EMC® NetWorker®

Version 9.0.x

VMware Integration Guide

302-000-701

REV 12

EMC²

Copyright © 1990-2017 Dell Inc. or its subsidiaries. All rights reserved. All rights reserved.

Published January 2017

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

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

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

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

CONTENTS

Figures 7

Tables 9

Preface 11

Chapter 1 Introduction 17
Introduction to VMware support 18
Backup and recovery types 18
Guest-based backup and recovery 20
Recommendations for NetWorker installed in a virtual machine 20
Advantages of guest-based backups 20
Disadvantages of guest-based backups 21
Installation for guest-based backup and recovery 21
Configuration of guest-based backup and recovery 21
Recommendations and considerations for guest-based backup 21
NetWorker VMware Protection 22
Advantages of NetWorker VMware Protection 22
Disadvantages of NetWorker VMware Protection 22
VADP backup and recovery (legacy) 22
Advantages of VADP 22
Disadvantages of VADP 23

Chapter 2 NetWorker VMware Protection 25
Introduction to NetWorker VMware Protection 26
NetWorker VMware Protection tasks 26
System requirements 27
Port requirements 29
Install the VMware Backup Appliance 31
Pre-installation requirements 32
Downloading the OVAs for the VMware Backup Appliance 34
Proxy assignment for backup and recovery 34
Deploying the VMware Backup Appliance 35
Deploy external proxy appliance in vCenter 36
Upgrade the VMware Backup Appliance and vCenter 41
Creating a dedicated vCenter user account and EMC Backup and Recovery role 46
Create vCenter user account 46
Create a customized role 47
vSphere Client user accounts 49
Restrict mapping of datastores 51
EMC Backup and Recovery Configuration Utility 51
Monitoring policy activity 56
Post-installation configuration 57
Starting and stopping services 58
Changing the maintenance window 59

Adding or swapping a NIC for VMXNET 3 on the VMware Backup appliance or external proxy..... 60
Dual NIC support..... 63
Dual vNIC setup and configuration requirements..... 64
Verify vNIC connectivity..... 65
Backing up the VMware environment using NMC..... 66
Setting user privileges for the root user in the NetWorker server.... 66
Accessing VMware Protection in NMC..... 67
VMware Backup Appliance monitoring and properties..... 69
VMware data protection policies in NMC..... 71
VMware View in NMC..... 91
Starting, stopping, and restarting data protection policies..... 96
Decommissioning the VMware Backup Appliance in NMC..... 96
Managing the VMware environment using the vSphere Web Client..... 96
Benefits of EMC Backup and Recovery user interface in the vSphere Web Client..... 97
Deduplication store benefits..... 97
Image-level Backup and Restore..... 98
Connecting to the EMC Backup and Recovery user interface in the vSphere Web Client..... 98
Available tasks in the EMC Backup and Recovery user interface... 99
Assigning virtual machines/VMDKs to a backup..... 109
Manually starting a workflow by using Backup Now..... 111
Stopping a workflow..... 112
Viewing workflow progress..... 112
Restoring the VMware environment..... 112
FULLVM (Image-level) Restore..... 113
File-level restore..... 119
Monitoring EMC Backup and Recovery activity..... 127
Viewing Recent Tasks in the vSphere Web Client..... 127
Viewing Alarms..... 127
Viewing the Event Console..... 128
Shutdown and Startup Procedures..... 129
EMC Backup and Recovery Capacity Management..... 129
Impact of selecting Thin or Thick Provisioned Disks..... 129
Save set lifecycle..... 130
Checkpoints and VMware Backup Appliance rollback..... 131
Creating a checkpoint using the EMC Backup and Recovery user interface..... 131
Rolling back to a checkpoint..... 132
Protecting checkpoints for the VMware Backup appliance..... 132
Cross Sync..... 133
Disaster Recovery..... 134
Disaster Recovery Guidelines..... 134
Disaster recovery without checkpoint..... 135
Preparing the VMware Backup appliance for disaster recovery.... 136
Performing a disaster recovery of the VMware Backup Appliance.... 137
Complete disaster recovery of the VMware Backup Appliance and the Data Domain or tape device..... 138
Recovery from a secondary site..... 139
Best practices and troubleshooting..... 140
Performance and scalability..... 140
NetWorker VMware Protection best practices..... 143
Limitations and unsupported features..... 146

Configuration checklist..... 148
IPv6 considerations.....149
VMware Backup Appliance installation..... 149
AV-NetWorker Communicator (avnwcomm) timeout.....149
Log in to the EMC Backup and Recovery Console as admin instead of root.....150
Launching the EMC Data Protection Restore Client after upgrade on Mozilla Firefox browser..... 150
Launching the EMC Backup and Recovery Configuration Utility after upgrade on Mozilla Firefox browser.....151
Restart the Enterprise Manager Web Application (emwebapp)....152
Log file locations..... 152
NetWorker operations.....153
vCenter server operations.....155
vSphere Client operations.....155
Backup operations.....157
Restore operations.....159
Adding external proxies.....161
Creating and analyzing crashes on Windows 2008 R2..... 161
Changing the Data Domain Boost password.....161
Accessing Knowledge Base Articles..... 161

Chapter 3 VADP Backup and Recovery (legacy) 163
Software and hardware requirements..... 164
Limitations and unsupported features..... 165
Limitations to vCenter on non-English versions of Windows..... 165
Limitation for VADP proxy host on non-English versions of Windows 166
Limitations to vSphere 5.5 and 6.0 support.....166
Transport modes..... 167
Changed Block Tracking (CBT).....168
Independent persistent disks are not backed up.....168
Configuring the VADP proxy host and Hypervisor resource..... 168
Creating a Hypervisor resource from the NetWorker server..... 169
Creating a NetWorker client for the VADP Proxy host by using the Client properties windows.....169
Configuring a virtual client for backup.....173
Configuring a virtual client.....174
Creating a VADP User role in vCenter..... 175
Creating a VADP Proxy role.....175
Assigning the VADP User role to the user specified in the NetWorker Hypervisor resource.....175
Minimum vCenter permissions needed to back up and recover using VADP.....176
Configuring Changed Block Tracking (CBT).....178
Configuring CBT using the variable VADP_DISABLE_CBT..... 178
Configuring CBT using the nsrvadp_modify_vm command..... 179
Enabling CBT using the vSphere Client GUI..... 179
Extending disk size with CBT enabled..... 180
Monitor VMs..... 180
Recovering VADP Backups..... 180
File based recovery of a VM..... 180
Image level (single step) recovery of a full VM.....182
VADP Planning and Best Practices.....189

Recommendations and considerations for VADP backup and recovery....189
Application-level consistent backups....190
Selection of physical vs. virtual proxy....191
VADP snapshot recommendations....192
Recommendations for Data Domain systems....195
Network and Firewall port requirements....196
Memory requirements for the VADP proxy....196
VADP mount point recommendations and space considerations...197
Support for tape drives in a VM....198
Recommendations and considerations for transport modes....199
Performance optimization recommendations....203
VADP proxy access to LUNs....203

Chapter 4 Licensing 205
Virtual environments simplified licensing....206
Physical ESX hosts in non-VADP configurations....206
Guest-based licensing....206
NetWorker VMware Protection licensing....207
VADP licensing....207
Using existing licenses to support VADP after upgrading....207

Glossary 209

FIGURES

1 Firewall configuration (VMware Backup Appliance with internal proxy)..... 30
2 Firewall configuration (VMware Backup Appliance with external proxy)..... 31
3 Selecting the OVA to deploy in vCenter/vSphere Web Client..... 35
4 EMC Backup and Recovery registration 36
5 Registering proxy with the VMware Backup appliance..... 39
6 Unlock the vCenter Registration in the EMC Backup and Recovery Configuration Utility..... 41
7 Upgrading order for NetWorker components when upgrading the VMware Backup Appliance..... 42
8 Take Snapshot in vSphere Client..... 44
9 Connect to ISO in vSphere Client..... 44
10 Accessing online help during upgrade..... 45
11 Hosts and Clusters in the vSphere Web Client..... 50
12 Welcome configuration page..... 52
13 Network Settings configuration page..... 52
14 Time Zone configuration page..... 53
15 EBR Credentials configuration page..... 53
16 vCenter Registration configuration page..... 54
17 NetWorker registration configuration page..... 54
18 Complete configuration page..... 55
19 Complete progress page..... 56
20 Post VMware Backup Appliance configuration..... 58
21 Change Adapter Type..... 61
22 Swap network for NICs in the Virtual Machine Properties window..... 62
23 Routing table with production network gateway..... 63
24 Sample backup and production network traffic flow..... 65
25 NMC Enterprise window..... 67
26 Protection window in the Administration window..... 68
27 VMware Backup appliance health monitoring in the Devices window..... 69
28 NSR VBA Server Properties window..... 70
29 Data Protection Policy..... 72
30 Platinum policy configuration..... 73
31 Gold policy configuration..... 73
32 Silver policy configuration..... 74
33 Bronze policy configuration..... 74
34 Create Group dialog box..... 80
35 VMware protection policy with associated actions..... 91
36 Map view of VMware environment in NMC..... 92
37 Cluster with child elements in VMware View..... 93
38 Filtering results in VMware View..... 93
39 VMware table view..... 94
40 Add group in VMware View..... 95
41 Selecting the Backup Appliance..... 99
42 EMC Backup and Recovery user interface in the vSphere Web Client..... 100
43 VMware Backup Appliance Backup tab..... 101
44 VMware Backup Appliance Restore tab..... 102
45 VMware Backup appliance Reports tab..... 103
46 VMware Backup Appliance Configuration tab..... 105
47 Log view 106
48 Email configuration view..... 107
49 Run Integrity Check option..... 109
50 Selecting virtual machines in the Editing backup policy wizard..... 111
51 Viewing workflow progress in the Task Console..... 112

52 Restore tab in EMC Backup and Recovery user interface.....113
53 Select a backup.....116
54 Set instant access options.....116
55 Ready to complete.....117
56 Emergency Restore window.....119
57 Deploy FLR Agent if not found 119
58 EMC Data Protection Restore Client User Login.....121
59 Select the backups to restore from page.....122
60 Select items to restore page.....123
61 Select destination to restore to page.....123
62 Accessing the restore monitor.....124
63 Restore Monitor panel.....124
64 EMC Data Protection Restore Client Admin Login.....125
65 Select and log in to the destination client.....126
66 Accessing the restore monitor.....126
67 Restore Monitor panel.....126
68 Running an integrity check.....131
69 Roll back to checkpoint.....132
70 Networker registration during new appliance configuration.....135
71 Starting a VMware Backup Appliance disaster recovery.....137
72 Starting a VMware Backup Appliance disaster recovery.....139
73 Entering appliance credentials.....140
74 Apps and Modules tab in NMC.....172
75 Recover Options dialog.....181
76 VMware vCenter restore.....184

TABLES

1 Revision history 11
2 Style conventions 15
3 Comparing Guest based, VADP, and NetWorker VMware Protection 18
4 NetWorker VMware Data Protection tasks 26
5 NetWorker VMware Protection requirements 27
6 Incoming port requirements 29
7 Outgoing port requirements — with external proxies 30
8 Recommended memory and swap space based on storage space utilization 34
9 Minimum required vCenter user account privileges 47
10 Policy status icons 56
11 Description of services running on the VMware Backup Appliance 58
12 Schedule icons 82
13 Schedule icons 87
14 Backup tab column descriptions 100
15 Task Failure column descriptions 103
16 Job Details column descriptions 104
17 Unprotected Clients column descriptions 104
18 Backup appliance detail descriptions 105
19 Email configuration field descriptions 107
20 EMC Backup and Recovery alarms 127
21 Scalability Factors 140
22 Maximum concurrent sessions per VMware Backup Appliance 142
23 Concurrency/parallelism recommendations 142
24 Application information values 169
25 Recovery options that are available based on the virtual client configuration 173
26 VADP backup privileges 176
27 VADP recovery privileges 177
28 Maximum virtual disk file size and corresponding block size for ESX/ESXi 4.0 194
29 Maximum virtual disk size and corresponding block size for ESX/ESXi 4.1 194

Preface

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

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

Note

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

Purpose

This document describes the integration of VMware with NetWorker.

Audience

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

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	September 24, 2015	First release of this document for EMC NetWorker 9.0.1
02	October 7, 2015	Revised instructions for Launching the EMC Backup and Recovery Configuration Utility after upgrade on Mozilla browser Revised the section Port requirements and added diagrams Removed Adobe Flash requirement for the **EMC Data Protection Restore Client** interface
03	November 12, 2015	Updated emergency restore limitations to indicate that the restore must be performed from a primary backup and not a cloned backup Clarified that NetWorker VMware Protection backup does not support independent (persistent and non-persistent) disks Added section Restore to new virtual machine not available for backups that included physical RDM disks Added a note to the section NetWorker VMware Protection best practices to indicate that adding

Table 1 Revision history (continued)

Revision	Date	Description
		containers or Virtual Machines to a policy will automatically enable CBT
04	December 16, 2015	Removed information about how to configure the VMware notification from the VADP Backup and Recovery (legacy) chapter Removed vSphere 6 support for VADP Added section IPv6 considerations Updates to the section System Requirements Added note about manually installing security roll-ups for the external proxy appliance to the topic Deploy external proxy appliance in vCenter
05	December 23, 2015	Updated section Limitations and unsupported features for an issue where backups to DDBoost over WAN fail if TLS is used
06	April 15, 2016	Updated concurrency/parallelism recommendations in the section Performance and Scalability Updated information for the nsrvbaflr command line utility in the section File level restore Updated VMware data protection policies in NMC to modify the order in which you create the data protection policy resources
07	May 20, 2016	Removed section on dual vNIC as this is no longer supported Restored VADP support for vSphere 6
08	June 29, 2016	Updated for the release of NetWorker 9.0.1
09	September 9, 2016	Removed statement from the topic "Protecting checkpoints for the VMware Backup appliance" recommending checkpoint actions as this is no longer the case with NetWorker 9.0 and later.
10	September 20, 2016	Clarified that NetWorker 9.0.1 with VMware vSphere 6.0 (which includes vCenter 6.0 and ESX 6.0) is supported for VADP Updated the steps in "Upgrading the VMware Backup Appliance" to indicate that after the procedure is complete you can remove the ISO image Updated the EMC Backup and Recovery Configuration Utility screens with the latest to show the tool icon, from which you can select vCenter registration to update the username after upgrading vCenter versions Updated "Limitations and unsupported features" with "VMware Backup Appliance versions must be the same when deploying multiple VMware Backup Appliances in same vCenter"

Table 1 Revision history (continued)

Revision	Date	Description
		Added a limitation to the section "Instant access restore (for Data Domain systems only)" to indicate that the free space on the Data Domain system must be equal to or greater than the total disk size of the VM being restored Updated "File based recovery of a VM" to indicate FLR is not supported for a VM operating system containing GPT disks
11	November 18, 2016	Restored information related to dual NIC support along with new requirements and considerations
12	January 27, 2017	Corrected EMC Backup and Recovery Configuration Utility screens to the version for NetWorker 9.0 in the section "Upgrading vCenter from version 5.1 to 5.5" Added steps required in diagnostic mode when configuring a virtual client for VADP.

Related documentation

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

- *EMC NetWorker Online Software Compatibility Guide*
  Provides a list of client, server, and storage node operating systems supported by the EMC information protection software versions. You can access the guide at https://support.emc.com. From the Support by Product pages, search for NetWorker using "Find a Product", and then select the Install, License, and Configure link.
- *EMC NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *EMC NetWorker Network Data Management Protocol (NDMP) User Guide*
  Describes how to use the NetWorker software to provide data protection for NDMP filers.
- *EMC NetWorker Cluster Integration Guide*
  Contains information related to configuring NetWorker software on cluster servers and clients.
- *EMC 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.
- *EMC NetWorker Updating from a Previous Release Guide*
  Describes how to update the NetWorker software from a previously installed release.
- *EMC NetWorker Release Notes*
  Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *EMC NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.

- *EMC 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.
- *EMC NetWorker Performance Optimization Planning Guide*
  Contains basic performance tuning information for NetWorker.
- *EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide*
  Describes how to design and plan for a NetWorker disaster recovery. However, it does not provide detailed disaster recovery instructions. The Disaster Recovery section of the NetWorker Procedure Generator (NPG) provides step-by-step disaster recovery instructions.
- *EMC 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 EMC storage arrays.
- *EMC NetWorker Snapshot Management for NAS Devices Integration Guide*
  Describes how to catalog and manage snapshot copies of production data that are created by using replication technologies on NAS devices.
- *EMC NetWorker VMware Integration Guide*
  Provides planning and configuration information on the use of VMware in a NetWorker environment.
- *EMC NetWorker Error Message Guide*
  Provides information on common NetWorker error messages.
- *EMC NetWorker Licensing Guide*
  Provides information about licensing NetWorker products and features.
- *EMC NetWorker REST API Getting Started Guide*
  Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.
- *EMC NetWorker REST API Reference Guide*
  Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.
- EMC 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.
- EMC 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

EMC uses the following conventions 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

EMC uses the following type style conventions in this document:

Table 2 Style conventions

Bold	Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)
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, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate non-essential information that is omitted from the example

Where to get help

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

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support

Go to EMC Online Support and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities

Go to EMC 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 EMC products.

Your comments

Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Introduction

This chapter contains the following topics:

- Introduction to VMware support 18
- Backup and recovery types 18
- Guest-based backup and recovery 20
- NetWorker VMware Protection 22
- VADP backup and recovery (legacy) 22

Introduction to VMware support

The NetWorker software provides support for three types of backup and recovery solutions for VMware virtual clients. Within each of the following solutions, you can use a NetWorker server residing on a host external to the vSphere server, or you can configure a NetWorker server on a guest host within the vSphere server:

- Guest-based backup and recovery — This option requires you to install a NetWorker client within each virtual machine host. This is a popular way to protect virtual machines due to the same workflow implemented for a physical machine. This means backup configurations and recovery options follow traditional methods that administrators are already familiar with. There are no added configuration requirements however, there is a load consideration on the physical servers and resources, and the requirement of maintaining NetWorker on each guest.
- NetWorker VMware Protection — A NetWorker-integrated VMware backup and monitoring solution. In this solution, when you deploy a VMware Backup Appliance in the vSphere server and register the appliance with NetWorker and vCenter, you can create backup and cloning policies for the VMware Backup Appliance, and assign to virtual machines/VMDKs to policies in NMC. Also, the EMC Backup and Recovery user interface in the vSphere Web Client provides management options. After running the policy, you can then perform image-level and VMDK recoveries from the vSphere Web Client, or file-level recoveries from the EMC Data Protection Restore Client interface.
- VADP (legacy) — Uses vStorage APIs for Data Protection (VADP) technology to offload backup processing from the NetWorker server to a separate backup proxy host. This option also provides notifications when the environment changes. With this option, you can avoid the challenges associated with resource utilization on the server because the proxy host inherits the workload. Also, VADP requires less maintenance than Guest-based backup and recovery because it does not require installation of the NetWorker client on each guest, however, this option is more complex to configure and requires additional hardware and infrastructure.

Backup and recovery types

The following table provides a quick comparison between Guest-based, NetWorker VMware Protection, and VADP (legacy) backup and recovery.

Table 3 Comparing Guest based, VADP, and NetWorker VMware Protection

Option	Guest-based	VADP (legacy)	NetWorker VMware Protection
Recommend for	• Application-consistent backups. • Shared storage not available	• LAN free backups • Disaster recovery • Shared storage environments • Direct backup to tape	• LAN free backups • Disaster recovery • Shared storage environments • Forever incrementals
VMDK level backups	No	Yes	Yes

Table 3 Comparing Guest based, VADP, and NetWorker VMware Protection (continued)

Option	Guest-based	VADP (legacy)	NetWorker VMware Protection
Individual file backups	Yes	Yes for Windows guest OS only	Not applicable
Incremental	File level	File level	Block level, CBT
CBT	Not supported	File level	Block level
Virtual full backup	Not supported	Not supported	Backup is always virtual full
File level restore	Yes	Yes for Windows guest OS only	Yes for Windows and Linux
Deduplication supported	Yes	Yes — Direct backup to Data Domain	Yes — Direct backup to Data Domain. Leverages source as well as target-level Deduplication
Impact on virtual machine	High	Low	Low
Impact on ESX/ ESXi server	High	Medium, if snapshots performed for multiple virtual machines on same ESX/Datastore	Medium, depending on number of snapshots of virtual machines on the same ESX
Backup performance	Slower	Faster - dependent on resources on proxy and whether FLR required	Faster
Additional hardware requirements	No	Uses a physical or virtual proxy, depending on the implementation	Uses internal or external proxies. Each EMC Backup and Recovery appliance and external proxy has 8 internal proxies embedded.
Proxy	Not applicable	Physical (for san backup), virtual (hotadd)	Virtual (hotadd, NBD)
vCenter auto-discovery	Not applicable	Supported	Not supported
Configuration	NetWorker client configured through Client Configuration wizard	Proxy and virtual machine as NetWorker client configured through Client Configuration wizard	EMC Backup and Recovery appliance registration through web interface
Configure virtual machine as a NetWorker client?	Yes	Yes	No
Transport mode supported	Not applicable	hotadd|san|nbd|nbdssl	hotadd (default), nbd(fallback)

Guest-based backup and recovery

Guest-based backup and recovery operations provide a simple and familiar implementation. Traditionally, most physical machine backup and recovery operations have been performed this way, which makes the transition to virtual machine backups using this technology a straightforward task. Regardless of the virtualization technologies involved, VMs are complete OS installations hosted on virtualized hardware. You can protect VMs by using the same basic techniques as their physical counterparts, that is, running a NetWorker client inside the virtual machine. The same OS support rules apply to a physical and virtual machine.

Recommendations for NetWorker installed in a virtual machine

Before you install the NetWorker software on VMs, consider the following recommendations:

- If not using a host outside of ESX as the NetWorker server, provide more CPU reservation and shares for the VM that hosts the NetWorker Server.
- Provide more memory reservation for the VM that hosts the NetWorker Storage Node.
- Set a high restart priority for the VMs that host the NetWorker Server and Storage Node.
- Connect the VMs that host the NetWorker Server, NetWorker Clients and NetWorker Storage Node to the same virtual switch.
- Leverage the guest-based deduplication for NetWorker clients.
- Do not start backups for all VM clients at the same time; stagger the backups to reduce the impact on the ESX/ESXi server.

Advantages of guest-based backups

Guest-based backups provide the following advantages:

- Supports database and application backups. The configuration is as simple as installing and configuring the appropriate NetWorker database or application module on the guest host.
- Supports single file backup and restore.
- The NetWorker server and client file index correctly references all protected data to the originating virtual machine.
- Supports the restore of individual files directly to the VM.
- Easy to configure Incremental backups.
- Supports advanced VMware features and configurations, like Distributed Resource Scheduling (DRS) and VMotion, with no impact on the performance of NetWorker.
- Supports host-based source deduplication.
- Supports all NetWorker directives.
- Easy to perform recovery; the recovery process is exactly the same as when you recover files to a physical host, and allows individual users to perform their own recoveries.

Disadvantages of guest-based backups

Disadvantages of guest-based backups include:

- No support for image level backup and recovery. Image level backup and recovery is mostly used to support disaster recovery.
- The backup processing load on one virtual machine will negatively impact system resources available to all VMs hosted on the same physical ESX server, even when using source-based deduplication.
- Resource-intensive backups often place a heavy load on shared network and CPU resources.
- Client software installed on each virtual machine needs to be maintained and updated.
- The virtual machine must be powered on for backup processing to occur.
- No support for Bare Metal Recovery (BMR).

Installation for guest-based backup and recovery

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

Configuration of guest-based backup and recovery

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

Recommendations and considerations for guest-based backup

Guest-based backup activities on a single virtual machine can create a significant load on the parent ESX Server and, therefore, indirectly impact every other virtual machine hosted on the ESX Server. Configure backup schedules to limit the number of simultaneous backup jobs that run on each physical ESX Server. For example, you can use NetWorker backup groups to back up a selection of VMs across multiple ESX servers in order to minimize the impact on individual ESX servers at different times and maximize the throughput of the backup.

NetWorker includes technology you can use to minimize or eliminate full backups. When you perform only incremental backups, NetWorker copies only the data that has changed since the previous backup to the storage node. This significantly decreases the I/O associated with backups and the amount of backup network traffic. Also, you can leverage guest-based deduplication to minimize the impact on the ESX servers shared resources by eliminating CPU and memory contention.

This backup technique is very effective for database and application backups. Configuring a database or application backup in a VM is essentially the same as configuring the same database and application backup on a physical machine. This technique simplifies and enhances database and application backups, often providing incremental capabilities and restores directly to the VM. Guest-based database deduplication is also supported for databases to help minimize impact on an ESX servers resources.

NetWorker VMware Protection

The NetWorker VMware Protection solution provides a VMware Backup Appliance that, when deployed and configured, allows you to set up backup and cloning policies, and then assign virtual machines/VMDKs to those policies. This solution makes use of multiple applications, including NMC's **Administration** window, the **EMC Backup and Recovery** user interface in the **vSphere Web Client**, and the **EMC Data Protection Restore Client**.

Advantages of NetWorker VMware Protection

The NetWorker VMware Protection solution provides the following advantages:

- Supports forever incremental backups.
- Uses existing AVE technology.
- Supports file-level recovery (FLR) directly into the virtual machine on Linux and Windows.
- Uses advanced FLR to perform recoveries from other virtual machines to a virtual machine.

Disadvantages of NetWorker VMware Protection

Disadvantages of the NetWorker VMware Protection solution include:

- No support for upgrading from the VMware VDP solution to the NetWorker VMware Protection solution.
- The VMware Backup Appliance cannot co-exist with VMware VDP or any third-party backup plug-in within the same vCenter server.

VADP backup and recovery (legacy)

NetWorker provides an alternate client backup technology for VMs in conjunction with VADP technology from VMware.

With VADP, you can perform backups from a VADP backup proxy server, which can be a physical or virtual machine, using the VMware snapshot technique (a point-in-time copy of the VM). You can use VADP with a vCenter Server.

Advantages of VADP

VADP provides the following advantages:

- Offloads backup processes from the ESX server to a VADP proxy server.
- Eliminates the need for a backup window by using VMware virtual machine snapshot technology.
- Supports backups of all files residing in VMs running a Microsoft Windows guest operating system using save set ALLVMFS.
- Supports backups of specific files or folders for VMs running a Microsoft Windows guest operating system.
- Supports incremental and non level-0 backups for VMs running on a Microsoft Windows guest operating system.

Note

The incremental and non level-0 backups allow recovery of files. Recovery of the full VM is only supported for level-0 *FULL* save set backups.

- Supports image level backups for VMs running any guest operating system supported by VMware.
- Supports the ability to recover individual files from an image level backup (Windows NTFS only).
- Supports deduplication across VMs and servers.
- Minimizes the backup impact on the target VM and other VMs hosted on the same ESX server.
- There is no need to install NetWorker software on each virtual machine.
- Provides LAN-Free backup because the VADP proxy server can be connected to the SAN through a Fibre Channel adapter.
- Supports advanced VMware features and configurations such as Distributed Resource Scheduling (DRS) and VMotion, which do not impact the performance of NetWorker.

Disadvantages of VADP

Disadvantages of VADP include:

- No support for File-level restore from Image-level backup of non-NTFS system.
- No support for Image-level recovery of an entire VM from an incremental CBT backup.

