EMC® NetWorker®

Version 8.2 SP1 and later

VMware Integration Guide

302-001-580

REV 16

EMC²

Published November 2016

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 appliances 31
Pre-installation requirements 31
Downloading the OVAs for EMC Backup and Recovery 33
Proxy assignment for backup and recovery 38
Deploying the VMware Backup appliance 39
Deploy external proxy appliance in vCenter 40
Upgrade the VMware Backup Appliance and vCenter 45
Creating a dedicated vCenter user account and EMC Backup and Recovery role 50
Create vCenter user account 50
Create a customized role 51
vSphere Client user accounts 53
Restrict mapping of datastores 55
Adding or swapping a NIC for VMXNET 3 on the VMware Backup appliance or external proxy 55
Dual NIC support 58
Dual vNIC Setup and configuration requirements 58
Verify vNIC connectivity 60

EMC Backup and Recovery Configure window setup....61
Post-Installation configuration in the EMC Backup and Recovery Configure window....63
Backing up the VMware environment using NMC....67
Setting user privileges for the root user in the NetWorker server....67
Accessing VMware Protection in NMC....68
VMware Backup Appliance in NMC....69
VMware Protection Policies in NMC....71
VMware View in NMC....77
Starting a policy manually from the NMC Monitoring window....81
Stopping a policy from the NMC Monitoring window....82
Viewing policy progress from the NMC Monitoring window....82
Managing the VMware environment using the vSphere Web Client....82
Benefits of EMC Backup and Recovery user interface in the vSphere Web Client....83
Deduplication store benefits....83
Image-level Backup and Restore....84
Connecting to the EMC Backup and Recovery user interface in the vSphere Web Client....85
Available tasks in the EMC Backup and Recovery user interface...86
Assigning VMs/VMDKs to a policy....91
Manually starting the backup policy using Backup Now....93
Stopping a policy in the EMC Backup and Recovery user interface...93
Viewing policy progress in the vSphere Web Client....93
Restoring the VMware environment....94
FULLVM (Image-level) Restore....94
File-level restore....101
Monitoring VMware Backup Appliance activity....104
Viewing Recent Tasks in the vSphere Web Client....105
Viewing Alarms....105
Viewing the Event Console....106
Monitoring VMware Backup Appliance events from NMC....106
Other options for monitoring sessions....107
Shutdown and Startup Procedures....107
EMC Backup and Recovery Capacity Management....108
Impact of selecting thin or thick provisioned disks....108
Save set lifecycle....108
Checkpoints and VMware Backup appliance rollback....109
Creating a checkpoint using the EMC Backup and Recovery user interface....110
Rolling back to a checkpoint....110
Protecting checkpoints for the VMware Backup appliance....111
Cross Sync....111
Decommissioning the VMware Backup Appliance....112
Disaster Recovery to the same vCenter....113
Disaster Recovery Guidelines....113
Preparing the VMware Backup appliance for disaster recovery....114
Performing a disaster recovery of the VMware Backup appliance....115
Complete disaster recovery of the VMware Backup appliance and the Data Domain or tape device....116
Recovery from a secondary site....117
Best practices and troubleshooting....118
Performance and scalability....118

NetWorker VMware Protection best practices..... 121
Limitations and unsupported features..... 124
Configuration checklist..... 126
Connectivity between the VMware Backup Appliance and the ESXi/ vCenter..... 129
Connectivity between the VMware Backup Appliance and the NetWorker server..... 130
AV-NetWorker Communicator (avnwcomm) timeout..... 131
Log in to the EMC Backup and Recovery Console as admin instead of root..... 132
Unable to add VM to a policy in NMC's VMware View when you register multiple VMware Backup Appliance's with a combination of IP and FQDN..... 132
Launch of EMC Backup and Recovery Configure window fails when using Chrome or Firefox web browsers..... 133
Removing VMware Protection Policy when VMware Backup Appliance is offline..... 134
Log file locations..... 134
NetWorker operations..... 135
vCenter server operations..... 137
vSphere Client operations..... 137
Backup operations..... 140
Restore operations..... 143
Adding external proxies..... 144
Creating and analyzing crashes on Windows 2008 R2..... 144
Network protection software exclusions..... 144
Ensure backup pool volumes mounted at all times..... 144
Missing permissions for sites with LDAP configured..... 144
Accessing Knowledge Base Articles..... 145
Checkpoint discover timeout..... 145
Regenerate SSL certificates on the VMware Backup Appliance... 145

Chapter 3 VADP Backup and Recovery (legacy) 147

Software and hardware requirements..... 148
Limitations and unsupported features..... 149
Limitations to vCenter on non-English versions of Windows..... 149
Limitation for VADP proxy host on non-English versions of Windows 150
Limitations to vSphere 5.5 and 6.0 support..... 150
Transport modes..... 151
Changed Block Tracking (CBT)..... 152
Independent persistent disks are not backed up..... 152
Configuration options..... 152
Configuring the VADP proxy host and Hypervisor resource..... 152
Configuring a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard... 153
Configuring a VADP proxy host and Hypervisor resource manually by using nsradmin..... 155
Configuring a virtual client for backup..... 160
Configuring a virtual client by using the Client Backup Configuration wizard..... 162
Configuring a virtual client manually by using the Client Properties window..... 164
Creating a VADP User role in vCenter..... 165
Creating a VADP Proxy role..... 165

Assigning the VADP User role to the user specified in the NetWorker Hypervisor resource....165
Minimum vCenter permissions needed to back up and recover using VADP....166
Configuring Changed Block Tracking (CBT)....168
Configuring CBT using the variable VADP_DISABLE_CBT....169
Configuring CBT using the nsrvadp_modify_vm command....169
Enabling CBT using the vSphere Client GUI....170
Monitor VMs....170
Launching the vSphere Web Client from the NetWorker Console (Windows only)....170
Recovering VADP Backups....170
File based recovery of a VM....170
Image level (single step) recovery of a full VM....172
Recovery of pre-NetWorker 7.6 SP2 VM backups....180
VADP Planning and Best Practices....180
Recommendations and considerations for VADP backup and recovery....180
Application-level consistent backups....181
Selection of physical vs. virtual proxy....183
VADP snapshot recommendations....184
Recommendations for Data Domain systems....186
Network and Firewall port requirements....187
Memory requirements for the VADP proxy....188
VADP mount point recommendations and space considerations..189
Support for tape drives in a VM....190
Recommendations and considerations for transport modes....191
Performance optimization recommendations....194
VADP proxy access to LUNs....195
Upgrading from VCB to VADP (pre-NetWorker 8.1)....196
Upgrading an existing NetWorker server and VCB proxy....197
Change vCenter role privileges after upgrading....199
Upgrading only the proxy client to NetWorker 7.6 SP2 or later...200
Upgrade to use vCenter if ESX/ESXi server was previously used for VM backups....200
Space requirement changes on proxy for VADP vs VCB....201
Post-upgrading steps for Virtual Center on a 64-bit Windows host...201

Chapter 4 Licensing 203
Virtual environments simplified licensing....204
Physical ESX hosts in non-VADP configurations....204
Guest-based licensing....204
NetWorker VMware Protection licensing....205
VADP licensing....205
Using existing licenses to support VADP after upgrading....205

Glossary 207

FIGURES

1 Selecting the OVA to deploy in vCenter/vSphere Web Client 39
2 EMC Backup and Recovery registration 40
3 Registering proxy with the VMware Backup appliance 43
4 Unlock the vCenter Registration in the EMC Backup and Recovery Configuration Utility 46
5 Upgrading order for NetWorker components when upgrading the VMware Backup appliance 47
6 Take Snapshot in vSphere Client 48
7 Connect to ISO in vSphere Client 49
8 Hosts and Clusters in the vSphere Web Client 54
9 Change Adapter Type 56
10 Swap network for NICs in the Virtual Machine Properties window 57
11 Sample backup and production network traffic flow 59
12 EMC Backup and Recovery Configure window's Welcome page 61
13 EMC Backup and Recovery Configure window during registration 62
14 EMC Backup and Recovery Configure window after registration 64
15 Collecting log files in the EMC Backup and Recovery Configure window 66
16 Configuration tab in the NMC Administration window 68
17 VMware Backup Appliance health monitoring in NMC 69
18 NSR VBA Server Properties window 69
19 Default VMware Protection policy in NMC 71
20 Create new policy in NMC 72
21 Create VMware policy window 72
22 Create VMware Action window 73
23 Select a VMware Backup Appliance in the Create/Edit VMware Protection Policy window 75
24 VMware Protection policy with associated actions 76
25 Enable and mark actions concurrent in Create VMware Policy window 76
26 Map view of VMware environment in NMC 78
27 Cluster with child elements in VMware View 78
28 Filtering results in VMware View 79
29 Select Table view in VMware View 80
30 Add policy in VMware View 81
31 Selecting the Backup Appliance 85
32 EMC Backup and Recovery user interface in the vSphere Web Client 86
33 Backup policies in the EMC Backup and Recovery user interface 88
34 Viewing the log on the Configuration tab 91
35 Selecting VMs in EMC Backup and Recovery user interface 92
36 Selecting at VMDK level in EMC Backup and Recovery user interface 93
37 Viewing policy progress in the Task Console 94
38 Restore tab in EMC Backup and Recovery user interface 95
39 Set Instant Access Options in the Restore a backup wizard 97
40 Emergency Restore in the EMC Backup and Recovery Configure window 99
41 EMC Data Protection Restore Client login page 101
42 Manage Mounted Backups in EMC Data Protection Restore Client 102
43 Browse and select files to recover 102
44 Select Destination window 103
45 vSphere PowerCLI example output 107
46 Run Integrity Check button in EMC Backup and Recovery user interface 110
47 Roll back in EMC Backup and Recovery Configure window 111
48 Start VBA Recover for Checkpoints in NMC 116
49 Recovery from a secondary site in the EMC Backup and Recovery user interface 118
50 Monitoring stream counts output 127

51 Specify Client name and type....153
52 Apps and Modules tab in NMC....160
53 Recover Options dialog....171
54 VMware vCenter restore....175

TABLES

1 Revision history 11
2 Comparing Guest based, VADP, and NetWorker VMware Protection 18
3 NetWorker VMware Data Protection tasks 26
4 NetWorker VMware Protection requirements 27
5 NetWorker version and supported VMware Backup Appliance 29
6 Incoming port requirements 29
7 Outgoing port requirements — with external proxies 30
8 Recommended memory and swap space based on storage space utilization 33
9 Files for VMware Backup Appliance 1.1.3.7 Charlie tar bundle 34
10 VMware Backup Appliance 1.1.3.7 Charlie tar bundle base package upgrade files 35
11 Fixed issues in VMware Backup Appliance 1.1.3.7 Charlie tar bundle 35
12 Upgrade files required to enable Data Domain 6.0 support on the VMware Backup Appliance 36
13 OVA versions for NetWorker 8.2 SP3 VMware Backup Appliances 36
14 OVA versions for NetWorker 8.2 SP2 VMware Backup Appliances 37
15 OVA versions for NetWorker 8.2 SP1 VMware Backup Appliances 38
16 Minimum required vCenter user account privileges 51
17 Description of services running on the VMware Backup appliance 64
18 Backup tab column descriptions 87
19 Email configuration fields 89
20 EMC Backup and Recovery alarms 105
21 Scalability Factors 118
22 Maximum concurrent sessions per VMware Backup Appliance 120
23 Concurrency/parallelism recommendations 120
24 OVA versions by NetWorker release 131
25 Application information values 156
26 Recovery options that are available based on the virtual client configuration 161
27 VADP backup privileges 166
28 VADP recovery privileges 167
29 Maximum virtual disk file size and corresponding block size for ESX/ESXi 4.0 185
30 Maximum virtual disk size and corresponding block size for ESX/ESXi 4.1 186
31 APPINFO variable replacements 198

Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions 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 properly 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	January 28, 2015	First release of this document for EMC NetWorker 8.2 SP1
02	March 20, 2015	Added topic AV-NW Communicator (avnwcomm) timeout to the "Troubleshooting" section
03	April 3, 2015	Added topics to Troubleshooting Revised Best Practices Revised Limitations and unsupported features Added OVA files for the NetWorker 8.2 SP1 VMware Backup Appliances Added note indicating NetWorker does not support vSphere 6. Note that vSphere 6 is now supported with OVA 1.1.1.50 Added note to FLR limitationsindicating that FLR of GPT file systems is supported only with external proxies
04	April 27, 2015	Further revisions to Troubleshooting Further revisions to Best Practices

Table 1 Revision history (continued)

Revision	Date	Description
		Further revisions to Limitations and unsupported features
05	May 4, 2015	Revised Best Practices for upgrading components and ensuring NetWorker server, storage node and VMware Backup Appliance are at the same version Revised System Requirements Revised Port Requirements
06	May 25, 2015	Added information about the new OVA version 1.1.1.50 of the VMware Backup Appliances Added knowledgebase article information to Limitations and unsupported features Created a new topic for VMware Backup Appliances best practices Updates to System Requirements for new OVA file versions, vSphere 6.0 support, and DD Boost Compatibility Guide references Updates to NTP configuration to address the leap second issue
07	June 3, 2015	Added more detailed information on Emergency Restore, including step-by-step procedure, best practices, and limitations, to Direct-to-host recovery (Emergency Restore)
08	June 12, 2015	Updated OVA references throughout to indicate that OVA version 1.1.1.50 is the latest version for NetWorker 8.2 SP1
09	September 30, 2015	Updated for the release of NetWorker 8.2 SP2. Updates include: • Added section Launch of EMC Backup and Recovery Configure window fails when using Chrome or Firefox web browsers • Added section After ESX upgrade to 6.0, EMC Backup and Recovery plug-in missing from vSphere Web Client • Added section Upgrade the vCenter server software • Added section OVA files for the NetWorker 8.2 SP2 VMware Backup Appliances
10	October 23, 2015	Added section Removing VMware Protection Policy when VMware Backup Appliance is offline
11	November 30, 2015	Added troubleshooting section Unable to add VM to a policy in NMC's VMware View when you register

Table 1 Revision history (continued)

Revision	Date	Description
		multiple VMware Backup Appliance's with a combination of IP and FQDN Added note to indicate disabling Backup Now functionality in NMC does not disable adhoc backups for individual VMs in the vSphere Web Client Added note to indicate that you may need to perform cross sync manually when you perform a disaster recovery after upgrading from a NetWorker 8.2 SP1 VMware Backup appliance to a NetWorker 8.2 SP2 version 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 Removed information about how to configure VMware notifications from the VADP Backup and Recovery (legacy) chapter
12	February 5, 2016	Removed VADP support for vSphere 6.0
13	February 26, 2016	Added references to VMXNET 3 vNIC type Updated section OVA files for the NetWorker 8.2 SP2 VMware Backup Appliances for NetWorker 8.2 SP2 OVA version 1.1.2.8 Updated concurrency/parallelism recommendations in the section Performance and Scalability for NetWorker VMware Protection.
14	March 25, 2016	Updated section OVA files for the NetWorker 8.2 SP3 VMware Backup Appliances for NetWorker 8.2 SP3 OVA version 1.1.3.7 Restored VADP support for vSphere 6.0
15	July 22, 2016	Removed section "Dual NIC" as this is no longer supported
16	November 18, 2016	Restored information related to dual NIC configuration and swapping to VMXNET 3 along with revised instructions and new considerations Added information about OVA files for the NetWorker 8.2 SP4 VMware Backup Appliance along with the VMware Backup Appliance 1.1.3.7 Charlie tar bundle Added information for support of Data Domain operating system version 6.0

Table 1 Revision history (continued)

Related documentation

The NetWorker documentation set includes the following publications:

- *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 Online Software Compatibility Guide on the EMC Online Support site 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 Cluster Installation 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 Avamar Devices Integration Guide*
  Provides planning and configuration information on the use of Avamar devices in a NetWorker environment.
- *EMC NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.
- *EMC NetWorker Data Domain Deduplication Devices 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 Error Message Guide*
  Provides information on common NetWorker error messages.
- *EMC NetWorker Licensing Guide*
  Provides information about licensing NetWorker products and features.
- *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 Help, click Help in the main menu.
- EMC NetWorker User Online Help
  The NetWorker User program is the Windows client interface. Describes how to use the NetWorker User program which is the Windows client interface connect to a NetWorker server to back up, recover, archive, and retrieve files over a network.

Special notice conventions used in this document

EMC uses the following conventions for special notices:

NOTICE

Addresses practices not related to personal injury.

Note

Presents information that is important, but not hazard-related.

Typographical conventions

EMC uses the following type style conventions in this document:

Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: • System code • System output, such as an error message or script • Pathnames, file names, prompts, and syntax • Commands and options
Monospace italic	Use for variables
`Monospace bold`	Use 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 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. You will see several options for contacting EMC Technical Support. 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

Visit 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 will help us continue 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 VMs 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 first introduced in NetWorker 8.1. 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 VMs/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 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, VADP, and NetWorker VMware Protection backup and recovery.

Table 2 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 2 Comparing Guest based, VADP, and NetWorker VMware Protection (continued)

Option	Guest-based	VADP (legacy)	NetWorker VMware Protection
Individual file backups	Yes	Windows guest OS only	Not required
Incremental	File level	File level	Block level, leverages CBT
CBT	Not supported	File level	Block level
Virtual full backup	Not supported	Not supported	Backup is always virtual full
File level restore	Yes	Windows guest OS only	Windows and Linux
Deduplication supported	Yes	Yes—Direct backup to Data Domain	Yes—Direct backup to VMware Backup appliance internal storage or to a Data Domain appliance. 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 VMs on same ESX/Datastore	Medium depending on number of snapshots on VMs of 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)
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	EMC Backup and Recovery appliance registration through web interface

Table 2 Comparing Guest based, VADP, and NetWorker VMware Protection (continued)

Option	Guest-based	VADP (legacy)	NetWorker VMware Protection
		Client Configuration wizard	
Configure VM 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 is available.
- 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 VMs/VMDKs to those policies. This solution makes use of multiple applications, including NMC, the vSphere Web Client, and the EMC Data Protection Restore Client.

Advantages of NetWorker VMware Protection

NetWorker VMware Protection provides the following advantages:

- Supports forever incrementals.
- Uses existing AVE technology.
- Supports file-level recovery directly into the VM on Linux and Windows.
- Uses advanced FLR to perform file-level recovery from other VMs to a VM.

Disadvantages of NetWorker VMware Protection

Disadvantages of NetWorker VMware Protection include:

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

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 appliances 31
- Creating a dedicated vCenter user account and EMC Backup and Recovery role 50
- Restrict mapping of datastores 55
- Adding or swapping a NIC for VMXNET 3 on the VMware Backup appliance or external proxy 55
- Dual NIC support 58
- Verify vNIC connectivity 60
- EMC Backup and Recovery Configure window setup 61
- Backing up the VMware environment using NMC 67
- Managing the VMware environment using the vSphere Web Client 82
- Restoring the VMware environment 94
- Monitoring VMware Backup Appliance activity 104
- Shutdown and Startup Procedures 107
- EMC Backup and Recovery Capacity Management 108
- Checkpoints and VMware Backup appliance rollback 109
- Cross Sync 111
- Decommissioning the VMware Backup Appliance 112
- Disaster Recovery to the same vCenter 113
- Best practices and troubleshooting 118

Introduction to NetWorker VMware Protection

NetWorker VMware Protection is a NetWorker-integrated VMware backup, monitoring and recovery solution available in NetWorker releases 8.1 and later. This solution allows you to create backup and cloning policies for a VMware Backup appliance using NMC, and then assign those policies to Datacenters, Clusters, VMs 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 backups, you can then perform full recoveries of these backups from 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 8.2 release to use the NetWorker VMware Protection solution.

