for Data Domain connectivity if DDVE is running in your Amazon VPC.

Amazon AWS web portal

In the AWS web portal, note the following requirements:

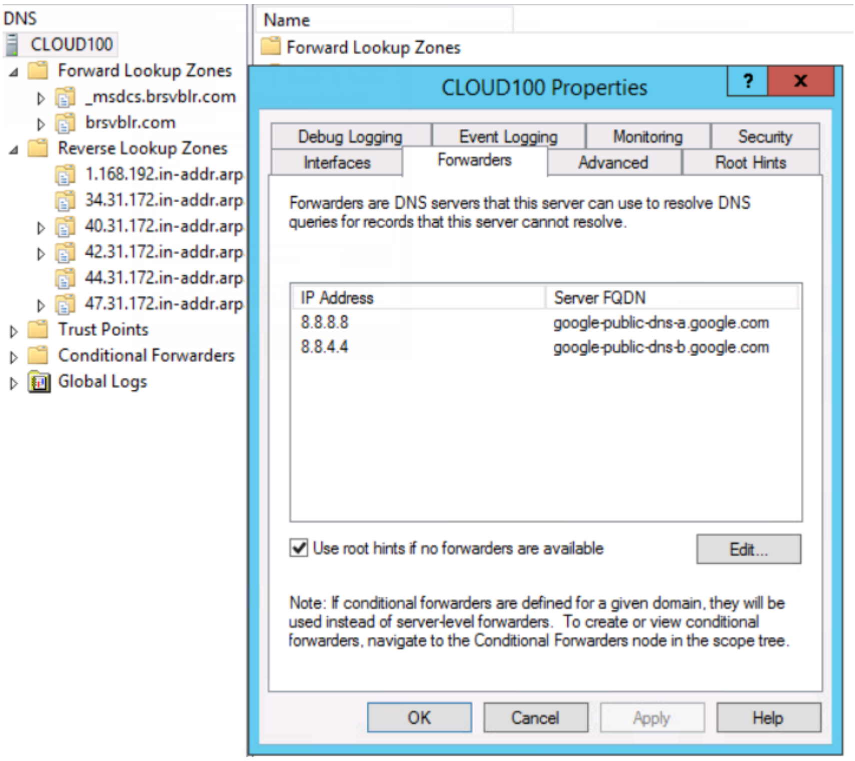
- Configure the inbound and outbound firewall rules of your Amazon VPC security group to provide connectivity between the VMware SDDC compute gateway and Data Domain connectivity if Data Domain is running in your Amazon VPC.
- If cloning from one Data Domain system to another, ensure that you configure the inbound rule for the security group in AWS to allow all traffic from the respective private IPs of Data Domain Virtual Editions running in your Amazon VPC.
- If you have more than one Data Domain running in AWS to perform cloning, then ensure that both Data Domain systems can ping each other using the FQDNs.

vCenter server inventory

In the vCenter Server inventory of your SDDC, note the following requirements:

- An internal DNS name lookup server must be running inside the vCenter inventory. This will be referenced by all the workloads running in the VMware SDDC.
- The internal DNS server must have Forwarders enabled to access the internet. This is required in order to resolve the vCenter Server's public FQDN

Figure 168 Enable internet access for Forwarders



Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
8.8.8.8	google-public-dns-a.google.com
8.8.4.4	google-public-dns-b.google.com

☑ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS

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

Before you begin

Review the Pre-requisites section.

Procedure

1. Log in to the HTML5 **vSphere Web Client** with the cloudadmin account credentials.
2. From the top-left of the window, select **Menu**, and then select **Hosts and Clusters** from the drop-down.
3. In the left inventory pane, expand the vCenter, and then expand the compute resource pool inside your SDDC cluster.
4. Right-click the resource pool where you want to deploy the OVA and select **Deploy OVF template**.
5. On the **Select an OVF template** window, type a URL path to the OVA package, or click **Choose Files** and navigate to the OVA package location, and then click **Next**.
6. On the **Select a name and folder** window, specify a name for the virtual appliance, and the inventory location (for example a virtual machine folder). Click **Next**.
7. On the **Select a compute resource** window, select the vApp or resource pool where you want to deploy the OVA, and then click **Next**.