CHAPTER 2

NetWorker VMware Protection

This chapter contains the following topics:

- Introduction to NetWorker VMware Protection 26
- System requirements 27
- Port requirements 29
- Install the VMware Backup Appliance 31
- Creating a dedicated vCenter user account and EMC Backup and Recovery role 46
- Restrict mapping of datastores 51
- EMC Backup and Recovery Configuration Utility 51
- Post-installation configuration 57
- Adding or swapping a NIC for VMXNET 3 on the VMware Backup appliance or external proxy 60
- Dual NIC support 63
- Verify vNIC connectivity 65
- Backing up the VMware environment using NMC 66
- Managing the VMware environment using the vSphere Web Client 96
- Restoring the VMware environment 112
- Monitoring EMC Backup and Recovery activity 127
- Shutdown and Startup Procedures 129
- EMC Backup and Recovery Capacity Management 129
- Checkpoints and VMware Backup Appliance rollback 131
- Cross Sync 133
- Disaster Recovery 134
- Best practices and troubleshooting 140

Introduction to NetWorker VMware Protection

NetWorker VMware Protection is a NetWorker-integrated VMware backup, monitoring and recovery solution. This solution allows you to create backup and cloning policies for a VMware Backup Appliance using NMC's **Administration** window, and then assign those policies to Datacenters, Clusters, virtual machines and VMDKs.

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 **EMC Backup and Recovery** user interface in the **vSphere Web Client**, or file-level recoveries from the **EMC Data Protection Restore Client** user interface.

EMC strongly recommends upgrading the NetWorker server, storage node, and VMware Backup Appliance to the latest NetWorker 9.0 release to use the NetWorker VMware Protection solution.

NetWorker VMware Protection tasks

The following table compares tasks in NMC's **Administration** window with tasks in the **vSphere Web Client** and the **EMC Data Protection Restore client**.

Table 4 NetWorker VMware Data Protection tasks

Program/Role	Task
NMC Administration window	• Create and edit 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 • 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 **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 the policy workflow created in NMC's **Administration** window. • Start an adhoc 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 VM (image-level) backup

Table 4 NetWorker VMware Data Protection tasks (continued)

Program/Role	Task
	• Restore a VMDK backup • Instant restore from a Data Domain system
EMC Data Protection Restore Client	• Perform file-level restores
CLI	• Perform FULL VM and VMDK-level backup and restore • Perform file-level restores • Perform proxy deployment

System requirements

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

When you install or upgrade NetWorker and deploy the VMware Backup Appliance, 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 9.0.1, install or upgrade to the latest OVA version 1.5.1.7. NetWorker 9.0.1 is not backwards compatible with earlier versions of the VMware Backup Appliance.

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 5 NetWorker VMware Protection requirements

Component	Requirements
NetWorker	9.0.1 or later 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)	• CPU: 4 * 2 GHz • Memory: 8GB • Disks: 3* 250 GB • Backup storage capacity: 0.5 TB • OS: 250 GB • Internet Protocol: IPv4 only or IPv6 only; dual stack not supported

Table 5 NetWorker VMware Protection requirements (continued)

Component	Requirements
VMware Backup Appliance (4 TB OVA)	• CPU: 4 * 2 GHz • Memory: Refer to Table 8 on page 34 • Disks: 6 * 1 TB • Backup storage capacity: 4 TB • OS: 250 GB • Internet Protocol: IPv4 only or IPv6 only; dual stack not supported
Proxy Appliance	• CPU: 4 * 2 GHz • Memory: 4 GB • Disks: 2 disks (16 GB and 1 GB) • Internet Protocol: IPv4 only or IPv6 only; dual stack not supported
vCenter server	• Version 5.5 and later • 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 access the EMC Backup and Recovery user interface.
ESX/ESXi server	• Version 5.5.x; Version 6 build 3247720 only (Update 1 Patch 22) • 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 5.5 and later

Table 5 NetWorker VMware Protection requirements (continued)

Component	Requirements
	Note The EMC Data Domain Boost Compatibility Guide, available at http://support.emc.com, provides detailed information on NetWorker and DD Boost version compatibility. • DDBoost user requires administrator privileges

Port requirements

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

Table 6 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
EMC Data Protection Restore Client interface	VMware Backup Appliance	8543	File-level recovery (FLR)
EMC Backup and Recovery Configuration Utility	VMware Backup Appliance	8580, 8543	VMware Backup Appliance configuration
vCenter	VMware Backup Appliance	7778, 7779, 8509, 9443	EMC Backup and Recovery user interface in the vSphere Web Client

Figure 1 Firewall configuration (VMware Backup Appliance with internal proxy)

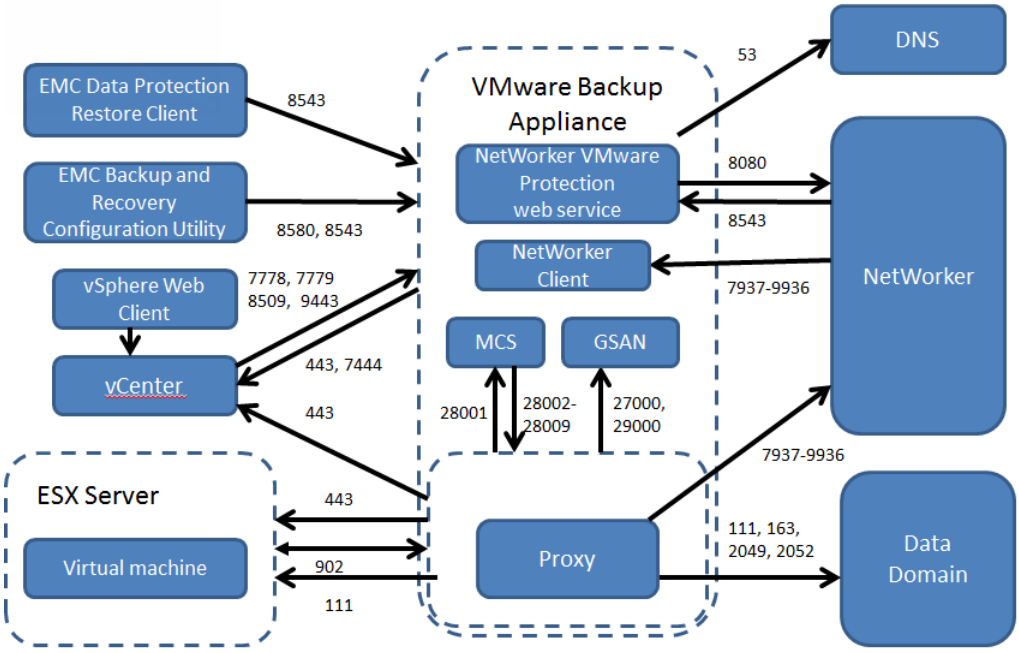


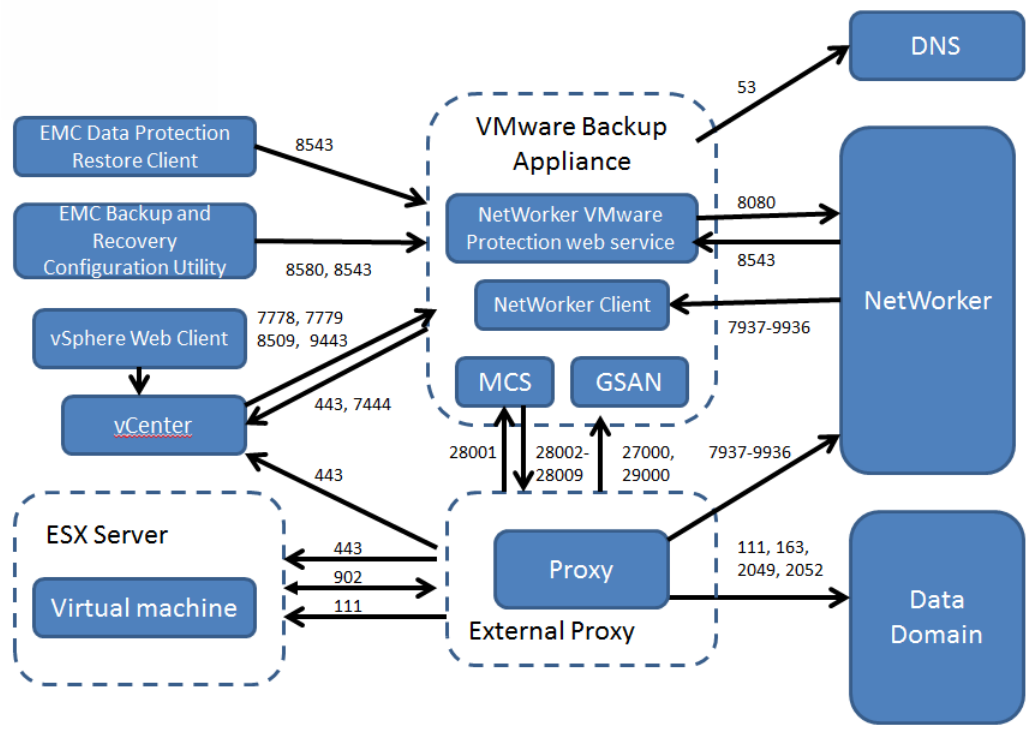
Table 7 Outgoing port requirements — with external proxies

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
VMware Backup Appliance	VMware SSO	7444	Auth to SSO
VMware Backup Appliance and external proxy	vCenter	443, 7444	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

Table 7 Outgoing port requirements — with external proxies (continued)

From	To	Port	Purpose
External proxy	VMware Backup Appliance	28001, 27000, 29000	External proxy to MCS and GSAN

Figure 2 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 **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.

Install the VMware Backup Appliance

To make use of all features of the NetWorker VMware Protection solution, you must install a NetWorker 9.0.1 or later VMware Backup Appliance. This section describes how to download and deploy the VMware Backup Appliance and external proxies in order to use the NetWorker VMware Protection solution. This section also provides instructions for upgrading the VMware Backup Appliance.

Pre-installation requirements

Before you deploy the VMware Backup Appliance, review the pre-installation requirements in this section.

VMware Backup Appliances best practices

Review the following best practices specific to VMware Backup Appliances to ensure successful deployment before you download and install the VMware Backup Appliance and external proxy appliance.

- Ensure that the NetWorker server, storage node, and VMware Backup Appliance are at the same version.
  When you upgrade NetWorker and the VMware Backup Appliance, upgrade in the following order and ensure that each component is at the same version:
  - NetWorker server
  - NetWorker storage node
  - VMware Backup Appliance along with external proxies
- Ensure that the DDOS version is compatible with the NetWorker server and VMware Backup Appliance version. The NetWorker 9.0 VMware Backup Appliance supports DDOS 5.5 and later.
  The EMC Data Domain Boost Compatibility Guide, available at http://support.emc.com, 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 VM in the environment, even if these hosts are not physically connected.
- For registration of the VMware Backup Appliance with vCenter, consider using a Service account.
- Deploy the VMware Backup Appliance on shared VMFS5 or higher to avoid block size limitations.
- For better performance, EMC recommends using 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 9.0.1 software.

Note

EMC does not recommend configuring a NetWorker 9.0.1 VMware Backup Appliance and an OVA 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 8 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
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 10 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.

Deploying 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

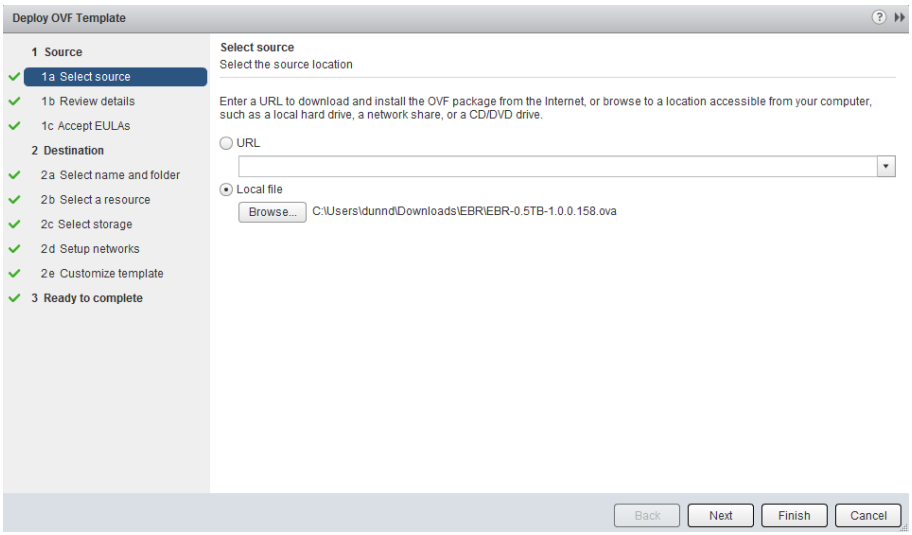
The VMware Backup Appliance does not include security roll-ups. As a result, you may also be required to manually install a security roll-up after you complete the appliance deployment. You can access the latest version of the ESA for the security roll-up, titled "EMC Avamar and NetWorker Security Update 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 3 Selecting the OVA to deploy in vCenter/vSphere Web Client



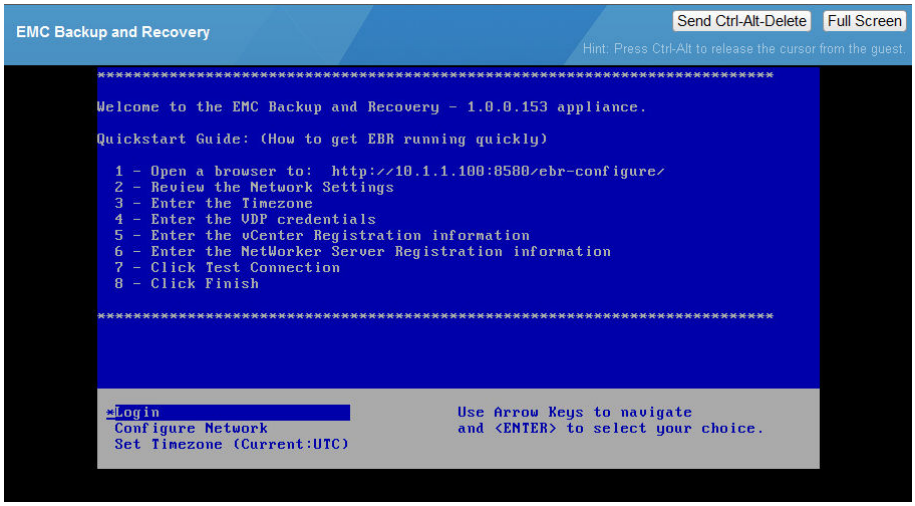
4. In the filetype drop-down, select OVA Packages then navigate to the directory that contains the ova files. Select the file and then click **Open**.
5. On the **Deploy OVF Template** window, click **Next**.
6. On the **Review Details** window, click **Next**.
7. Accept the EULA and click **Next**.
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**. EMC recommends 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 4 EMC Backup and Recovery registration



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 34.

   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 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.

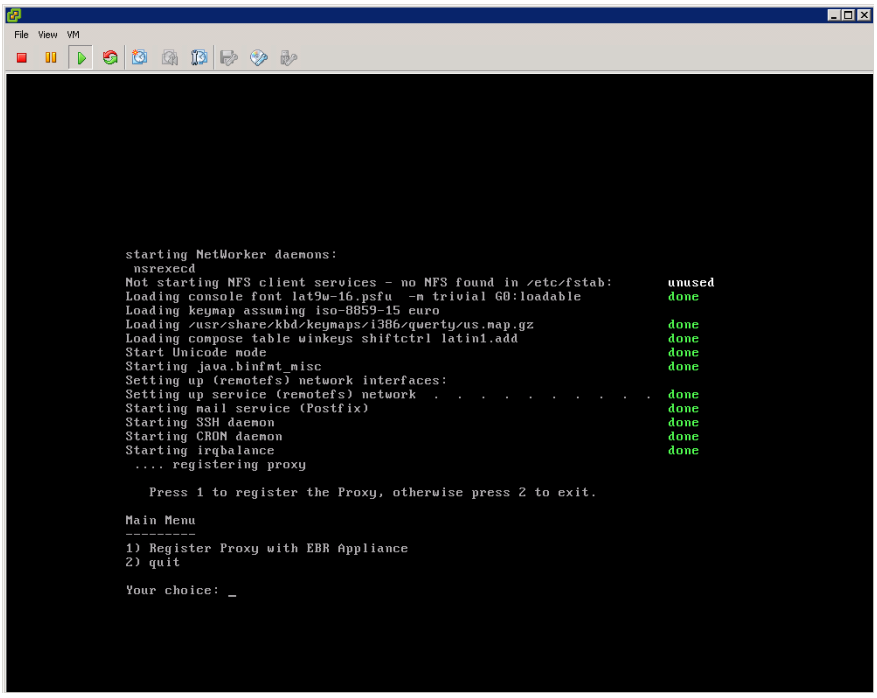
    This might take several minutes.

    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 5 Registering proxy with the VMware Backup appliance