NetWorker VMware Protection tasks

The following table compares tasks in NMC with tasks in the vSphere Web Client and the EMC Data Protection Restore client.

Table 3 NetWorker VMware Data Protection tasks

Program/Role	Task
NMC	• Create and edit Data Protection policies to perform actions such as backup, clone, and checkpoint backup for disaster recovery • Assign a policy to the VMware Backup Appliance • Assign VMs/VMDKs to the policy • Start or schedule a policy to run any backup and clone actions associated with the policy When you start a policy from NMC, 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 created in NMC. • Start an adhoc backup (Backup Now), which runs the entire policy (backup and clone actions associated with the policy) • Restore a full VM backup • Restore a VMDK backup • Instant restore from a Data Domain system Supports only Windows platforms and requires Adobe Flash Player version 11.5.

Table 3 NetWorker VMware Data Protection tasks (continued)

Program/Role	Task
EMC Data Protection Restore Client	• Perform file-level restores Supports both Windows and Linux platforms; Linux platforms require Adobe Flash Player version 11.2.

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, with the appropriate version of the VMware Backup Appliance. The section Downloading the OVAs for EMC Backup and Recovery provides more information about the OVA versions for specific NetWorker releases.

Note

The VMware Backup appliance is available in 2 capacities—0.5 TB and 4 TB. You only need to download one of these appliances, based on your system requirements.

Table 4 NetWorker VMware Protection requirements

Component	Requirements
NetWorker	• 8.2 or later Server software with NMC NetWorker VMware Protection only supports the following NetWorker server architectures: -Windows 64-bit -Linux x86_64 -Solaris SPARC 64-bit (VMware View in NMC is not supported on Solaris)
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
VMware Backup appliance (4 TB OVA)	• CPU: 4 * 2 GHz • Memory: Refer to Table 8 on page 33 • Disks: 6 * 1 TB • Backup storage capacity: 4 TB • OS: 250 GB

Table 4 NetWorker VMware Protection requirements (continued)

Component	Requirements
Proxy Appliance	• CPU: 4 * 2 GHz • Memory: 4 GB • Disks: 2 disks (16 GB and 1 GB)
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) **Note** vSphere 6.0 is only supported with VMware Backup Appliance OVA versions 1.1.1.50 and later. 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 on Windows platforms. 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.
VMware Hardware	• Version 7 and later
ESX/ESXi server	• Version 5.1 and later • Changed Block Tracking (CBT) enabled. If you enable CBT on ESXi version 6.0.x, refer to the VMware knowledgebase article at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2136854
Data Domain	• For NetWorker 8.2 through 8.2 SP3, Data Domain Boost OS at DDOS 5.4.2.1 and later, up to version 5.6.x. • NetWorker 8.2 SP4 additionally supports DDOS 6.0. The section provides more information.

Table 4 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

Table 5 NetWorker version and supported VMware Backup Appliance

NetWorker server and storage node version	OVA version
8.2 SP1	1.1.1.50
8.2 SP2	1.1.2.8
8.2 SP3	1.1.3.7
8.2 SP4	1.1.3.7 with Charlie tar bundle

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
EMC Data Protection Restore Client interface	VMware Backup Appliance	8543	File-level recovery (FLR)
EMC Backup and Recovery Configuration Utility	VMware Backup Appliance	8543	VMware Backup Appliance configuration

Table 6 Incoming port requirements (continued)

From	To	Port	Purpose
vCenter	VMware Backup Appliance	8543	EMC Backup and Recovery user interface in the vSphere Web Client

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	vCenter integration
VMware Backup Appliance and External Proxy	ESX servers	443, 111, 902	Backup and recovery operations
VMware Backup Appliance	External proxy	28002-28009 (pre-NetWorker 8.2). 28009 (NetWorker 8.2 and later)	MCS to proxy communications
External proxy	VMware Backup Appliance	28001, 27000, 29000	External proxy to MCS and GSAN

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. 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 appliances

To make use of all features of the NetWorker VMware Protection solution, you must install a 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. Compatibility of the VMware Backup Appliance for NetWorker with DDOS support is as follows:
  - NetWorker 8.1.2 VMware Backup Appliance requires DDOS 5.4. DDOS 5.5 is not supported.
  - NetWorker 8.2.0 VMware Backup Appliance supports DDOS 5.4 or DDOS 5.5.
  - NetWorker 8.2.1 VMware Backup Appliance supports DDOS 5.4 or DDOS 5.5.
  - NetWorker 8.2.2 VMware Backup Appliance supports DDOS 5.5.

  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.
- Backups to a Data Domain system occur faster than backups to VMware Backup Appliance internal storage. To determine whether to use the 0.5 TB or the 4 TB VMware Backup Appliance:
  - If using a Data Domain system, select the 0.5 TB OVA.

  - If not using Data Domain system, select the 4 TB OVA.
    EMC does not recommend using a mixed environment of Data Domain and VMware Backup appliance internal storage.
- For better performance, EMC recommends using a dedicated datastore for the VMware Backup appliance, especially for backups and recoveries performed from internal storage of the 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 EMC Backup and Recovery

You can obtain the VMware Backup appliance by downloading the VMware bundles, which appear as OVAs. Access these OVAs from the Downloads for NetWorker page of the EMC online support site at http://support.emc.com. In the Support by Product page, search for NetWorker, and then select Downloads. The Downloads page allows you to select NetWorker by release.

Note

EMC does not recommend configuring a NetWorker 8.2 VMware Backup Appliance and an OVA earlier than NetWorker 8.2 in the same vCenter.

Three VMware bundles and one ISO update are available. Each fulfills a specific requirement:

- 0.5 TB OVA—Download the 0.5TB appliance when performing backups to a Data Domain system, or when protecting fewer than 10 VMs using internal storage.
- 4 TB OVA—Download the 4TB appliance when performing backups to internal storage and protecting more than 10 VMs. 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

Table 8 Recommended memory and swap space based on storage space utilization (continued)

Utilization	Physical Memory	Swap Space
up to 100% (4.0 TB)	24 GB	16 GB

- 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 EMC Backup and Recovery Configure window setup on page 61 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.

Other system requirements for the appliances are provided in NetWorker VMware Protection requirements. Download the desired OVA and place in shared storage.

Note

In the event of a discrepancy between the OVA versions listed in the following sections and the **NetWorker Server-VBA Compatibility matrix** in the Online Compatibility Guide available at https://support.emc.com/products/1095_NetWorker, the Online Compatibility Guide takes precedence.

OVA files for the NetWorker 8.2 SP4 VMware Backup Appliance

NetWorker 8.2 SP4 uses the same VMware Backup Appliance as NetWorker 8.2 SP3, version 1.1.3.7. However, in order to update the VMware Backup Appliance for NetWorker 8.2 SP4, you must install the VMware Backup Appliance 1.1.3.7 Charlie tar bundle.

This tar bundle contains important fixes for several issues, and optional support for Data Domain operating system version 6.0. For instructions on applying the tar bundle, refer to the Charlie tar bundle README file.

If you are using an older version of the VMware Backup Appliance, upgrade to version 1.1.3.7 before applying the Charlie tar bundle. For information on VMware Backup Appliance 1.1.3.7, refer to the section "OVA files for the NetWorker 8.2 SP3 VMware Backup Appliances."

Download the tar bundle files from https://support.emc.com/downloads/1095_NetWorker.

Table 9 Files for VMware Backup Appliance 1.1.3.7 Charlie tar bundle

Filename	Description
`VBA-1.1.3.7-Charlie-TLA.tar`	Tar bundle package
`VBA-1.1.3.7-Charlie-README.txt`	README file with installation instructions

You can choose to upgrade the VMware Backup Appliance with the base package that supports Data Domain 5.4 to 5.7, or upgrade with Data Domain 6.0 support. The following table describes the upgrade files needed from `VBA-1.1.3.7-Charlie-TLA.tar` to install the base package. Refer to the section "Support for Data Domain operating system 6.0" for information about enabling the optional Data Domain 6.0 support.

Table 10 VMware Backup Appliance 1.1.3.7 Charlie tar bundle base package upgrade files

Environment	Upgrade files
VMware Backup Appliance on Linux SLES 11	• `AvamarVMwareCombined-linux-sles11-x86_64-7.1.163-10.rpm` • `commons-collections-3.2.1.jar` • `ebr-nw-2.0.3-9.x86_64.rpm` • `mcserver.jar`
External Proxy on Linux SLES 11 SP3	• `AvamarVMwareCombined-linux-sles11sp3-x86_64-7.1.163-10.rpm`

VMware Backup Appliance 1.1.3.7 Charlie tar bundle fixes

VMware Backup Appliance tar bundle 262411 fixes the following issues.

Table 11 Fixed issues in VMware Backup Appliance 1.1.3.7 Charlie tar bundle

Package	Issue Number	Description
Base package	257945	"VBA Internal Proxies" attribute set to disabled but internal proxies still process workorders.
	257168	Tivoli Java Collections Library vulnerability detected on Nessus scan.
	256099	Move of clients unsuccessful.
	255638	Data Domain 5.7 NFS client compatibility issue.
Optional Data Domain 6.0 package **Note** This package also includes the base package fixes.	266609	Incorporate Data Domain Boost 3.2.1.2 into VMware Backup Appliance version 1.1.3.7 (NetWorker 8.2 SP4).
	262783	lgtoclnt RPM and libnwp.so for NetWorker 8.2 SP4 support.

Support for Data Domain operating system 6.0

NetWorker 8.2 SP4 offers support for Data Domain operating system version 6.0.

In order to enable support for Data Domain 6.0, you must install the optional files for Data Domain 6.0 support while applying the VMware Backup Appliance 1.1.3.7 Charlie tar bundle. If you choose not to install the Data Domain 6.0 files, the VMware Backup Appliance will continue to support Data Domain versions 5.4 through 5.7.

The following table describes the files required to upgrade the tar bundle with Data Domain 6.0 support on the VMware Backup Appliance and External Proxy. These files are located in the `VBA-1.1.3.7-Charlie-TLA.tar` file.

Table 12 Upgrade files required to enable Data Domain 6.0 support on the VMware Backup Appliance

Environment	Upgrade files
VMware Backup Appliance on Linux SLES 11	• AvamarVMwareCombined-linux-sles11-x86_64-7.1.163-9.rpm • dpnavclient-7.1.163-9.sles11_64.x86_64.rpm • dpnddrmaint-7.1.63-9.sles11_64.x86_64.rpm • lgtoclnt-8.2.4.0-1.x86_64.rpm • libnwp.so
External Proxy on Linux SLES 11 SP3	• AvamarVMwareCombined-linux-sles11sp3-x86_64-7.1.163-9.rpm • libnwp.so

Refer to the VBA 1.1.3.7 TLA Charlie README file for instructions on installing the files for Data Domain 6.0 support. Download the VMware Backup Appliance 1.1.3.7 Charlie tar bundle and README from the EMC Online Support site at https://support.emc.com/downloads/1095_NetWorker.

Note

If you install the optional package for Data Domain 6.0, the VMware Backup Appliance will not support Data Domain operating system version 5.4. It is not currently possible to support both Data Domain 6.0 and 5.4. If you will be using Data Domain operating system version 5.4, do not install the Data Domain 6.0 package.

OVA files for the NetWorker 8.2 SP3 VMware Backup Appliances

NetWorker 8.2 SP3 provides the following OVA files for the 0.5 TB, 4 TB, and external proxy VMware Backup Appliances, in addition to the appliance for upgrading your virtual backup appliance (VBA) version.

Table 13 OVA versions for NetWorker 8.2 SP3 VMware Backup Appliances

File name	Description
EBR-0.5TB-1.1.3.7 ova	NetWorker 8.2.3 OVA for the 0.5 TB VMware Backup Appliance
EBR-4.0TB-1.1.3.7 ova	NetWorker 8.2.3 OVA for the 4 TB VMware Backup Appliance
EBR-Proxy-1.1.3.7 ova	NetWorker 8.2.3 OVA for the External proxy that supports EXT4 backup and recovery
EbrUpgradeFrom70To-7.1.63-5.iso	NetWorker 8.2.3 ISO file for upgrading the VBA

If you previously deployed VBA versions 1.1.2.6/1.1.2.8, you can directly upgrade to VBA version 1.1.3.7. If you have applied hotfix/tarball 252861 on VBA 1.1.2.8, you can

still preform a direct upgrade to VBA version 1.1.3.7. Download the ISO file for VBA version 1.1.3.7 from https://support.emc.com/downloads/1095_NetWorker.

Note

EMC strongly recommends also upgrading your NetWorker Server and Storage Nodes to Networker 8.2 SP3.

OVA files for the NetWorker 8.2 SP2 VMware Backup Appliances

Networker 8.2 SP2 provides the following OVA files for the 0.5 TB, 4 TB, and external proxy VMware Backup Appliances, in addition to the appliance for upgrading your VBA version.

Table 14 OVA versions for NetWorker 8.2 SP2 VMware Backup Appliances

File name	Description
EBR-0.5TB-1.1.2.8.ova	NetWorker 8.2.2 OVA for the 0.5 TB VMware Backup Appliance
EBR-4.0TB-1.1.2.8.ova	NetWorker 8.2.2 OVA for the 4 TB VMware Backup Appliance
EBR-Proxy-1.1.2.8.ova	NetWorker 8.2.2 OVA for the External proxy that supports EXT4 backup and recovery
EbrUpgradeFrom70To-7.1.62-5.iso	NetWorker 8.2.2 ISO file for upgrading the VBA

OVA 1.1.2.8 fixes the following issues:

- 247651—VMware Backup Appliance Upgrade to 7.1.62.4 ISO fails at 92% with message "Installation of the package stalled"
- 247985—VMware Backup Appliance email summary displays blank information after upgrade to OVA 1.1.2

If you previously deployed VBA versions 1.1.1.50, you can directly upgrade to VBA version 1.1.2.8. If you have applied hotfix/Charlie tarball 250328 on VBA 1.1.1.50, you can still preform a direct upgrade to VBA version 1.1.2.8. Download the ISO file for VBA version 1.1.2.8 from https://support.emc.com/downloads/1095_NetWorker.

Information about the hotfix/Charlie tarball 250328 is available at the following location:

https://emcservice--c.na16.visual.force.com/apex/KB_BreakFix_clone?id=kA2j0000000R5bw

Note

EMC strongly recommends also upgrading the NetWorker Server and Storage Nodes to Networker 8.2 SP2.

OVA files for the NetWorker 8.2 SP1 VMware Backup Appliances

Networker 8.2 SP1 provides the following OVA files for the 0.5 TB, 4 TB, and external proxy VMware Backup Appliances, in addition to the appliance for upgrading your VBA version.

Table 15 OVA versions for NetWorker 8.2 SP1 VMware Backup Appliances

File name	Description
EBR-0.5TB-1.1.1.50.ova	NetWorker 8.2.1 OVA for the 0.5 TB VMware Backup Appliance
EBR-4.0TB-1.1.1.50.ova	NetWorker 8.2.1 OVA for the 4 TB VMware Backup Appliance
EBR-Proxy-1.1.1.50.ova	NetWorker 8.2.1 OVA for the External proxy that supports EXT4 backup and recovery
EbrUpgradeFrom70To-7.1.61-10.iso	NetWorker 8.2.1 ISO file for upgrading the VBA

Note

EMC strongly recommends also upgrading the NetWorker Server and Storage Nodes to latest Networker cumulative build.

OVA 1.1.1.50 fixes the following issues:

- Knowledge Base 201864 - FLR Fails for VMs with larger disks and shows 'Failed to get disks: Unable to browse as proxies are unavailable'
- Knowledge Base 201865 - Clients VMs are removed from VMware Protection Policies

Proxy assignment for backup and recovery

When you have more than 10 VMs to protect, backup and recover operations require the deployment of proxy VMs. The OVA described in the section Deploying the VMware Backup appliance on page 39 has 8 internal proxies that allow you to backup 8 VMs concurrently. To back up more than 8 VMs concurrently, you must deploy an external proxy VM that encompasses 8 internal proxies. The section Deploy external proxy appliance in vCenter describes how to deploy the external proxy OVA. You assign a proxy for 1 backup or 1 recover of a VM at a point in time.

EMC Backup and Recovery selects a proxy 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

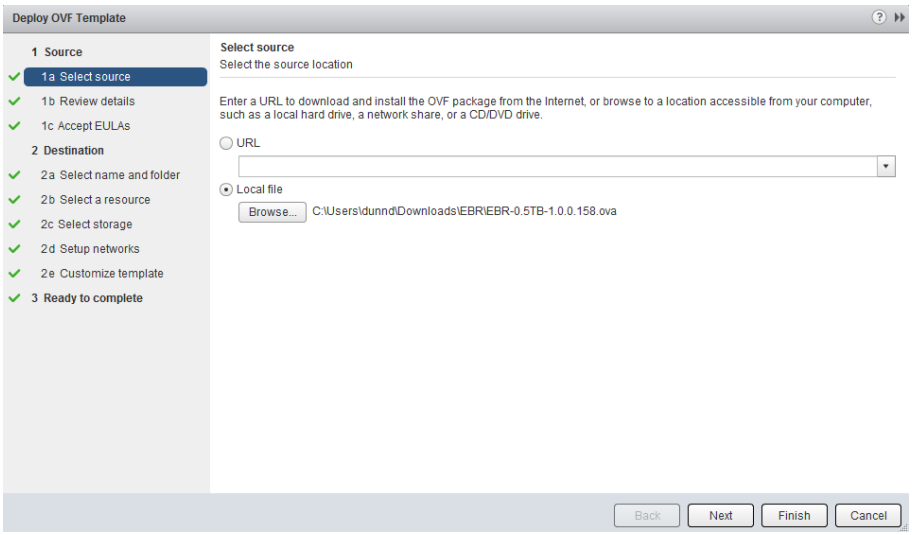
Note

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.

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 1 Selecting the OVA to deploy in vCenter/vSphere Web Client



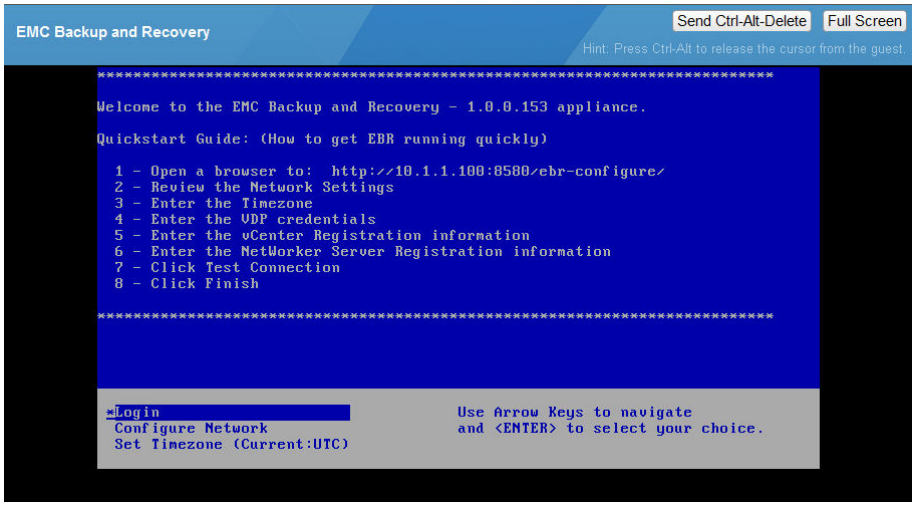
4. In the filetype drop-down, select **OVA Packages** and then navigate to the directory that contains the ova files. Select the file and then click **Open**.
5. On the **Deploy OVF Template** window, click **Next**.
6. On the **Review Details** window, click **Next**.
7. Accept the EULA and click **Next**.
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 2 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 EMC Backup and Recovery on page 33.