8. On the **Review details** window, review the product details such as the product name, version, vendor, publisher, and download size, and then click **Next**.
9. On the **License agreements** window, review and accept the EULA, and then click **Next**.
10. On the **Select storage** window, select the disk format and the destination datastore where the virtual appliance files will be stored, and then click **Next**.

    It is recommended that you select **Thick Provision Lazy Zeroed** to ensure that amount of storage space allocated to the virtual appliance is available.
11. On the **Select networks** window, select the **Destination Network**. Provide the IP address in the text box and click **Next**.
12. On the **Customize template** window, expand **Networking properties**, and then specify the following attributes:

    a. In the **Network IP address** field, specify the IP address for the vProxy appliance.

    b. In the **Default gateway** field, specify the IP address of the gateway host.

    c. In the **Network Netmask/Prefix** field, specify the netmask for an IPv4 Network IP address. vProxy backups do not support the use of IPv6 Network IP addresses.

    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 password for the root account or leave the field blank to use the default password. The default password is `changeme`.

    b. In the **Admin password** field, specify a password for the admin account or leave the field blank to use the default password. The default password is `a3dp@m8n`.
15. Click **Next**.

    The **Ready to Complete** window displays.
16. On the **Ready to Complete** window, review the deployment configuration details, and then click **Finish**.

Results

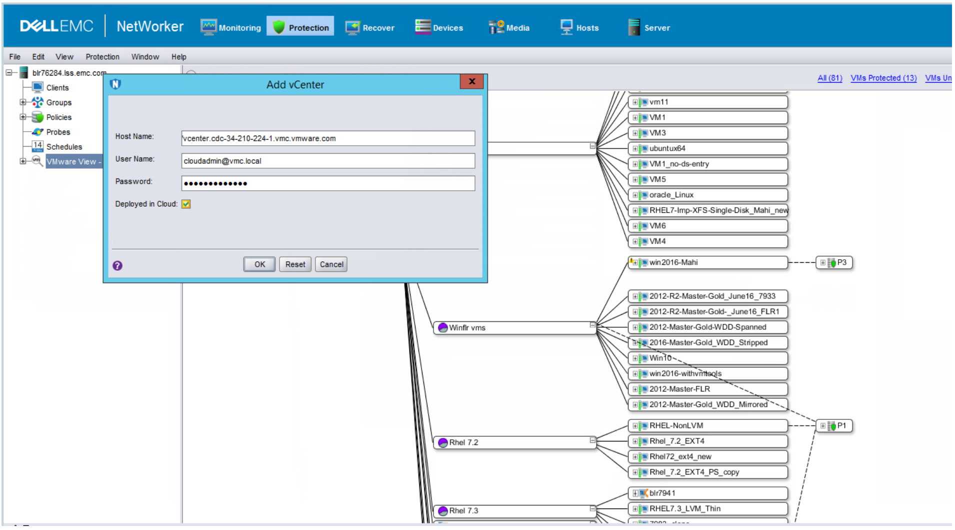
The **Deploying template** task appears in the vCenter and provides status information about the deployment.

NetWorker VMware Protection for VMware Cloud on AWS best practices

Observe the following best practices when using NetWorker to protect virtual machines running in VMware Cloud on AWS:

- When deploying or configuring the NetWorker Server or vProxy, ensure that you specify the DNS server IP that points to the internal DNS server running in the vCenter inventory.
- Ensure that both forward and reverse lookup entries in the internal DNS server are in place for all of the required components, such as the NetWorker Server, NetWorker vProxy appliance, Data Domain Virtual Edition (DDVE), and CloudBoost appliance.
- When adding the vCenter Server to NMC's **VMware View**, ensure that you select the **Deployed in Cloud** checkbox. Note that this setting is required for any vCenter Servers running in VMware Cloud on AWS, If you do not select this option, then some NetWorker operations will fail in the VMware Cloud on AWS.