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 36, 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
```

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 9.0 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.

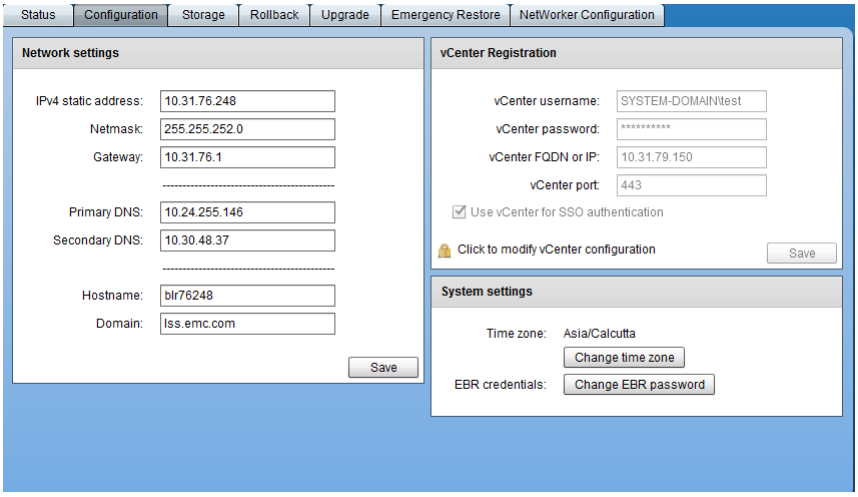
Upgrading vCenter from version 5.1 to 5.5

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.
  2. Click the **Configuration** tab and unlock the vCenter registration.
  3. Change the username to `DOMAIN\test`, and then save and reboot the appliance.

Figure 6 Unlock the vCenter Registration in the EMC Backup and Recovery Configuration Utility



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, perform the following steps to upgrade vCenter to 6.0 and the VMware Backup Appliance to the latest version for NetWorker 9.0.

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. 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.

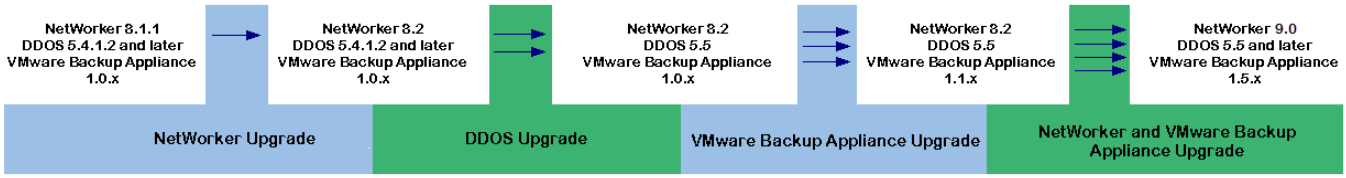
Procedure

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 NetWorker 9.0.

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 7 Upgrading order for NetWorker components when upgrading the VMware Backup Appliance



Before upgrading, also review the following considerations:

- VMware Backup Appliance version 1.5.x is only compatible with NetWorker 9.0.1 and higher.

  Note

  If you upgrade to NetWorker 9.0.1, you must also upgrade the VMware Backup Appliance to version 1.5.x.

- 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, the 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 5.5 if you upgrade to the VMware Backup Appliance 1.1.x or 1.5.x.
- 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. Make note of the current NIC configuration including NIC type, IPs, operating system routes and any other custom settings before deploying a new OVA.

Upgrading 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. EMC does not recommend manually changing 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.

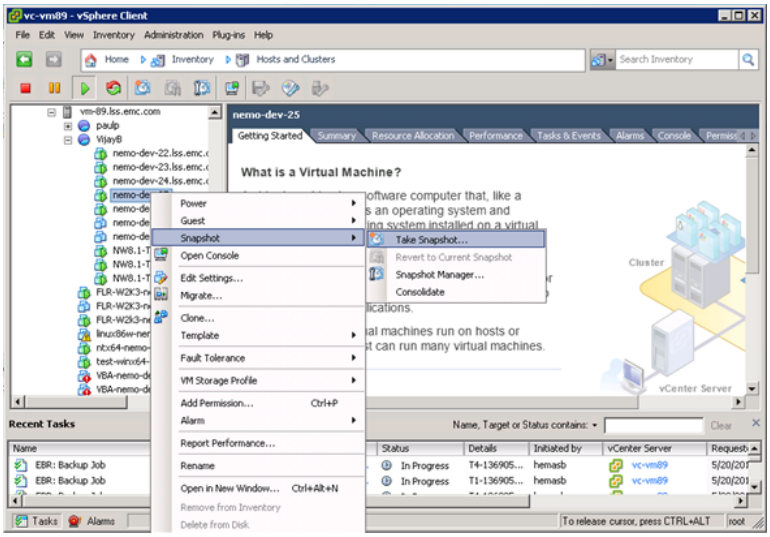
   a. Select the **Configuration** tab.

   b. Select the **Run integrity Check** option, as shown in Running an integrity check on page 109.

   c. Make sure that the integrity check passes successfully.

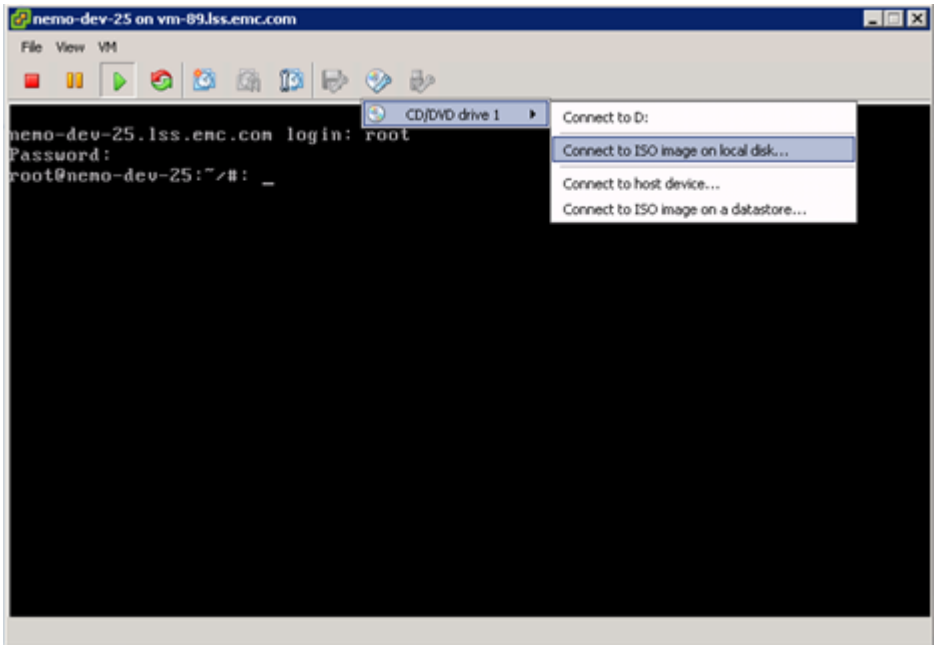
4. Shut down the VMware Backup appliance, and then create a snapshot of the EMC Backup and Recovery virtual machine by right-clicking the VM in the **vSphere Client** and selecting **Snapshot** > **Take Snapshot...**, as shown in the following figure.

Figure 8 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 9 Connect to ISO in vSphere Client



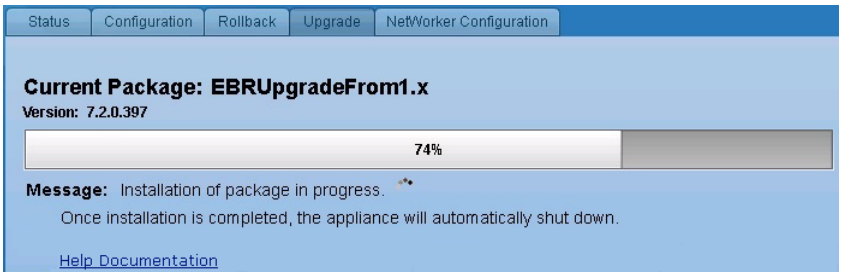
8. Open the **EMC Backup and Recovery Configuration Utility** window. See Post-installation configuration on page 57 for more information.
9. Navigate to the **Upgrade** tab and click **Check Upgrades**. The available upgrade package appears.
10. Navigate to the **Status** tab to ensure all services 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 10 Accessing online help during upgrade



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.

Enable VMware View in NMC's Administration window after upgrading by creating a NSR Hypervisor resource

When you upgrade the NetWorker server to NetWorker 9.0.1 or later 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.

Perform one of the following to create the NSR Hypervisor resource.

- Download and deploy a NetWorker 9.0.1 or later VMware Backup Appliance from vCenter, following the registration steps described in EMC Backup and Recovery Configuration Utility on page 51.
- Manually create a NSR Hypervisor resource by using the `nsradmin` program. Configuring the VADP proxy host and Hypervisor resource on page 168 provides steps to create the NSR Hypervisor resource.

Note

If you created a NSR Hypervisor resource for VADP prior to the upgrade, then VMware View will work.

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

EMC strongly recommends that you set up a separate vCenter user account 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, EMC 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 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
Network	• Assign network

Table 9 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 required privileges
	• 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 setting • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Set annotation • Settings • Swapfile placement • Upgrade virtual machine compatibility

Table 9 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 required privileges
Guest Operations	• Guest operation modifications • Guest operation program execution • Guest operation queries
Interaction	• 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 the VMware Backup Appliance, or before you can use the Single Sign-on (SSO) admin user with the VMware Backup Appliance, 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 VMware Backup Appliance. Table 9 on page 47 provides the account permission categories.

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

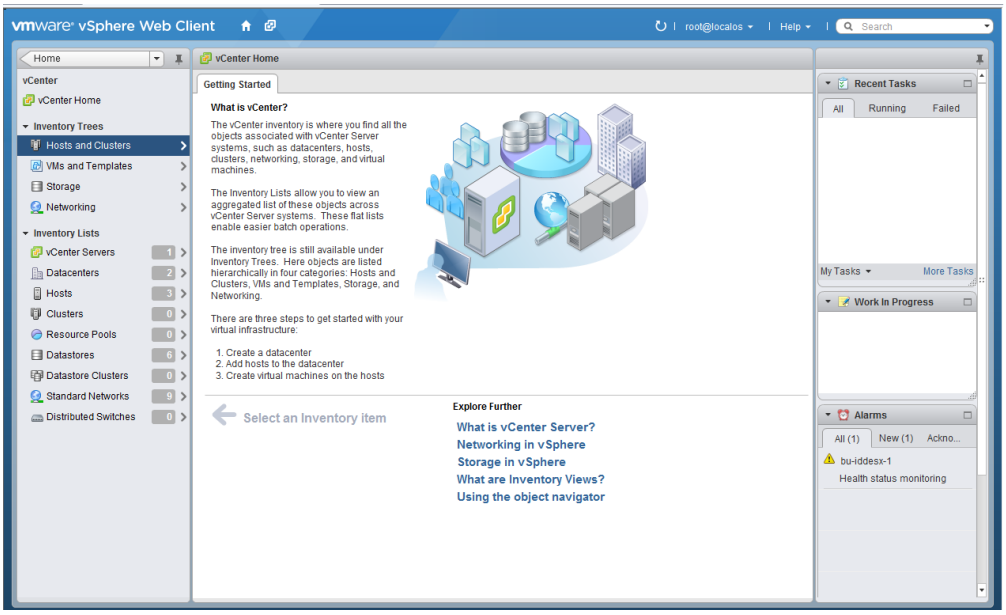
Procedure

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 11 Hosts and Clusters in the vSphere Web Client



4. Select the **Manage** tab and then click **Permissions**.
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 EMC Backup and Recovery, or the SSO admin user, and then click **Add**.

   If the EMC 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 69.

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.

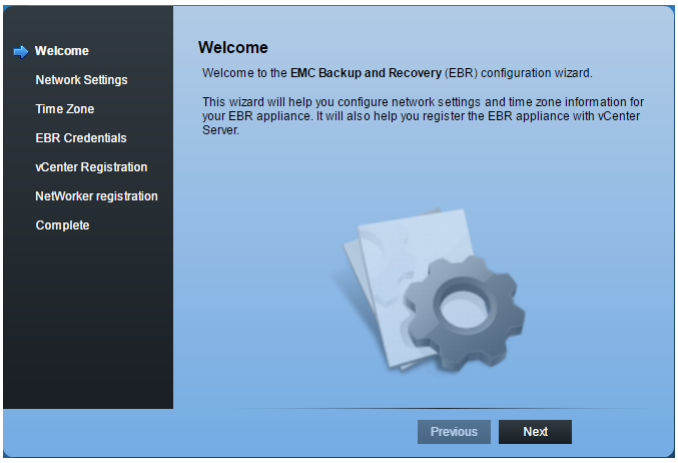
2. Log in with the userid `root`, and create a password that is a minimum of 9 characters long and contains a combination of one more more upper and lower-case letters, one or more numbers from 0-9, and at least one special character.

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.

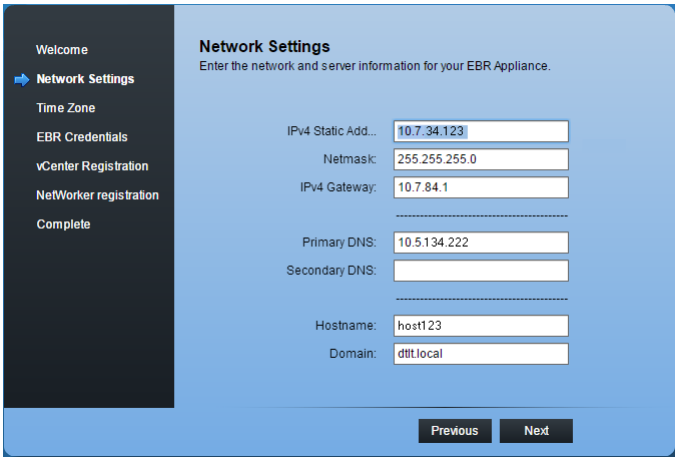
Figure 12 Welcome configuration page



3. Click **Next**.

The **Network Settings** page displays.

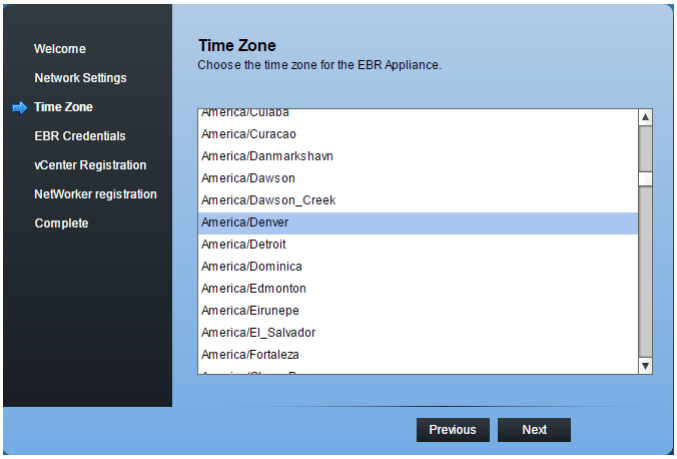
Figure 13 Network Settings configuration page



4. Verify the network settings, and click **Next**.

The **Time Zone** page displays.

Figure 14 Time Zone configuration page



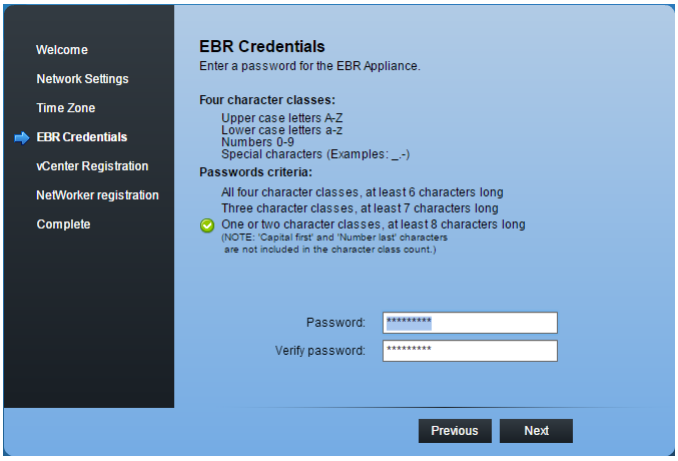
5. Set the time zone to match that of the vCenter appliance, and click **Next**.

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.

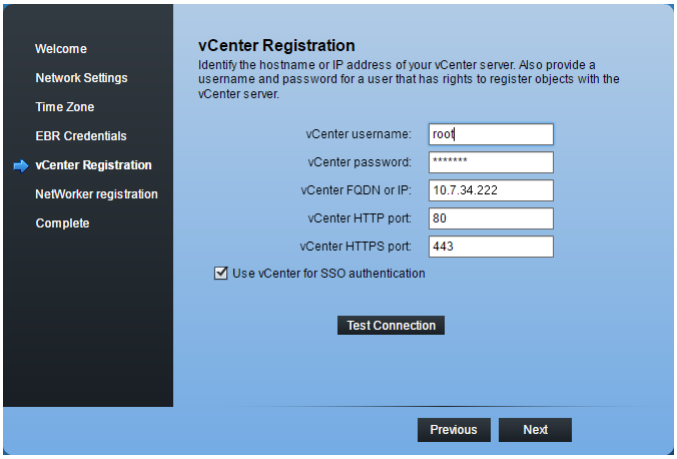
Figure 15 EBR Credentials configuration page



6. Specify a new EMC Backup and Recovery password for the root account, and click **Next**.

   The **vCenter Registration** page displays.

Figure 16 vCenter Registration configuration page



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 17 NetWorker registration configuration page

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.

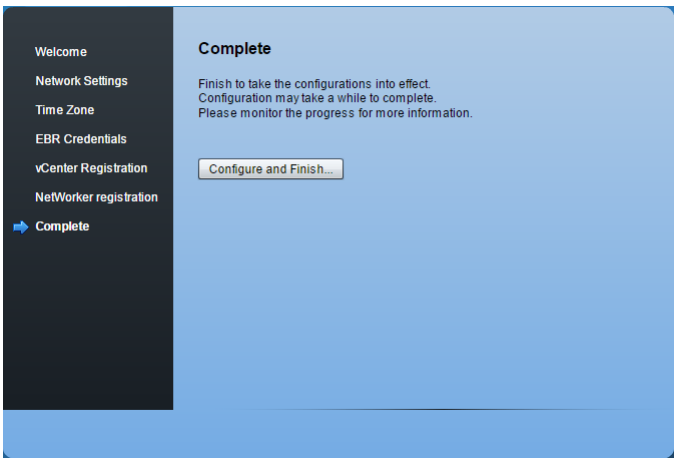
11. Click **Test NetWorker connection**.

    You should see a message that the connection test completed successfully.

12. Click **Next**.

    The **Complete** page appears.

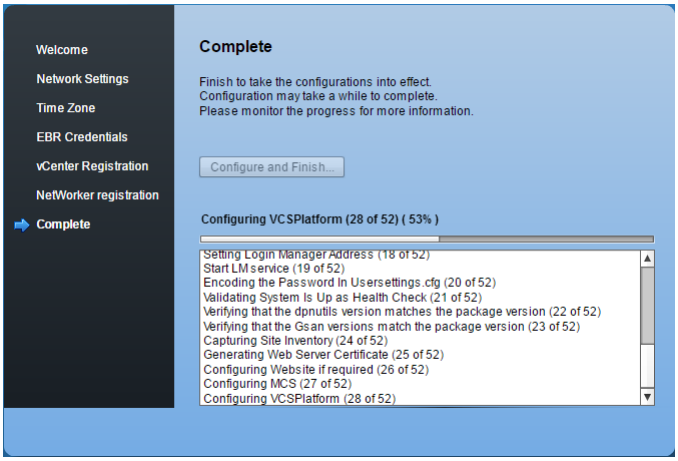
Figure 18 Complete configuration page



13. **Click Complete and Finish**.

    Configuration begins, and the progress is shown.

Figure 19 Complete progress page



Monitoring policy activity

The **Monitoring** window in the **NetWorker Administration** window enables you to monitor activities for specific policies, workflows, and actions.

Policies/Actions pane

The **Policies/Actions** pane at the top of the **Monitoring** window lists the policies on the NetWorker server by default. Click the + (plus) sign next to a policy in the list to view the workflows in the policy, and the + (plus) sign next to a workflow to view the actions for a workflow.

The **Policies** pane provides the following information for each item (where applicable):

- Overall status

  The following table provides details on the status icons that may appear in the **Policies** pane.

  Table 10 Policy status icons

Icon	Status
	Never run
	Running
	Succeeded
	Failed
	Probing

- Most recent start time
- Duration of the most recent run
- Next scheduled runtime
- Name of the assigned save set

- Device on which the save set is stored
- Backup level
- Data transfer rate
- Size of the save set
- Messages that resulted from an action

Right-click an action in the **Policies** pane, and select **Show Details** to view details on currently running, successfully completed, and failed activities for the action.

When you sort the items on the **Policy/Actions** pane by using the **Status** column, NetWorker sorts the items in alphabetical order that is based on the label of the icon.

Consider the following when a policy/action is in a probing state:

- A message is sent when the group starts and finishes the probe operation.
- The results of the probe operation (run backup/do not run backup) are also logged.
- Probes do not affect the final status of the group, and the group status does not indicate the results of the probe.
- If probing indicates that a backup should not run, then the group status reverts to its state before the group running.
- Check the results of the probe in the **Log** window to ensure that the probe indicates that the backup can be taken.

Actions pane

To view a list of all actions, click the **Actions** tab at the bottom of the **Policies** pane. The **Policies** pane becomes the **Actions** pane.

The **Actions** pane provides the following information for each action:

- Overall status

  Note

  The **Actions** pane displays the same status icons as the **Policies** pane.

- Name
- Assigned policy
- Assigned workflow
- Type
- Date and time of the most recent run
- Duration of the most recent run
- Percent complete, for actions that are in progress
- Next scheduled runtime

Right-click an action in the **Actions** pane, and select **Show Details** to view details on currently running, completed, and failed activities for the action.

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:

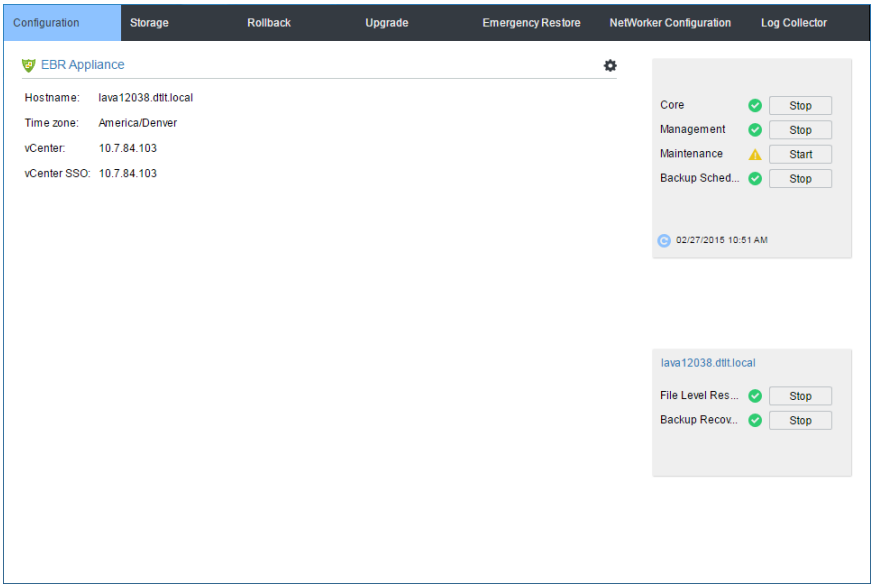
   `NetWorker server, 'server_name' registration succeeded for VMware Backup Appliance VBA_hostname`

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 20 Post VMware Backup Appliance configuration



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 11 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.

Table 11 Description of services running on the VMware Backup Appliance (continued)

Service	Description
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.
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.

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

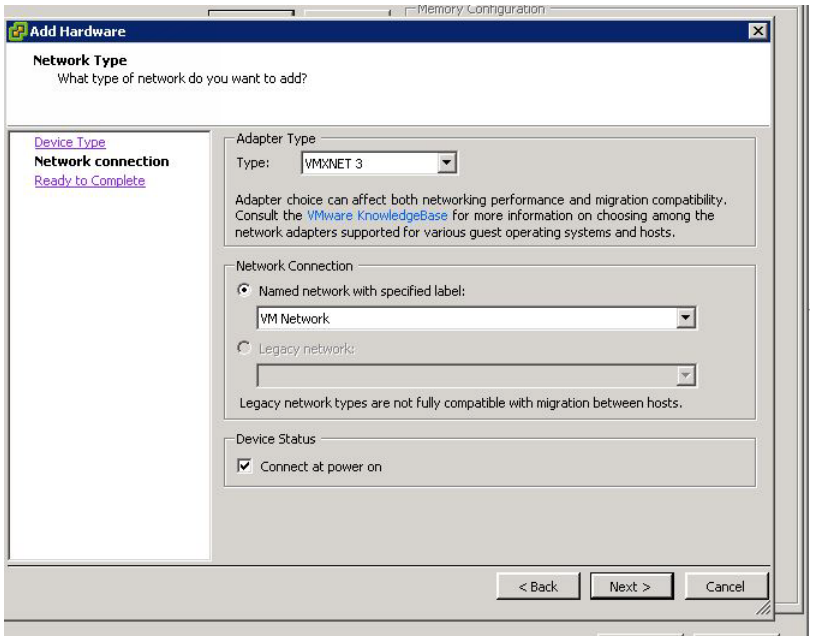
   c. In the **Hardware** tab, click **Add**.

      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.

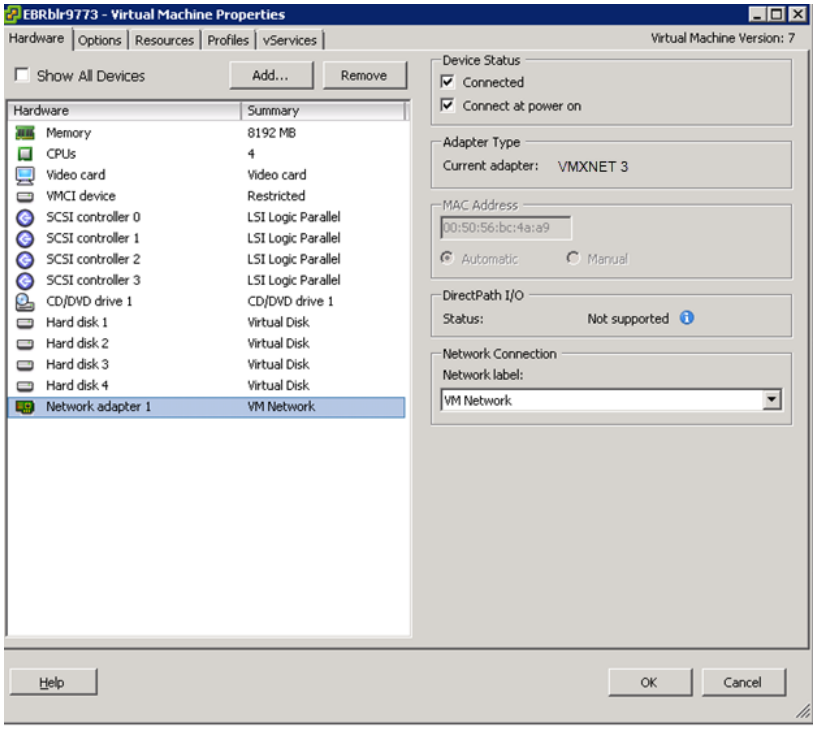
   Figure 21 Change Adapter Type



   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**.

Figure 22 Swap network for NICs in the Virtual Machine Properties window



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**.

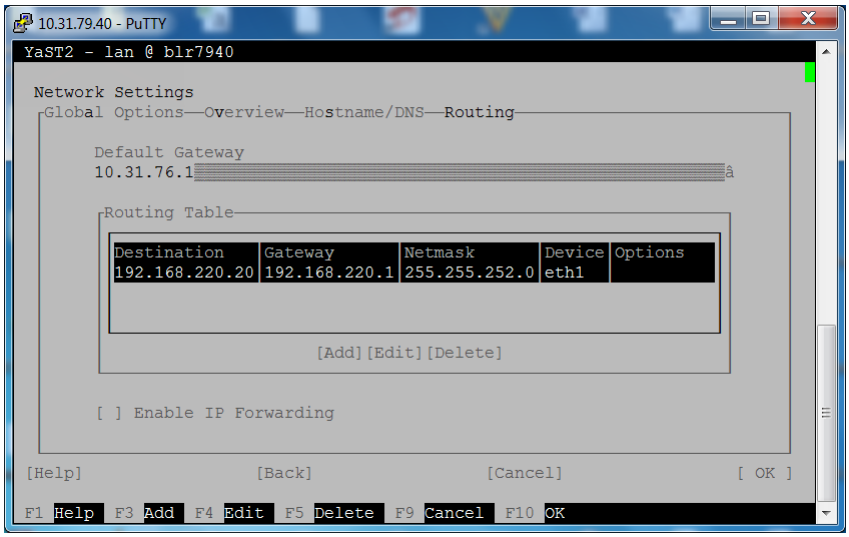
      The **Network Settings** dialog appears.
   e. In the **Overview** tab, select the Second Ethernet Adapter labeled **eth1**.
   f. Use the tab key to select **Edit** and press **Enter**.
   g. From the Network Card Setup, use the tab key to access **Statically assigned IP Address** and select using the 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 23 Routing table with production network gateway



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:

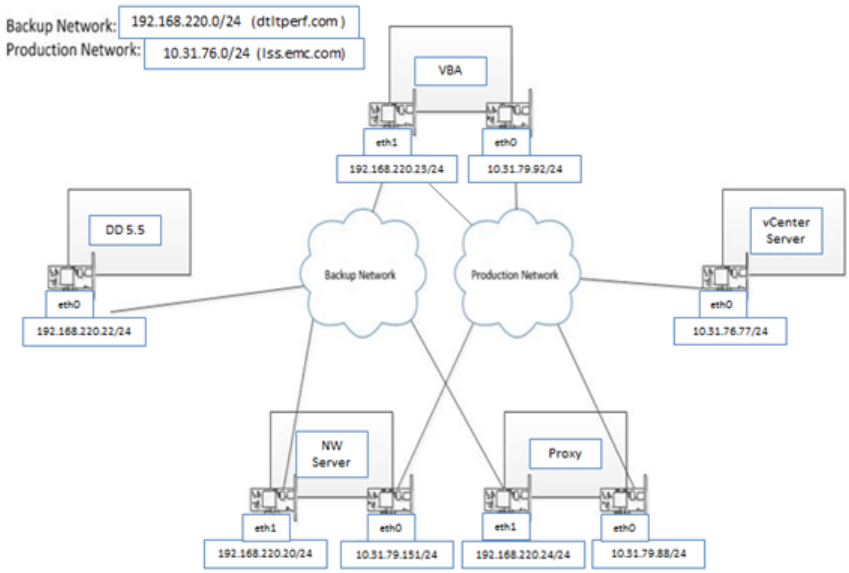
- Manually add a new vNIC of type **VMXNET 3** according to the instruction in step 3b of the section "Adding or swapping a NIC on the VMware Backup appliance or external proxy."
- Configure the two vNICs with two separate and unique subnets in order to facilitate the direction of production traffic (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 two NICs on the VMware Backup appliance should have the capability to communicate bi-directionally with the vCenter server
- 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 24 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

After a successful OVA deployment, you can create a policy with a workflow for VMware backup within the NMC GUI's **Administration** window, and assign VMs and VMDKs to the workflows for backup and recovery by using the **Administration** window. The NMC GUI is the user interface for the NMC server.

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:

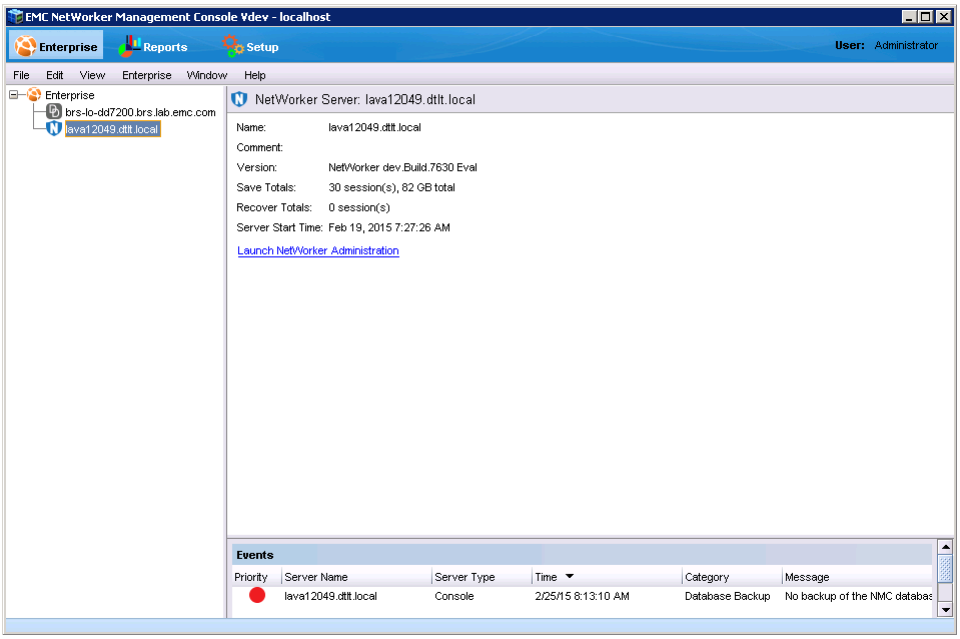
   username@VBA node
   where username is the name of a user with root privileges.

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 25 NMC Enterprise window

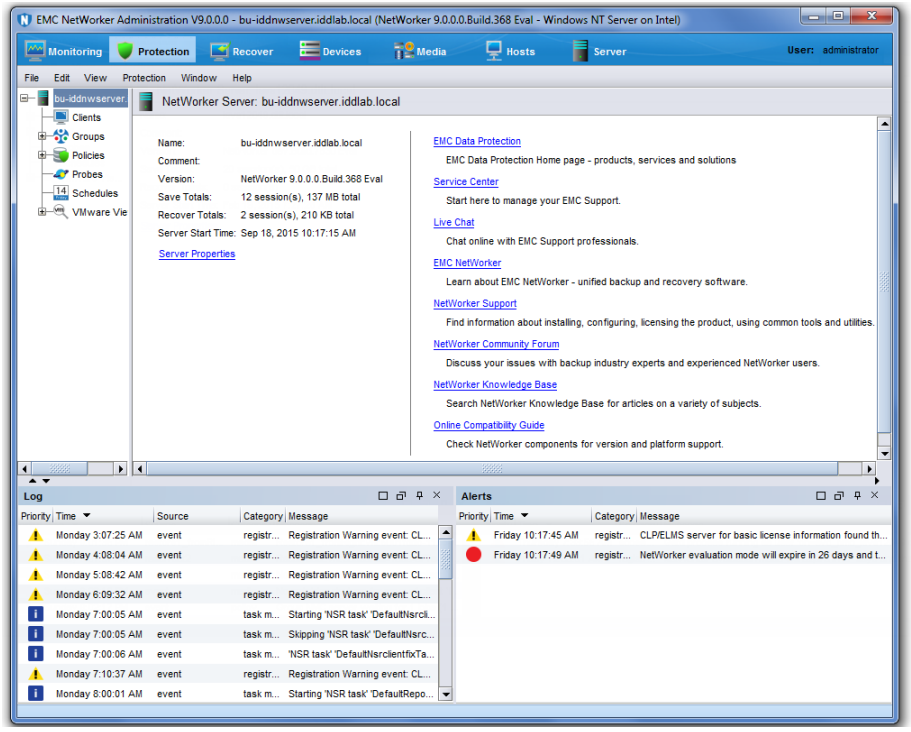


Procedure

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.
   You can access many of the options for the VMware Protection solution in the **Protection** window, as shown in the following figure.

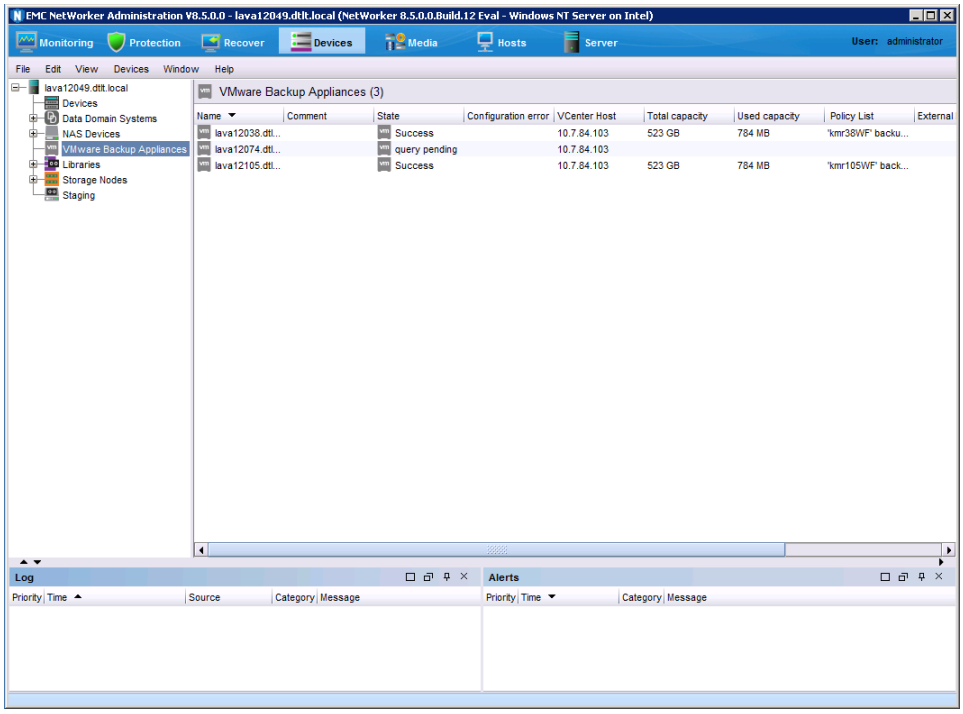
Figure 26 Protection window in the Administration window



VMware Backup Appliance monitoring and properties

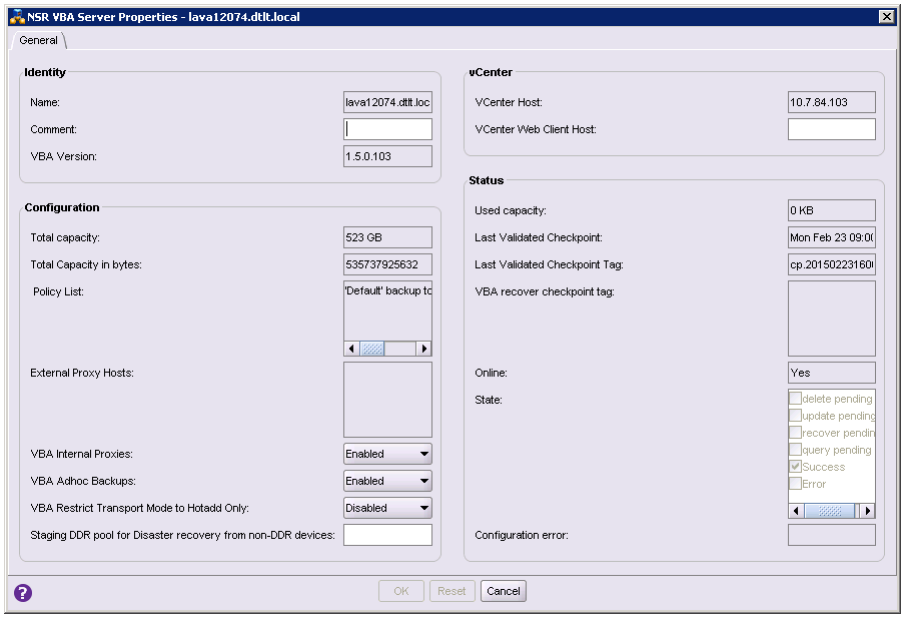
In the **Devices** window, select **VMware Backup Appliances** and the available VMware Backup Appliances appear in the right pane. From the right pane, you can monitor the state of the VMware Backup appliance, as shown in the following figure.

Figure 27 VMware Backup appliance health monitoring in the Devices window



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 28 NSR VBA Server Properties window



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**, this setting allows for storage on internal proxies. When set 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 EMC Backup and Recovery 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 in NMC

When you expand **Policies** in the **Protection** window, all existing resources appear.

Setting up and configuring data protection policies 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-catalogue 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, 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

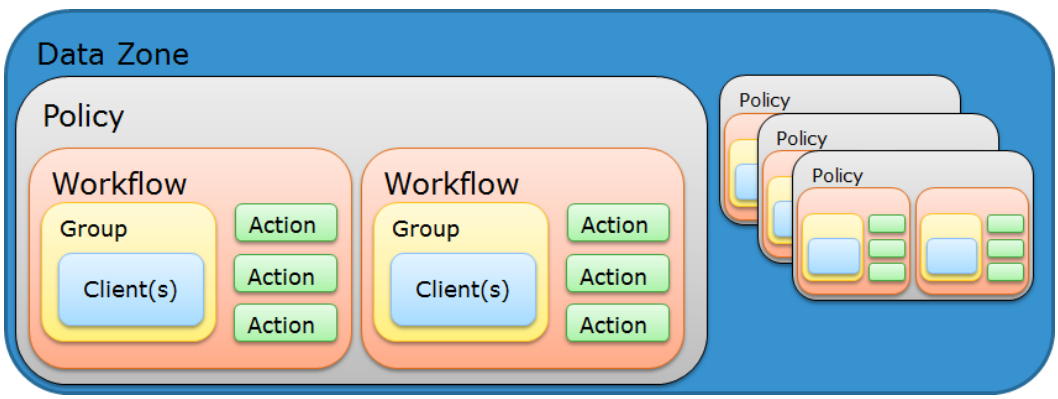
Actions are the key resources in a workflow for a data protection policy and define a specific task, for example, a backup, clone, or snapshot. NetWorker uses a work list to the define task. A work list is composed of one or several work items. Work items include client resources, virtual machines, save 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 29 Data Protection Policy



Default data protection policies

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

Each protection policy provides an example of the EMC best practices that you should follow when you design your data protection solution:

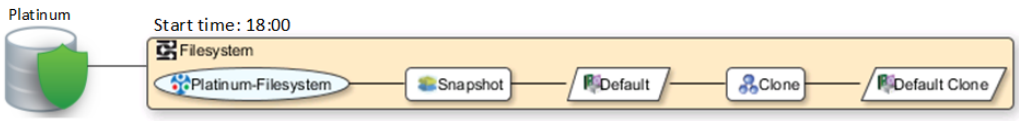
- Separate file system backups from application database backups, to provide ease of access at recovery time.
- Stagger the start times for file system backup from the application database backups, to prevent disk contention on the target hosts.

The default data protection policy resources mimic the requirements of a service provider, with different policies to that are designed to provide protection based on service level agreements.

Platinum policy

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

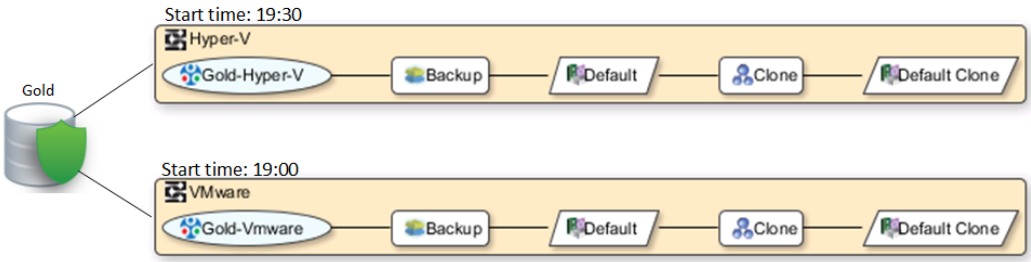
Figure 30 Platinum policy configuration



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. The policy contains two workflows, one to protect Hyper-V hosts and one to protect VMware hosts. Each workflow contains a backup action followed by a clone action.

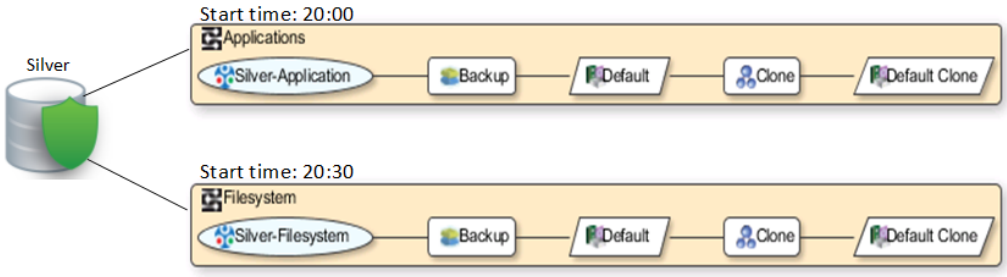
Figure 31 Gold policy configuration



Silver policy

The Silver policy provides an example of a data protection policy for an environment that contains non-virtualized machines and requires backup data redundancy. The policy contains two workflows, one to protect hosts file systems and one to protect database applications. Each workflow contains a backup action followed by a clone action.

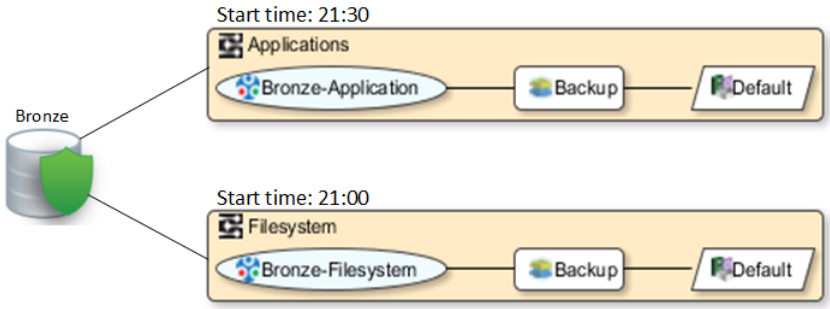
Figure 32 Silver policy configuration



Bronze policy

The Bronze policy provides an example of a data protection policy for an environment that contains non-virtualized machines. The policy contains two workflows, one to protect hosts file systems and one to protect database applications. Each workflow contains a backup action.

Figure 33 Bronze policy configuration



Creating a policy

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

   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** or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` action to write the notifications to a log file or configure an email notification.