   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.

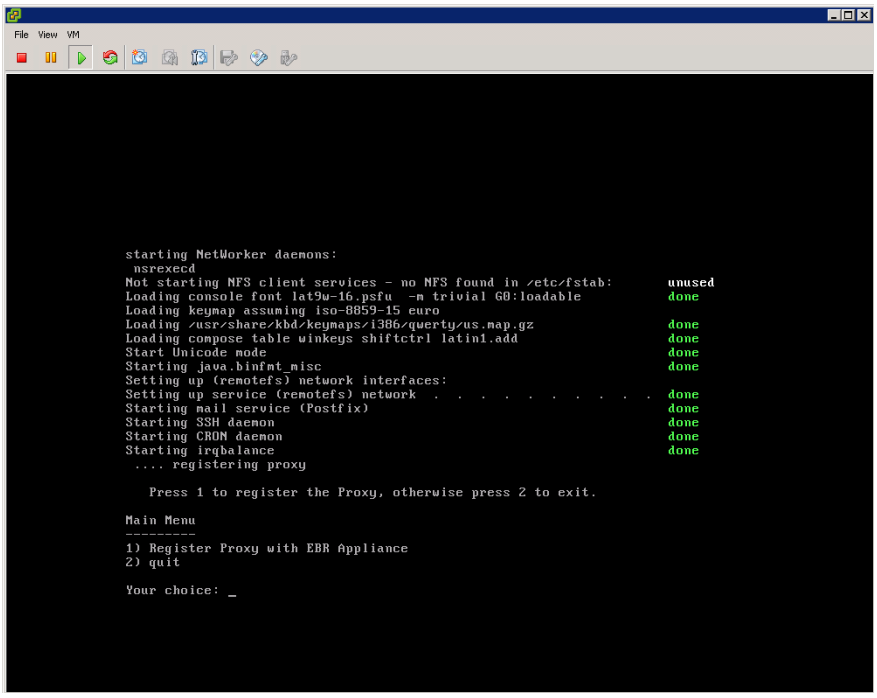
    This might take several minutes.

    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 3 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 40, 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
   ```

Unregister proxies no longer required

Check to ensure that the VMware Backup Appliance does not have any unrequired or unsuccessfully deployed proxy clients, and unregister these proxies.

To check for unrequired or unsuccessfully deployed proxy clients, run the following command on the VMware Backup Appliance:

```
mccli client show --recursive=true | grep i Proxy
```

Example 1 Output for unsuccessfully deployed proxy client

The following example shows an unsuccessfully deployed proxy created with localhost.localdomain:

Example 1 Output for unsuccessfully deployed proxy client (continued)

```
mccli client show --recursive=true | grep i Proxy
ebr.my.local /clients        VMware Image Proxy with Guest Backup
localhost.localdom /clients  VMware Image Proxy with Guest
```

For sites experiencing such registrations, please contact EMC support to unregister the proxies in error, and then check all of your external proxy appliances using the above command to ensure the hostname is correct before registering the name with the VMware Backup Appliance.

Note

The proactive_check.pl script includes a check discover proxies that have not been checked in the last 24 hours.

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 8.2 SP2 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

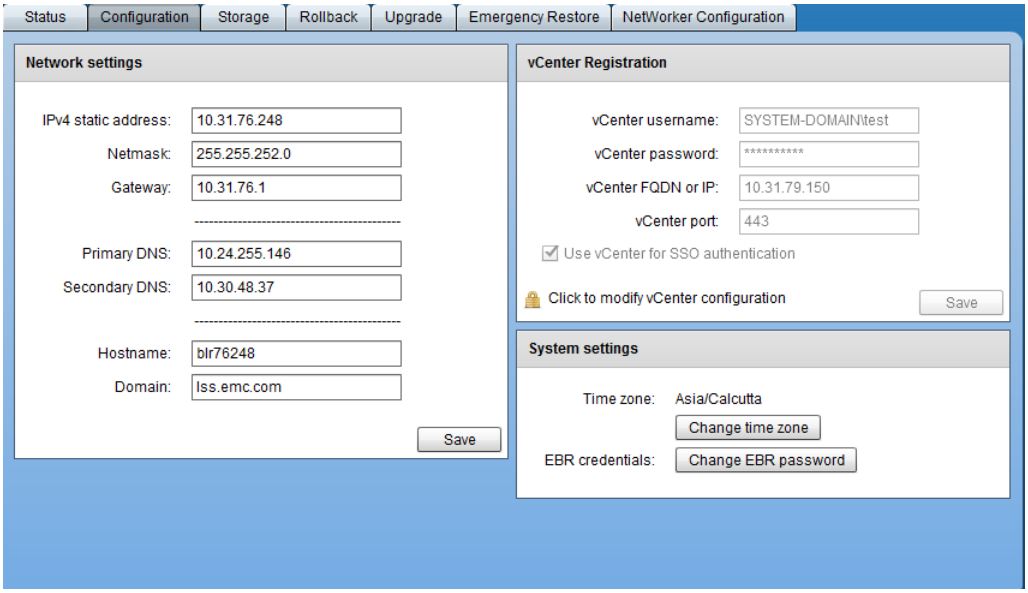
The following considerations apply if upgraded your vCenter version from vCenter 5.1 to vCenter 5.5.

- 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 4 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 8.2 SP2, perform the following steps to upgrade vCenter to version 6.0 and the VMware Backup Appliance to the latest version for NetWorker 8.2 SP2.

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 8.2 SP2. 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 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**.

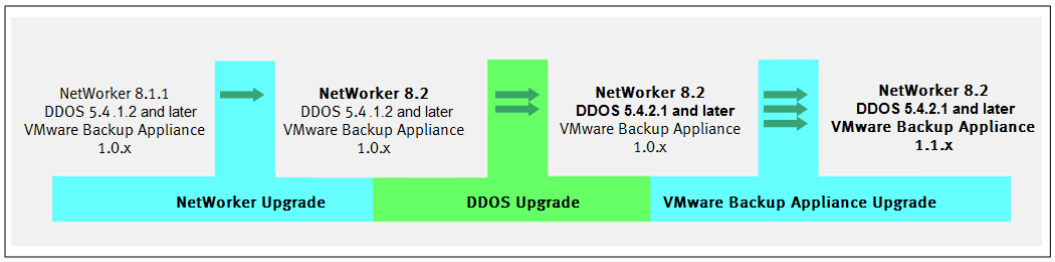
3. Open the **EMC Backup and Recovery Configuration Utility** window as shown in the figure above, and change the vCenter username from `test@system-domain` to `test1@vsphere.local` to re-register the VMware backup Appliance with vCenter, and then restart the appliance to apply the changes.
4. Upgrade the VMware Backup Appliance to NetWorker 8.2 SP2.

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.

The bold components in the following diagram illustrate the order of upgrading for supported versions.

Figure 5 Upgrading order for NetWorker components when upgrading the VMware Backup appliance



Before upgrading, also review the following considerations:

- The VMware Backup appliance version 1.1.x is only compatible with the NetWorker 8.2 server software.
- 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.
- The VMware Backup Appliance and external proxy appliances must be at the same version. Note, however, that you cannot upgrade external proxies. If using a previous version of the external proxy, 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.
  If you deployed an external proxy prior to upgrading the VMware Backup appliance, restart all external proxy VMs.

Upgrade the VMware Backup appliance

Use the following procedure to upgrade the VMware Backup appliance.

Procedure

1. Verify that the account connecting to vCenter has the required level of permissions, particularly if a non-admin user. The section Create a customized role provides a list of permissions.

   If the permissions are not correct before the upgrade, then the upgrade process may fail or leave the system in an inconsistent state.
2. If you made any changes to the /etc/hosts file, remove these changes. EMC does not recommend manually changing entries in the etc/hosts file on the VMware Backup appliance.

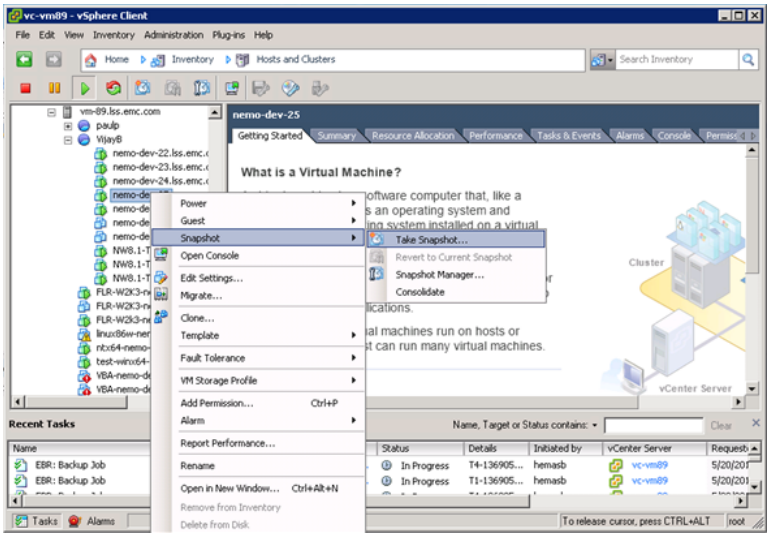
3. Create and validate a checkpoint of the existing VMware Backup appliance by running an integrity check.

   a. Click the **Configuration** tab.

   b. Select the **Run integrity Check** option, as shown in Figure 46 on page 110.

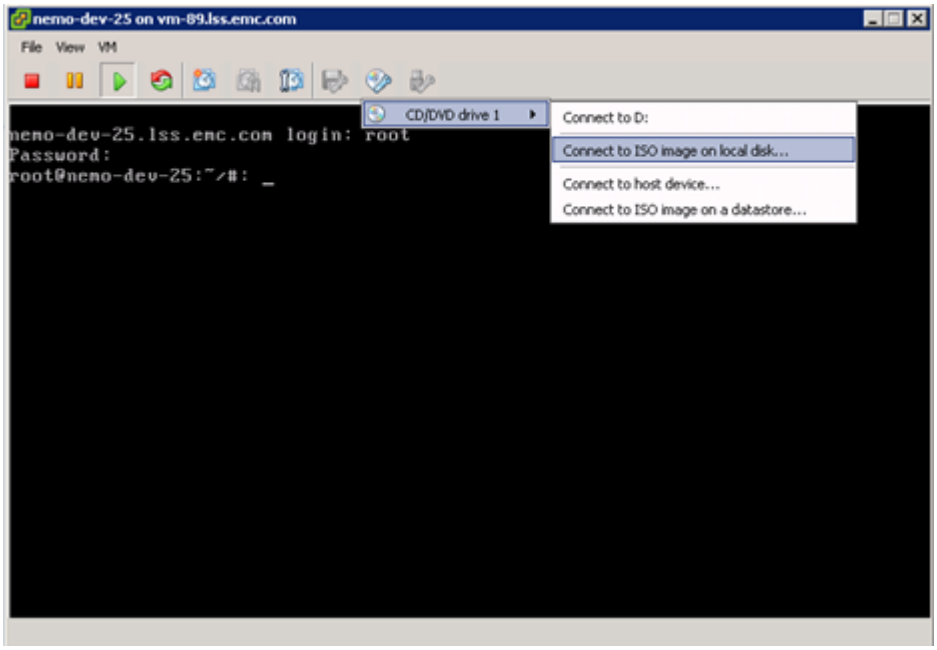
4. Shut down the VMware Backup appliance, and then create a snapshot of the EMC Backup and Recovery VM by right-clicking the VM in the **vSphere Client** and selecting **Snapshot** > **Take Snapshot...**, as shown in the following figure.

Figure 6 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**, as shown in the following figure.

Figure 7 Connect to ISO in vSphere Client



8. Open the **EMC Backup and Recovery Configure** window. The section Post-Installation configuration in the EMC Backup and Recovery Configure window on page 63 provides information about the **EMC Backup and Recovery Configure** window.
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**.

    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

When you complete a successful upgrade and verify that all backup and restore functionality is working as expected, return to the **vSphere Client** to delete the snapshot taken in step 4.

Enable VMware View in NMC after upgrading by creating a NSR Hypervisor resource

When you upgrade the NetWorker server to NetWorker 8.2 or later and upgrade to the latest VMware Backup appliance(s), VMware View may not appear in NMC until you create a NSR Hypervisor resource.

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

- Download and deploy a NetWorker 8.2 or later VMware Backup appliance from vCenter, following the registration steps outlined in the section EMC Backup and Recovery Configure window setup on page 61.
- Manually create a NSR Hypervisor resource by using the **nsradmin** program. The section Configuring a VADP proxy host and Hypervisor resource manually by using nsradmin on page 155 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 login.
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 and assign a password. Click **Save settings**.
5. Click the **Summary** tab, and then click the **Start** button next to the Server service in the vCenter pane. Log out of the session.
6. From a web browser, connect to the vSphere Web Client:

   https://<IP_address_vCenter_Server>:9443/vSphere-client/
7. Login as user administrator@vsphere.local with the password you created in step 4.
8. Navigate to **Home** > **Administration** > **SSO Users and Groups**.
9. On the **Users** tab, click on the green **+**. The **New User** window appears.
10. In the **Username** field, specify a username (for example, EMC Backup and Recovery).
11. In the **Password** and **Confirm Password** fields, specify a password. You can leave the First name, last name and password fields blank.
12. 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 16 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
Host	• Configuration > Storage partition configuration
Network	• Assign network • Configure

Table 16 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 required privileges
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 • 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
Guest Operations	• Guest operation modifications • Guest operation program execution • Guest operation queries

Table 16 Minimum required vCenter user account privileges (continued)

Setting	vCenter 5.5 required privileges
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 theVMware 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 16 on page 51 provides the account permission categories.

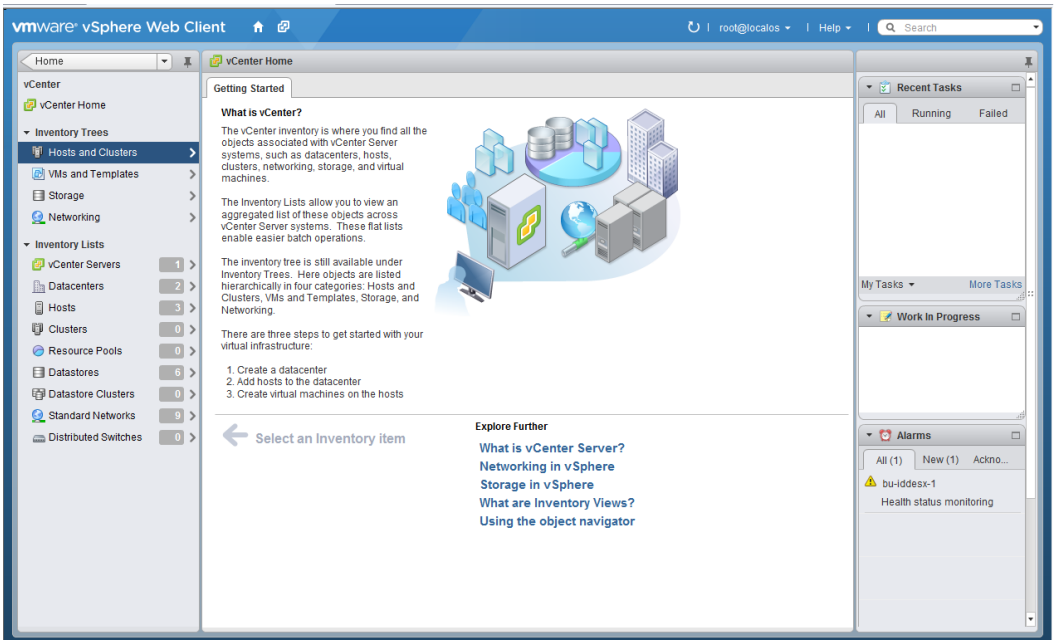
The following steps allow you to configure the EMC Backup and Recovery user or SSO admin user by using the vSphere Web Client.

Procedure

1. From a web browser, access the vSphere Web Client.
   https://<IP_address_vCenter_Server>:9443/vsphere-client/

2. Login with administrative rights.
3. Select **vCenter** > **Hosts and Clusters**.

Figure 8 Hosts and Clusters in the vSphere Web Client



4. On the left side of the page, click on `vCenter Servers`. It is important that you select this from the root level of the tree structure (represented under Hosts and Clusters). If you select the vCenter VM, the configuration fails.
5. Click the **Manage** tab and then select **Permissions**.
6. Click the **Add permission** (+) icon.
7. In the **Users and Groups** pane, click **Add**...

   The Select Users/Groups dialog box appears.

8. From the Domain drop-down select **domain**, **server**, or **SYSTEM-DOMAIN**.
9. 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, then 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.

10. Click **OK**.
11. From the **Assigned Role** drop-down list, select the role you created.
12. Confirm that the **Propagate to children objects** box is checked.
13. 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 in NMC on page 69.

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**.

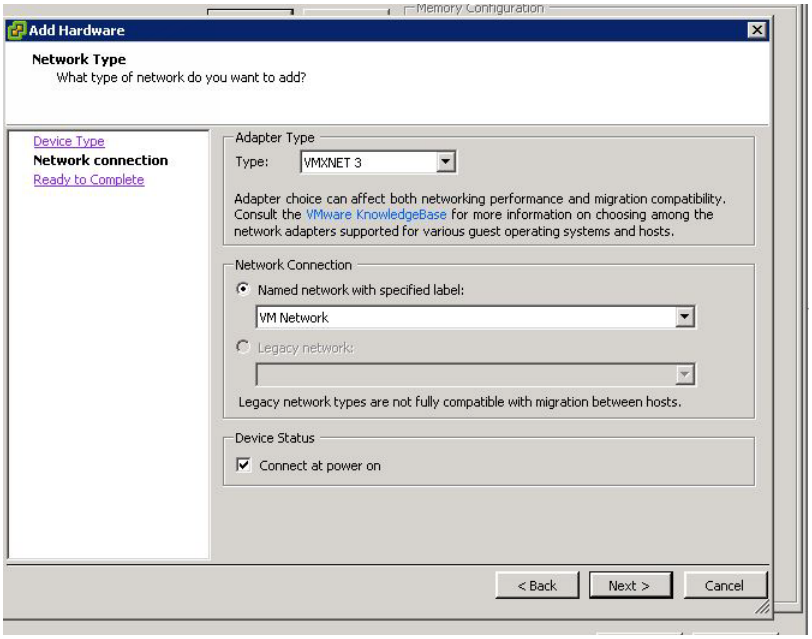
c. In the **Hardware** tab, click **Add**.

   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.

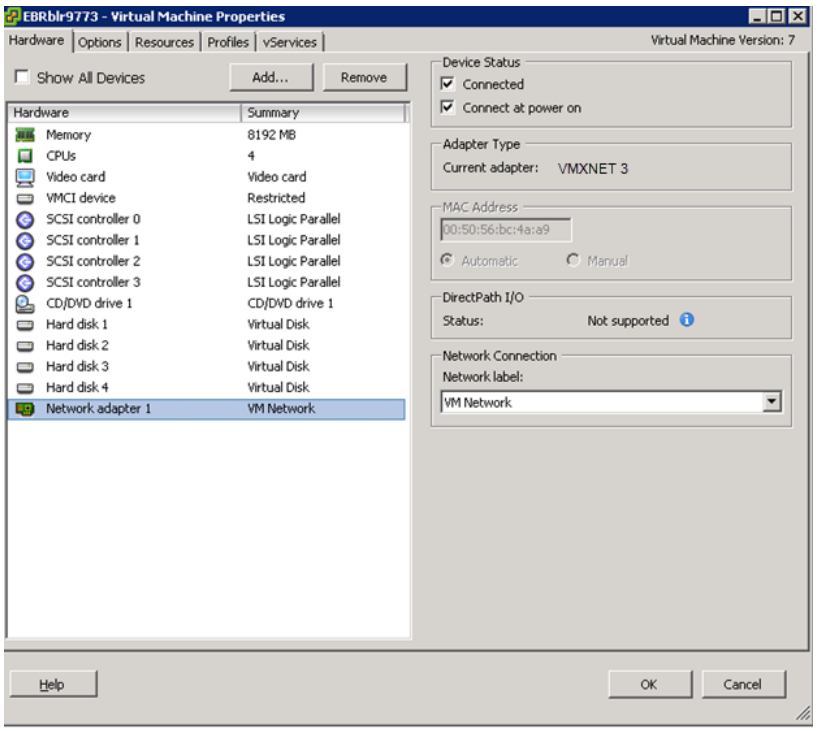
Figure 9 Change Adapter Type



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 10 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 then 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 **Next**, 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 (use the default policy)

- 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 set the Default Gateway to the gateway/address for the production network if not already set.

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.
- Every NIC on the VMware Backup appliance must meet one of the following requirements:
  –Have only one NIC on the VMware Backup appliance and disable the internal proxies. The internal proxies will not be used for backups and the VMware Backup appliance will rely on external proxies to perform the backups.

–The two NICs on the VMware Backup appliance should have the capability to communicate bi-directionally with the vCenter server.

–Add a secondary NIC to the vCenter server which can communicate to the VMware Backup appliance over the backup network.

- 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 the following:
  –vCenter

  – ESX hosts

  –Data Domain systems

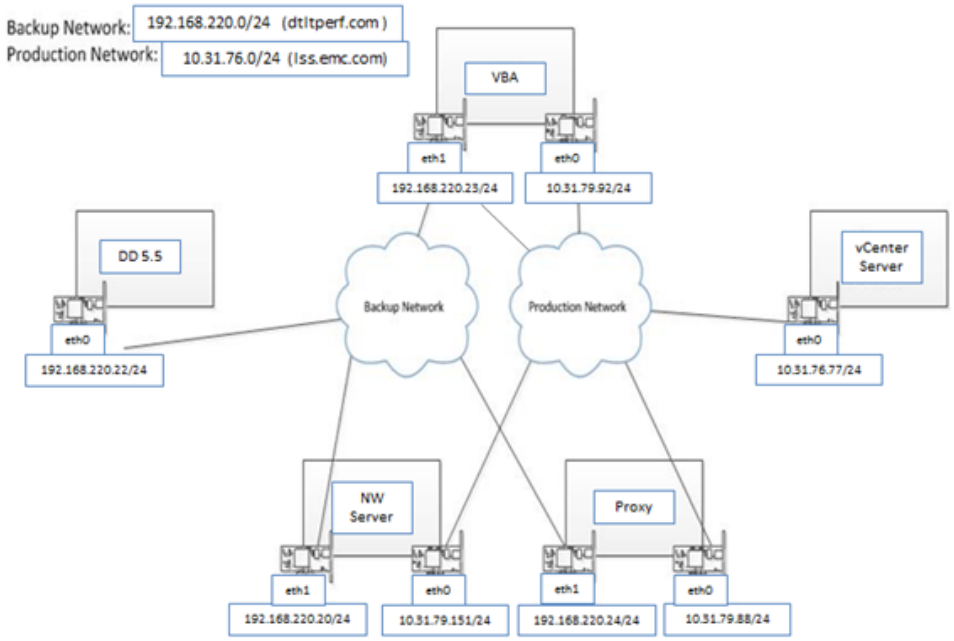
  –NetWorker server and storage nodes.

  Note

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

- The VMware Backup Appliance and external proxy appliance must have eth0 belong to the production network and contained within the same subnet which includes your vCenter Server eth0. Also, for the VMware Backup Appliance and external proxy appliance, eth1 must belong to the backup network and contained within the same subnet as the Data Domain device.
- NetWorker server/storage node communication should be available to VMware Backup Appliances and external proxy appliances.

Figure 11 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

EMC Backup and Recovery Configure window setup

Complete the VMware Backup appliance registration and configuration by using the **EMC Backup and Recovery Configure** window.

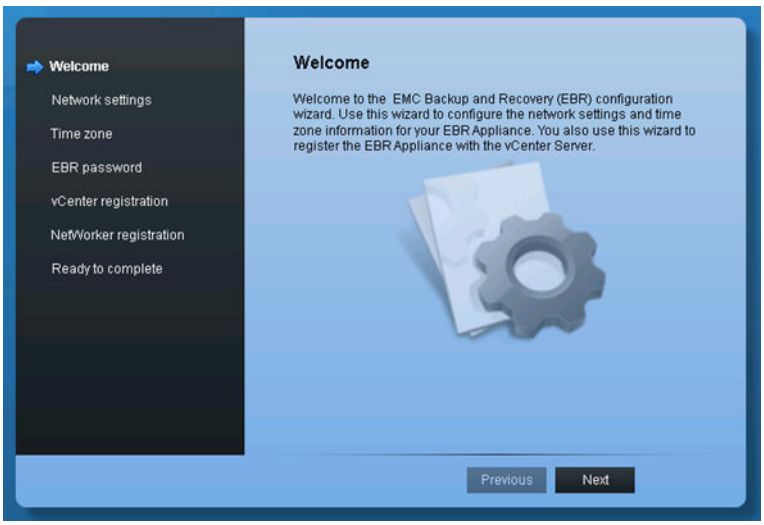
Procedure

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 FQDN:8580/ebr-configure
   ```