  Figure 169 Add a vCenter Server to VMware View with Deployed in Cloud enabled



Add vCenter

Host Name: vcenter.cdc-34-210-224-1.vmc.vmware.com

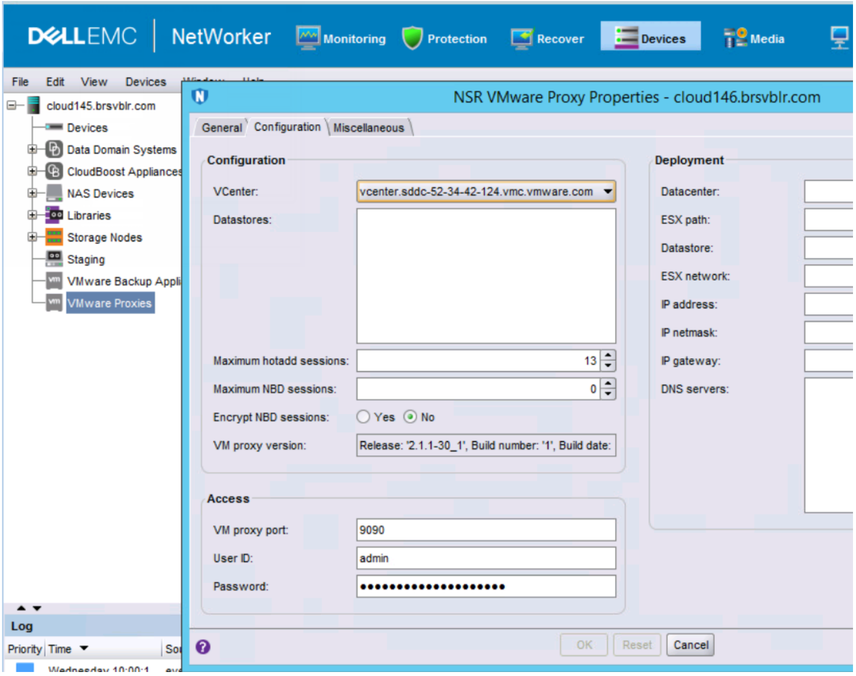
User Name: cloudadmin@vmc.local

Password: ••••••••••••••

Deployed in Cloud: ☑

- 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 170 NSR VMware Proxy Properties



NSR VMware Proxy Properties - cloud146.brsvblr.com

Configuration

VCenter: vcenter.sddc-52-34-42-124.vmc.vmware.com

Datastores:

Maximum hotadd sessions: 13

Maximum NBD sessions: 0

Encrypt NBD sessions: ○ Yes ● No

VM proxy version: Release: '2.1.1-30_1', Build number: '1', Build date:

Access

VM proxy port: 9090

User ID: admin

Password: ••••••••••••••••••••

Deployment

Datacenter:

ESX path:

Datastore:

ESX network:

IP address:

IP netmask:

IP gateway:

DNS servers:

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.
- vProxy appliance configured with dual stack or IPv6 only is not supported.
- Application-consistent data protection for MS-SQL with the vProxy appliance.
- If the datacenter is placed inside a folder in the SDDC, image backup and restore is not supported

APPENDIX B

Regular expressions for NetWorker vProxy dynamic policies rule definitions

This appendix includes the following topic:

Regular expression syntax accepted by dynamic policy rule definition

Rule definitions for NetWorker vProxy policies with dynamic association enabled can contain regular expressions.

The following tables list the acceptable rules, syntax, and grammar to use when writing such regular expressions.