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

   For example:

   - To log notifications to a file named `policy_notifications.log`, type the following command:

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

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

     ```
     mail -s subject recipient
     ```

   - 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. To specify the Restricted Data Zone (RDZ) for the policy, select the **Restricted Data Zones** tab, and then select the RDZ from the list.
8. Click **OK**.

After you finish

Create the workflows 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.

Creating a workflow in a new policy

A policy must contain one or more workflows.

Procedure

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

   The maximum number of characters for the name of the group is 64.
4. In the **Comment** box, type a description for the workflow. The maximum number of characters for the **Comment** field is 128.
5. 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 determine when to send the notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after all the actions in the workflow complete, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after all the actions in the workflow complete, select **On Failure**.
6. In the **Send notification** attribute when you select the **On Completion** or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` action to write the notifications to a log file or configure an email notification.

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

   For example:
   - To log notifications to a file named `policy_notifications.log`, type the following command:

     `nsrlog` **`-f policy_notifications.log`**
   - On Linux, to send a notification email, 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.

7. In the **Running** group box, define when and how often the workflow runs.
   a. To ensure that the actions contained in the workflow run when the policy or workflow is started, 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 is started, clear this option.
   b. To ensure that the workflow starts 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 running at the time that is specified in the **Start time** attribute, clear this option.
   c. To define the time to start the actions in the workflow, in the **Start Time** attribute, use the spin boxes.

      The default value is 9:00 P.M.
   d. To define how frequently to repeat the actions that are defined in the workflow over a 24 hour period, In the **Interval** attribute, use the spin boxes.

      The default 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 define the last time to start a workflow in a defined interval period, use the spin boxes .
   e. To define 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, when you set the **Start Time** to 7:00 PM, the **Interval** to 1 hour, and the **Interval end time** to 11:00 P.M., then the workflow automatically starts every hour beginning at 7:00 P.M. and the last start time is 11:00 PM.
8. 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.

Creating a workflow in an existing policy

A policy can have 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 characters for the name of the group is 64.
7. In the **Comment** box, type a description for the workflow. The maximum number of 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 determine when to send the notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after all the actions in the workflow complete, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after all the actions in the workflow complete, select **On Failure**.
9. In the **Send notification** attribute when you select the **On Completion** or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` action to write the notifications to a log file or configure an email notification.

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

   For example:
   - To log notifications to a file named `policy_notifications.log`, type the following command:

     `nsrlog` **`-f policy_notifications.log`**
   - On Linux, to send a notification email, 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** group box, define when and how often the workflow runs.
    a. To ensure that the actions contained in the workflow run when the policy or workflow is started, 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 is started, clear this option.
    b. To ensure that the workflow starts 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 running at the time that is specified in the **Start time** attribute, clear this option.
    c. To define the time to start the actions in the workflow, in the **Start Time** attribute, use the spin boxes.

       The default value is 9:00 P.M.
    d. To define how frequently to repeat the actions that are defined in the workflow over a 24 hour period, In the **Interval** attribute, use the spin boxes.

       The default 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 define the last time to start a workflow in a defined interval period, use the spin boxes .
    e. To define 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, when you set the **Start Time** to 7:00 PM, the **Interval** to 1 hour, and the **Interval end time** to 11:00 P.M., then the workflow automatically starts every hour beginning at 7:00 P.M. 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**.

Creating a VMware group

A VMware group defines the virtual machines or virtual disk files to back up.

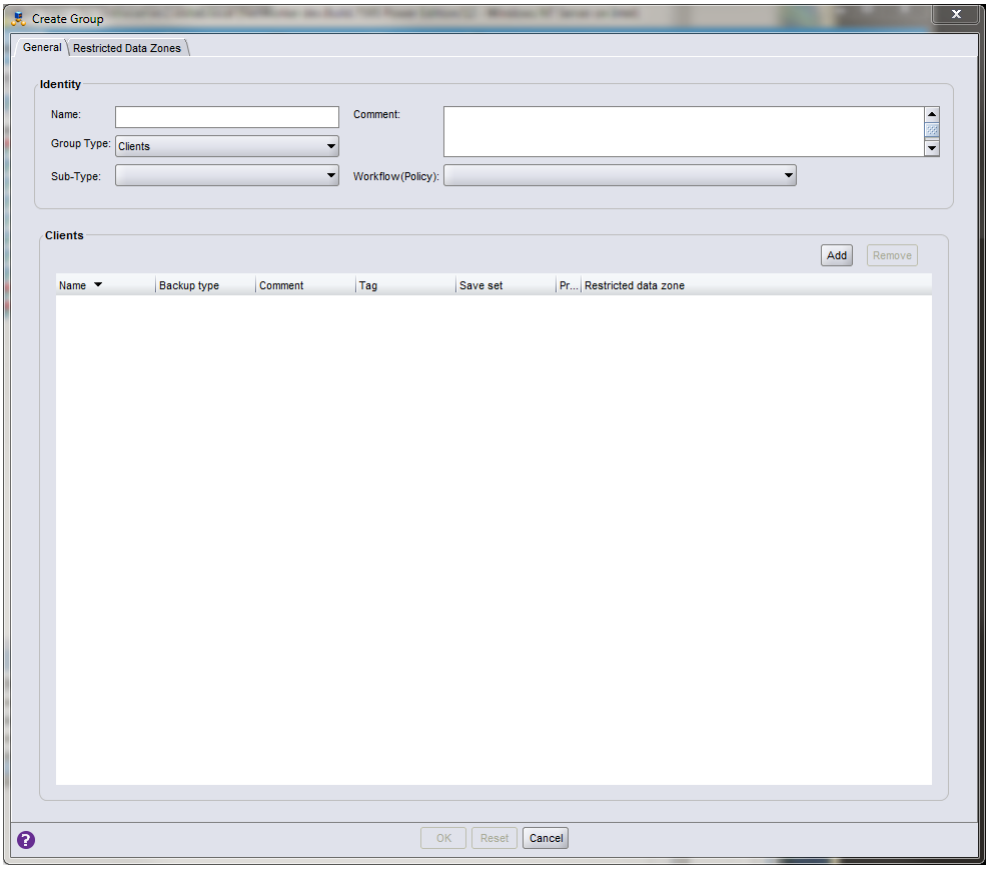
Procedure

1. On the **Administration** window, click **Protection**.

2. In the expanded left pane, right-click **Groups** and select **New**.

   The **Create Group** dialog box appears, starting with the **General** tab.

Figure 34 Create Group dialog box



3. Type a name for the group in the **Name** box.
4. From the **Group Type** list, select **VMware**.
5. From the **Sub-Type** list, select whether to create a **VirtualMachine** group, or a **VMDK** group for disk level backup.
6. Type a description of the group in the **Comment** box.
7. (Optional) To associate the group with an existing workflow, select the workflow from the **Workflow(Policy)** list.

   You can also assign the group to a workflow when you create or edit a workflow.
8. From the **vCenter** list, select the vCenter with the virtual machines or VMDKs.

   If the vCenter list is empty, do the following:

   a. Cancel the task.

   b. In the **Protection** window, right-click **VMware View** in the left pane, and select **Refresh**.
9. To specify the restricted data zone (RDZ) for the group, select the **Restricted Data Zones** tab, and then select the RDZ from the list.
10. Click **OK**.

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 VMware Backup Appliance, you can select the following:

- VMware backup—Performs a backup of virtual machines in vCenter to a Data Domain system. You can only perform one VMware backup action per workflow. The VMware backup action must occur before clone actions.
- Clone—Performs a clone of the VMware backup on a Data Domain system to any clone device that NetWorker supports (including Data Domain system or tape targets). You can specify multiple clone actions. Clone actions must occur after the VMware backup action.
- VBA Checkpoint discover—Performs a discovery of the last validated checkpoint backup of the VMware Backup Appliance. If a validated checkpoint is not available, the action discovers the last non-validated checkpoint. The VBA Checkpoint discover action must occur before the VBA Checkpoint backup action, but cannot occur before the VMware backup action.
- VBA Checkpoint backup—Performs a checkpoint backup of the VMware Backup Appliance at a scheduled time, typically once daily, to be used in case of a disaster recovery. This action must occur after the checkpoint discover action. You can only perform a VBA Checkpoint backup to a Data Domain pool, and the backup requires a local storage node device. The checkpoint backup fails if the backup device is configured on the remote storage node.

Note

Since the backup to internal storage option is no longer available in NetWorker 9.0, EMC does not recommend using the VBA Checkpoint discover and VBA Checkpoint backup actions for disaster recovery.

Creating a VMware backup action

A VMware backup is a scheduled backup of VMs within a vCenter.

Before you begin

- Create the policy and workflow that contain the action.
- (Optional) Create actions to precede the backup action in the workflow. Supported actions that can precede a backup include:
  - Probe
  - Check connectivity

Procedure

1. In the expanded left pane, select the workflow, and then perform one of the following tasks in the right pane to start the Policy Action wizard:
   - If this 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 **Specify the Action Information** page appears.

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, any action that occurs after a disabled action will not start, even if the succeeding options are enabled.

5. From the **Action Type** list, select **Backup**.
6. From the secondary action list, select the backup type, for example, **VMware**.
7. When you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is grayed out.
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, select the action that should precede this action from the **Previous** box.
   - If the action should run concurrently with an action, select the concurrent action from the **Previous** box, and then select the **Concurrent** checkbox.
9. Select whether to use 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.

    The following table provides details about the backup level that each icon represents. To support the same type of backup on each day, select the backup type from the list and click .

Table 12 Schedule icons

Icon	Label	Description
	Full	Perform a full backup on this day. Full backups include all files, regardless of whether the files changed.
	Incr	Perform an incremental backup on this day. Incremental backups include files that have changed since the last backup of any type (full or incremental).
	Logs Only	Perform a backup of only database transaction logs.

Table 12 Schedule icons (continued)

Icon	Label	Description
	Skip	Do not perform a backup on this day.

Make All

11. Click **Next**.

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

12. From the **Destination Storage Node** box, select the storage node with the devices on which to store the backup data.
13. From the **Destination Pool** box, select the media pool in which to store the backup data.
14. From the **Retention** boxes, specify the amount of time to retain the backup data.

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

15. From the **Client Override Behavior** box, specify how NetWorker uses certain client configuration attributes that perform the same function as attributes in the Action resource.
    - **Client Can Override**—The values in the Client resource for **Schedule**, **Pool**, **Retention policy**, and the **Storage Node** attributes will take precedence over the values that are defined in the equivalent Action resource attributes.
    - **Client Can Not Override** —The values in the Action resource for the **Schedule**, **Destination Pool**, **Destination Storage Node**, and the **Retention** attributes take precedence over the values that are defined in the equivalent Client resource attributes.
    - **Legacy Backup Rules**—This value only appears in actions that are created by the migration process. The updating process sets the **Client Override Behavior** for the migrated backup actions to **Legacy Backup Rules**.

16. Click **Next**.

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

17. In the **Retries** box, specify the number of times that NetWorker should retry a failed probe or backup action, before NetWorker considers the action as failed. When the **Retries** value is 0, NetWorker will not retry a failed backup or probe action.

    Note

    The **Retries** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

18. In the **Retry Delay** field, specify a delay in seconds to wait before retrying a failed backup or probe action. When the **Retry Delay** value is 0, NetWorker retries the failed backup or probe action immediately.

Note

The **Retry Delay** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

19. In the **Inactivity Timeout** field, specify the maximum number of minutes that a job run by an action is allowed to fail to communicate back to the server.

    If the job fails to respond within the timeout value, the server considers the job a failure. If a job fails, NetWorker retries the job immediately. This ensures that no time is lost due to failures.

    Increase the timeout value if a backup consistently aborts due to inactivity. Inactivity timeouts may occur for backups of large save sets, backups of save sets with large sparse files, and incremental backups of many small static files.

    Note

    The **Inactivity Timeout** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

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

    Note

    The **Parallelism** value should not exceed 25.

21. 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 current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action**.

      Note

      The **Abort action** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types.
    - 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.

22. From the **Soft Limit** list, specify the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no limit.
23. From the **Hard Limit** list, specify the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no limit.
24. (Optional) Configure overrides for the task that is scheduled on a specific day.

To change the month on which to schedule the override, use the navigation buttons and the month list box. To change 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, 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**, then use the drop downs. Click **Add Rules based override**.
  - To perform the action task on the last day of the calendar month, select **Last day of the month**. Click **Add Rules based override**.
  - In the **Override** field, type an override.

    Note

    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:
    - Select **Set at policy level** to use the notification configuration that is defined in the Policy resource to send the notification.
    - Select **On Completion** to send a notification on completion of the action.
    - Select **On Failure** to send a notification only if the action fails to complete.
26. In the **Send notification** attribute when you select the **On Completion** or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` action to write the notifications to a log file or configure an email notification.

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

    For example:

    - To log notifications to a file named `policy_notifications.log`, type the following command:

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

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

- `-h` *`mailserver`*—Specifies the hostname of the mail server to use to relay the SMTP email message.
- *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

27. Click **Next**.

    The **Action Configuration Summary** page appears.

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

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 workflow, and then perform one of the following tasks in the right pane to start the Policy Action wizard:
   - If this 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 **Specify the Action Information** page appears.
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, any action that occurs after a disabled action will not start, even if the succeeding options are enabled.

5. From the **Action Type** list, select **Clone**.
6. When you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is grayed out.
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, select the action that should precede this action from the **Previous** box.
   - If the action should run concurrently with an action, select the concurrent action from the **Previous** box, and then select the **Concurrent** checkbox.
8. Select whether to use 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. Click the icon on each day to specify whether to perform cloning.

   The following table provides details on the icons.

Table 13 Schedule icons

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

   To perform cloning every day, select **Execute** from the list and click **Make All**.

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