   When connected, the **EMC Backup and Recovery Configure** window appears, as shown in the following figure.

Figure 12 EMC Backup and Recovery Configure window's Welcome page



NOTICE

The EMC Backup and Recovery Configure window 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. 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 default userid and password:

- userid: root
- password: 8RttoTriz

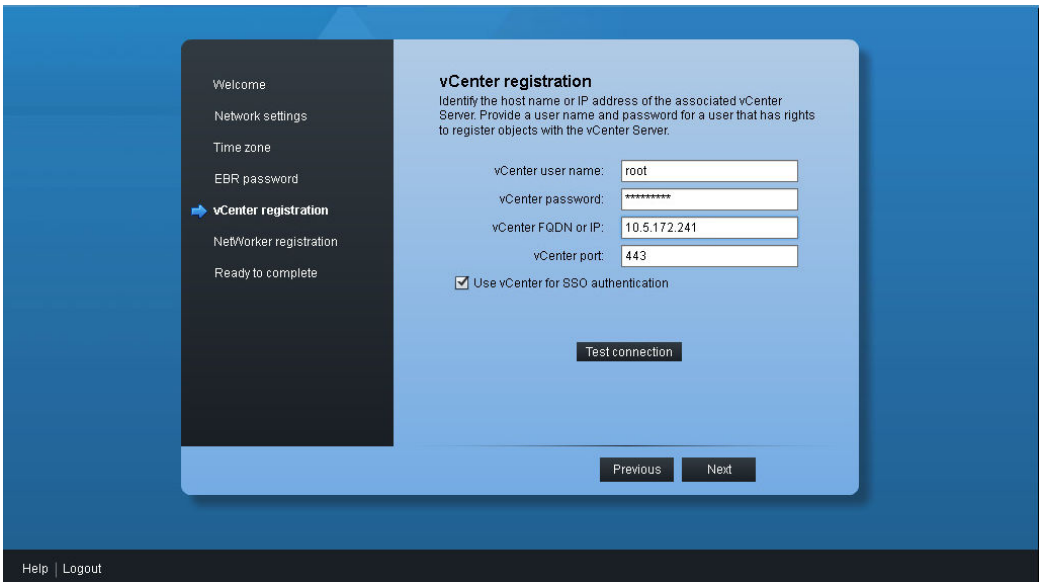
3. In the Welcome page, click **Next**.
4. Verify the IP configuration in the Network settings, then click **Next**.
5. Set the time zone to match that of the vCenter appliance, otherwise you may encounter issues connecting with EMC Backup and Recovery from vCenter. The default time zone for vCenter is UTC. Click **Next**.
6. Specify a new EMC Backup and Recovery password for the root account, then click **Next**.
7. In vCenter registration, 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**.
9. Ensure that **Use vCenter for SSO authentication** remains selected as shown in the following figure. Click **Next**.

Figure 13 EMC Backup and Recovery Configure window during registration



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.

10. In **NetWorker Registration**, type the details required to connect to the NetWorker Server:
    - NetWorker user name = VMUser (default).
    - NetWorker password = changeme (default)

- NetWorker FQDN or IP
- NetWorker web service 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 **NetWorker Registration**.

11. Click **Test NetWorker connection** to test the connection. If performing a disaster recover, select the **Override NetWorker registration** option if the VMware Backup appliance has registered to the NetWorker server.
12. Click **Finish**. A message appears indicating that configuration is complete and the VMware Backup appliance will reboot.

Results

Once the reboot completes, allow up to one hour for the deployed VMware Backup appliance to appear in NMC. During this time, do not make any changes to the EMC Backup and Recovery configuration or the NetWorker server configuration. When the deployment completes successfully, the state of the VMware Backup appliance appears in NMC, and a message appears in the Logs pane of the NMC Configuration tab.

Post-Installation configuration in the EMC Backup and Recovery Configure window

To confirm that the installation process successfully registered and configured the VMware Backup Appliance in NetWorker:

Procedure

1. Ensure that the Log window in NMC displays:

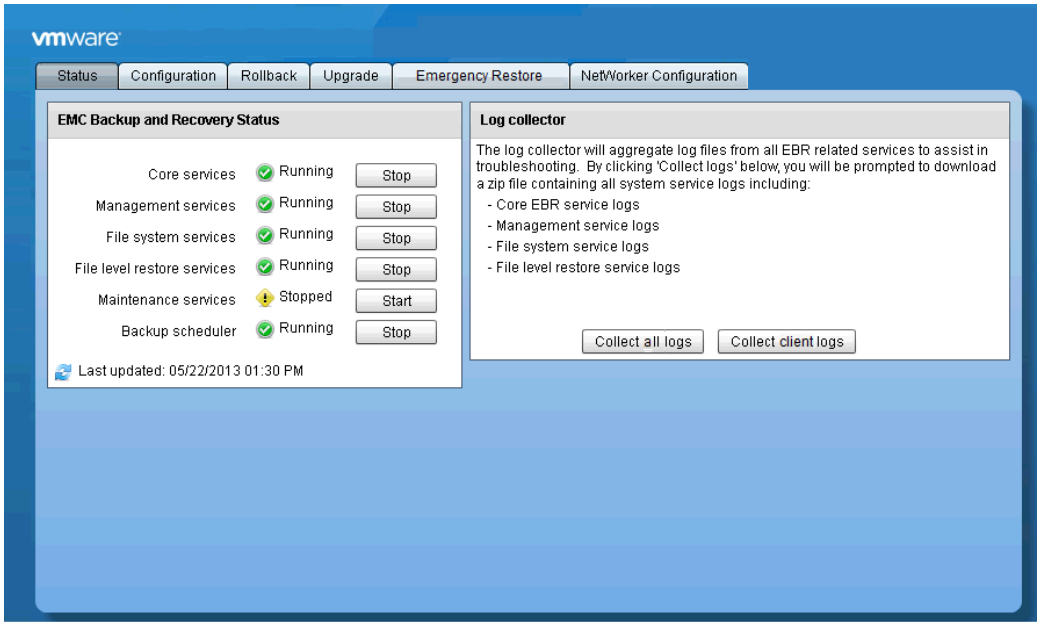
```
NetWorker server, 'server_name' registration succeeded for
VMware Backup Appliance VBA_hostname
```

2. Log in to the **EMC Backup and Recovery Configure** window by using the new EMC Backup and Recovery password that you defined during configuration.

Results

When you open the EMC Backup and Recovery Configure window after registration, the window in the following figure displays, allowing you to verify information about your configuration and to ensure the required services are running.

Figure 14 EMC Backup and Recovery Configure window after registration



Status tab

The Status 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 17 Description of services running on the VMware Backup appliance

Service	Description
Core services	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 services	Stop these services only under the direction of technical support.
File system services	Allow mounting of backups for file-level restore operations.
File level restore services	Support the management of file-level restore operations.
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.

Table 17 Description of services running on the VMware Backup appliance (continued)

Service	Description
	You can make changes to the default maintenance window by using the command line. The section Changing the Maintenance window on page 66 provides more information. Maintenance services would not be running after deployment, as shown in the above figure.

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.

Starting and Stopping Services

If all services are stopped, then start the services in the following order:

1. Core services
2. Management services
3. Maintenance services
4. File system services
5. File level restore services

Results

To stop a service, click **Stop** next to the service on the **Status** tab of **EMC Backup and Recovery Configure** window. In general, you should only stop running services under the direction of Technical Support.

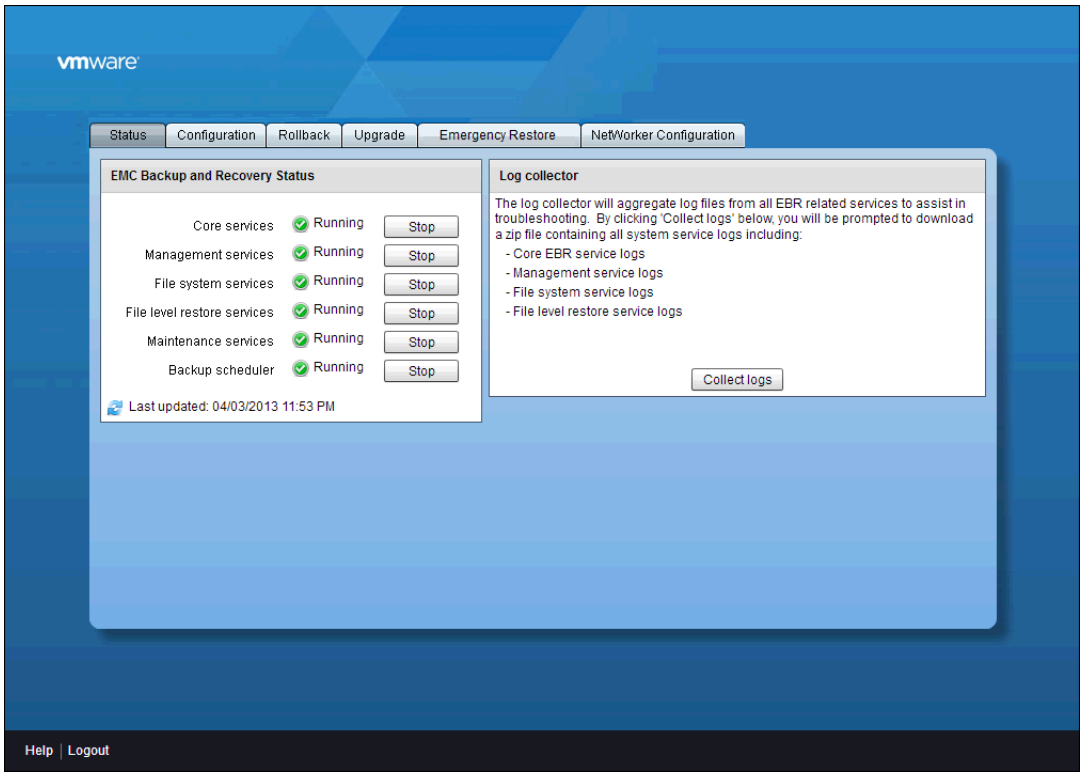
If you stop a service, you can attempt to restart it by clicking **Start**. In some cases, additional troubleshooting steps may be required for the service to work properly.

Collecting log files

You can collect log files by clicking the Collect Logs button on the Status tab of the EMC Backup and Recovery Configure window. The Log Collector zips the log files

which you can save to the machine that launched the EMC Backup and Recovery Configure window.