Types of single-character expressions	Examples
Any character, possibly including newline (s=true)	.
character class	[xyz]
negated character class	[^xyz]
Perl character class	\d
negated Perl character class	\D
ASCII character class	[[:alpha:]]
negated ASCII character class	[[:^alpha:]]
Unicode character class (one-letter name)	\pN
Unicode character class	\p{Greek}
negated Unicode character class (one-letter name)	\PN
negated Unicode character class	\P{Greek}

Composites	
xy	x followed by y
x|y	x or y (prefer x)

Repetitions	
x*	zero or more x, prefer more
x+	one or more x, prefer more
x?	zero or one x, prefer one
x{n,m}	n or n+1 or ... or m x, prefer more
x{n,}	n or more x, prefer more
x{n}	exactly n x
x*?	zero or more x, prefer fewer
x+?	one or more x, prefer fewer
x??	zero or one x, prefer zero
x{n,m}?	n or n+1 or ... or m x, prefer fewer
x{n,}?	n or more x, prefer fewer

Repetitions	
x{n}?	exactly n x

Note

The counting forms x{n,m}, x{n,}, and x{n} reject forms that create a minimum or maximum repetition count above 1000. Unlimited repetitions are not subject to this restriction.

Grouping	
(re)	numbered capturing group (submatch)
(?P<name>re)	named & numbered capturing group (submatch)
(?:re)	non-capturing group
(?flags)	set flags within current group; non-capturing
(?flags:re)	set flags during re; non-capturing

Flags	
i	case-insensitive (default false)
m	multi-line mode: ^ and $ match begin/end line in addition to begin/end text (default false)
s	let . match \n (default false)
U	ungreedy: swap meaning of x* and x*? , x+ and x+? , etc (default false)

Flag syntax is xyz (set) or -xyz (clear) or xy-z (set xy , clear z).

Empty strings	
^	at beginning of text or line (m =true)
$	at end of text (like \z not \Z) or line (m =true)
\A	at beginning of text
\b	at ASCII word boundary (\w on one side and \W , \A , or \z on the other)
\B	not at ASCII word boundary
\z	at end of text

Escape sequences	
\a	bell (≡ \007)
\f	form feed (≡ \014)
\t	horizontal tab (≡ \011)
\n	newline (≡ \012)
\r	carriage return (≡ \015)

Escape sequences	
\v	vertical tab character (≡ \013)
*	literal * , for any punctuation character *
\123	octal character code (up to three digits)
\x7F	hex character code (exactly two digits)
\x{10FFFF}	hex character code
\C	match a single byte even in UTF-8 mode
\Q...\E	literal text ... even if ... has punctuation

Character class elements	
x	single character
A-Z	character range (inclusive)
\d	Perl character class
[:foo:]	ASCII character class foo
\p{Foo}	Unicode character class Foo
\pF	Unicode character class F (one-letter name)

Named character classes as character class elements	
[\d]	digits (≡ \d)
[^\d]	not digits (≡ \D)
[\D]	not digits (≡ \D)
[^\D]	not not digits (≡ \d)
[[:name:]]	named ASCII class inside character class (≡ [:name:])
[^[:name:]]	named ASCII class inside negated character class (≡ [:^name:])
[\p{Name}]	named Unicode property inside character class (≡ \p{Name})
[^\p{Name}]	named Unicode property inside negated character class (≡ \P{Name})

Perl character classes (all ASCII-only)	
\d	digits (≡ [0-9])
\D	not digits (≡ [^0-9])
\s	whitespace (≡ [\t\n\f\r])
\S	not whitespace (≡ [^\t\n\f\r])
\w	word characters (≡ [0-9A-Za-z_])
\W	not word characters (≡ [^0-9A-Za-z_])