    a. Time filter—Use the **Time** section to define the time range in which NetWorker should inspect, when searching for eligible save sets to clone in the media database. Use the spin boxes to specify the start of the time range and the end of the time range. The **Time** filter list includes three options, which define how NetWorker determines save set eligibility, based on the time criteria:

       - **Do Not Filter**—NetWorker inspects the save sets in the media database to create a clone save set list that meets the filter criteria.
       - **Accept**—The clone save set list includes save sets whose save time is within the time range that is specified by the spin boxes and meet all the other defined filter criteria.

- **Reject**—The clone save set list does not include save sets whose save time is within the time range that is specified by the spin boxes and meet all the other defined filter criteria.

b. Save Set filter—Use the **Save Set** section to instruct NetWorker to include or exclude ProtectPoint and Snapshot save sets, when searching for eligible save sets to clone in the media database. The **Save Set** filter list includes three options, which define how NetWorker determines save set eligibility, based on the save set criteria:

- **Do Not Filter**—NetWorker inspects the save sets in the media database to create a clone save set list that meets the filter criteria.
- **Accept**—The clone save set list includes eligible ProtectPoint or Snapshot save sets, when you also enable the ProtectPoint or Snapshot checkboxes.
- **Reject**—The clone save set list does not include eligible ProtectPoint and Snapshot save sets when you also enable the ProtectPoint and Snapshot checkboxes.

c. Clients filter—Use the **Client** section to define a list of clients to include or exclude, when NetWorker searches for eligible save sets to clone in the media database. The **Client** list includes three options, which define how NetWorker determines save set eligibility, based on the client criteria:

- **Do Not Filter**—NetWorker inspects save sets that are associated with the clients in the media database, to create a clone save set list that meets the filter criteria.
- **Accept**—The clone save set list includes eligible save sets for the selected clients.
- **Reject**—The clone save set list does not include eligible save sets for the selected clients.

d. Levels filter—Use the **Levels** section to define a list of backup levels to include or exclude, when NetWorker searches for eligible save sets to clone in the media database. The **Levels** filter list includes three options, which define how NetWorker determines save set eligibility, based on the level criteria:

- **Do Not Filter**—NetWorker inspects save sets regardless of level in the media database, to create a clone save set list that meets all the filter criteria.
- **Accept**—The clone save set list includes eligible save sets with the selected backup levels.
- **Reject**—The clone save set list does not include eligible save sets with the selected backup levels.

13. Click **Next**.

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

14. Configure advanced options, including notifications and schedule overrides.

Note

Although the **Retries**, **Retry Delay**, or the **Inactivity Timeout** options appear, the clone action does not support these options and ignores the values.

---

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

    Note

    The **Parallelism** value should not exceed 25.

16. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action**.

      Note

      The **Abort action** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types.

    - To abort the entire workflow if there is a failure with one of the jobs in the action, select **Abort workflow**.

    Note

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

17. From the **Send Notifications** list box, select whether to send notifications for the action:
    - Select **Set at policy level** to use the notification configuration that is defined in the Policy resource to send the notification.
    - Select **On Completion** to send a notification on completion of the action.
    - Select **On Failure** to send a notification only if the action fails to complete.

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

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

    For example:

    - To log notifications to a file named `policy_notifications.log`, type the following command:

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

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

      ```
      mail -s subject recipient
      ```

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

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

where:

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

19. From the **Soft Limit** list, specify the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no limit.
20. From the **Hard Limit** list, specify the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no limit.
21. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To change the month on which to schedule the override, use the navigation buttons and the month list box. To change 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, 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**, then use the drop downs. Click **Add Rules based override**.
      - To perform the action task on the last day of the calendar month, select **Last day of the month**. Click **Add Rules based override**.
      - In the **Override** field, type an override.

        Note

        To remove an override, delete the entry from the **Override** field.

22. Click **Next**.

    The **Action Configuration Summary** page appears.
23. Review the settings that you specified for the action, and then click **Configure**.

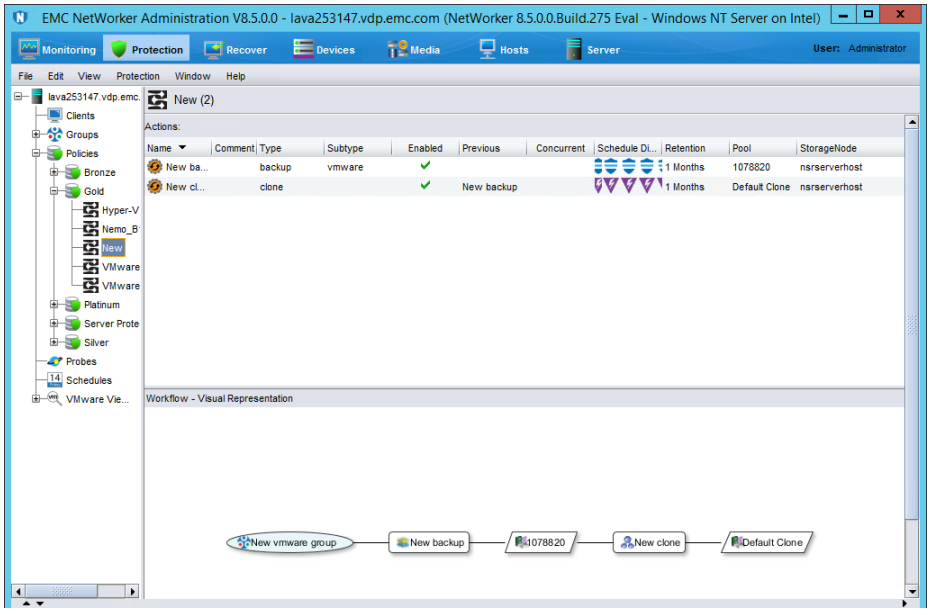
After you finish

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

Visual representation of VMware policy and associated actions

After you have finished creating a policy, a visual representation of it is displayed in the lower panel of the Protection tab as shown in the following figure.

Figure 35 VMware protection policy with associated actions



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 the policies you created in "VMware data protection policies in NMC."

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

Note

After upgrading to NetWorker 9.0.1, **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

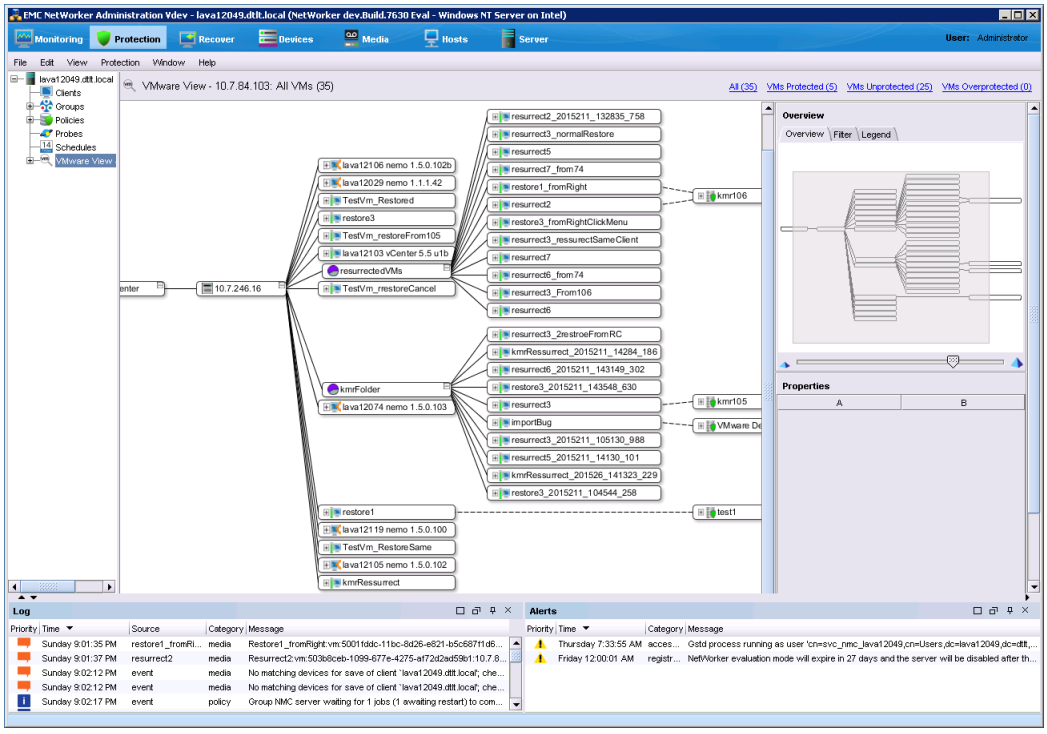
You can use several operations to navigate within the map view:

- 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.

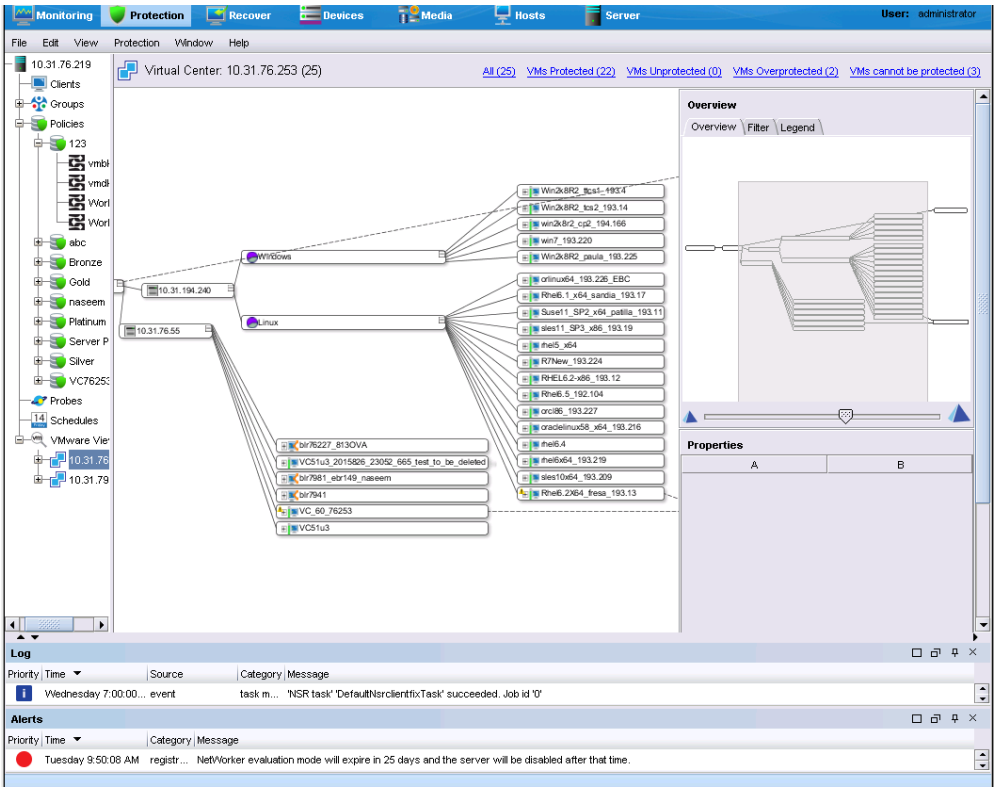
Figure 36 Map view of VMware environment in NMC



To refine items displayed in the right details pane, select containers in the Virtualization node hierarchy in the left pane. For example, if an individual Cluster is

selected in the Virtualization node, only child elements associated with that Cluster display.

Figure 37 Cluster with child elements in VMware View



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

Figure 38 Filtering results in VMware View

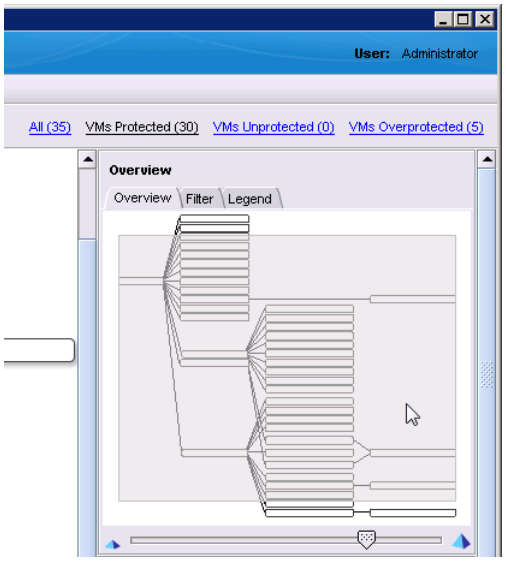


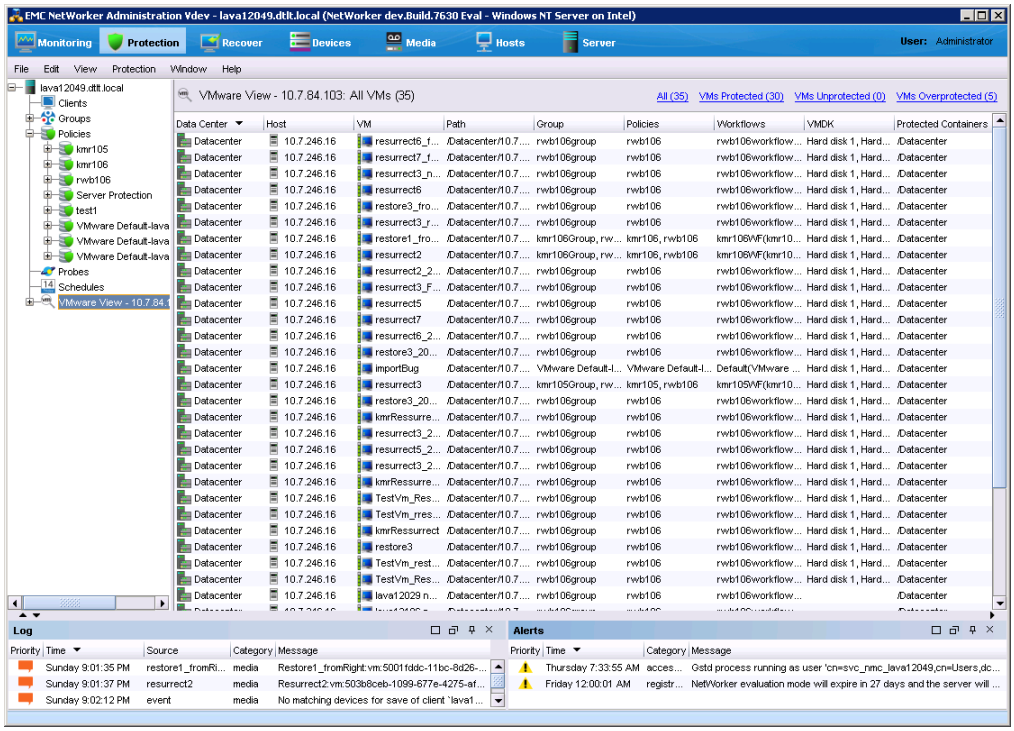
Table view of the VMware environment

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 39 VMware table view



The filtering function works the same in Table view as in Map view. Links provided above the details pane allow you to display only overprotected virtual machines, unprotected virtual machines, or all virtual machines in the environment. The *EMC 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.

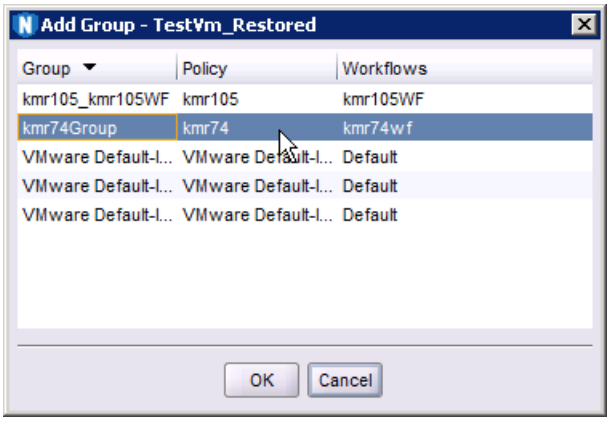
Procedure

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 40 Add group in VMware View



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

   VMware View refreshes and displays the new association.

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

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 38 on page 93, to narrow your view to only overprotected or only unprotected virtual machines.

Assigning a group to a disconnected ESX server in VMware View

When you disconnect an ESX host from the vCenter server, the ESX is removed from the EMC Backup and Recovery user interface in the vSphere Web Client, but 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 connect the disconnected 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.

Starting, stopping, and restarting data protection policies

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

Note

You cannot stop, restart, or start individual actions.

You can restart any failed or canceled workflow. However, the restart must happen within the restart window that you specified for the workflow.

You can also start specific policies and workflows in the **Protection** window by right-clicking the policy or workflow, and selecting **Start**.

Procedure

1. Select the workflow, or action in the **Monitoring** window.
2. Right-click and select **Start**, **Stop**, or **Restart**.

   A confirmation message appears.
3. Click **Yes**.

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 94, is available within NMC, EMC recommends that you only use NMC to assign VMs/VMDKs to policies.
- Ad-hoc VM backups (also known as Backup Now functionality)
- Image-level (FULLVM) recoveries
- 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 97 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

Procedure

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

   `https://IP_address_vCenter_Server:9443/vsphere-client/`

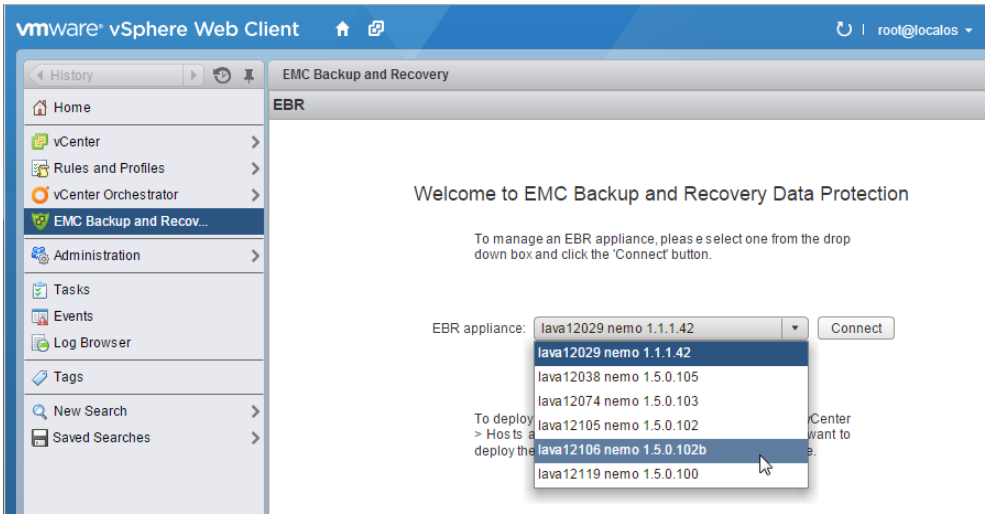
Note

If you receive an SSL certificate error in your web browser, refer to the VMware knowledgebase article 1021514.

2. In the **VMware vSphere Web Client** 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 left panel of the vSphere Web Client, select **EMC Backup and Recovery**.
4. In the **Welcome to EMC Backup and Recovery Data Protection** window, select a Backup Appliance from the drop-down list. The list contains all the VMware Backup appliances registered in the vCenter.

   Each vCenter Server supports up to 10 appliances. The **EBR appliance** drop-down list, shown in the following figure, contains the appliance names in alphabetical order.

Figure 41 Selecting the Backup Appliance



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 following command:

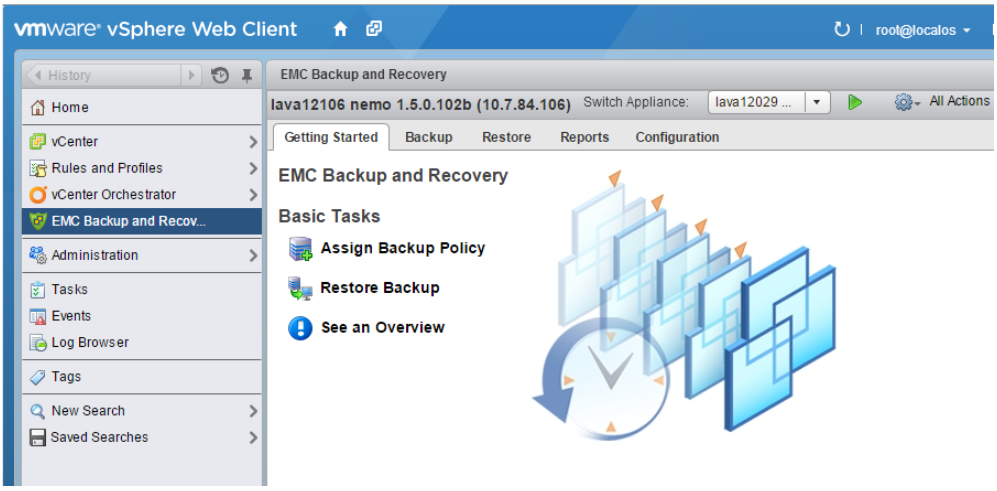
```
ebrserver.pl --restart
```

Available tasks in the EMC Backup and Recovery user interface

The **EMC Backup and Recovery** user interface allows you to configure and manage the VMware Backup Appliance.

When you connect to the **EMC Backup and Recovery** user interface in the **vSphere Web Client**, the following page displays.

Figure 42 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 14 Backup tab column descriptions

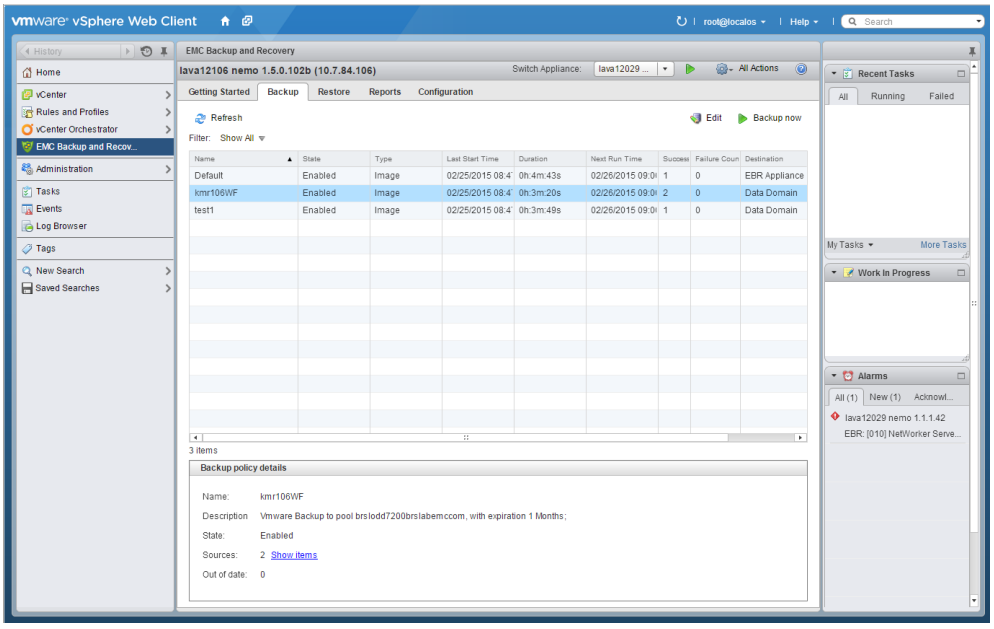
Column	Description
Name	The name of the backup policy.
State	Whether the policy is enabled or disabled. Disabled backup policies will not run. Also, a “No Schedule” state displays when you disable **Autostart** in NMC for a policy.
Type	The type of backup specified in the policy; for example, Image.
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.
Success Count	The number of virtual machines that were backed up successfully the last time the policy ran. This number updates after each backup.

Table 14 Backup tab column descriptions (continued)

Column	Description
	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.

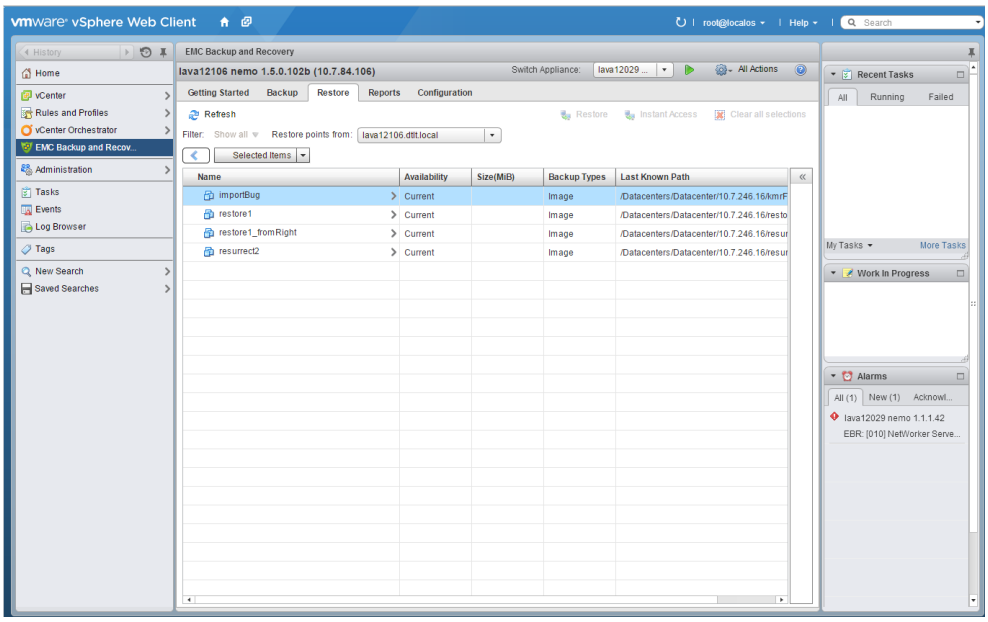
Figure 43 VMware Backup Appliance Backup tab



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 44 VMware Backup Appliance Restore tab



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**.

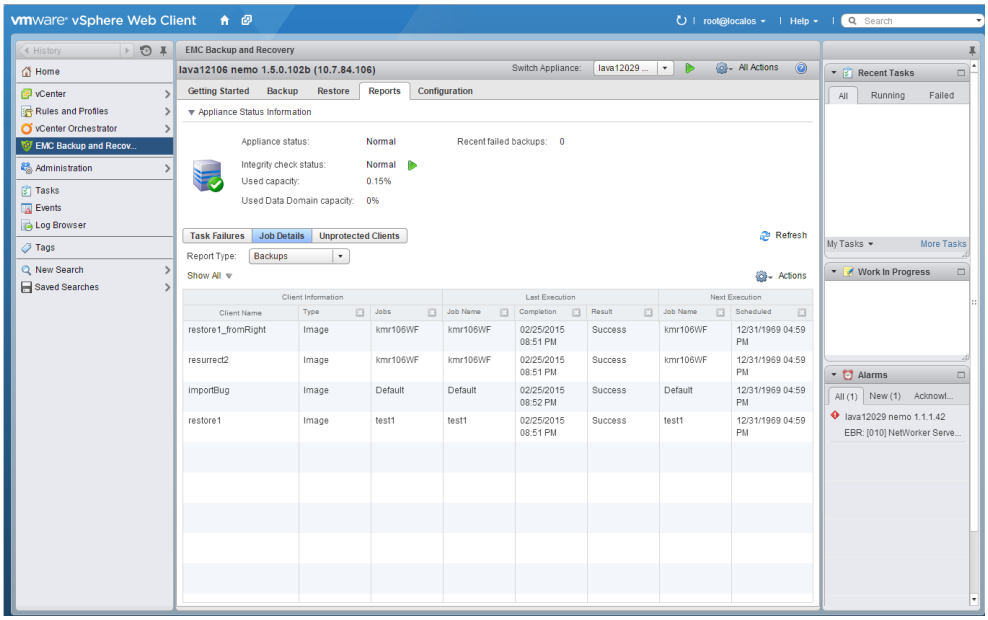
More information on restore is provided in the section Restoring the VMware environment on page 112.

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 45 VMware Backup appliance Reports tab



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 15 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 16 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.

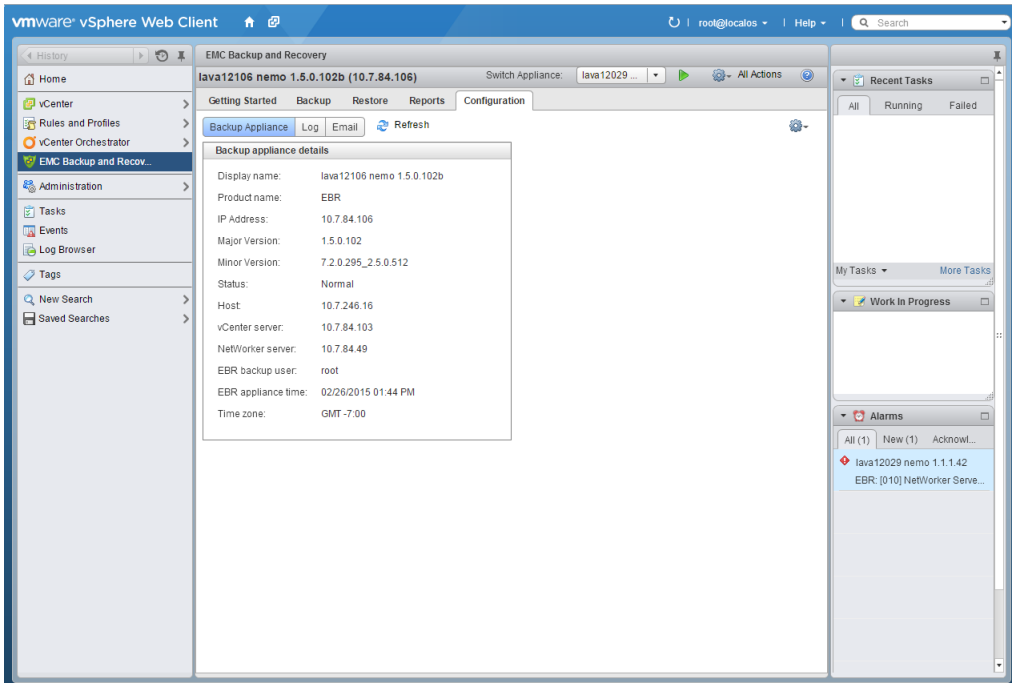
Table 17 Unprotected Clients column descriptions

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 46 VMware Backup Appliance Configuration tab



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 18 Backup appliance detail descriptions

Detail	Description
Display name	The name of the VMware Backup Appliance in the vCenter.
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.

Table 18 Backup appliance detail descriptions (continued)

Detail	Description
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 57.

Viewing and exporting logs

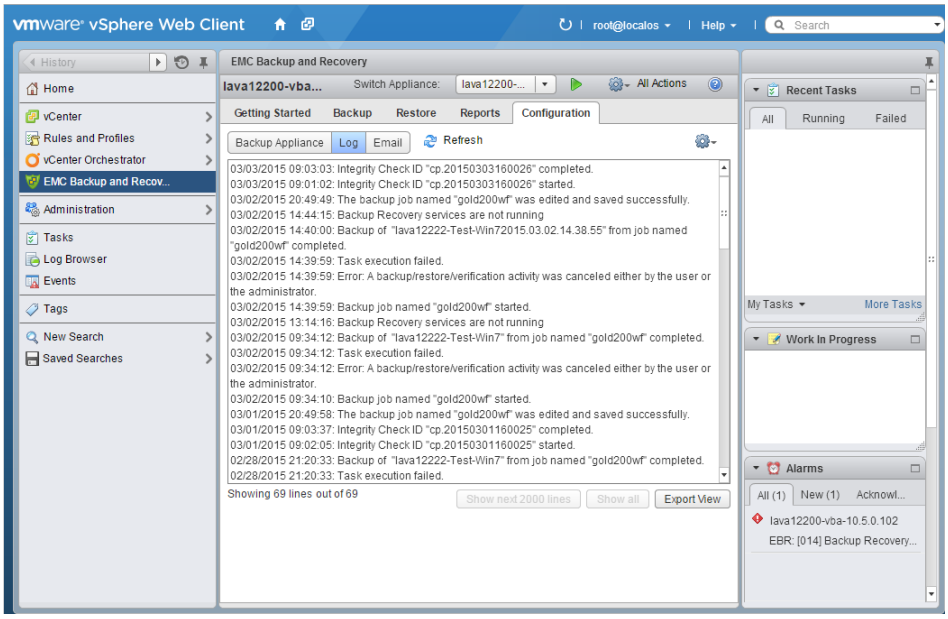
The **Log** view on the **Configuration** tab displays a log that lists the activities that have been initiated with the user interface and that identifies some key status items. You can export the log information as a .log file if needed.

Procedure

1. On the **Configuration** tab, click **Log**.

   A high-level log is displayed.

Figure 47 Log view



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

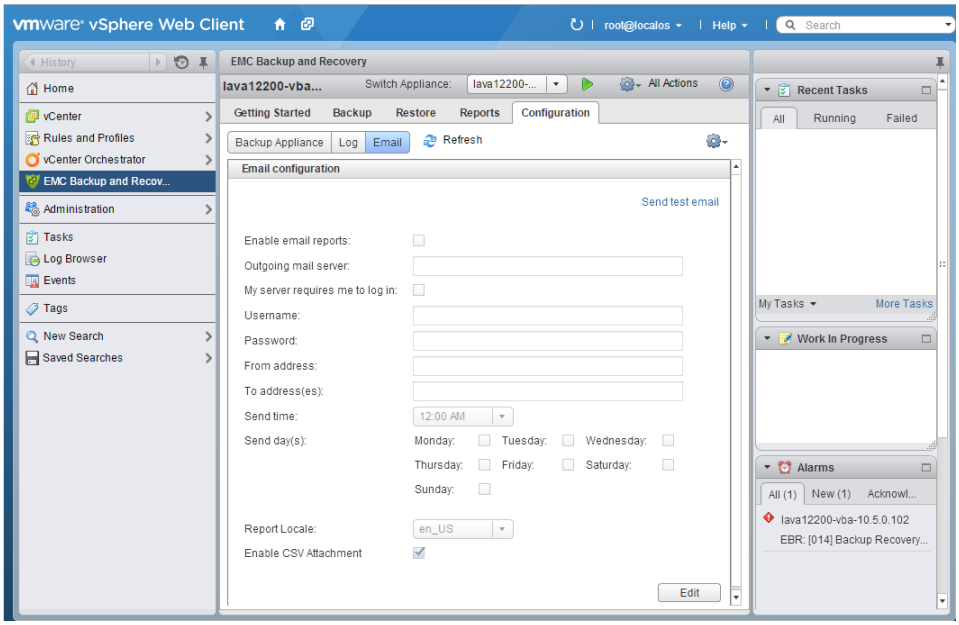
The **Email** view on the **Configuration** tab lets you configure EMC Backup and Recovery to send SMTP email reports to specified recipients.

Procedure

1. On the **Configuration** tab, click **Email**.

   The **Email configuration** screen displays.

Figure 48 Email configuration view



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 19 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.

Table 19 Email configuration field descriptions (continued)

Field name	Description
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.
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 49 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.

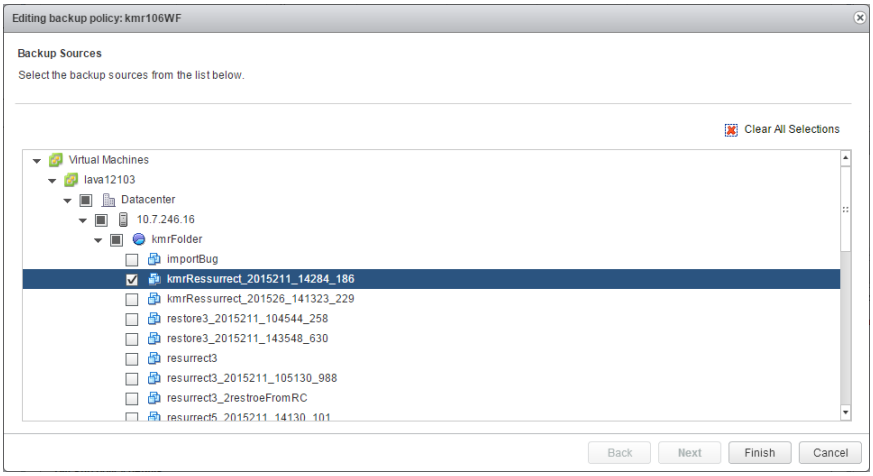
4. Click the checkboxes to select the virtual machines that you want to include in the selected workflow, as shown in the following figure, or expand the virtual machines to select VMDKs. You can also select other inventory objects, for example, Resource Pools or Clusters in addition to specific virtual 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 50 Selecting virtual machines in the Editing backup policy wizard



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 69, 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

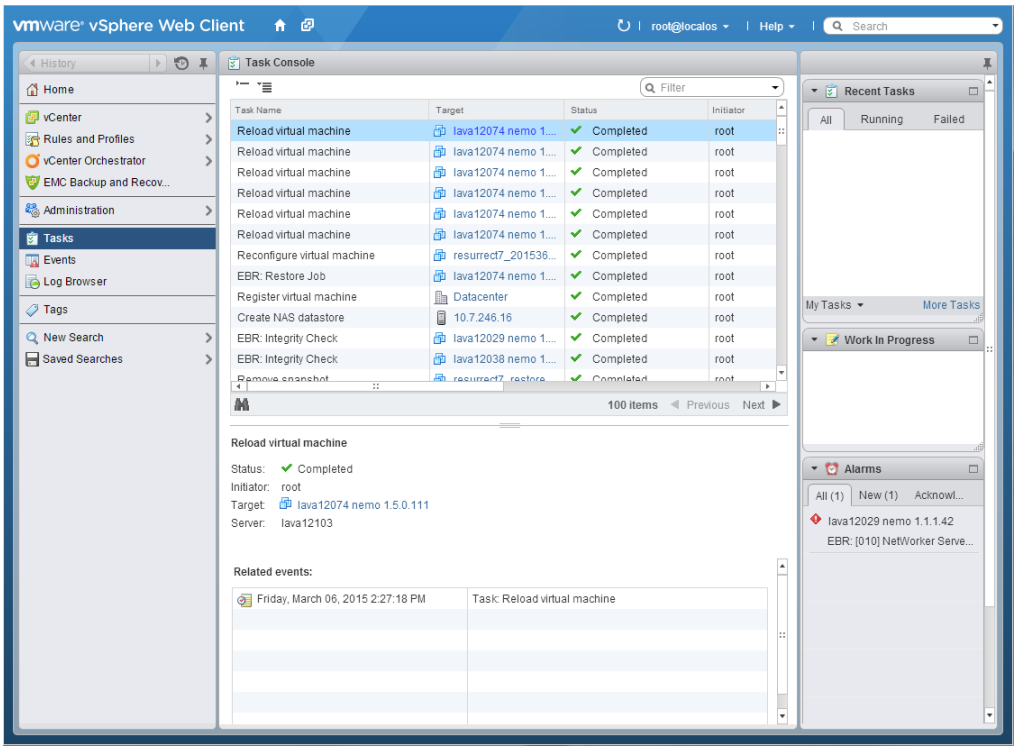
1. Select the **Backup** tab.
2. in the **Recent Tasks** pane, click the circular **x** symbol associated with the workflow.

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 51 Viewing workflow progress in the Task Console



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. Also, when performing any file-level restore, you cannot restore more than 5,000 folders or files, nor can you browse more than 14,498 folders or files in the same file-level restore operation.

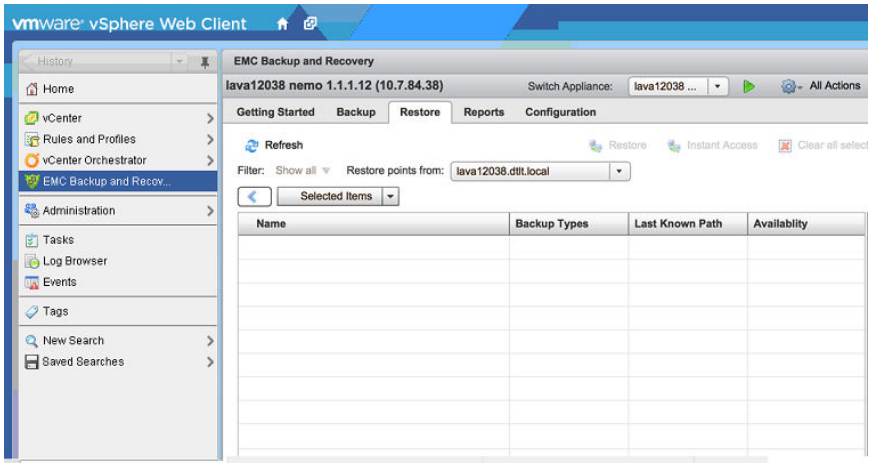
FULLVM (Image-level) Restore

When the backup completes, you can restore full VMs 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 52 Restore tab in EMC Backup and Recovery user interface



Note

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.

Performing a FULLVM restore

Procedure

1. Power off each virtual machine that you want to restore.
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, 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.

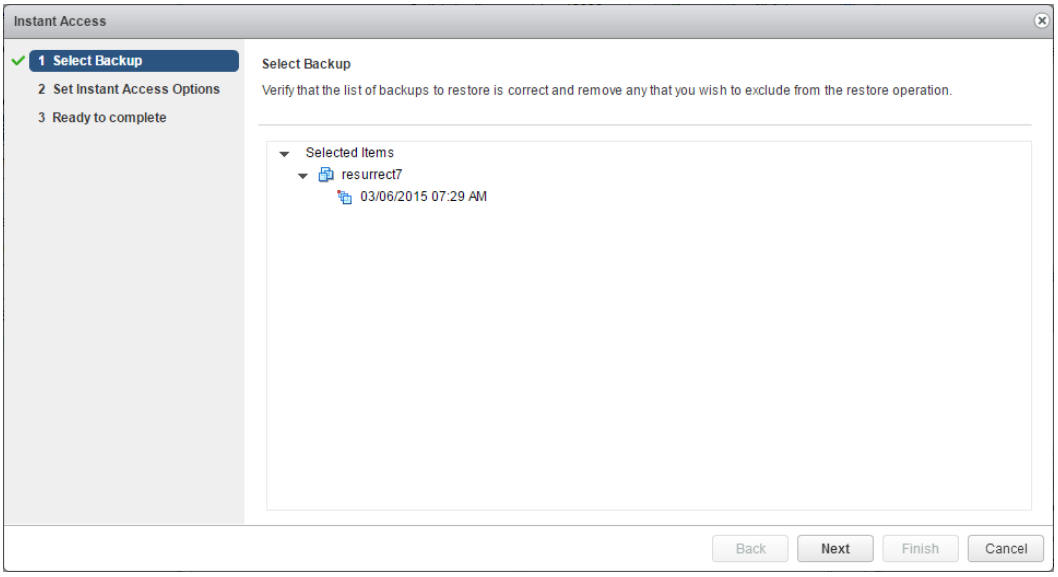
   Note

   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.

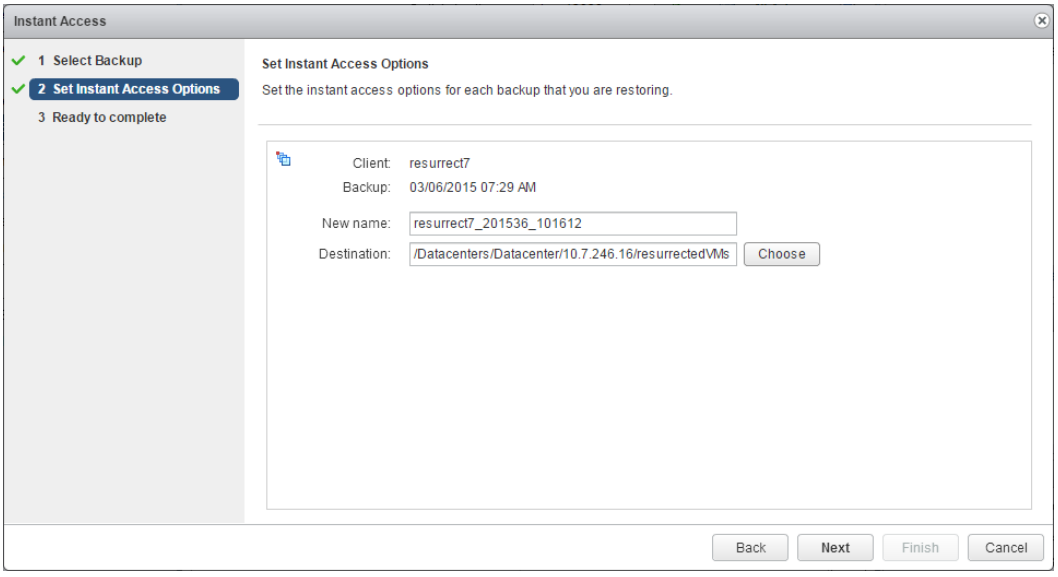
Figure 53 Select a backup



4. Verify that the list of backups is correct, remove any backups that you want to exclude from the restore, and click **Next**.

   The **Set Instant Access Options** page displays.

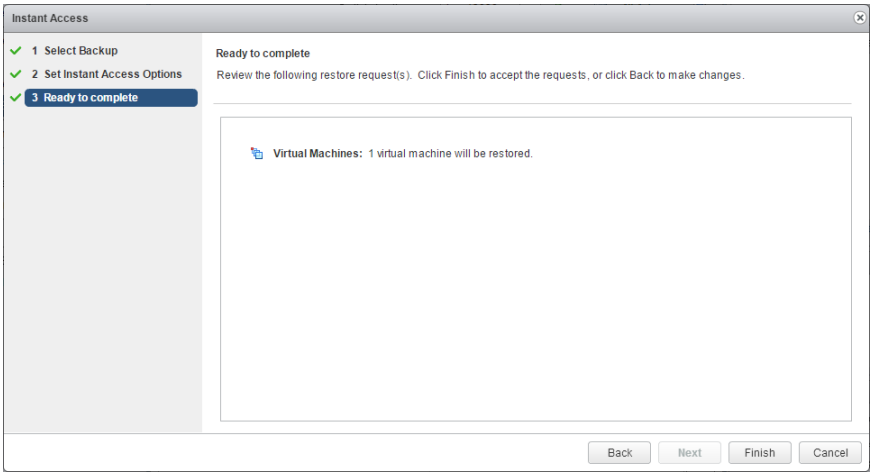
Figure 54 Set instant access options



5. Specify a new name and destination for the restore, and click **Next**.

   The **Ready to complete** page displays.

Figure 55 Ready to complete



6. Review the restore request, and click **Finish**.

   You should see a message that indicates that the instant access operation was successfully completed.

Instant Access restore after applying a security roll-up

If you applied a security roll-up after deploying a VMware Backup Appliance or Proxy appliance, you may be required to manually start the `avagent-ir` service if the service is not running in order to complete an Instant Access restore.

Procedure

1. Use ssh to connect or login to the **EMC Backup and Recovery** Console, and then start the **Instant Access** restore.
2. Switch to the root user, as shown in the following example:

```
# ssh <VBA-host> -l admin
Password:
#su
Password:
```

3. Check the status of `avagent-ir` to determine if it is running:

   `<service avagent-ir status>`

4. If `avagent-ir` is not running, start the service:

   `<service avagent-ir start>`

5. Cancel any running **Instant Access** sessions from the vCenter by using the **EMC Backup and Recovery** user interface in the **vSphere Web Client**, and wait until the sessions are stopped.
6. Start another **Instant Access** restore session.

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

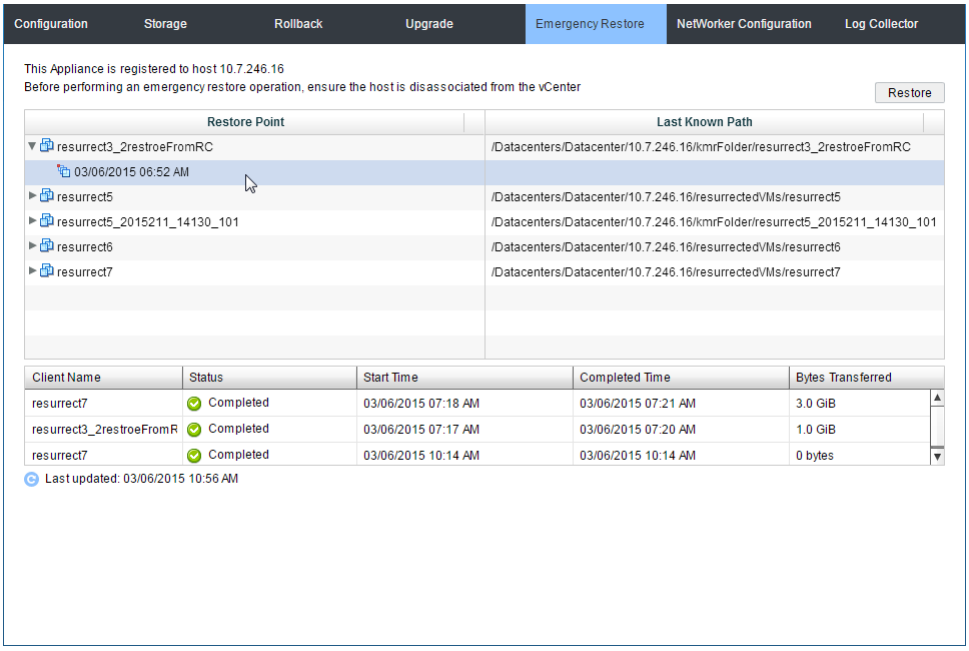
1. Log in to the **EMC Backup and Recovery Configure** window at the following URL using the EMC Backup and Recovery username and password credentials that you defined during configuration:

   `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 56 Emergency Restore window

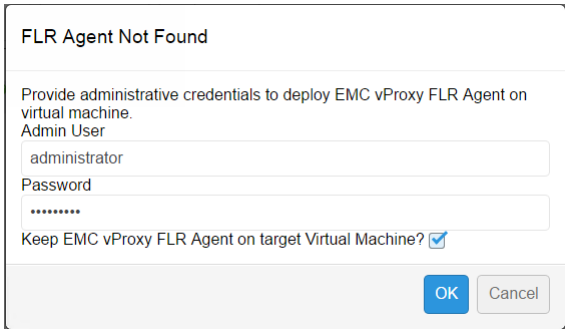


File-level restore

File-level restore allows you to restore specific files and folders from virtual machines by using the **EMC Data Protection Restore Client**, which is part of the base NetWorker client install.

In order to perform file-level restore, the FLR Agent gets installed automatically on the target virtual machine. If the FLR Agent does not get installed and you try to perform a file-level restore, the following message appears. This message additionally presents the option to deploy the FLR Agent.

Figure 57 Deploy FLR Agent if not found



Note

Before you start a file-level restore, review the limitations specified in the section FLR limitations to ensure that you can perform file-level restores in your configuration.

FLR limitations

This section provides a list of limitations that apply to file-level restores.

Note

Before performing a file-level restore, make sure that your browser is updated to the latest version.

- For problems accessing the **EMC Data Protection Restore Client** on the Mozilla Firefox browser, refer to the troubleshooting topic Launching the EMC Data Protection Restore Client after upgrade on Mozilla Firefox browser.
- 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, EMC recommends that you use Internet Explorer or Chrome rather than Firefox 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 FLR. 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.
- All virtual machines must belong to the vCenter that is dedicated to EMC Backup and Recovery. You cannot perform an FLR across multiple vCenters .
- FLR does not support the following virtual disk configurations:
  - Unformatted disks
  - Dynamic 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
- FLR 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 69 provides more information.
- FLR 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 EMC Backup and Recovery appliance, from which you can then perform FLR.
- FLR does not restore ACLs.
- FLR does not restore or browse symbolic links.

- FLR cannot restore more than 5,000 folders or files in the same file-level restore operation.
- FLR cannot browse more than 14,498 folders or files in the same file-level restore operation.
- When you create partitions, fill the lower ordered indices first. That is, 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.
- FLR of Windows 8 and Windows Server 2012 VMs does not support the following file systems:
  - Deduplicated NTFS
  - Resilient File System (ReFS)
  - EFI bootloader

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.

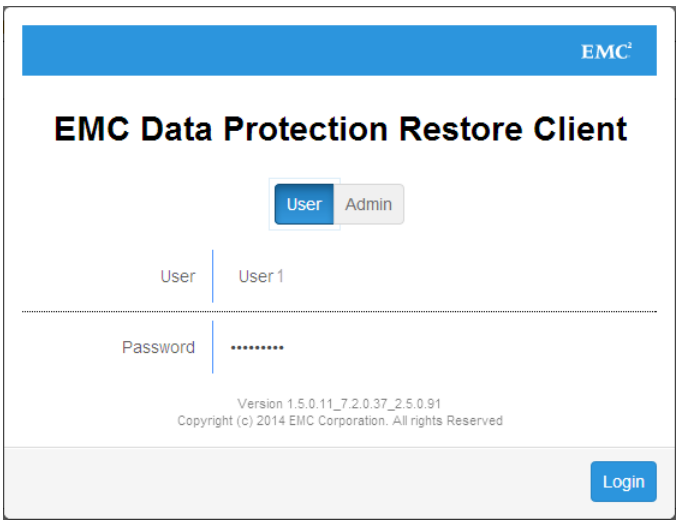
Procedure

1. Connect to the host that will receive the FLR 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 figures provides an example of the user login window.

Figure 58 EMC Data Protection Restore Client User Login



Note

You must connect to the VMware Backup Appliance from a web browser on the virtual machine that will receive FLR data.

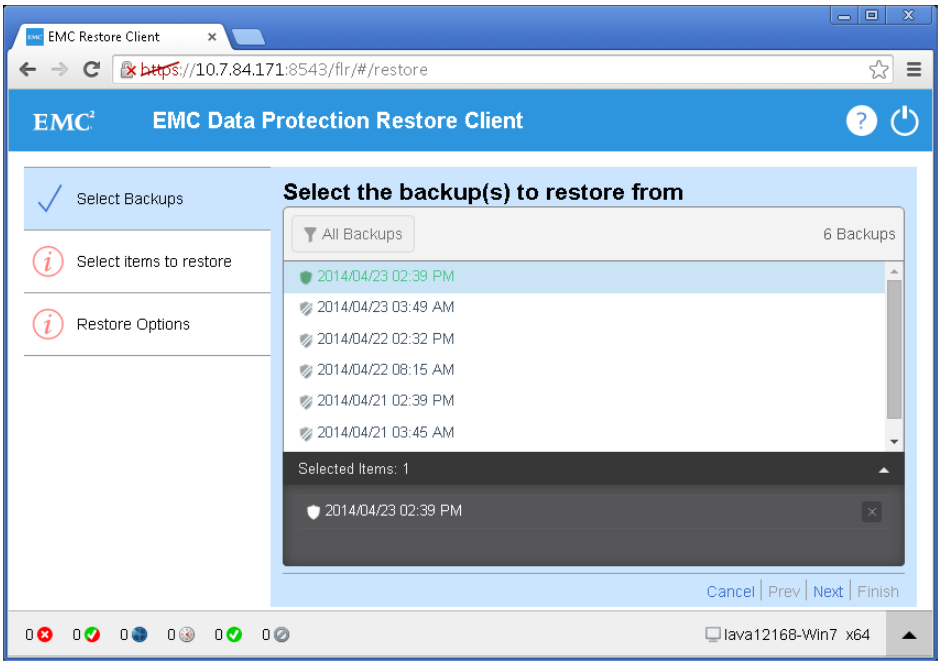
3. Select the **User** tab, and then log in to the Restore Client with the local administrative credentials of the virtual machine to which you are logged in.

   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 59 Select the backups to restore from page

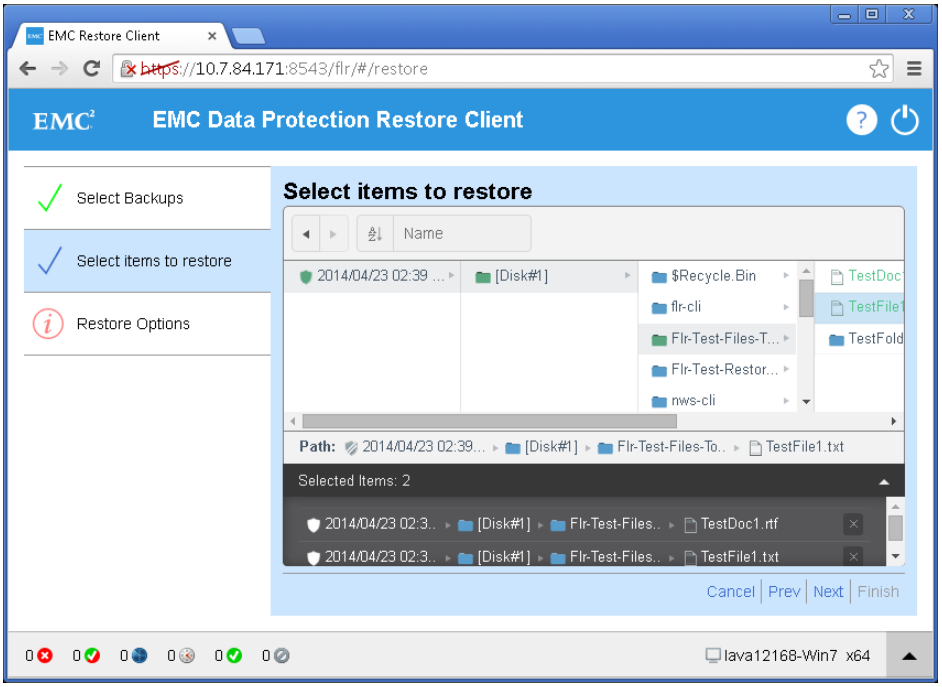


Note

When you click **Next**, if a folder hierarchy does not appear, FLR may not support the file system in use on the virtual machine. The section FLR limitations on page 120 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 recovery 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.

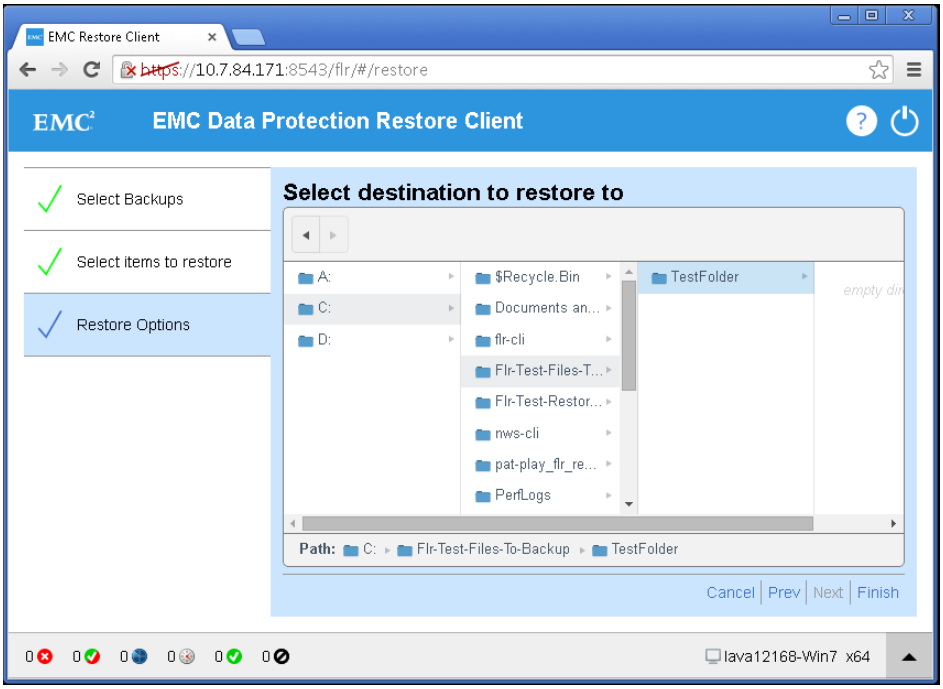
Figure 60 Select items to restore page



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 61 Select destination to restore to page



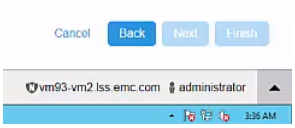
7. Click **Yes** when you are prompted to continue the restore.

   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 62 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 63 Restore Monitor panel

   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 FLR, as in the following example:

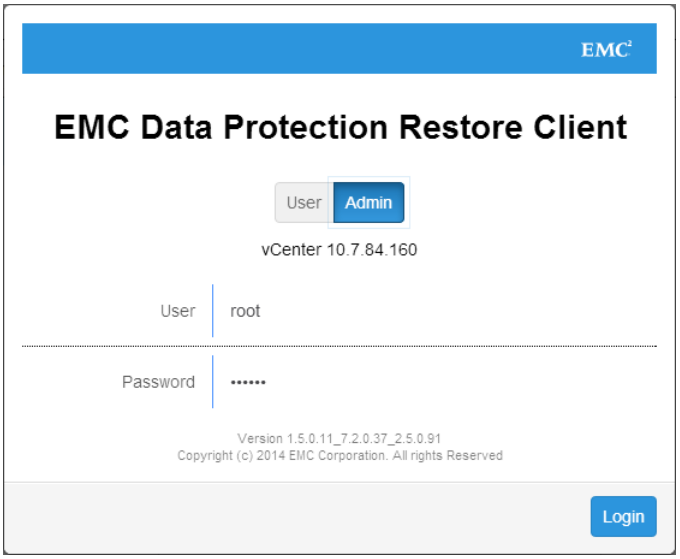
   `http://VMware_Backup_appliance_host:8580/flr`

   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 EMC Backup and Recovery appliance to the vCenter Server.

   The following figure provides an example of the Admin login window.

Figure 64 EMC Data Protection Restore Client Admin Login



Note

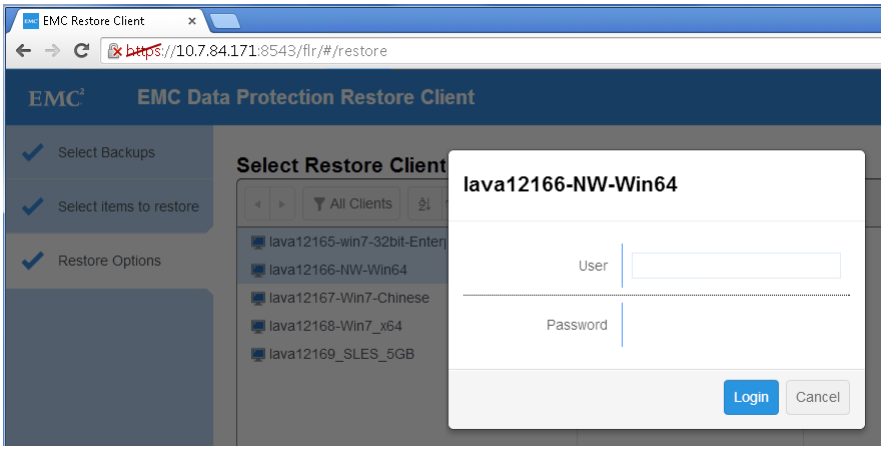
When you use **Admin** mode, ensure that the user you specify for the vCenter login has the correct privileges to use this option.

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 recovery. You can sort items by Name, Date, and so on. Items marked for recovery 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 65 Select and log in to the destination client

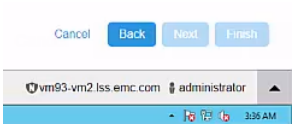


6. Log in to the client.
7. Select the destination location where you want to restore the file.
8. Click **Finish**.
9. Click **Yes** when you are prompted to continue with the restore.

   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 66 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 67 Restore Monitor panel

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 20 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

Table 20 EMC Backup and Recovery alarms (continued)

Alarm Name	Alarm Description
	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.
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.	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.	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 129
- Save set lifecycle on page 130

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 are lost.

Thick provisioning allocates all of the required storage when the disk is created. EMC recommends that you create a thin provisioned disk when you deploy the EMC Backup and Recovery appliance, and then convert the disk to thick provisioning after the deployment completes. This allows you to deploy the appliance rapidly

Note

VMware documentation provides for details about how to inflate thin provisioned disks to thick provisioned disks. This procedure requires that you shut down the VMware Backup Appliance and might 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.

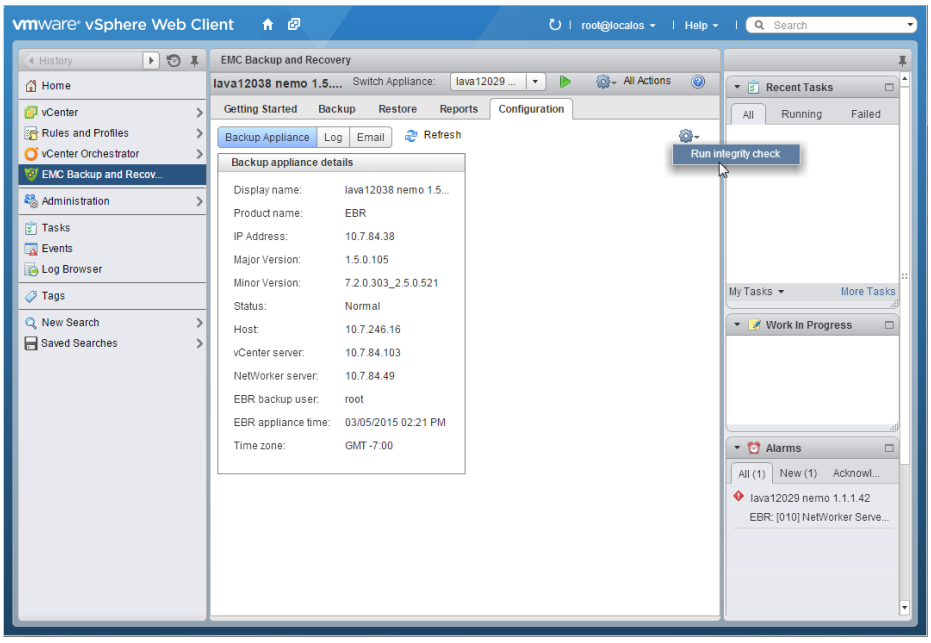
Creating a checkpoint using the EMC Backup and Recovery user interface

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 136 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 68 Running an integrity check



Rolling back to a checkpoint

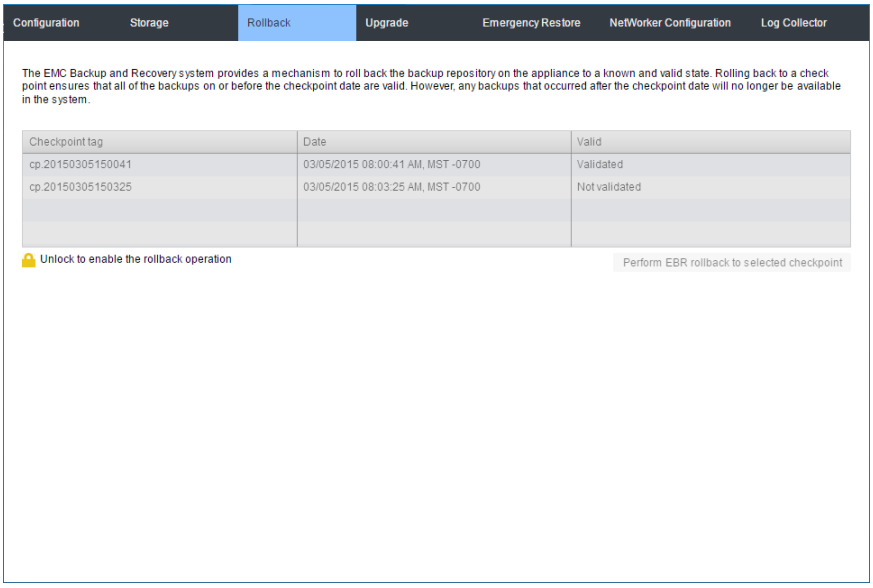
Rollback is a setting in the EMC Backup and Recovery **Configure** window that allows you to automatically roll back to the last validated checkpoint when performing a disaster recovery.

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 69 Roll back to checkpoint



Note

NetWorker does not support disaster recovery from a checkpoint backup that was performed when the appliance used an OVA version that is earlier than the currently installed OVA version. For example, if you upgrade to a NetWorker 9.0.1 server and OVA 1.5.0.159 from NetWorker 8.2 SP1 and OVA 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 136 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 OVA version as the OVA version currently installed on the appliance. NetWorker does not support a disaster recovery from a checkpoint backup that was created when the using a previously installed OVA version. For example, if you upgrade to a NetWorker 9.0.1 server and OVA 1.5.0.159 from NetWorker 8.2 and OVA 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 129 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.

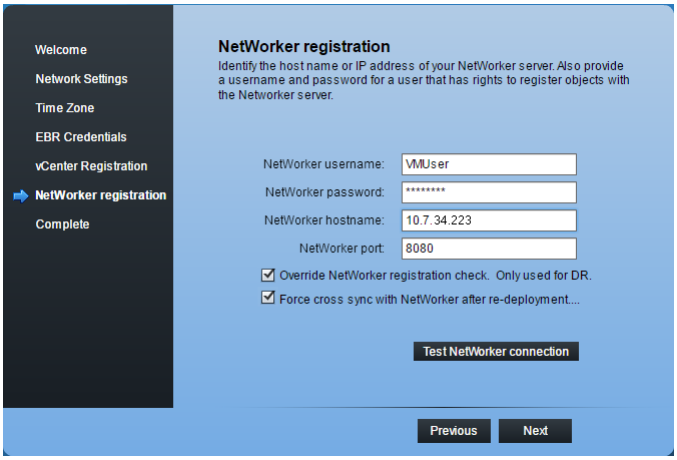
   EMC Backup and Recovery Configuration Utility on page 51 provides instructions.

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 70 Networker registration during new appliance configuration



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 150 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 51.

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:

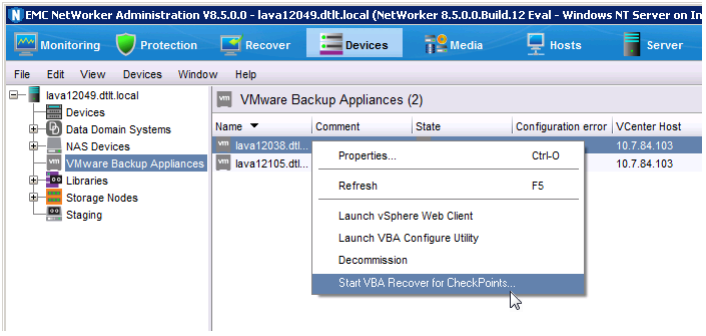
   ```
   /usr/local/avamarclient/etc/initproxyappliance.sh start
   ```

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 71 Starting a VMware Backup Appliance disaster recovery



   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 136.
- 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:

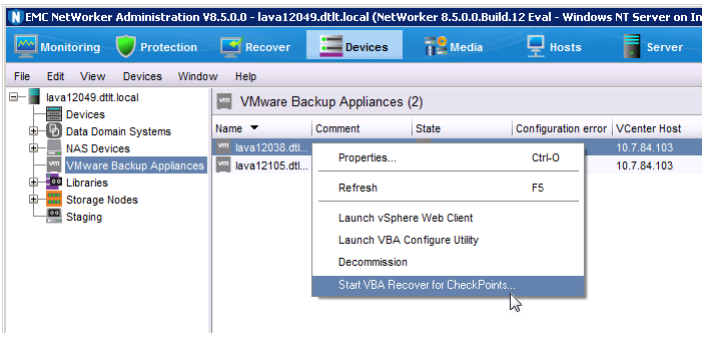
   ```
   /usr/local/avamarclient/etc/initproxyappliance.sh start
   ```

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 72 Starting a VMware Backup Appliance disaster recovery



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.

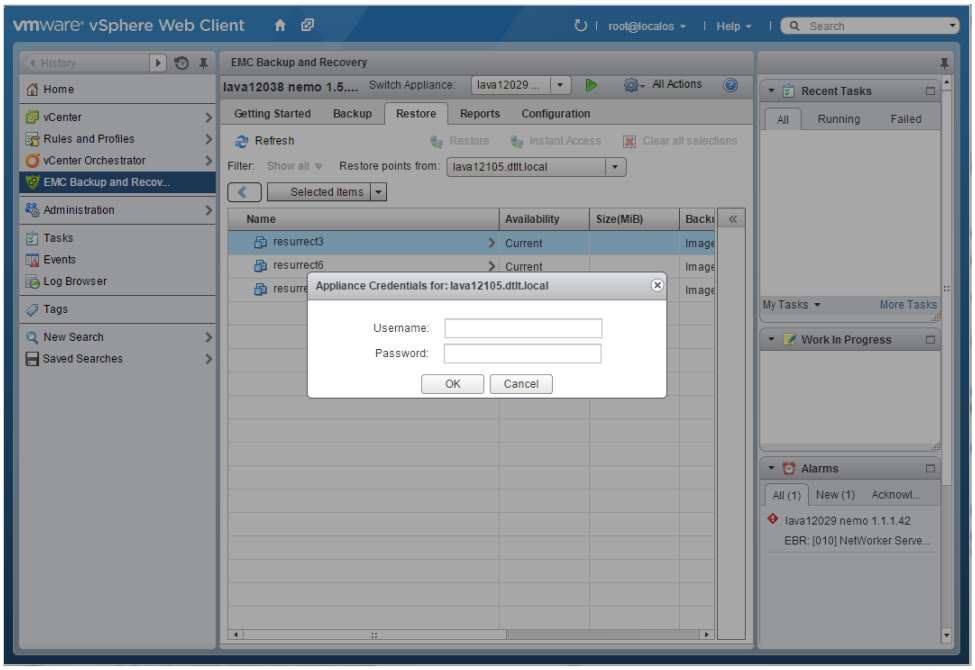
This feature allows you to perform restores for all backups using any available VMware Backup Appliance on any available vCenter as long as they are connected to the same NetWorker server where the backup was performed.

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 73 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 113 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 21 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

Table 21 Scalability Factors (continued)

Component	Recommended count	Notes
		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. 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

Table 21 Scalability Factors (continued)

Component	Recommended count	Notes
		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 22 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
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 23 Concurrency/parallelism recommendations

Component	Concurrency count	Notes
vCenter	50 concurrent sessions	EMC recommends a maximum of 50 concurrent virtual

Table 23 Concurrency/parallelism recommendations (continued)

Component	Concurrency count	Notes
		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.

NetWorker VMware Protection best practices

Observe the following best practices when using the NetWorker VMware Protection solution.

For best practices specifically related to deployment of the VMware Backup Appliance, the section VMware Backup Appliances best practices provides details.

- 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 9.0.1 with OVA 1.5.0.159.
- 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.
- EMC recommends 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 *EMC 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, review the following limitations and unsupported features.

Note

Ensure that you also review the VMware limitations at: http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-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.

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 spaces or other special characters

Using spaces and other 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 202211 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 168524 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 201908 at http://support.emc.com provides possible workarounds and more information on this issue.

Data Domain SMT not supported

NetWorker VMware Protection does not support Data Domain SMT. You can create a different user to segregate access to specific DD Boost devices, but not to a specific secure multi-tenancy (SMT) unit. If you want to protect both Guest and VM images, you must create two specific DD Boost users; one for the guest backup with SMT, and one for the VM image backup without SMT.

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.

The following knowledgebase article provides more information about this issue and instructions on how to perform successful backups to a Data Domain device over WAN when TLS is used.

https://emc--c.na5.visual.force.com/apex/KB_BreakFix_1?id=kA1700000001ED5 .

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 EMC Backup and Recovery 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 5.5 and later
- Ensure that the Data Domain system does not reach the MTree limit and max-streams limit
- Ensure that the DDBoost user has administrator privileges
- 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 NetWorker services are up before you configure the EMC Backup and Recovery appliance
- Ensure that the relevant devices are mounted
- Wait until you successfully configure a policy before you run the policy.

VMware Backup Appliance configuration

- Supports configuration on thin disks.
- Use the EMC Backup and Recovery Configure window 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 27 provides more information.
- Confirm that the hardware meets the minimum hardware requirements (see System requirements on page 27 provides more information.
- Confirm that DNS is properly configured for the VMware Backup Appliance (see Pre-installation requirements on page 32 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:#suPassword:
```