Figure 15 Collecting log files in the EMC Backup and Recovery Configure window



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
```

Backing up the VMware environment using NMC

After a successful OVA deployment, you can create VMware protection policies and assign VMs, VMDKs and so on to the policies for backup and recovery using NMC. NMC is the user interface for the NetWorker Console 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 the 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** > **Configuration** > **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 Console window appears. To access the VMware Protection solution in NMC:

Procedure

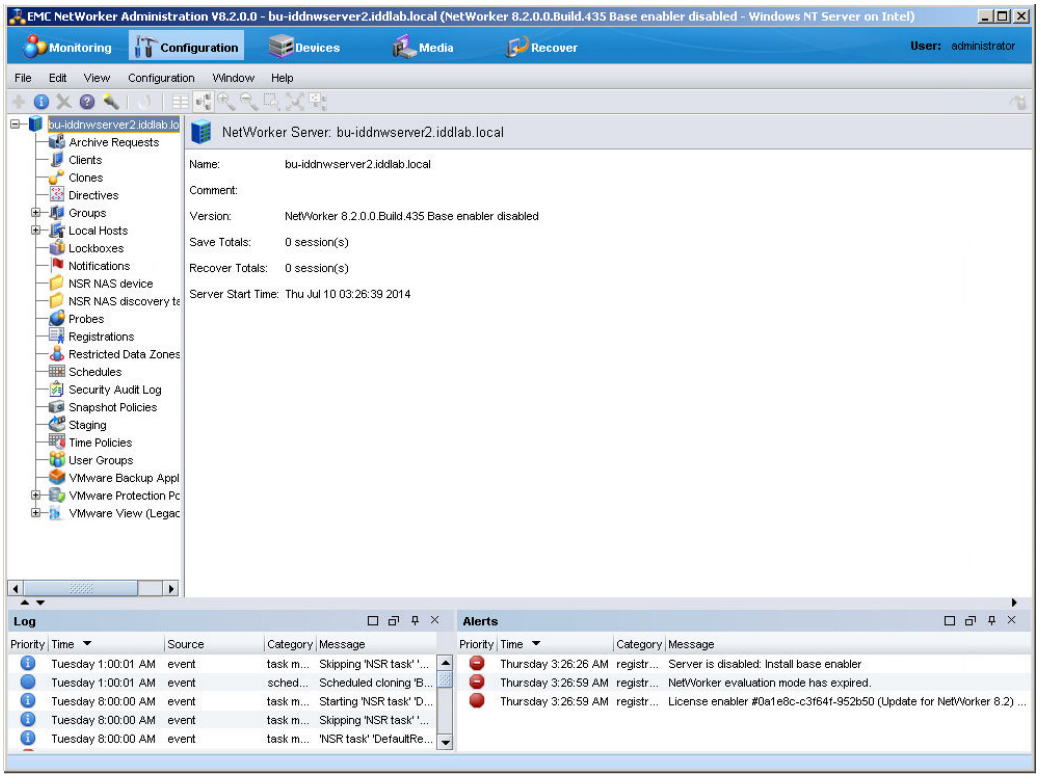
1. On the **Enterprise** tab, select the appropriate server.
2. Right-click on the server in the left pane of the Console window, and select **Launch Application**. The **Administration** window displays.

Results

NetWorker automatically creates a default device for the VMware Backup Appliance, based on the media type AFTD, for the VMware Backup Appliance's internal storage. This resource appears in the Devices window when you click the Devices tab.

You can access most of the options for the VMware Protection solution by selecting the Configuration tab, as shown in the following figure.

Figure 16 Configuration tab in the NMC Administration window



Three selections related to VMware Protection appear in the lower part of the left pane, described in the following sections:

- VMware Backup Appliance in NMC on page 69
- VMware Protection Policies in NMC on page 71
- VMware View in NMC on page 77

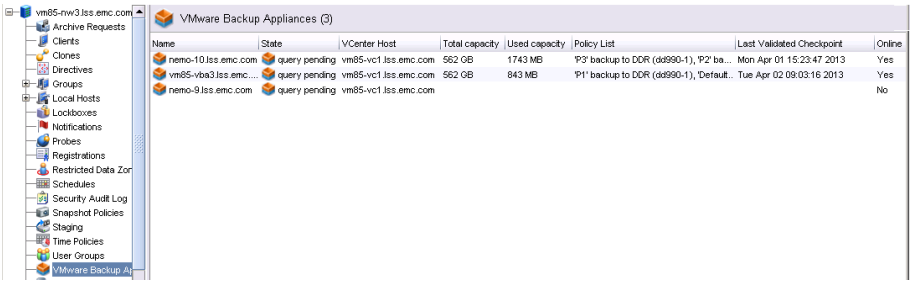
Additionally, the Monitoring tab provides the following options:

- Starting a policy manually from the NMC Monitoring window on page 81
- Stopping a policy from the NMC Monitoring window on page 82
- Viewing policy progress from the NMC Monitoring window on page 82

VMware Backup Appliance in NMC

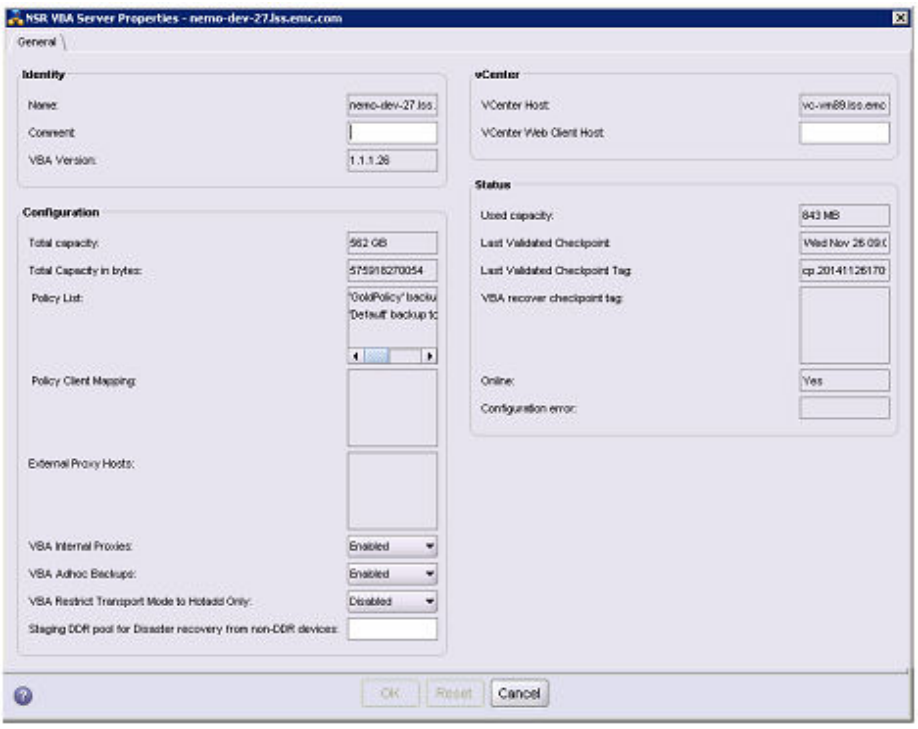
When you select VMware Backup Appliances, the available VMware Backup Appliances appear in the right pane. From the right-pane, you can monitor the state (offline/online) of the VMware Backup Appliance, as shown in the following figure.

Figure 17 VMware Backup Appliance health monitoring in NMC



To view more VMware Backup Appliance related properties, right-click on an appliance resource and select Properties, or double-click on an appliance. The NSR VBA Server Properties window displays, as shown in the following figure.

Figure 18 NSR VBA Server Properties window



NMC 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 State and Error

In addition to the fields that NetWorker populates automatically based on the current settings, the NSR VBA Server Properties window includes the following fields you can edit:

- VBA Internal Proxies—When set to Enabled (the default 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.
- VBA Adhoc Backups—When set to Enabled (the default setting), allows you to run a policy (which includes any backup and clone actions associated with the policy) immediately from NMC or the vSphere Web Client, in addition to scheduled backups. When set to Disabled, you can only perform adhoc backups for policies from NMC, and the Backup Now functionality in the vSphere Web Client will not be available for policy backups. You can, however, still initiate ad-hoc backups for individual VMs from the vSphere Web Client by navigating to **Hosts** > **Clusters**, right-clicking the VM and selecting **Backup Now**.
- VBA Restrict Transport Mode to Hotadd Only—When set to Enabled, NetWorker uses only Hotadd transport mode for policy backups, and no fallback to NBD mode (backups over IP) will occur, even if hotadd mode is not available. When set to Disabled (the default setting), NetWorker will use hotadd mode and fallback to NBD mode if hotadd mode is not available. The section Restrict mapping of datastores on page 55 provides more information on transport modes.

  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 command **`mccli activity show | grep Eligible`**.

  An output similar to the following displays:

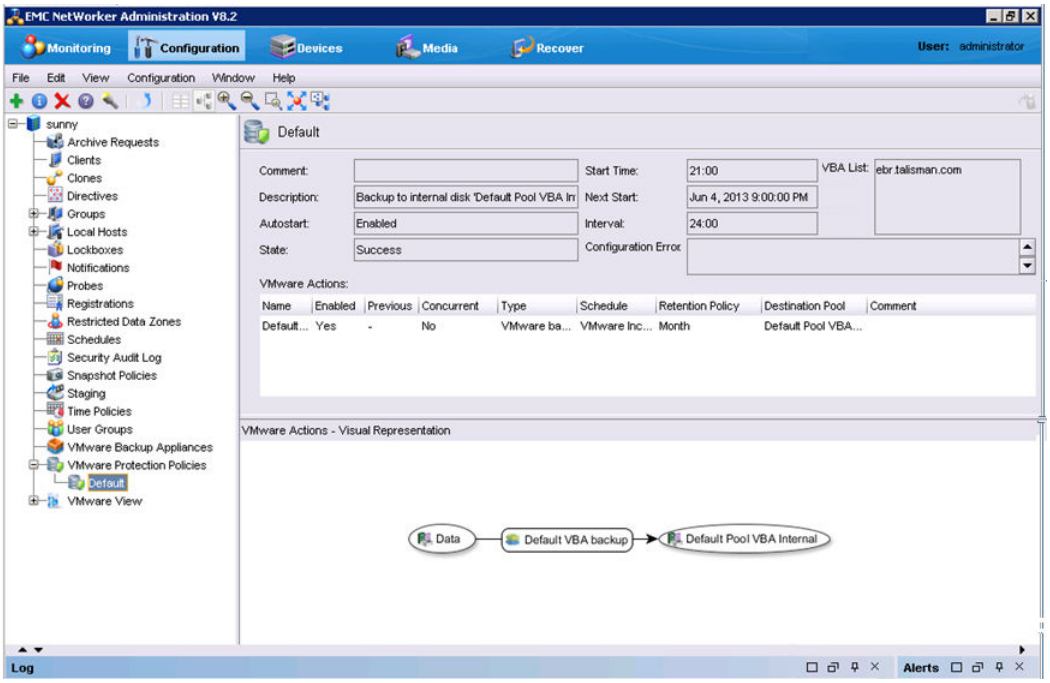
  ```
  9139905687058209 No Eligible Proxies 0 2014-05-03 00:24 IST
  00h:00m:00s 2014-05-03 00:24 IST On-Demand Backup 0 bytes 0%
  VM-Local
  ```

- Staging DDR pool for Disaster recovery from non-DDR devices—Allows you to select a different Data Domain pool for staging in cases where you perform a recovery from a non-Data Domain device on a remote site and for resurrection want to use a Data Domain device different from the one used originally for the backup. Changing the DDR pool can be useful in situations where the original Data Domain device is no longer available, or the original Data Domain device is in a different location than the clone device and you do not want to impact recovery performance.

VMware Protection Policies in NMC

When you expand VMware Protection Policies, NMC displays the default policy, which gets created after NetWorker registers the first VMware Backup Appliance. The following figure displays the Default VMware Protection policy.

Figure 19 Default VMware Protection policy in NMC



NetWorker automatically applies the default VMware Protection policy to all VMware Backup Appliances after you register the first appliance, and enables the policy to run once every 24 hours starting at 21:00. NetWorker saves the backups created by this policy on the internal storage of the appliance. The backup level used is determined by the levels defined in the Default schedule, and a one month data retention policy is used.

Setup and configure policies in NMC

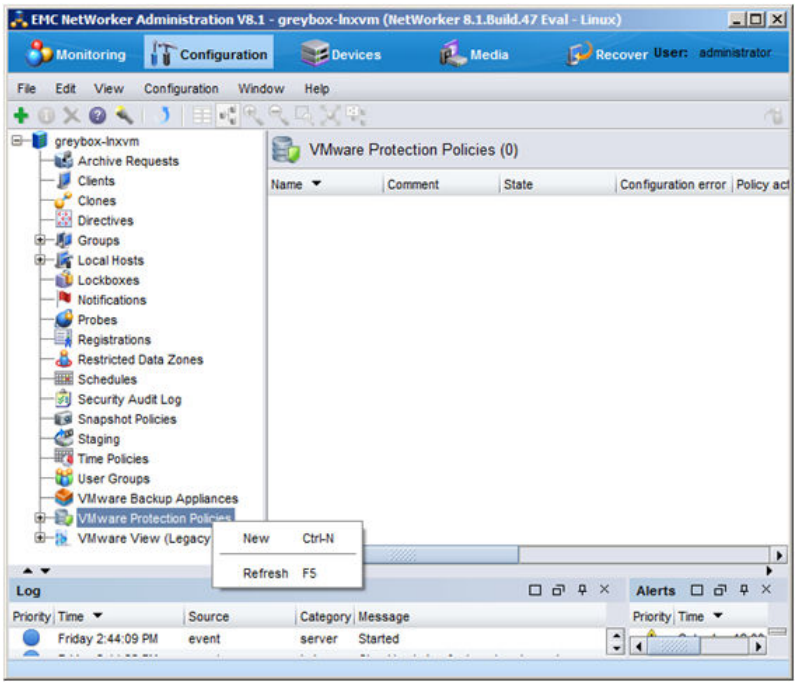
You may require more than one policy to back up the VMs in your environment. For example, there may be VMs you want to protect based on retention, how many clones you need, and so on.

To create a new protection policy:

Procedure

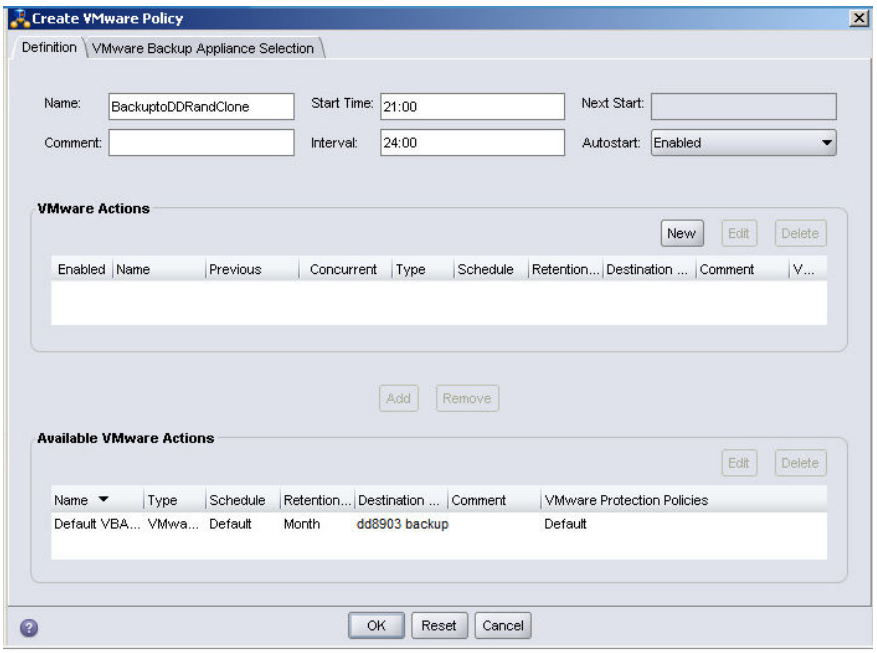
1. On the **Configuration** tab of the NMC **Administration** window, right-click **VMware Protection Policies** in the left pane and select **New**, as shown in the following figure.

Figure 20 Create new policy in NMC



2. On the **Definition** tab of the **Create VMware Policy** window, type a descriptive name for the policy, and specify a Start Time and Interval. NetWorker provides default values in these fields. In the following figure, a policy named **BackuptoDDRandClone** is being created to backup and clone VMs to a Data Domain system.

Figure 21 Create VMware policy window

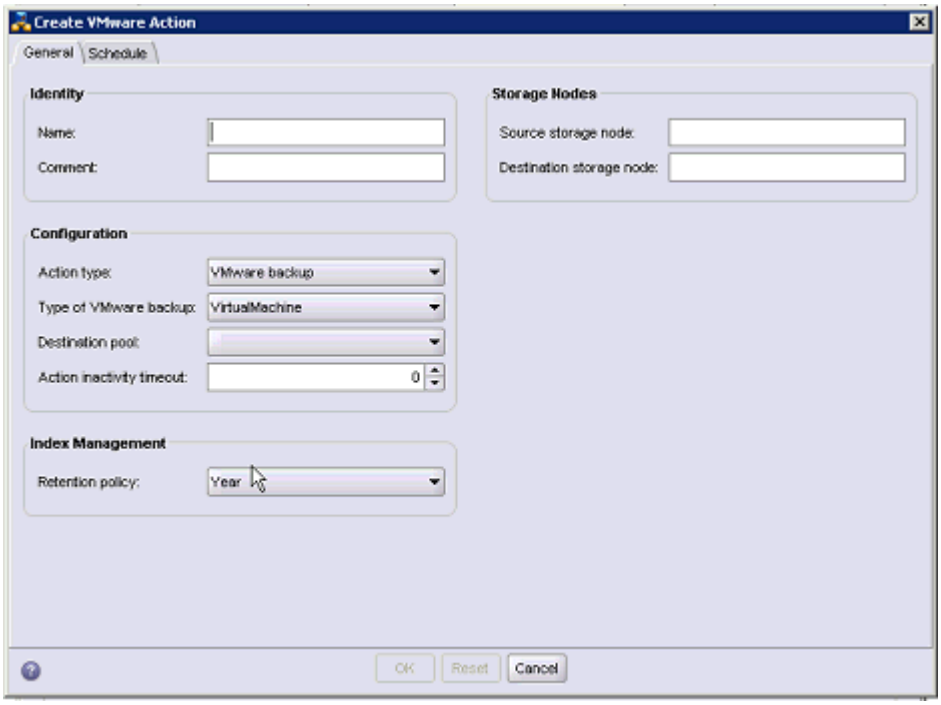


Note

Autostart is enabled by default.

3. To create the VMware action (for example, **action type=VMware backup**), click the **New** button in the VMware Actions pane. The following page displays.

Figure 22 Create VMware Action window



Four action types appear in the drop-down:

- VBA checkpoint discover—Performs a discovery of the last validated checkpoint backup of the VMware Backup appliance. If there is no validated checkpoint available, this action discovers the last non-validated checkpoint. This action must occur before the VBA checkpoint backup action.

  Note

  Currently, the VBA checkpoint discover action cannot be specified before the VMware backup action. The *EMC NetWorker 8.2 Release Notes* provide more information about this issue (NW154275).

- 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.

  Note

  You can only perform a VBA checkpoint backup to a Data Domain pool.

- VMware backup—Performs a backup of the VMware Backup appliance to internal storage or a Data Domain system. You can only perform one VMware backup action per VMware Protection policy. The backup action must occur before clone actions.

Note

Only backups to a Data Domain system can be cloned.

- Clone—Performs a clone of the VMware backup on a Data Domain system to any cloning 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. You can also clone a VBA checkpoint backup, but only to a Data Domain destination pool.

Note

Cloning to tape will clone a full backup each time, even if the VMware backup is an incremental backup. When cloning to tape, ensure that tapes contain sufficient space for the full backup.

4. Repeat the following steps for each action type:
   a. Type a name that describes the action.
   b. In the Action type field, select the action type.
   c. Select the type of VMware backup:
      - Select VirtualMachine to back up VMs only. This is the default selection. When you select this backup type, VMware View will display contents down to the VM level.
      - Select VMDK to back up individual virtual disk files, which store the contents of the virtual machine's hard disk drive. When you select this backup type, VMware View will display contents down to the VMDK level.
   d. Choose a destination pool:
      - For VBA checkpoint backup, select the Data Domain backup pool.
      - For VMware backup actions, select Default Pool VBA Internal to backup to internal storage, or the Data Domain backup pool to backup to a Data Domain device.
      - For clone actions, select the pool for your created Data Domain device, or a clone pool containing tapes for cloning to tape.
        When you select the pool for the Data Domain device, the VMware backup occurs to the Data Domain device instead of VBA internal storage. For example, to create the BackuptoDDRandClone policy, the Data Domain device requires a backup pool, because you cannot clone a backup to Default Pool VBA Internal.
   e. Select a retention policy for Index Management, or use the default value.
   f. On the **Schedule** tab, NetWorker uses the default **VMware Incremental Forever** schedule. You can use the default schedule, select an alternate schedule from the drop-down, or click the green **+** to create a new schedule or edit a schedule.

Note

The Schedule drop-down does not allow you to select schedule overrides.

Note

You must select a schedule for each clone action. If you do not specify a schedule for a clone action, any subsequent actions in the policy will not run. When you select a schedule for clone actions, EMC recommends a weekly or monthly schedule, depending on your requirements, due to the time required to complete this action. Since save sets are synthesized on the source Data Domain device after performing an incremental backup, a scheduled clone will clone the entire save set chain, including data from previous backups.

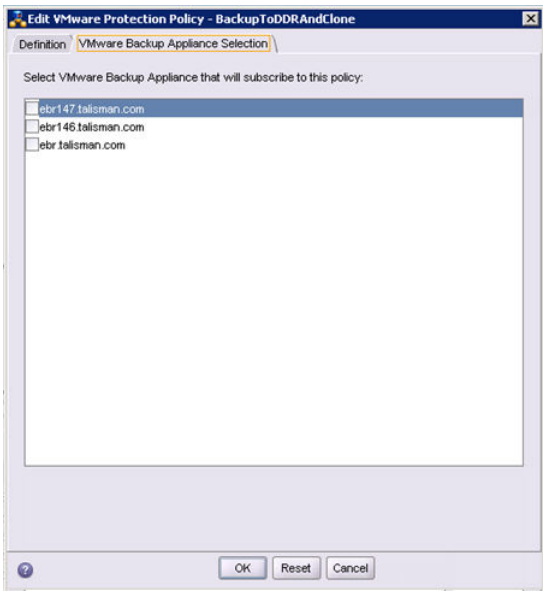
When you click OK to create the VMware backup action, the Create/Edit VMware Protection Policy window displays again, with the new action in the VMware Actions pane, along with all of the policy details. You must now assign a VMware Backup Appliance to the policy.

5. In the **Create/Edit VMware Protection Policy** window, select an appliance on the **VMware Backup Appliance Selection** tab, as shown in the following figure, and then click **OK**.

Note

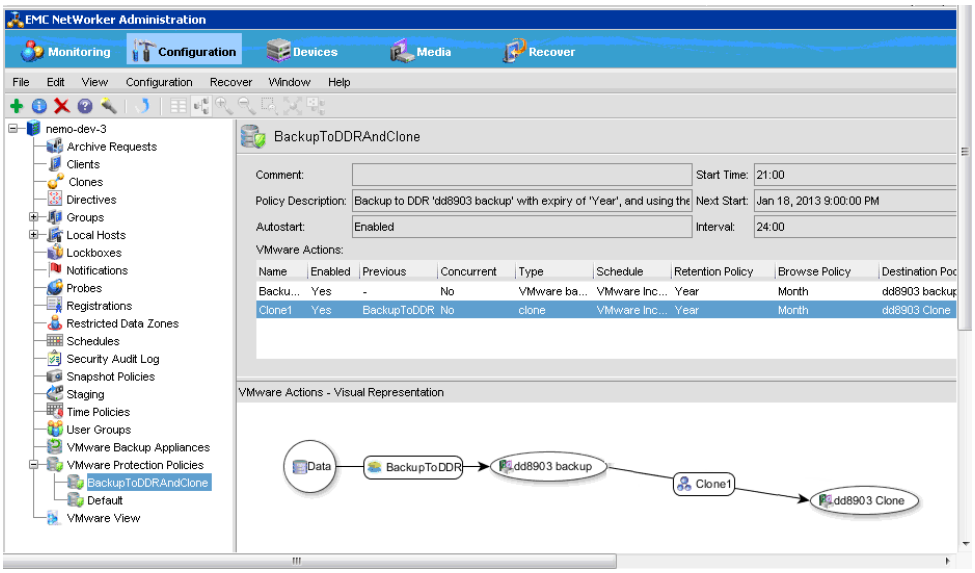
If you do not select a VMware Backup Appliance for the policy, NMC displays a warning message indicating there is no appliance attached to this policy, and asks if you want to proceed. If this warning displays, click **No**, and then return to this window to assign a VMware Backup Appliance.

Figure 23 Select a VMware Backup Appliance in the Create/Edit VMware Protection Policy window



When you complete these steps, the following page displays, showing the completed VMware Protection Policy and associated actions. A map also appears at the bottom of the window displaying a visual representation of the policy and actions.

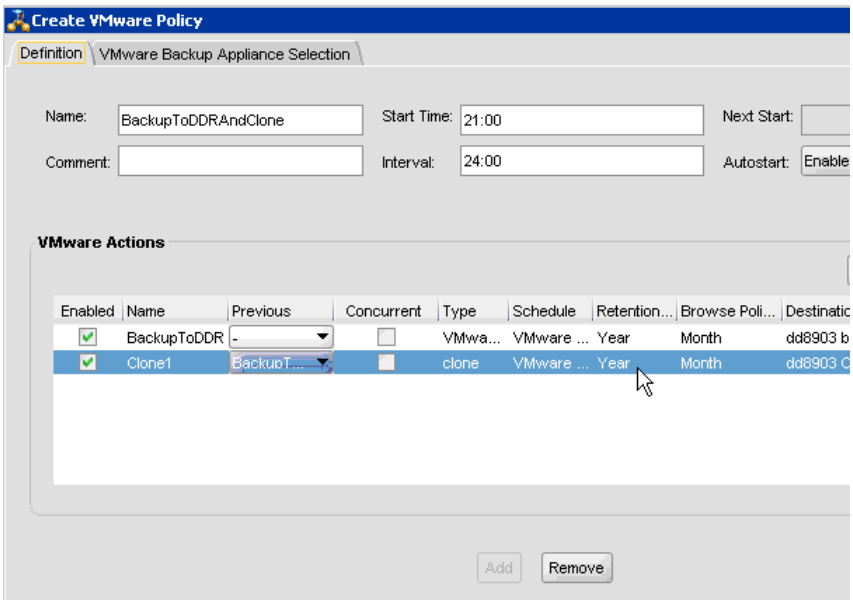
Figure 24 VMware Protection policy with associated actions



To avoid waiting until all backups complete before the clone action begins, you can choose to make the operations concurrent, similar to NetWorker's immediate cloning option which allows a group to start cloning upon each save set completion.

To enable and mark actions to run concurrently with their preceding actions, open the **Create VMware Policy** or **Edit VMware Protection Policy** window, and then select the appropriate checkboxes under the Definition tab, as shown in the following figure.

Figure 25 Enable and mark actions concurrent in Create VMware Policy window



Once you create the policy and complete the Actions, select the VMware backup appliance that the policy applies by selecting the VMware Backup Appliance Selection tab, available from the **Create VMware Policy** or **Edit VMware Protection Policy** windows.

VMware View in NMC

After detecting VMware environments, the NetWorker console provides a visual representation of these environments when you select VMware View in the left pane of the NMC Configuration window. Using VMware View, you can also assign the policies you created in Setup and configure policies in NMC on page 71.

The following sections describe options available in VMware View:

- Map view of the VMware environment on page 77
- Table view of the VMware environment on page 79
- Assigning policies within VMware View on page 80
- Overprotected and unprotected VMs in VMware View on page 81
- Assigning a policy to a disconnected ESX server in VMware View on page 81

Note

After upgrading to NetWorker 8.2, VMware View may not be visible. The section Enable VMware View in NMC after upgrading by creating a NSR Hypervisor resource on page 49 provides more information.

Map view of the VMware environment

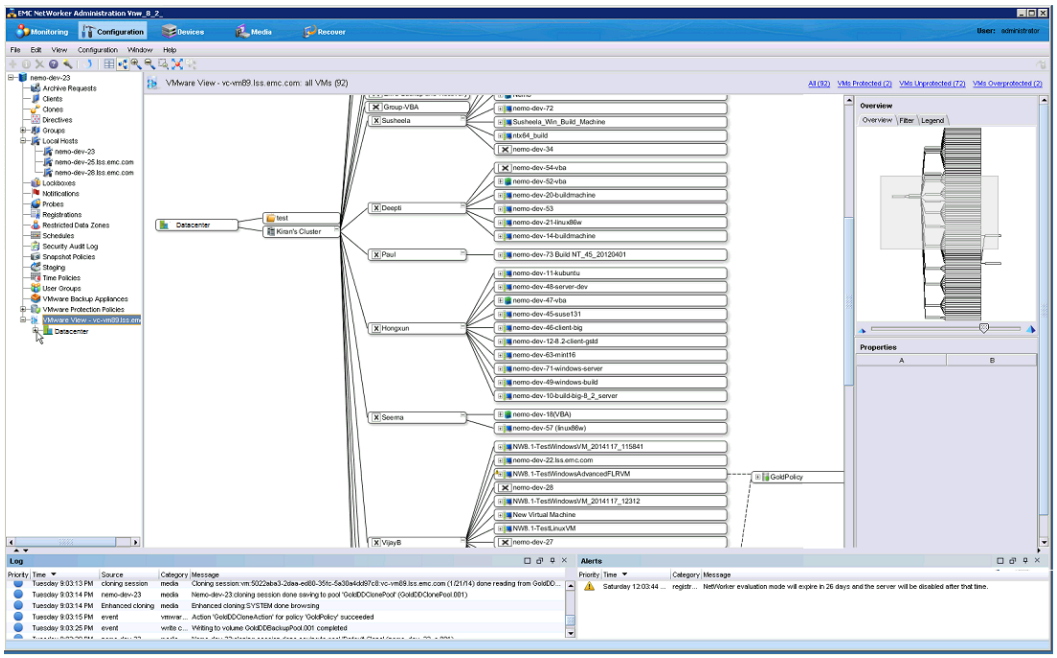
When you expand VMware View, a hierarchical display of the VMware environment appears. The following containers display:

- vCenters
- DataCenters within the vCenter
- Clusters within the DataCenter
- ESX servers
- vApps
- Resource Pools
- Folders

Clicking on any container in the hierarchical tree provides a detailed map view of that container and all of its children in the right pane. For example, selecting the top level virtualization node will display a complete view of your VMware environment across all configured vCenters, while selecting an individual ESX server or Cluster in the hierarchy will display the resource pool — 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.

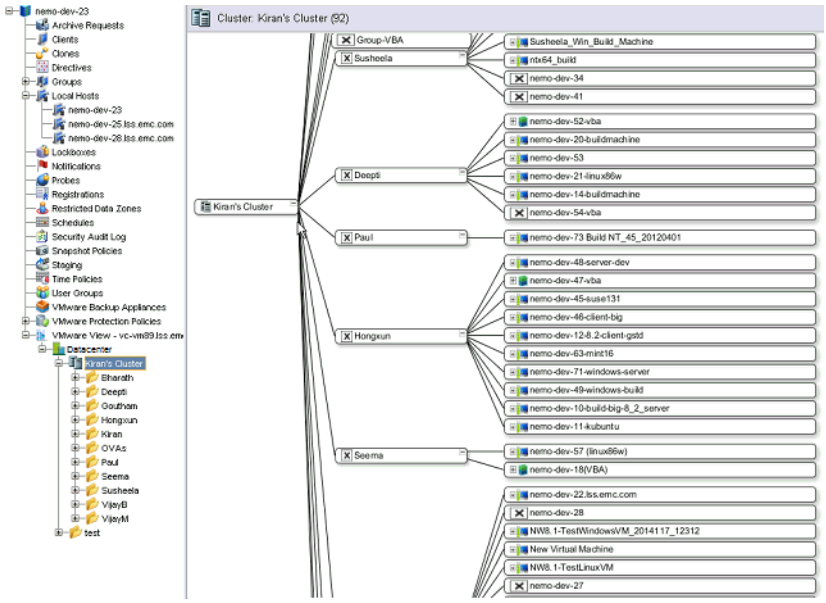
Lines connect each child element to its parent, with child elements proceeding hierarchically from left to right in the display, as shown in the following figure.

Figure 26 Map view of VMware environment in NMC



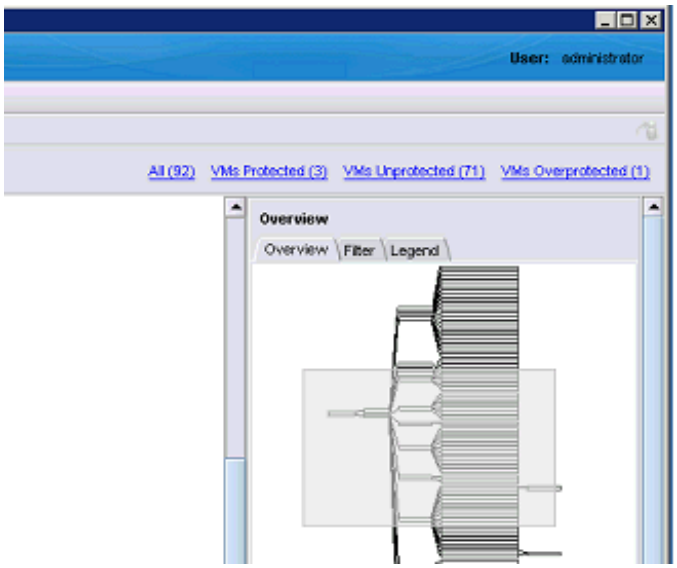
You can refine items displayed in the right details pane by selecting containers in the Virtualization node hierarchy in the left pane. For example, if an individual Cluster is selected in the Virtualization node, only child elements associated with that Cluster display.

Figure 27 Cluster with child elements in VMware View



You can also filter the visible items to show only protected VMs, unprotected VMs, or overprotected VMs, by clicking the links located above the right pane, as shown in the following figure.

Figure 28 Filtering results in VMware View



Navigating within the Map view

VMware View provides several operations to facilitate navigation within the map view:

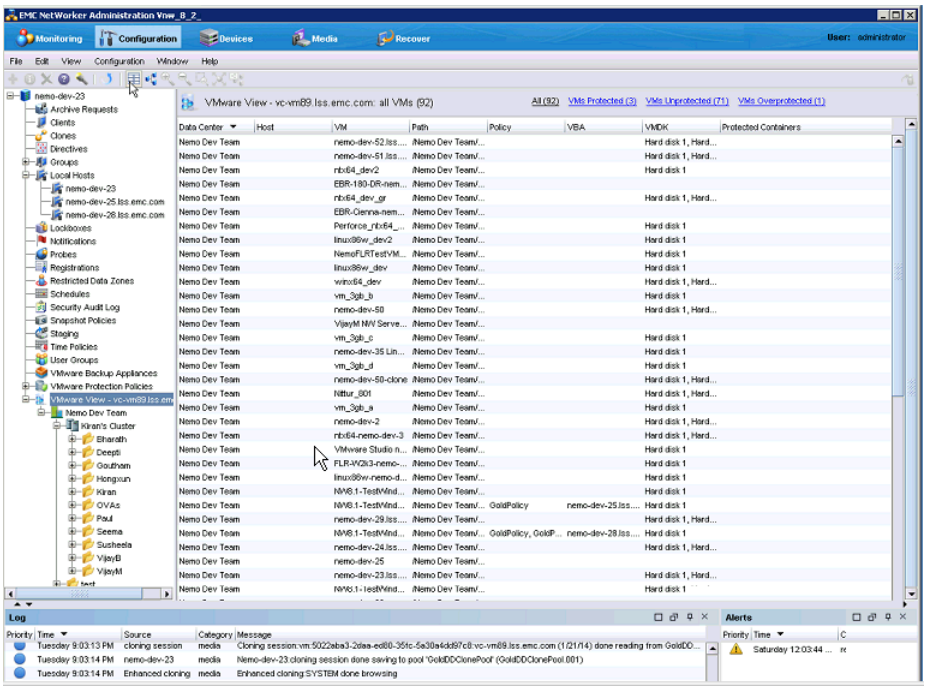