ASCII character classes	
[[:alnum:]]	alphanumeric (≡ [0-9A-Za-z])
[[:alpha:]]	alphabetic (≡ [A-Za-z])
[[:ascii:]]	ASCII (≡ [\x00-\x7F])
[[:blank:]]	blank (≡ [\t])
[[:cntrl:]]	control (≡ [\x00-\x1F\x7F])
[[:digit:]]	digits (≡ [0-9])
[[:graph:]]	graphical (≡ [!-~] ≡ [A-Za-z0-9!"#$%&'()*+, \-./:;<=>?@[\\\]^_`{|}~])
[[:lower:]]	lower case (≡ [a-z])
[[:print:]]	printable (≡ [-~] ≡ [[:graph:]])
[[:punct:]]	punctuation (≡ [!-/:-@[-`{-~])
[[:space:]]	whitespace (≡ [\t\n\v\f\r])
[[:upper:]]	upper case (≡ [A-Z])
[[:word:]]	word characters (≡ [0-9A-Za-z_])
[[:xdigit:]]	hex digit (≡ [0-9A-Fa-f])

Unicode character class names--general category	
C	other
Cc	control
Cf	format
Co	private use
Cs	surrogate
L	letter
Ll	lowercase letter
Lm	modifier letter
Lo	other letter
Lt	titlecase letter
Lu	uppercase letter
M	mark
Mc	spacing mark
Me	enclosing mark
Mn	non-spacing mark
N	number
Nd	decimal number
Nl	letter number

Unicode character class names--general category	
No	other number
P	punctuation
Pc	connector punctuation
Pd	dash punctuation
Pe	close punctuation
Pf	final punctuation
Pi	initial punctuation
Po	other punctuation
Ps	open punctuation
S	symbol
Sc	currency symbol
Sk	modifier symbol
Sm	math symbol
So	other symbol
Z	separator
Zl	line separator
Zp	paragraph separator
Zs	space separator

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

GLOSSARY

This glossary contains terms related to disk storage subsystems. Many of these terms are used in this manual.

B

backup

1. Duplicate of database or application data, or an entire computer system, stored separately from the original, which can be used to recover the original if it is lost or damaged.
2. Operation that saves data to a volume for use as a backup.

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

C

changed block tracking A VMkernel feature that keeps track of the storage blocks of virtual machines as they change over time. The VMkernel keeps track of block changes on virtual machines, which enhances the backup process for applications that have been developed to take advantage of VMware's vStorage APIs.

checkpoint A system-wide backup, taken only after 24 hours (and at the time of the checkpoint after that first 24 hours have elapsed), that is initiated within the vSphere Web Client and captures a point in time snapshot of the EMC Backup and Recovery appliance for disaster recovery purposes.

client Host on a network, such as a computer, workstation, or application server whose data can be backed up and restored with the backup server software.

client file index Database maintained by the NetWorker server that tracks every database object, file, or file system backed up. The NetWorker server maintains a single index file for each client computer. The tracking information is purged from the index after the browse time of each backup expires.

Console server See NetWorker Management Console (NMC).

D

datastore A virtual representation of a combination of underlying physical storage resources in the datacenter. A datastore is the storage location (for example, a physical disk, a RAID, or a SAN) for virtual machine files.

E

EMC Backup and Recovery Appliance The EMC Backup and Recovery appliance (or VMware Backup Appliance) is an appliance that, when deployed, enables VMware backup and clone policy creation in NMC, and enables the EMC Backup and Recovery plug-in in the vSphere Web Client to assign VMs to those policies.

EMC Data Protection Restore Client A browser that allows for file-level restores, where specific folders and files are restored to the original virtual machine on Windows and Linux virtual machines.

F

file index See client file index.

file-level restore (FLR) Allows local administrators of protected virtual machines to browse and mount backups for the local machine. From these mounted backups, the administrator can then restore individual files. FLR is accomplished using the EMC Data Protection Restore Client. See “Using File Level Restore” on page 63 for additional information on FLR.

G

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

H

hotadd A transport mode where the backup related I/O happens internally through the ESX I/O stack using SCSI hot-add technology. This provides better backup I/O rates than NBD/NBDSSL.

I

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

inactivity timeout Time in minutes to wait before a client is considered to be unavailable for backup.