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 EMC Data Protection Restore Client after upgrade on Mozilla Firefox browser

After upgrading the VMware Backup Appliance from a NetWorker 8.1 or 8.2 release to NetWorker 9.0, the **EMC Data Protection Restore Client** window may not launch when using the Mozilla Firefox browser.

If you cannot launch the **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 8.1 or 8.2 release to NetWorker 9.0, 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`.

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 150 provides more information.

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*
```

Log file locations

Review the following EMC Backup and Recovery 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 57.
2. On the **Status** tab, click **Collect Logs**.
3. Click **Collect logs**.
4. Save the zip file 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.

Adding or removing a policy to or from a VM using VMware view results in "RPC server is unavailable" error

If you are using version 9.0 of the NMC, and add a NetWorker 8.2 server and an 8.2 compatible Virtual Backup appliance, you may see the error, `RPC server is unavailable`.

To address this issue, do one of the following:

- Use the EMC Backup and Recovery UI for the 8.2 Virtual Backup appliance to add and remove VMs to and from policies.

- If the first choice is not suitable, use an 8.2 version of the NMC to use the Networker server to add and remove VMs to and from policies.

“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, EMC recommends updating 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 *EMC 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 32 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.

Backups fail with external proxy after upgrading from NetWorker 8.1.*x* to 9.0.1

Backups may fail with the external proxy after an upgrade from NetWorker 8.1.*x* to version 9.0.1 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.emc.networker.ebr**".
4. From the Methods table, select **UnregisterExtension**.
5. Type **com.emc.networker.ebr** 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 129.

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 VMs from one physical server to another. You cannot run vMotion operations on the 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 VM name, datastore, folder, or datacenter names

When you use special characters in the VM name, datastore, folder, or datacenter names, the .vmx file is not included in the backup. The VMware Backup appliance does not backup 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 34 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 3

VADP Backup and Recovery (legacy)

This chapter contains the following topics:

- Software and hardware requirements 164
- Limitations and unsupported features 165
- Transport modes 167
- Changed Block Tracking (CBT) 168
- Configuring the VADP proxy host and Hypervisor resource 168
- Configuring a virtual client for backup 173
- Creating a VADP User role in vCenter 175
- Configuring Changed Block Tracking (CBT) 178
- Monitor VMs 180
- Recovering VADP Backups 180
- VADP Planning and Best Practices 189

Software and hardware requirements

The software and hardware requirements for VADP include the following.

Note

The NetWorker Online Compatibility Guide available on the EMC Online Support site at https://support.emc.com/products/1095_NetWorker provides the most up-to-date compatibility information.

- One or more VADP proxy systems running any of the following 64-bit operating systems (English versions only):
  - Windows Server 2003 R2
  - Windows 2008 R2
  - Windows 2008
  - Windows 2012
- One or more vCenter servers running any of the following versions:
  - vSphere 5.0 with ESX 5.0 and vCenter 5.0
  - vSphere 5.1 with ESX 5.1 and vCenter 5.1 U3
  - 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 5.0, 5.1, 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

     The section Limitations to vSphere 5.5 and 6.0 support provides information on limitations when using vSphere 5.5 or 6.0 with the VADP solution.
- 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 8.0 or later client software on the VADP Proxy host.
- The NetWorker server requires NetWorker 8.0 or later software.
- The VADP proxy host must have access to the LUNs required for backing up 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 203 provides more information.
- You must install VMware tools on the VM to ensure consistent state backups. Also, backups via FQDN/hostname require VMware tools.

Note

The **comreg.exe** program, part of the VMware tools installer, contains a Windows 2008 R2 bug that prevents registration of the VMware Snapshot Provider with VSS. VADP backups of a Windows Server 2008 R2 or Windows 7 VM may fail for certain versions of ESX 4.0.0 due to this issue.
The following knowledgebase article provides Instructions for fixing this issue: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1022720
To resolve this issue, upgrade to ESX 4.0 update 2 or ESX 4.1, or to upgrade your ESX 4.0.0 server with a VMware patch, navigate to the following link: http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1013127.

Limitations and unsupported features

The following limitations apply to the VADP solution with NetWorker:

- NetWorker supports the backup/recovery of non-English versions of guest operating systems for the VMs. However, if using non-English versions of the Windows operating system for the vCenter or VADP proxy host, note the limitations in the sections Limitations to vCenter on non-English versions of Windows on page 165 and Limitation for VADP proxy host on non-English versions of Windows on page 166.
- Global directives are not supported by NetWorker for VADP backup and recovery. Both encryption and compression directives result in backup failure in *FULL* and ALLVMFS workflows. FLR-disabled image backups complete successfully.
- For image-level backups, an incremental backup of a VM is not supported after a hardware change, OS patch update, Service Pack update, drivers update and so on. Perform a full image-level backup after every change made at the operating system and hardware level on the VM.

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.

Limitations to vSphere 5.5 and 6.0 support

The following limitations apply to vSphere 5.5 and 6.0 support with NetWorker:

- VADP does not support backups to the vCenter server with the Transport Layer Security (TLS) protocol in vSphere 6.0. In the **vCenter Server Settings** window, under **Advanced Settings** set **SSL version** to either **All** or **SSLv3**.
- Intermittent VADP backup failures occur when using NBDSSL as the transport mode. If you restart the backup after the failure, the backup completes successfully. To ensure the backup does not fail, use NBDSSL|NBD as the backup transport mode. When this mode is specified, if NBDSSL fails at some point, the backup continues with NBD mode.
- When you run many backup processes at the same time, some of the processes might crash with aSIGSEGV segmentation fault after many iterations due to a possible race condition in VixDiskLib.
- When using NBD transport mode, EMC recommends backing up no more than 4 clients in parallel. When you use NBD transport mode to back up more than four VADP clients in parallel, the backup fails with a message indicating “Unable to download config file with more than 5 clients parallel backups with NBD as transport mode.”

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 backup or recovery:

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

  SAN mode requires a physical proxy with SAN access, and the VMs need to be hosted on either 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 backup related I/O happens internally through the ESX I/O stack using SCSI hot-add technology. This provides better backup I/O rates than NBD/NBDSSL. However, selecting this mode places backup related CPU, memory and I/O load on the ESX hosting the VADP proxy.

  Hotadd mode requires a virtual proxy, and the ESX hosting the virtual proxy should have access to all the datastores where the VMs are hosted So, if the datastores are SAN/iSCSI/NFS and if the ESX server where the VADP proxy resides is separate from the ESX server where the VMs are hosted, then:
  - In the case of SAN LUNs the ESX hosting the proxy and the ESX hosting the VMs should be part of the same fabric zones.
  - In the case of iSCSI LUNs the ESX hosting the proxy and the ESX hosting the VMs should be configured for the same iSCSI-based storage targets.
  - In the case of NFS datastores, the ESX hosting the proxy and the ESX hosting the VMs should be configured for the same NFS mount points.
- NBD (Network Block Device): in this mode, the CPU, memory and I/O load gets directly placed on the ESX hosting the production VMs, because the backup data has to move through the same ESX and reach the proxy over the network. NBD mode can be used either for physical or virtual proxy, and also supports all storage types.
- NBDSSL (Network Block Device with SSL): NBDSSL transport mode is the same as NBD except that the data transferred over the network is encrypted. Data transfer in NBDSSL mode can therefore be slower and use more CPU due to the additional load on the VADP host from SLL encryption/decryption.

  For recovery of VMs using NBDSSL mode, refer to the section Recovering a VM using NBDSSL, SAN, or Hotadd transport mode on page 188.

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 24 on page 169.

Changed Block Tracking (CBT)

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

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

Check if your VM has CBT enabled, or enable CBT, by performing the steps outlined in Configuring Changed Block Tracking (CBT) on page 178.

Independent persistent disks are not backed up

VADP does not support the backup and recovery of independent persistent disks. If NetWorker detects these disks during backup, they are skipped and a message is logged that indicates the disks were skipped. If using independent persistent disks, you must use the traditional NetWorker style backup for protecting the data on the independent persistent disks via the backup client installed inside the VM.

Configuring the VADP proxy host and Hypervisor resource

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

You can create a NetWorker client for the VADP proxy host manually by using the `nsradmin` command.

Note

The VADP proxy host can be the NetWorker server. Also, 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 45.

Before creating a Hypervisor resource for vCenter, ensure that the NetWorker client software is installed on the vCenter server.

If vCenter is not configured in the environment, there must be a Hypervisor resource created for each server in the environment.

VADP backups will work even if you do not install the NetWorker client on vCenter or VirtualCenter, however, you must create the corresponding Hypervisor resource in the NetWorker server prior to starting the VADP backups.

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
```

Note

If using the NetWorker VMware Protection solution, 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 NetWorker client for the VADP Proxy host by using the Client properties windows

Table 24 Application information values

Attribute name	Description	Default value
VADP_BACKUPROOT	• Directory in which all of the VM backup jobs are supposed to reside. Ensure that the directory already exists or VADP backup jobs will fail with “directory does not exist” error. • The directory must be on a local disk and not on a CIFS share. • This directory cannot be encrypted. • For each backup job, a directory with a unique name derived from the *	C:\mnt

Table 24 Application information values (continued)

Attribute name	Description	Default value
	backup type and the VM name will be created here. • "If omitted, BACKUPROOT defaults to c:\\mnt. Example: VADP_BACKUPROOT=C:\\mnt"	
VADP_DISABLE_FLR	If a virtual client is set up for image level backup and image level recovery (single step), setting VADP_DISABLE_FLR=Yes will disable file level recoveries from the image backup. This variable only takes effect if the virtual client's backup saveset is specified as *FULL*, which indicates an image level backup, and the backup level is full (0) with no incremental backup levels selected. Setting this variable in the proxy application information and not specifying it at the virtual client level will disable file level recovery from all subsequent image backups done via the proxy	No
VADP_HOST 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. Example: VADP_HOST=any.vc VADP_HOST=another.vc	
VADP_MAX_RETRIES	Number of times an operation is re-tried after it fails. Use this option if you see a large number of backup jobs fail with "resource busy" errors. Usually, backup software will retry failed jobs, but it might be hours until the backup	0

Table 24 Application information values (continued)

Attribute name	Description	Default value
	software retries. Example VADP_MAX_RETRIES=1	
VADP_MAX_BACKOFF_TIME	Number of seconds to wait before retrying a failed operation. If you change this default, also change the default for MAX_RETRIES (because this setting only applies if MAX_RETRIES is larger than 0). VADP_BACKOFF_TIME=20	10
VADP_TRANSPORT_MODE	Specify the transport mode to transfer data from a VMFS data store to a VADP proxy server. The following options are supported: • SAN – Virtual disk data is read directly off a shared storage device that the virtual disk resides on. This requires VMFS storage on SAN or iSCSI and the storage device has to be accessible from both ESX and the VADP proxy. • Hotadd – This mode can be used when VADP is used in a virtual proxy. Because it uses the ESX I/O stack to move data, Hotadd is more efficient than the transport mode NBD. • NBDSSL – This mode is the same as nbd except that the data transferred over the network is encrypted. The data transfer in nbdssl mode can be slower and use more CPU than in the nbd transport mode. Also, For recovery of VMs using NBDSSL mode, refer to the section Recovering a VM using NBDSSL, SAN, or Hotadd transport mode on page 188.	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.

Table 24 Application information values (continued)

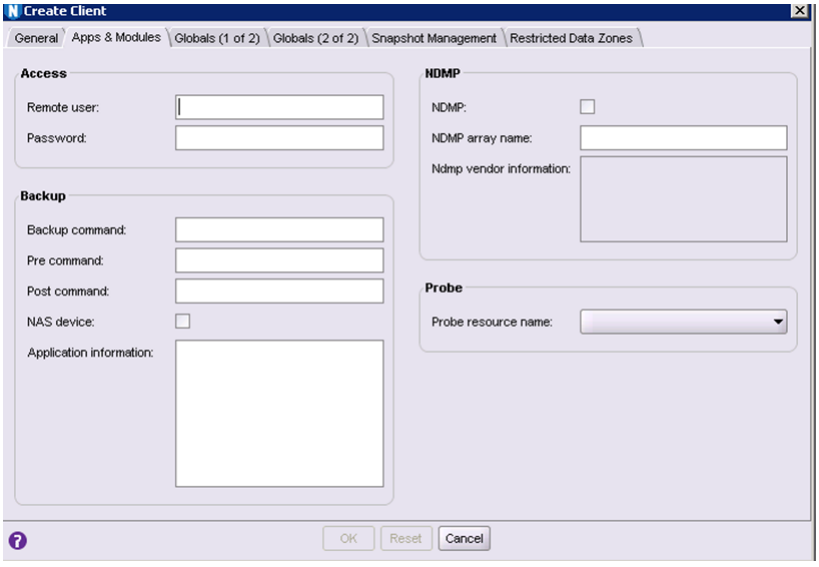
Attribute name	Description	Default value
	• NBD – VADP will use an over-the-network protocol to access the virtual disk. Data is read from the storage device by the ESX host and then sent across an unencrypted network channel to the VADP proxy. Please note that this mode does not provide the offload 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.	

Procedure

1. In the NMC **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 74 Apps and Modules tab in NMC



5. In the **Application Information** field, type the following:

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

6. Click **OK**.

Configuring a virtual client for backup

You can configure a virtual client manually by using the **Client Properties** window. You can create a new Client resource or modify an existing one. Instructions are provided in Configuring a virtual client manually.

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

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

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

Note

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

The following table lists the recovery options that are available based on the virtual client's configuration. Recovery steps are described in Recovering VADP Backups on page 180.

Table 25 Recovery options that are available based on the virtual client configuration

Backup Configuration	File level recovery	Image level (single step) recovery
Virtual client with NTFS** OS and the ALLVMFS save set is selected.	Yes	No
Virtual client with NTFS** OS and the *FULL* save set is selected.	Yes	Yes
Virtual client with NTFS** OS and the *FULL* save set is specified and the backup level is full (no incremental	No	Yes

Table 25 Recovery options that are available based on the virtual client configuration (continued)

Backup Configuration	File level recovery	Image level (single step) recovery
backups) and the `VADP_DISABLE_FLR` APPINFO variable is set to Yes.*		
Virtual clients that are not using the NTFS** OS and that have the *FULL* save set selected.	No	Yes

*The VADP_DISABLE_FLR variable, if set to Yes, performs an image-level backup of the entire VMDK file.

The VADP_DISABLE_FLR variable, if set to No (default), performs an image-level backup using the VMware Virtual Disk Development Kit (VDDK), which performs file reads of the VMDK data. Backup and recovery takes longer using this method due to the different workflow to accommodate file level recovery.

The VADP_DISABLE_FLR variable does not apply to virtual clients that have the ALLVMFS save set selected for backup. Additionally, if the VADP_DISABLE_FLR variable is specified on both the virtual client and on the VADP proxy, the setting on the virtual client takes precedence.