- Zoom in/out: You can zoom in and out of the map view by selecting the zoom icons on the map view icon bar or by clicking on the right details pane and scrolling with the mouse wheel. You can also select an area to zoom into by selecting the Zoom Area button, or fit the entire display into the right details pane by selecting the Fit Content button. These operations are also available by right-clicking in the details pane.
- Moving the display: You can move the graphical display by left-clicking in the details pane and dragging the mouse cursor.
- Expanding and collapsing containers: You can expand or collapse any container in the map view to display or hide the child elements associated with the container by double-clicking the container.
- Overview: You can display an overview of the map view by selecting 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.
- Filter: You can limit items displayed and search for specific items in the map view by using the Filter VM by and Show functions, available from the Filter tab within the Overview pane.

Table view of the VMware environment

You can switch to view the VMware environment in table form, rather than map form, by selecting the Table icon on the map view icon bar, as shown in the following figure,

or by right-clicking anywhere in the details pane and selecting Table. The Table view functions like other table views in the NetWorker Console.

Figure 29 Select Table view in VMware 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 VMs, unprotected VMs, or all VMs in the environment. The NetWorker *Administration Guide* provides general information on using tables in the NetWorker Console.

Note

In table view, the Host field contains an undefined value for VMs or containers that are part of a cluster. The map view provides a link to the cluster.

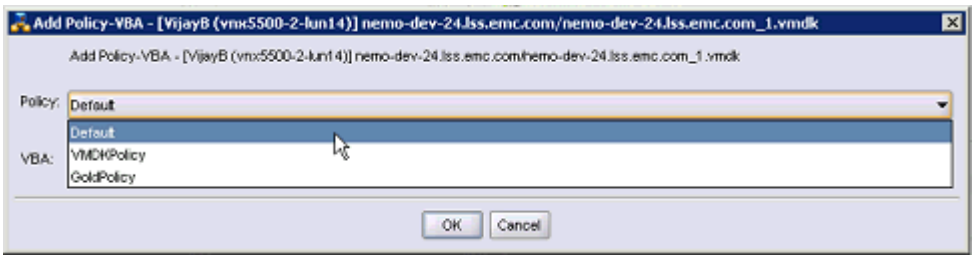
Assigning policies within VMware View

You can assign policies at any level (for example, you can assign a policy to the entire datacenter, a cluster, a resource pool, a VM, or even a VMDK) by using VMware View.

Procedure

1. Right-click on any container, or expand the container and right-click on an element within VMware View.
2. Select **Add Policy-VBA**. The available policies display, as shown in the following figure.

Figure 30 Add policy in VMware View



When you select a policy, VMware View refreshes and displays the new association.

3. To assign a policy at the VMDK level, expand a VM and highlight the VMDK(s) you want to associate to the policy, and then right-click and select Add Policy-VBA. Ensure that you select a policy that has been specifically configured to back up VMDKs using the backup type option specified in the section Setup and configure policies in NMC on page 71.

Overprotected and unprotected VMs in VMware View

NMC uses a warning icon within VMware View to show VMs that are overprotected (when a particular VM is protected by two different policies, or two different VMware Backup Appliances) or unprotected (when there are no policies assigned to protect a particular VM 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 policies to VMs/VMDKs. When overprotection occurs, you can remove a policy by right-clicking the object and selecting Remove policy-VBA. When you unselect the additional policy in the resulting dialog, the warning sign disappears.

You can use the Filter links, as shown in Figure 28 on page 79, to narrow your view to only overprotected or only unprotected VMs.

Assigning a policy 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 VMware Protection policy to an ESX host that is disconnected from the vCenter server, however, if you start the policy, the policy will remain in “interrupted” state until you connect the disconnected ESX back to the vCenter server and run the Policy again.

Note

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

Starting a policy manually from the NMC Monitoring window

You can manually start a VMware Protection policy by right-clicking the policy in the Groups and Policies section on the Monitoring window and selecting Start. Otherwise, wait for NetWorker to start the backup policy based on the scheduled start time.

Stopping a policy from the NMC Monitoring window

To cancel a policy in NMC, right-click the backup policy in the Groups and Policies section on the NMC Monitoring window and select the Stop option.

Viewing policy progress from the NMC Monitoring window

You can view the progress of a policy in the Policy Details dialog, which appears when you double-click the policy in the Groups and Policies section on the Monitoring window.

NetWorker displays the session progress for a policy in the All Sessions section on the NMC Monitoring window. You can view NMC Reports for completed policies on the Reports tab by selecting NetWorker Data Protection Policy reports.

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 policies within VMware View on page 80, 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

The following sections provide more information about using the EMC Backup and Recovery user interface in the vSphere Web Client:

- Benefits of EMC Backup and Recovery user interface in the vSphere Web Client on page 83
- Deduplication store benefits on page 83
- Image-level Backup and Restore on page 84
- Connecting to the EMC Backup and Recovery user interface in the vSphere Web Client on page 85
- Available tasks in the EMC Backup and Recovery user interface on page 86
- Assigning VMs/VMDKs to a policy on page 91
- Manually starting the backup policy using Backup Now on page 93
- Stopping a policy in the EMC Backup and Recovery user interface on page 93
- Viewing policy progress in the vSphere Web Client on page 93

Note

You cannot use the VMware Backup appliance without a vCenter Server. In linked mode, the appliance works only with the vCenter to which it is associated.

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 VMs/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 83 provides more information.
- Reduces the cost of backing up VMs and minimizes the backup window by using Changed Block Tracking (CBT) and VM snapshots.
- Allows for easy backups without the need for third-party agents installed in each VM.
- 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 VM to the EMC Backup and Recovery appliance. The EMC Backup and Recovery appliance communicates with the vCenter Server to make a snapshot of a VM'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 VMs. All VMs 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 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 VM image and provides the ability to process a large number of VMs within a particular backup window.

By leveraging CBT during restores, EMC Backup and Recovery offers fast and efficient recoveries when recovering VMs 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 VM 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 VMs, 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 VM
- Supports simultaneous backup and recovery for superior throughput

Connecting to the EMC Backup and Recovery user interface in the vSphere Web Client

Perform the following to connect to the **EMC Backup and Recovery** user interface within the **vSphere Web Client**.

Procedure

1. From a web browser, open the **vSphere Web Client**:

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

   Note

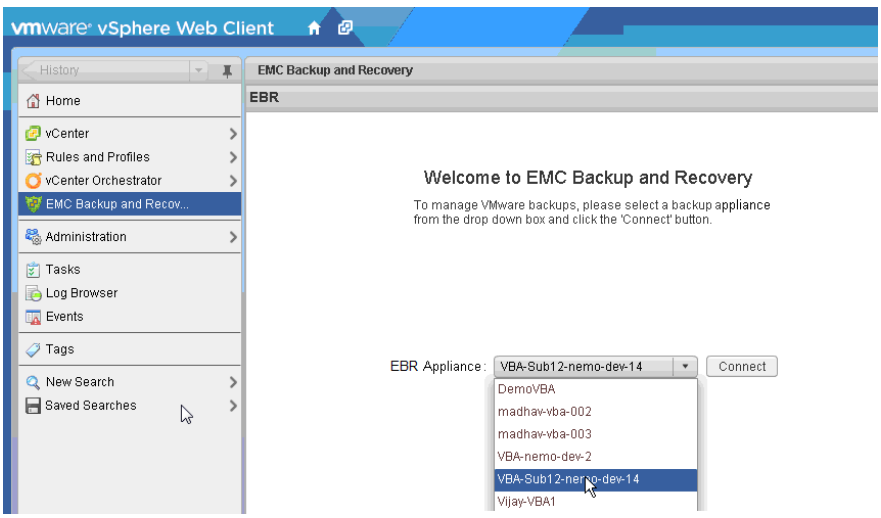
   If you receive an SSL certificate error in your web browser, refer to the VMware knowledgebase article 1021514 at the following link:

   http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021514

2. In the **Credentials** window, type the vCenter user name and password for the dedicated EMC Backup and Recovery user you created and then click **Login**.
3. In the vSphere Web Client, select **EMC Backup and Recovery**.
4. In the **Welcome to EMC Backup and Recovery** window, select an appliance from the drop-down. This drop-down lists all the VMware Backup appliances registered in the vCenter.

   Each vCenter Server supports up to 10 appliances. The EBR Appliance field, as shown in the following figure, displays the appliance names alphabetically in a drop-down list. In the EMC Backup and Recovery user interface, the name of the active appliance displays on the left pane, and the appliance name in the drop-down list is the first in the list of available appliances.

Figure 31 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 command

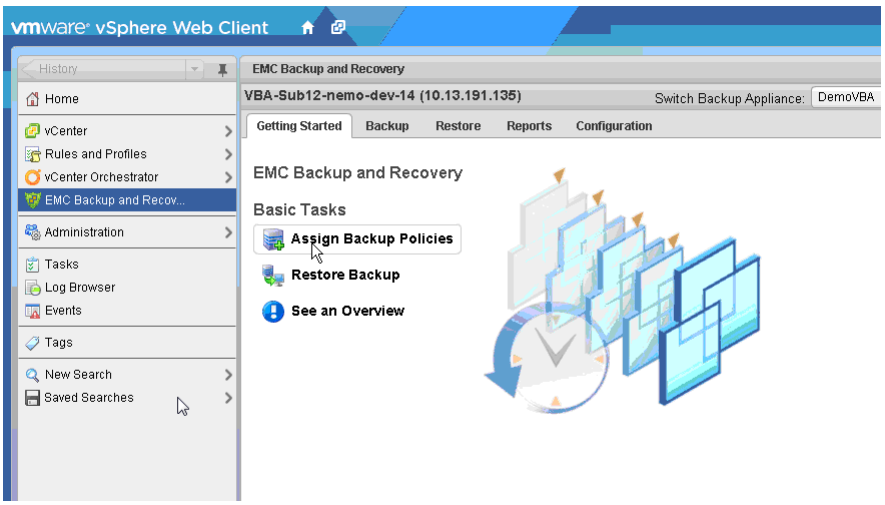
```
ebrserver.pl --restart.
```

Available tasks in the EMC Backup and Recovery user interface

The **EMC Backup and Recovery** user interface in the **vSphere Web Client** allows you to configure and manage the VMware Backup appliance.

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

Figure 32 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 VMs to a policy and perform restores.
- Backup—Provides a list of scheduled backup policies as well as details about each policy created in NMC. This window enables users to add the VMs/VMDKs you want to protect to the policies, and to run policies on demand. About the Backup Tab on page 87 provides additional information on adding VMs to the backup policies and starting backup policies on demand.
- Restore—Provides a list of successful backups that you can restore. About the Restore Tab on page 88 provides additional information.
- Report—Provides backup status reports for the VMs on the vCenter Server that you added to the policy. About the Reports Tab on page 88 provides additional information.
- Configuration—Displays configuration information and allows you to edit some of these settings. Also allows you to run integrity checks (for example, checkpoint creation and validation). About the Configuration Tab on page 88 provides additional information.

The following sections describe the contents of the tabs.

About the Backup Tab

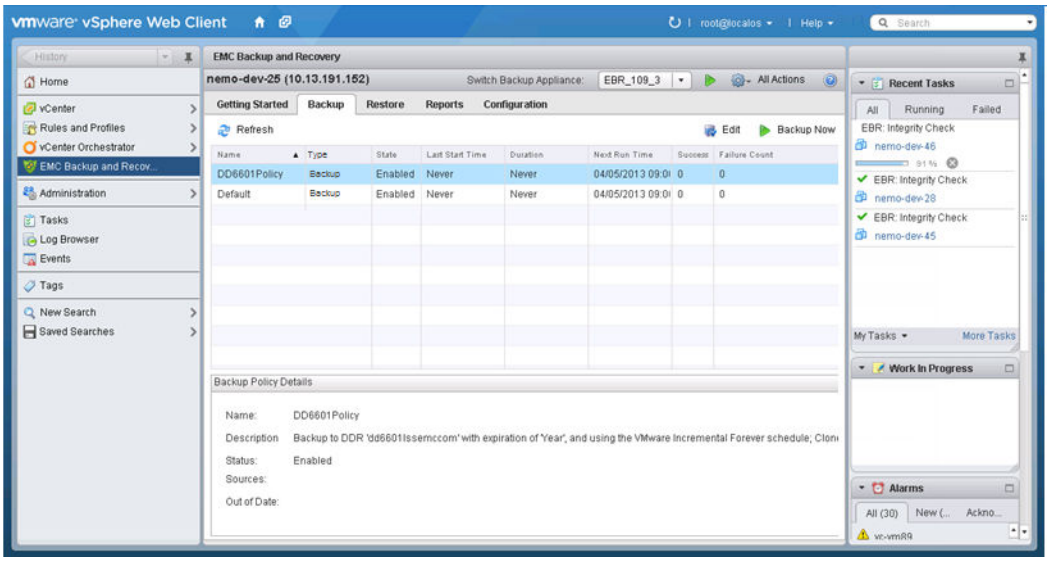
The Backup tab displays information about available backup policies in a tabular list.

Table 18 Backup tab column descriptions

Column	Description
Name	The name of the backup policy.
Type	The type of policy, for example, backup or clone.
State	Whether the backup 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.
Last Start Time	The last time you started the policy.
Duration	The length of time for the last policy to complete.
Next Run Time	The policy will run again at this scheduled time.
Success Count	The number of VMs that were backed up successfully the last time the backup 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 VMs successfully backed up, and then you edit the policy so that only one VM remains, this number remains at 10 until the policy runs again and, if successful, the number changes to one.
Failure Count	The number of VMs that did not back up successfully the last time the backup 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 VMs failed to back up, and then you edit the policy so that only one VM remains, this number remains at 10 until the policy runs again and, if the backup fails, the number changes to one.

The following figure displays two example backup policies.

Figure 33 Backup policies in the EMC Backup and Recovery user interface



About the Restore Tab

The Restore tab displays a list of VMs that you backed up by using the VMware Backup appliance. By navigating through the list of backups, you can select and restore specific backups.

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 94.

About the Reports Tab

The top half of the Reports tab lists information for each of the VMs associated with the vCenter Server.

From the bottom section on the Reports tab, you can select a VM and view detailed information about the selected client.

The left pane on the Reports tab provides links to the Event Console and the Task Console. Clicking on these links displays the vCenter Server Event Console or Tasks Console.

About the Configuration Tab

The Configuration tab allows you to manage the maintenance tasks for the VMware Backup appliance. You can perform the following tasks on this tab:

- Viewing backup appliance configuration on page 88
- Configuring Email on page 89
- Viewing the Log on page 91

Viewing backup appliance configuration

Backup Appliance information provides information for Backup Appliance Details, and Backup Windows Configuration.

Backup Appliance Details include (in the following order):

- Display name
- Product name
- IP Address
- Major Version
- Minor Version
- Status
- Host
- vCenter Server
- NetWorker Server
- EBR backup user
- EBR appliance time
- Time zone

You can configure these options during the VMware Backup appliance installation. You can also edit these options by using the EMC Backup and Recovery Configure window. Post-Installation configuration in the EMC Backup and Recovery Configure window on page 63 provides additional details.

Configuring Email

You can send SMTP email reports to specified recipients when you enable email notification. The email includes the following information:

- VMware Backup appliance status
- Backup jobs summary
- Virtual machines summary

Email configuration requires the information defined in the following table.

Table 19 Email configuration fields

Field Name	Description
Enable email reports	Check this box to enable email reports.
Outgoing mail server	Enter the name of the SMTP server you want to use to send email. You can enter this name as either an IP address, a host name, or a FQDN. The VMware Backup 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 fields (continued)

Field Name	Description
Username	Enter the user name you want to authenticate with.
Password	Enter the password associated with the username. EMC Backup and Recovery does not validate the password.
From address	Enter the email address that sends the email report. You can only specify a single address.
To address	Enter a comma-separated recipient 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 the reports.
Send days	Check the days that you want EMC Backup and Recovery to send the reports.
Report Locale	From the drop-down list, choose the locale for the email reports. en-us is the default.

Note

EMC Backup and Recovery email notification does not support carbon copies (CCs), blind carbon copies (BCCs), and SSL certificates.

Before you configure email notifications, ensure that the email account that sends the email reports exists.

Procedure

1. From the **EMC Backup and Recovery** user interface, select the **Configuration** tab.
2. Select **Email**.
3. In the bottom right corner of the window, click the **Edit** button.
4. Specify the following:
   a. Enable email reports
   b. Outgoing mail server
   c. (optional) My server requires me to log in
   d. User name
   e. Password
   f. From address
   g. To address(es)
   h. Send day(s)
   i. Send time
   j. Report Locale

5. Click the **Save** button.

Results

To test your email configuration, click Send test email.

Viewing the Log

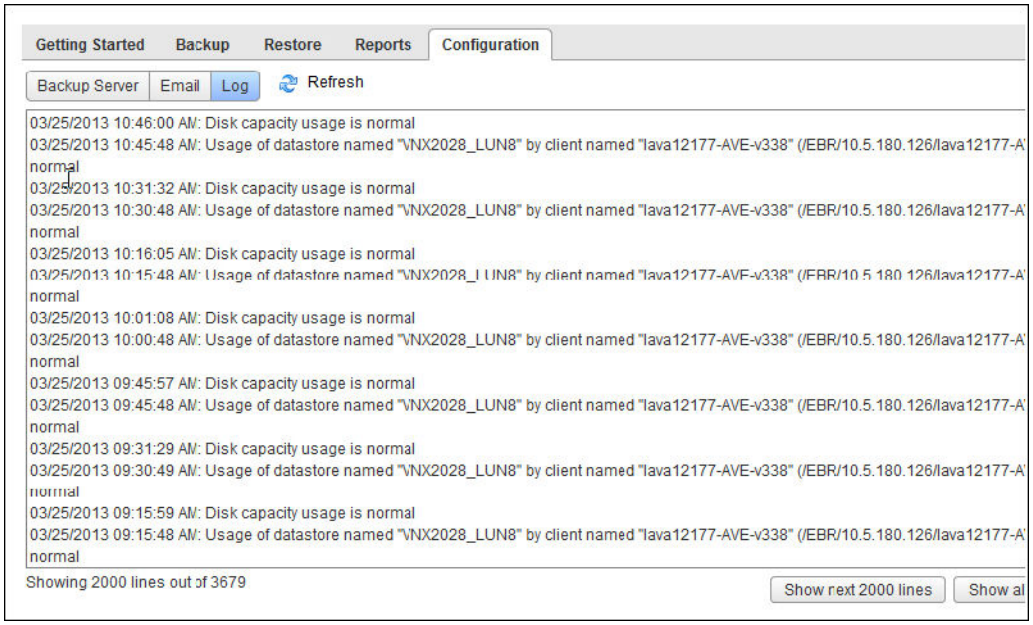
Click **Log** on the Configuration tab to display the user interface log for EMC Backup and Recovery.

A high-level log details the activities initiated with the user interface and identifies some key status items.

Click **Refresh** to view the latest user interface log entries.