J

JAR (Java Archive) A file that contains compressed components needed for a Java applet or application.

L

label Electronic header on a volume used for identification by a backup application.

M

managed application Program that can be monitored or administered, or both from the Console server.

media database Database that contains indexed entries of storage volume location and the life cycle status of all data and volumes managed by the NetWorker server.

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

N

NBD A transport mode over LAN that is typically slower than hotadd mode. In NBD mode, the CPU, memory and I/O load gets directly placed on the ESX hosting the production VMs, since the backup data has to move through the same ESX and reach the proxy over the network. NBD mode can be used either for physical or virtual proxy, and also supports all storage types.

NBDSSL A transport mode that is the same as NBD except that the data transferred over the network is encrypted. Data transfer in NBDSSL mode can therefore be slower and use more CPU due to the additional load on the VADP host from SLL encryption/decryption.

NetWorker administrator NetWorker server user who may add, change, or delete NetWorker server users.

NetWorker client See client.

NetWorker Management Console (NMC) Software program that is used to manage NetWorker servers and clients. The NMC server also provides reporting and monitoring capabilities for all NetWorker processes.

NetWorker server Computer on a network that runs the NetWorker server software, contains the online indexes, and provides backup and restore services to the clients and storage nodes on the same network.

NetWorker storage node See storage node.

O

online indexes Databases located on the NetWorker server that contain all the information pertaining to the client backups (client file index) and backup volumes (media index).

R

recover To restore data files from backup storage to a client and apply transaction (redo) logs to the data to make it consistent with a given point-in-time.

S

SAN (storage area network) A transport mode that, when used, completely offloads the backup related CPU, memory or I/O load on the virtual infrastructure. The backup I/O is fully offloaded to the storage layer where the data is read directly from the SAN or iSCSI LUN. SAN mode requires a physical proxy.

save NetWorker command that backs up client files to backup media volumes and makes data entries in the online index.

save set

1. Group of tiles or a file system copied to storage media by a backup or snapshot rollover operation.
2. NetWorker media database record for a specific backup or rollover.

single step backup and recovery See image level backup and recovery.

storage node Computer that manages physically attached storage devices or libraries, whose backup operations are administered from the controlling NetWorker server. Typically a “remote” storage node that resides on a host other than the NetWorker server.

U

update enabler Code that updates software from a previous release. It expires after a fixed period of time.

V

VADP An acronym for vStorage APIs for Data Protection. VADP enables backup software to perform centralized virtual machine backups without the disruption and overhead of running backup tasks from inside each virtual machineVADP supersedes the VCB framework for VMware backups.

vCenter An infrastructure management tool that provides a central point for configuring, provisioning, and managing virtualized IT environments, and is part of the VMware Virtual Infrastructure package.

Virtual machine Software that creates a virtualized environment between the computer platform and its operating system, so that the end user can install and operate software on an abstract machine.

VM An acronym for virtual machine.

VMDK Virtual Machine Disk (VMDK) is a file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. These files are commonly called VMDK files because of the .vmdk extension that VMware adds to these files.

VMware Backup Appliance The VMware Backup Appliance (or EMC Backup and Recovery appliance) is an appliance that, when deployed, enables VMware backup and clone policy creation in NMC, and enables the EMC Backup and Recovery plug-in in the vSphere Web Client to assign VMs to those policies.

VMware Tools Installed inside each virtual machine, VMware Tools enhance virtual machine performance and add additional backup-related functionality.

VSS (Volume Shadow Copy Service) Microsoft technology that creates a point-in-time snapshot of a disk volume. NetWorker software backs up data from the snapshot. This allows applications to continue to write data during the backup operation, and ensures that open files are not omitted.

VSS component A subordinate unit of a writer. **See** writer.

W

writer Database, system service, or application code that works with VSS to provide metadata about what to back up and how to handle VSS components and applications during backup and restore. **See** VSS (Volume Shadow Copy Service).