** NTFS implies NTFS of the following operating systems:

- Windows 2003
- Windows 2008
- Windows 2008 R2
- Windows Vista
- Windows XP
- Windows 7

Configuring a virtual client

Procedure

1. In the NMC **Protection** window, right-click **Clients** and select **New**.
2. Select the **General** tab.
3. In the **Name attribute** field, type the name of the proxy client.
4. In the **Save Set** attribute, type the name of the files or directories to be backed up:
   - To specify a file or directory for backup such as C drive, type `c:\`.
   - To backup all VM file systems, type `ALLVMFS`.
   - To backup up the entire VM image, type `*FULL*`.
5. Disable the **Backup renamed directories** field, which is enabled by default.
6. Select the **App and Modules** tab.

a. In the **Backup command** field, type `nsrvadp_save`.

b. In The **Application Information** field, add the vCenter name or IP address; for example, **VADP_HYPERVISOR=vcenter.ebr.com**.

7. In diagnostic mode, select **VADP** for the **Proxy backup type**, and specify the **Proxy backup host**.
8. Select the **Globals (2 of 2)** tab.
9. Under **Configuration**, type `*@*` in the **Remote access** field.
10. 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 back up and recover using VADP on page 176 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 back up and recover using VADP

EMC recommends creating a single VADP User role with the backup and recovery privileges specified in the following tables. You can then use the associated user for VADP backup and recovery operations.

The following table provides VADP backup privileges.

Table 26 VADP backup privileges

Setting	Privileges
Virtual machine > Configuration	• Add existing disk • Add or Remove device • Change Resource • Disk Change Tracking • Disk Lease • Raw device • Remove disk • Settings
Virtual machine > Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download
Virtual machine > Snapshot Management	• Create snapshot • Remove snapshot
Datastore	• Browse datastore • Low level file operations
Session	• Validate session
Global	• Cancel task • Licenses • Log Event • Settings
Tasks	• Create task • Update task

The following table provides VADP recovery privileges.

Table 27 VADP recovery privileges

Setting	Privileges
Global	• Cancel task • Licenses • Log Event • Settings
Resource	• Assign virtual machine to resource pool
Datastore	• Allocate space • Browse datastore • Low level file operations • Remove file • Update virtual machine files (only found in 4.1 and later)
Virtual machine > Inventory	• Create new • Register • Remove • Unregister
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 setting • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility

Table 27 VADP recovery privileges (continued)

Setting	Privileges
Virtual machine > Interaction	• Power Off • Power On • Reset
Virtual machine > Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download
Virtual machine > State	• Create snapshot • Remove snapshot • Revert to snapshot
Network	• Assign network • Configure
Session	• Validate session
Tasks	• Create task • Update task

Configuring Changed Block Tracking (CBT)

You can check if your VM has CBT enabled or enable/disable CBT by setting the variable VADP_DISABLE_CBT, or by using the command line executable, nsrvadp_modify_vm.exe.

Note

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

Configuring CBT using the variable VADP_DISABLE_CBT

Setting the variable *VADP_DISABLE_CBT* allows you to control the enabling or disabling of CBT. This option is available in NetWorker 8.0 SP1 and later.

Setting VADP_DISABLE_CBT = YES disables CBT. CBT will not be used for incremental backups.

Setting VADP_DISABLE_CBT = NO enables CBT prior to performing image backups. Handling of FLR based incremental backups does not change.

Note

If VADP_DISABLE_CBT is not configured, no attempt is made to enable CBT before performing image backups. Handling of FLR based incremental backups does not change.

Configuring CBT using the nsrvadp_modify_vm command

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

From the command line, specify the following format:

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

Where:

- *directory* is the location of the executable (for example, c:\bin\nw762\nsr\bin)
- *vCenter server* is the vCenter server hostname
- *protocol* is the protocol to use with the web service. Can be one of the following:
  - http
  - https
- *user* is the vCenter user name
- *password* is the vCenter user password
- *lookup method* is the lookup method to use. Can be one of the following:
  - vm-name
  - ip-addr
  - dns-name
- *lookup key* is the lookup key to use
- *command* is where you specify one of the following CBT options:
  - cbt-disable
  - cbt-enable
  - info

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

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

Enabling CBT using the vSphere Client GUI

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

Extending disk size with CBT enabled

After performing a full VADP backup of a VM with CBT enabled, if you extend the disk size beyond 128 GB, subsequent CBT incremental backups may be inconsistent.

To avoid inconsistent backups, disable CBT after you change the disk size, and then turn CBT back on.

The VMware knowledgebase article 2090639, available at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2090639, provides more information about this issue.

Monitor VMs

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

Recovering VADP Backups

This section covers these topics:

- File based recovery of a VM on page 180
- Image level (single step) recovery of a full VM on page 182

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 VADP proxy.

To perform a file based recovery on the local host:

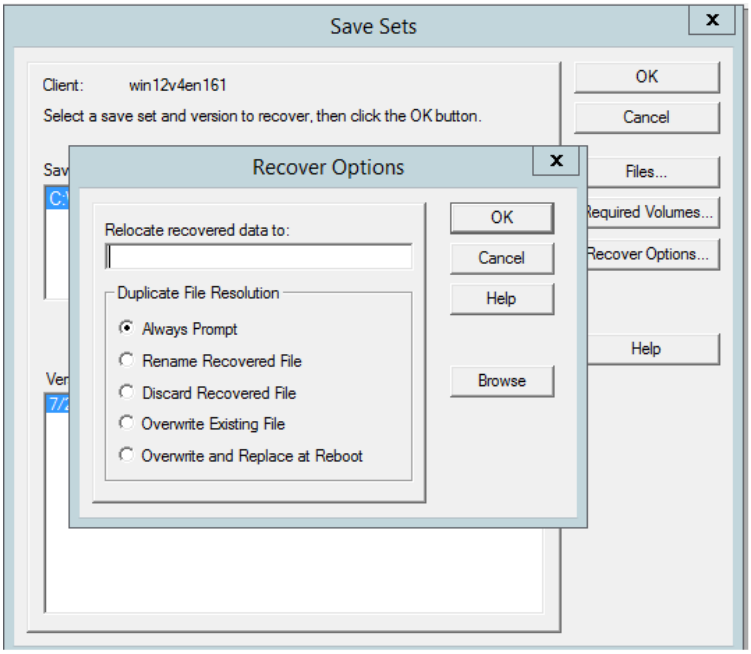
Procedure

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 75 Recover Options dialog



Performing a file based recovery using CIFS share

Before you begin

Ensure that the remote access list of the VM client includes either user@server or user@proxy and that you add the proxies to the DD Boost access list. To add a client to the DDBoost access list, run the following command from the DDBoost command line:

```
 ddboost access add clients (- Add clients to a DD Boost access
list)
ddboost access add clients client-list
```

Procedure

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

Performing a file based recovery using directed recovery

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

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 183
- Performing an image level recovery from the command line on page 184

Recommendations and considerations

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

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

  Note

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

- The VADP proxy system must be running one of the following:
  - Microsoft Windows 2008
  - 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).

Note

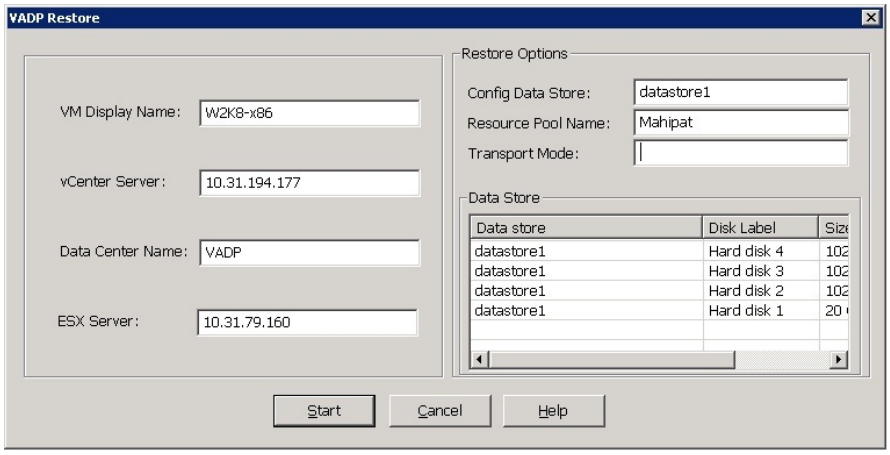
NBDSSL mode fails for recovery of VMs in NetWorker. The transport mode Hotadd fails for ESX 5.0 and with VC 5.0. Recovering a VM using NBDSSL, SAN, or Hotadd transport mode on page 188 provides a workaround to this issue.

- **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 76 VMware vCenter restore



Note

During an image level recovery operation, multiple browse sessions will be displayed in NMC's Monitoring window. This is expected behavior.

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 one of the following recovery procedures depending on the build number of your NetWorker software:

- Image-level recoveries of non-Windows VMs on page 185
  This issue applies only to NetWorker 7.6.2 build 631 or earlier.
- Unable to browse guest based backups on non NTFS file systems on page 187
  This issue applies only to NetWorker 7.6.2.1 build 638 or later.

Image-level recoveries of non-Windows VMs

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

If using traditional NetWorker guest based backups along with VADP image-based backups for the same VM client, then you must first remove the indices of the

previous traditional save sets before you can perform an image-level recovery of the full VM, otherwise the image-level recovery will fail. The only indices that need to be removed are those indices of the traditional save sets whose backups were performed prior to the VADP image-level backup that you have selected for restore.

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

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

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

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

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

Removing indices of browsable save sets

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

```
C:\>mminfo -avot -q "client=mars,volume=delve.001"
volume type client date time size ssid fl lvl name
delve.001 adv_file mars 4/14/2011 9:55:55 AM 3483 MB 4154881857 cb
full /usr
delve.001 adv_file mars 4/14/2011 10:01:35 PM 103 MB 3953675679 cb
incr /usr
delve.001 adv_file mars 4/14/2011 10:07:10 AM 15 GB 4104550902 cb
full FULLVM
delve.001 adv_file mars 4/14/2011 2:55:31 PM 3481 MB 4003904887 cb
full /usr
delve.001 adv_file mars 4/14/2011 3:03:18 PM 103 MB 3903242058 cb
incr /usr
delve.001 adv_file mars 4/14/2011 3:28:30 PM 15 GB 3852911942 cb full
FULLVM
```

If you want to recover the latest image-level backup (in the above example, SSID=3852911942), first remove all the indices of browsable save sets that are from the previous traditional backups.

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

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

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

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

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

Note

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

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

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

Unable to browse guest based backups on non NTFS file systems

The following issue applies to NetWorker releases 7.6.2.1 build 638 and later. Traditional guest based (client based) backups are not browsable in the recovery GUI for VMs that are running a non NTFS 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 *EMC NetWorker Command Reference Guide* provides more information about using the recover command to mark (select) files and to perform the recovery.

Recovering a VM using NBDSSL, SAN, or Hotadd transport mode

Recovery of a VM in NetWorker fails for the transport modes NBDSSL, SAN, and for Hotadd mode for ESX 5.0 and with VC 5.0. Use the following steps to work around the issue:

Note

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

Procedure

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

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 backup and recovery

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

- Ensure that VC and ESX/ESXi are updated to the latest released update.
- VADP supports backup and recovery via VMware VirtualCenter or vCenter. The section Software and hardware requirements on page 164 provides more information on supported vCenter versions.

  Note

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

- VADP does not support IPv6. Instructions for disabling IPv6 and using IPv4 are provided in the section Network and Firewall port requirements on page 196.
- Ensure that the client parallelism on the VADP proxy machine is set to the maximum number of VM backups to be run concurrently. The section Recommendations and considerations for transport modes on page 199 provides information on the maximum supported concurrent backups for each transport mode.
  For example if running 10 VM backups simultaneously, ensure that the client parallelism in the VADP proxy Client resource is set to 10.
- It is recommended to keep the vCenter and VADP proxy as separate machines to avoid contention of CPU and memory resources.
- 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.

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

Application-level consistent backups

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

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

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

```
disk.EnableUUID = "true"
```

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

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

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

Note

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

Option to enable or skip quiescing on the Application Information tab in NMC

An option on the Application Information tab in NMC allows you to enable or skip quiescing during VADP backup.

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

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

If this attribute is not specified, then NetWorker initiates quiesced snapshots for VM clients by default.

Note

The attribute VADP_QUIESCE_SNAPSHOT can be applied either at the VM level or proxy level. If applied at the VADP proxy level, all the VMs that use this VADP proxy will be affected.

Advanced use and troubleshooting

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

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

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

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

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

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

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

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

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

Selection of physical vs. virtual proxy

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

Backup targets for virtual proxy hosts

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

- If the backup is directed to disk (either AFTD or DDBoost), there are no special configuration requirements.
- If the backup is directed to tape drives, then review the requirements and limitations of using tape drives inside a VM in the section Support for tape drives in a VM on page 198.

  Note

  This requires that data transport is set to NBD/NBDSSL mode since VMware does not allow Hotadd mode in conjunction with VMDirectPath.

Proxy node sizing and performance considerations

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

Note

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

- The maximum number of concurrent sessions when using a physical proxy is higher than that of a virtual proxy. The section Recommendations and considerations for transport modes on page 199 provides more information on concurrent sessions for specific transport modes.
- Recommendations for a physical proxy is 4 CPU cores with 8GB of RAM. Recommendations for a virtual proxy is 4 vCPUs and 8GB vRAM per proxy, where each vCPU is equal to or greater than 2.66 GHz.
- NetWorker supports up to 12 parallel sessions using a single virtual proxy. This refers to the number of virtual disks processed in parallel, so if a single VM contains multiple virtual disks, this must be taken into account.
- Number of virtual proxies per ESX host depends only on the type of hardware on which the ESX has been installed.
- For lower-end ESX hosts, it is recommended not to mix I/O load on ESX (with the virtual proxy and backup VMs residing on a single ESX), but to have a separate ESX for the virtual proxy.
- For high-end ESX hosts, it is recommended to have a maximum of 5 virtual proxies concurrently running on a single ESX host.
- Optimal CPU load and performance when using DDBoost devices is observed with 4 concurrent backups per device. Lower number of parallel sessions to a single device does not achieve full performance while higher number increases CPU load without additional performance gain. Based on the CPU load, there is typically no performance improvement from adding more than 3 DDBoost devices per proxy node.

VADP snapshot recommendations

The following are recommendations for VADP snapshots:

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

Note

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

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

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

- In the case of VMs that have a large amount of change rate during backups, the snapshots can grow in size considerably while the backup is running. Therefore, ensure that the snapshot working directory on the VMFS datastore has enough space to accommodate the snapshot during the backup.
- VMs with physical and virtual compatibility RDM disks are not supported for VADP backups, because VM snapshots cannot be applied to such VMs. During NetWorker backup of a VM, no RDM related information is backed up, and no RDM disks/data are restored upon VM recovery. If RDM disks are required, they must be reattached after the recovery.

Note

If reattaching RDM disks after recovery, make note of all LUNs that are zoned to the protected VMs.

- VMware snapshots by default reside on the datastore where the VM configuration files are located. Therefore, ensure that the snapshot working directory supports the size of all the disks attached to a given VM.
  Starting with version 4.0, ESX and ESXi will compare the maximum size of a snapshot redolog file with the maximum size of files on the datastore. If the file could grow beyond the maximum size, ESX cancels the Create Snapshot operation and displays the following error:

  ```
  File is larger than the maximum size supported by datastore.
  ```

  For example, if VM01 has the following disk layout:

  - Disk01 - 50GB stored on VMFS01 datastore with a 1MB Block size
  - Disk02 - 350GB stored on VMFS02 datastore with a 4MB Block size
    Attempting to take a snapshot of this VM would fail with the error indicated above. This is because VMFS01 contains the working directory of the VM01, and snapshots get stored in the working directory. In the case of Disk02, this may indicate that the redolog file has grown beyond VMFS01's maximum file limit of 256GB, which is where it will be stored.

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

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

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1004040

To change the workingDir directory to a datastore with enough block size, refer to the VMware KB article at the following link:

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

The following table indicates the maximum virtual disk file size corresponding to block sizes on a datastore in ESX/ESXi 4.0:

Table 28 Maximum virtual disk file size and corresponding block size for ESX/ESXi 4.0

Block Size	Maximum File Size
1 MB	256 GB - 512 Bytes
2 MB	512 GB - 512 Bytes
4 MB	1024 GB - 512 Bytes
8 MB	2048 GB - 512 Bytes

The following table identifies the maximum virtual disk file size corresponding to block sizes on a datastore in ESX/ESXi 4.1:

Table 29 Maximum virtual disk size and corresponding block size for ESX/ESXi 4.1

Block Size	Maximum File Size
1 MB	256 GB
2 MB	512 GB
4 MB	1024 GB
8 MB	2048 GB - 512 Bytes

Manually quiescing VADP snapshots

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

http://kb.vmware.com/selfservice/documentLink.do?externalID=1018194&micrositeID=null

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

Procedure

1. Uninstall VMware Tools from the VM.
2. Reboot the system.

3. Reinstall VMware Tools. Ensure to select **Custom Install**.
4. Deselect **VSS**.

Recommendations for Data Domain systems

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

- When using DD VTLs, SAN transport mode is required; as a result, the proxy host cannot be a VM.
- 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 VM being backed up if small to medium sized VMs are in use (VMs with less than 100GB virtual disks attached). If the largest VM being backed up has more than 100GB of virtual disks attached, the RAM can be further increased.
    More information on calculating the optimal memory for a given proxy is provided in the section Memory requirements for the VADP proxy on page 196.
- Better throughput is observed with DD Boost when there is less commonality between the VMs being backed up. As a best practice, it is recommended that VMs related to the same parent VM template/clone should be part of different backup groups, and these backup groups should have different start times.
- In the case of both Hotadd and SAN modes, a 20-40% improvement is observed in the backup throughput for every additional proxy, provided the backend storage where the VMs reside is not a bottleneck.
- If using Hotadd mode:
  - Refer to the section Recommendations and considerations for transport modes on page 199 for memory requirements. These requirements may increase depending on the size of the VM virtual disks, as described in the RAM recommendation above and the section Memory requirements for the VADP proxy on page 196.
  - Virtual proxy parallelism should not be set to a value greater than 12. This limit can further be decreased if the VMs have more than one disk attached. More information related to best practices when using Hotadd mode is provided in the section Recommendations and considerations for transport modes on page 199.
  - 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 168 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>*

Memory requirements for the VADP proxy

The following NetWorker processes are related to VADP backup operations:

- nsrvadp_save
- nsrvddk
- save

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

Note

Once the backup of the VM completes, all the above processes exit, releasing the memory consumed on the proxy host.

Memory sizing requirements for the VADP proxy are as follows:

- For Linux VMs or FLR-disabled Windows backups, approximately 200MB per VM is required.
- For FLR-enabled Windows backups, use the following information to calculate the memory required:
  - When VADP backups are running, **nsrvadp_save** > **, which runs on the VADP proxy machine,** consumes up to 2MB for every 1GB of virtual disk being backed up.
  - The **nsrvddk** and **save** processes consume approximately 200MB memory per VM
    As an example, if you are running backups for a maximum of 4 VMs concurrently, then take the 4 Windows VMs with the largest disk sizes in the environment; in this example, if each VM has the following disk layout:
  - VM1: Windows= Disk1-50GB, Disk2-100GB, Disk3-512GB
  - VM2: Windows=Disk1-50GB, Disk2-512GB, Disk3-1TB
  - VM3: Windows=Disk1-50GB, Disk2-100GB, Disk3-256GB
  - VM4: Windows=Disk1-100GB, Disk2-1.5TB
    The memory consumed by VADP processes on the proxy would then be:
  - VM1: (Maximum sized disk in GB for VM* 2 MB) + 200 MB**= 1224 MB
  - VM2: (Maximum sized disk in GB for VM* 2 MB) + 200 MB** = 2248 MB
  - VM3: (Maximum sized disk in GB for VM* 2 MB) + 200 MB** = 712 MB
  - VM4: (Maximum sized disk in GB for VM* 2 MB) + 200 MB** = 3272 MB
    Therefore, the total memory needed on the proxy for VADP processes would be 7456 MB.

    Note

    200 MB is the memory needed per Windows VM for the **nsrvddk and **save** processes.
- If the proxy is also being used as storage node, the following nsrmmd overhead needs to be included in the total memory requirement:
  - DD BOOST per device memory usage- approximately 500MB
  - backup to disk per device memory usage- approximately 50MB

VADP mount point recommendations and space considerations

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

- Ensure the mount point is not located in the system folder (for example, c:/Windows/temp) as this folder is skipped during backup. Having the mount point in this folder may result in backup failures or backups that skip data due to directives that are applied during VADP backups.
- Do not use any special characters (for example, *, # and so on) in the VM name or the name of the datastore associated with the VM. If these names contain special characters, the mount operation fails.
- The VADP mount point cache requires temporary space equal to at least 5-10% of the total amount of data being backed up in the case of Windows VMs. This space is required for storing the VMDK index during the backup, and is only used during the parsing of metadata while the backup is in progress. The space required for

this task clears once the backup completes. In the case of Linux or FLR-disabled Windows VMs, minimal space is required as indicated in the note below.
For a VM with a large number of files, using a faster disk to cache files will help during parsing

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

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

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

- Total amount of data being backed up=40GB*2*5=400GB
- Total amount needed for mount point=400*10%=40GB
  In this case, ensure that the drive specified for VADP_BACKUPROOT has at least 40GB of free space.

Note

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

Support for tape drives in a VM

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

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

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

VMDirectPath requirements and recommendations

The following requirements and recommendations apply when using VMDirectPath:

- VMDirectPath requires Intel Virtualization Technology for Directed I/O (VT-d) or AMD IP Virtualization Technology (IOMMU). You may need to enable this option in the BIOS of the ESX/ESXi system.
- The ESX/ESXi version should be 4.0 Update 2 or later version.
- The VM should be Hardware version 7. For example, vmx-07.
- The optimal VMDirectPath PCI/PCIe devices per ESX/ESXi host is 8.
- The optimal VMDirectPath PCI/PCIe devices per 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 204.
- Memory usage per DD BOOST device should be approximately 500MB.
- A maximum of 50 concurrent backups should be performed per proxy when using a backup-to-disk device.
- A maximum of 100 concurrent backups should be performed per proxy when using a DDBoost device.
- A maximum of 100 concurrent backups can be run at any given time against a given VC.

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 204.
- A minimum of 4 vCPUs must be allocated per virtual proxy, with 8GB vRAM per proxy and each vCPU equal to or greater than 2.66 GHz.
- Memory usage per DD BOOST device should be approximately 300MB.
- The ESX server must be running ESX 3.5 update 4 or later.
- Client parallelism on the VADP virtual proxy should not be set to a value greater than 12 where the VMs being backed up have a maximum of 1 disk per VM in the environment.
  If the VMs in the environment have more than 1 disk per VM but less than 12 disks per VM, then the maximum client parallelism value on the VADP virtual proxy should not exceed *N*, where *N* is based on the following calculation:

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

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

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

  Note

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

- The virtual proxy can only back up those VMs whose virtual disk size does not exceed the maximum size supported by the VMFS datastore where the configuration files of the virtual proxy reside.
  As a best practice, always place the configuration files of the virtual proxy on a datastore that has a block size of 8MB. This will ensure that the virtual proxy can back up all of the supported virtual disk sizes.
- The datastore for the VADP proxy VM must have sufficient free space before the Hotadd backup begins.
- If there are multiple virtual proxies, it is recommended to host all the virtual proxies in a dedicated ESX/ESXi server. This would keep the virtual proxy resource consumption of CPU and memory isolated within that ESX/ESXi environment without impacting the production VMs.
- VMs having IDE virtual disks are not supported for Hotadd mode. Instead, nbd mode is recommended for these.
- The VM to back up and the VM that contains the Hotadd VADP proxy host must reside in the same VMware datacenter. This requirement also applies to VM restore — the VM to restore and the VM where the restore is initiated must reside in the same VMware datacenter.
- If a backup failure occurs, the virtual proxy may sometimes fail to unmount 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 (i.e., VADP_TRANSPORT_MODE=NBD):

- If NBDSSL mode fails for recovery of VMs, apply the workaround in the section Recovering a VM using NBDSSL, SAN, or Hotadd transport mode on page 188.
- One can only run a concurrent backup of 20 virtual disks against a given ESX/ESXi. The limit refers to the maximum number of virtual disks and is per ESX/ESXi host, irrespective of the number of proxies being used in the environment.
  Due to this limitation, it is recommended to apply the following best practices:
  - If the ESX is not part of a VMware cluster or is part of a DRS-disabled VMware cluster, then apply one of the following:
    - When using a single proxy to backup a given ESX via NBD/NBDSSL, set the client parallelism of the VADP proxy Client resource such that the limit of 20 concurrent disk connections per ESX host is not exceeded.
    - When using multiple proxies to backup a given ESX via NBD/NBDSSL, then the client parallelism on each VADP proxy should be calibrated such that the total concurrent disk connections per ESX host does not exceed 20.
  - If ESX is part of a DRS-enabled VMware cluster, then apply one of the following best practices:

- When using a single proxy to backup via NBD/NBDSSL, set the client parallelism of the VADP proxy Client resource such that the limit of 20 concurrent disk connections per cluster is not exceeded.
- When using multiple proxies to backup via NBD/NBDSSL, then the client parallelism on each VADP proxy should be calibrated such that the total concurrent disk connections per cluster does not exceed 20.

Note

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

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.

Performance optimization recommendations

The following section provides recommendations for optimizing VADP performance.

- The success of the VADP snapshot creation and deletion is based on two things:
  - The amount of I/O occurring on the VM datastore during snapshot creation.
  - The design of the I/O substructure associated with each datastore.
- To avoid snapshot-associated issues, backups should be scheduled during times of relatively low I/O activity on the VM. Reducing the number of simultaneous backups can also help with this.
- The use of multiple backup proxy servers is supported with NetWorker. Depending on the number of VMs/ESX servers in use, another backup proxy can be added to increase backup throughput capacity.
- During VADP backups, the backup proxy server performs a significant amount of backup processing. Proper sizing of the backup proxy server can help ensure maximum backup performance of the VM environment. In some instances, a physical proxy may be preferable.
  The capacity of the backup proxy can be broken down into two main areas:
  1. VADP data path — This is the path that the backup data created by VADP will follow during the backup lifecycle. The VADP proxy server accesses backup data using the configured network transport mode. The configured transport mode can be set to the following values:
     - SAN (Storage Area Network)
     - Hotadd
     - NBD (Network Block Device)
     - NBDSSL (Network Block Device with SSL)
  2. NetWorker data path — The VADP proxy can also be a NetWorker server, client or storage node. To maximize backup throughput, the VADP proxy should be configured as a storage node so that client data is written directly to the backup media.

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

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

VADP proxy access to LUNs

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

SAN transport mode

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

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

Hotadd transport mode

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

NBD/NBDSSL transport modes

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

Diskpart utility for SAN and Hotadd transport modes

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

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

Note

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

---

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

CHAPTER 4

Licensing

This chapter contains the following topics:

- Virtual environments simplified licensing 206
- Physical ESX hosts in non-VADP configurations 206
- Guest-based licensing 206
- NetWorker VMware Protection licensing 207
- VADP licensing 207

Virtual environments simplified licensing

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

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

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

The *EMC NetWorker Licensing Guide* provides more information on virtual licensing.

Physical ESX hosts in non-VADP configurations

The client license used for physical ESX hosts in non-VADP configurations is the Virtual Edition Client license. This license enables backup from any resident guest VM that has the NetWorker client software installed.

Guest-based licensing

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

Guest based backups that use this license include:

- VMWare ESX servers
- Solaris zones
- LDOMs
- LPARs
- nPARs
- VPARs
- Microsoft Hyper-V
- Xen and others

The following licensing model is used:

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

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

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

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

NetWorker VMware Protection licensing

For the NetWorker VMware Protection solution, using the EMC Backup and Recovery appliance with the traditional license requires a disk backup enabler, since this solution uses a single AFTD for NetWorker registration with the EMC Backup and Recovery appliance.

The *NetWorker Licensing Guide* provides more information on the disk backup enabler.

VADP licensing

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

Using existing licenses to support VADP after upgrading

When upgrading to NetWorker 8.1 and later from a release previous to NetWorker 7.6 SP2, note that the VADP proxy is used instead of VCB. The existing license used by the VCB proxy will automatically be migrated to support the VADP proxy.

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 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).