Click **Export View** to save the details that display on the screen to file on the machine where your browser runs.

Figure 34 Viewing the log on the Configuration tab



Assigning VMs/VMDKs to a policy

Note

EMC recommends using NMC to assign VMs/VMDKs to a policy, as described in the section Assigning policies within VMware View on page 80.

You can assign collections of VMs (such as all VMs in a datacenter), individual VMs, and VMDKs to be included in a policy backup using the EMC Backup and Recovery user interface in the vSphere Web Client. If you select an entire resource pool, host, datacenter, or folder, any new VMs in that container are included in subsequent backups. If you select a VM, then any disk added to the VM is included in the backup. If you move the VM from the selected container to another unselected container, then the VM is no longer part of the backup.

You can also manually select a VM to be backed up, which ensures that NetWorker backs up the VM, even when you move the VM.

Note

EMC Backup and Recovery will not back up the following specialized VMs:
-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 VMs; however, when you click Finish the Wizard displays a warning that the job does not contain these special VMs.

Procedure

1. Select **EMC Backup and Recovery** in the vSphere Web Client.
2. On the **Getting Started** tab, select **Assign Backup Policies**. The **Backup** tab displays, which shows the available policies in upper half of the window, and the Backup Policy Details in the lower half.

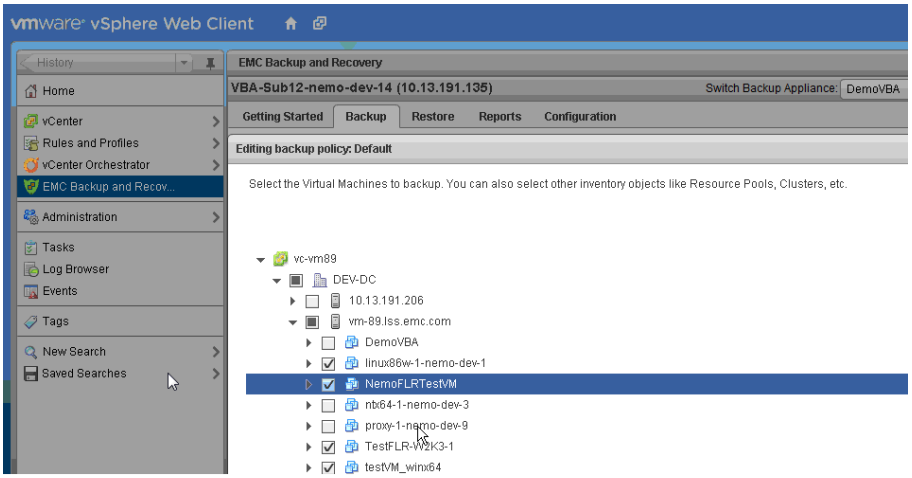
   The policy description matches the description in NMC (for example, Default). Backup to internal disk means that any VMs you assign to this default policy will go to the storage of the deployed VMware Backup appliance. When you perform backups to the internal storage of a VMware Backup appliance, these details appear in NMC and as part of the policy description in EMC Backup and Recovery in vCenter.

3. Click **Edit**. All the VMs in the vCenter display.
4. Use the checkboxes next to the VMs to select the VMs that you want to include in the selected policy, as shown in the following figure, or expand the VMs to select VMDKs. You can also select other inventory objects such as Resource Pools or Clusters in addition to specific VMs.

   Note

   You can only assign VMs/VMDKs to the policies that you create in NMC.

Figure 35 Selecting VMs in EMC Backup and Recovery user interface



1**Figure 36** Selecting at VMDK level in EMC Backup and Recovery user interface

5. Click **Finish**. A dialog box displays to indicate that the backup policy was saved successfully.

Results

To return at any time to the Backup Policy Details window and verify which VMs that you selected, click Edit. This information also appears in the lower half of the window, in the Show Items link next to the Sources field.

Manually starting the backup policy using Backup Now

You can manually start the backup policy in the EMC Backup and Recovery user interface by selecting Backup Now in one of the following ways:

- Click Backup Now on the EMC Backup and Recovery user interface's Backup tab. Two options display:
  - Backup all sources
  - Backup only out of date sources
- Right-click individual VMs in vCenter and select Backup Now.

When you start the policy from the EMC Backup and Recovery user interface in the vSphere Web Client, any clone actions associated with the policies will also run.

Note

If you disabled Backup Now functionality in the NSR VBA Server Properties window in NMC, as described in the section VMware Backup Appliance in NMC on page 69, this will disable Backup now for policy backups. A message displays indicating that Backup Now is locked and not available. You can, however, still initiate ad-hoc backups for individual VMs from the vSphere Web Client by navigating to **Hosts** > **Clusters**, right-clicking the VM and selecting **Backup Now**.

Otherwise, you can wait for NetWorker to start the backup policy based on the scheduled start time.

Stopping a policy in the EMC Backup and Recovery user interface

Procedure

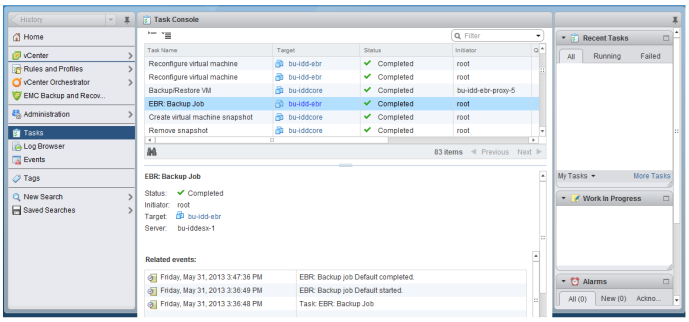
1. Navigate to the **Backup** tab.
2. Click the circular **x** symbol associated with the backup job in the **Recent Tasks** pane.

Viewing policy progress in the vSphere Web Client

To view the progress for a backup policy, select Tasks in the left pane of the vSphere Web Client.

The Task Console displays, as shown in the following figure.

Figure 37 Viewing policy progress in the Task Console



After the backup completes, you can recover the backed up VMs in the vSphere Web Client or perform a file-level restore by using the EMC Data Protection Restore Client.

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 restores 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.

The following sections describe the restore options:

- FULLVM (Image-level) Restore on page 94
- File-level restore on page 101

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:

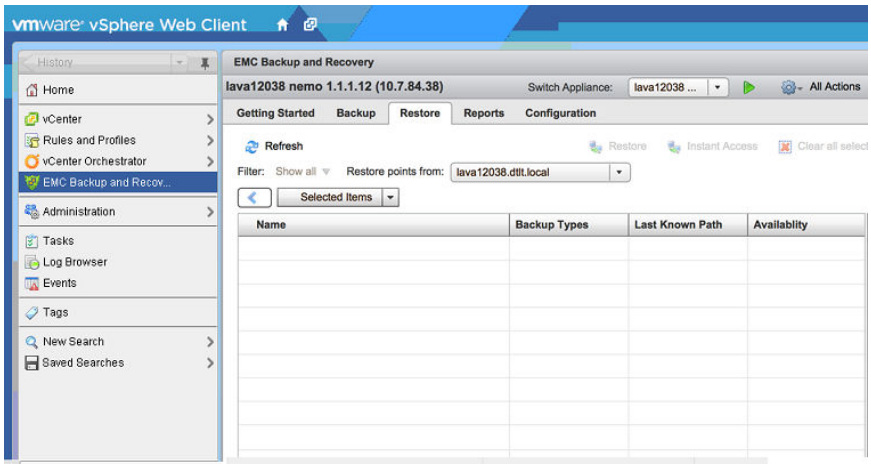
- Click Restore Backup on the Getting Started tab.
- Select the Restore tab.

When you select the Restore tab, available VMs for the selected appliance display. Additionally, you can select a different appliance from the **Restore points from** drop-down, as described in the section Recovery from secondary storage. For every clone, a backup is listed under the restore point.

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.

Figure 38 Restore tab in EMC Backup and Recovery user interface



The following sections describe FULLVM restore options:

- Performing a FULLVM restore on page 95
- Cancelling a FULLVM restore on page 96
- Instant access restore (for Data Domain systems only) on page 96
- Restore from last backup on page 98
- Direct to host recovery (Emergency Restore) on page 98
- Restore from a secondary site

Performing a FULLVM restore

Procedure

1. Power off each VM that you want to restore.
2. On the **Restore** tab, click the **Restore points from** drop-down to select the appliance you want to restore from.

   Note

   Once you perform a restore from a secondary VMware Backup appliance for a particular VM's restore point, you can no longer use this restore point for Instant access or VMDK level restores. You can use file-level restore or image-level restore as an alternative to restore the data. The knowledgebase article 196887, available at http://support.emc.com, provides more details.
3. Expand the VM that you want to restore. You can filter by using the **Filter** drop-down to show a specific VM and related items. You can also browse to the

VMDK level and select a single VMDK for restore if you only want to restore that disk.

4. Select a restore point and click **Restore**. The **Restore backup** wizard launches.
5. On the **Select Backup** page, select the correct restore point (the wizard displays all restore points for the backup by date and time). Typically, you only select one restore point at a time. Click **Next**.
6. On the **Set Restore Options** page, specify where you want to restore the backup:
   - **Restore to Original Location**—When you select **Restore to Original Location**, then the backup restores to its original location. If the VMDK file still exists at the original location, then the restore process overwrites the file.
   - **Restore to New Location**—When you unselect **Restore to Original Location**, you can then specify a new location (new Name, destination, and datastore) where the VM/VMDK will be restored.

     Optionally, set the VM to Power On and Reconnect NIC after the restore process completes. Click Next.

     Note

     Reconnect NIC is enabled by default and greyed out. Only when you select **Power On** are you given the option to unselect Reconnect NIC.
7. 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).

Results

To change any of the settings for your restore request, either use the Back button to return to the appropriate screen, or click on the appropriate numbered step title to the left of the wizard. If the settings are correct, then click Finish. If the settings are not correct, then click Back to go back to create the correct configuration.

The Restore wizard displays a message that the restore process initiated successfully. 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 that the network configuration for the newly-created VM. Once the restore completes, the new VM NIC might use the same IP address as the original VM, which will cause conflicts.

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.

Cancelling 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)

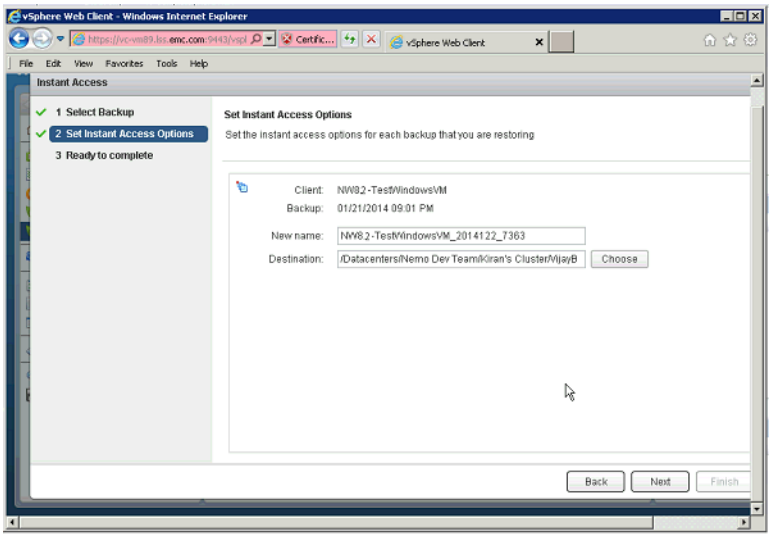
If your primary backup is located on a Data Domain system, clicking the Instant Access button, located on the Restore tab, allows you to perform a quick restore of these

backups, the same as you would perform a typical FULLVM restore. No further configuration is required to use this feature.

When you click Instant Access, the Instant Access wizard launches and displays the Select Backup page for selecting a backup to restore.

After selecting a backup to restore, click Next to display the Set Instant Access Options page, where you can specify a name and destination.

Figure 39 Set Instant Access Options in the Restore a backup wizard



When you click Finish, the Data Domain system gets added as a datastore to the ESX server, and the VM gets created within the datastore.

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.

Instant Access restore limitations

The following limitations apply to Instant Access restore operations:

- You cannot use the Instant Access button when you select more than one different Data Domain system backup for multiple VMs.
- Instant Access restore is restricted to one 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.

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 using this option, ensure 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 (Emergency Restore)

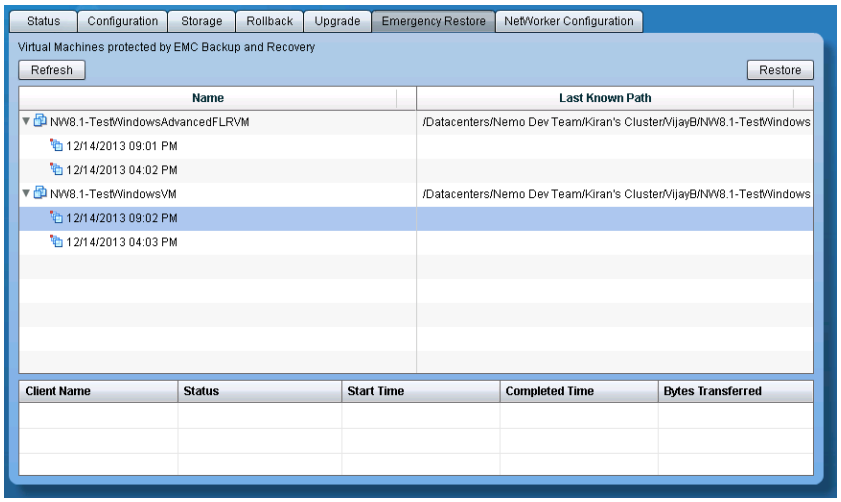
In NetWorker 8.2 and later releases, you can recover image-level backups directly to an ESX host without requiring a vCenter server by using the **Emergency Restore** tab in the **EMC Backup and Recovery Configure** window, as shown in the following figure. Direct to host recovery is available only for VMs that you back up to a VMware Backup appliance.

Before you begin

Before performing an emergency restore, ensure 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

Figure 40 Emergency Restore in the EMC Backup and Recovery Configure window



Procedure

1. Log in to the **vSphere Client** of the ESX host.
2. In the **vSphere Client**, right-click on the ESX host that the VMware Backup Appliance resides on:
   a. Select **Disconnect**.
   b. Click **Yes** when prompted to disassociate the ESX host from its vCenter.
3. Log in to the **EMC Backup and Recovery Configure** window at https://<IP_address_VMware_Backup_Appliance>:8543/ebr-configure/.
4. In the **EMC Backup and Recovery Configure** window, select the **Emergency Restore** tab

   The **Emergency Restore** dialog box lists VMs protected by the VMware Backup Appliance. Click **Refresh** to view the most recent available VM backups. Highlight a VM and click the down arrow to view the date and time of previous backups.
5. Select the VM that will serve as the restore point and click **Restore**.

   The **Host Credentials** dialog box displays.
6. In the **Host Credentials** dialog box, enter the valid ESX host credentials for the following fields:
   a. ESXi hostname or IP address – enter the host name or IP address of the ESXi hosting the VMware Backup Appliance
   b. Port – pre-populated with the default port, 443
   c. Username – enter the username for ESX host. The recommended host username is root. For any other host username, you must assign the **Create VM** privilege to the user account
   d. Password – enter the password for the ESX host.
7. Click **OK** to continue.

   The **Restore a Backup** dialog box displays.
8. Enter a new name in the **New Name** field. The name must be unique and can be up to 255 characters long.

Note

The following characters cannot be used in the name: ~ ! @ $ ^ % { } [ ] | , ` ; # \ / : * ? < > & . In addition, diacritical characters cannot be used (for example: â, é, ì, ü, and ñ).

9. Select a datastore as the destination target for the backup.

   CAUTION

   The datastore capacity size is listed. Make sure you select a datastore with enough disk space to accommodate the restore. Insufficient space causes the restore to fail.

10. Click **Restore**.
11. In the **vSphere Client**, right-click on the ESX host that the VMware Backup Appliance resides on:
    a. Select **Connect**.
    b. Click **Yes** when prompted to associate the ESX host back with its vCenter.
12. Verify that the restore was initiated successfully by checking the progress in the **Recent Tasks** window in the **vSphere Web Client**.

Note

The restored VM is listed at the vSphere host level in the inventory. Restoring to a more specific inventory path is not supported.

Emergency Restore limitations and unsupported features

The following limitations apply to emergency restore operations performed from the **EMC Backup and Recovery Configure** window.

- You cannot perform an emergency restore from a cloned backup; the backup you select for restore must be the primary backup.
- The vSphere host on which the emergency restore operation is being performed cannot be part of the vCenter inventory.
- Emergency restore allows you to restore only to the root of the host level in the inventory.
- Emergency restore requires that the DNS server used by EMC Backup and Recovery is available and can fully resolve the target vSphere host name.
- Emergency restore will restore the VM in Powered Off state. You must manually log in to the host and power on the restored VM.
- Emergency restore will restore the VM as a new VM. You must ensure that the name provided for the VM is not a duplicate of a VM that already exists.
- Emergency restore does not list MSapp clients.
- An internal proxy is automatically activated when an emergency restore operation is performed. If both the internal and external proxies are activated, you must disable the internal proxy in the **EMC Backup and Recovery Configure** window for the emergency restore to complete successfully.

File-level restore

Use the EMC Data Protection Restore Client interface to perform file-level restore (FLR). The following sections provide information about FLR:

- Restoring specific folders or files to the original VM on page 101
- Restoring specific folders or files from a different VM on page 103
- FLR limitations on page 103

Note

Before you start a file-level restore, review the limitations specified in the section FLR limitations on page 103 to ensure that you can perform FLR in your configuration.

Restoring specific folders or files to the original VM

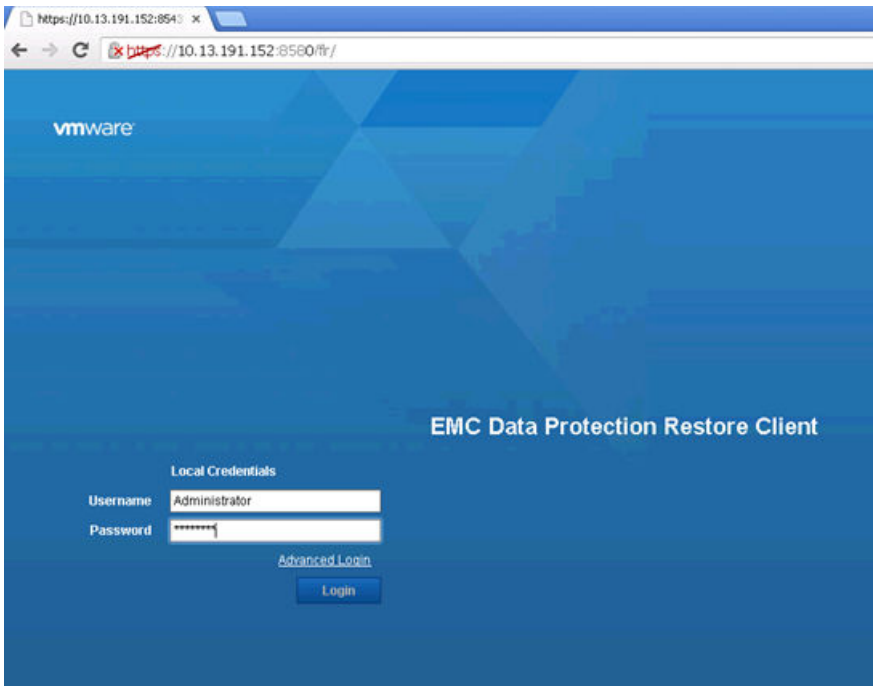
This topic describes what occurs when you restore specific folders and files to the original VM on Windows and Linux VMs.

Procedure

1. Open a browser and enter a URL that points to the VMware Backup appliance and indicates file-level restore, as in the following example:

```
http://VMware_Backup_appliance_host:8580/flr
```

Figure 41 EMC Data Protection Restore Client login page

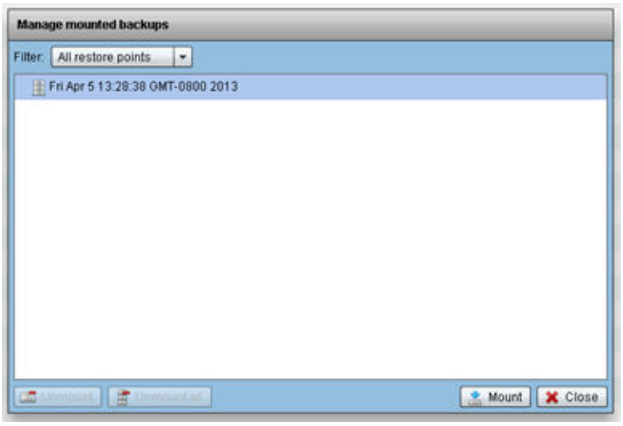


Note

The browser must point to a VMware Backup appliance from the VM that is being restored using FLR, and you must be part of the Administrators group to perform FLR restore.

2. When you log in, the **Manage Mounted Backups** dialog displays, as shown in the following figure. Click **Mount** to mount a restore point.

Figure 42 Manage Mounted Backups in EMC Data Protection Restore Client

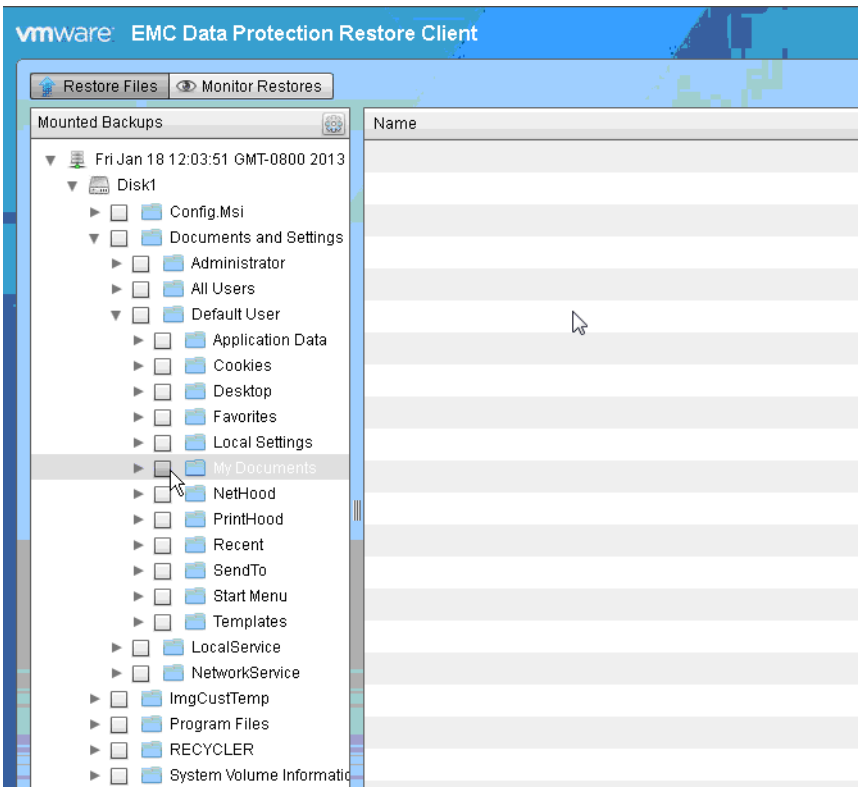


Note

When you click **Mount**, if a folder hierarchy does not appear, the file system in use on the VM may not be supported. The section FLR limitations on page 103 provides more information.

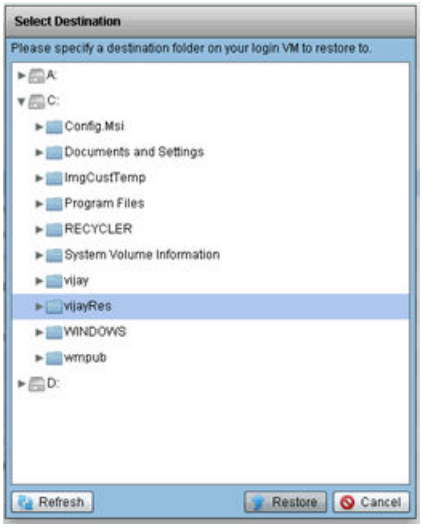
3. Browse the files and select files to recover, then click **Restore selected files**.

Figure 43 Browse and select files to recover



4. In the **Select Destination** window, select the folder to which you want to restore the VM, as shown in the following figure.

Figure 44 Select Destination window



5. Click **Restore** to start the recovery.

Restoring specific folders or files from a different VM

To restore specific folders or files from a different VM, use the Advanced login in the EMC Data Protection Restore Client login screen. The EMC Data Protection Restore Client help provides more information about the Advanced login.

Note

When using the Advanced login, ensure that you launch the EMC Data Protection Restore Client from a VM that has been backed up using the same VMware Backup appliance, and that the user you specify for the vCenter login has the necessary permissions to perform FLR restore. These permissions are typically the same as the user role specified in the section Creating a dedicated vCenter user account and EMC Backup and Recovery role on page 50.

FLR limitations

The following limitations apply to file-level restores:

- EMC Backup and Recovery does not support restoring specific folders or files to a different VM.
- You must install VMware Tools to use FLR. For best results, ensure that all VMs run the latest available version of VMware Tools. Older versions are known to cause failures when browsing during the file-level restore operation.
- All VMs must belong to the vCenter dedicated to EMC Backup and Recovery. Multiple vCenters are not supported.
- 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
  - XFS
- FLR of ext4 or GPT file systems is supported only with external proxies. To perform FLR of ext4 or GPT file systems, you must disable the internal proxies from the NSR VBA Server Properties window in NMC, as described in the section VMware Backup Appliance in NMC on page 69.
- FLR does not support 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

Monitoring VMware Backup Appliance activity

You can monitor VMware Backup Appliance activities from the EMC Backup and Recovery user interface in the **vSphere Web Client**, or from NMC.

Most VMware Backup Appliance tasks, events, and alarms are prefaced by "EBR:", for EMC Backup and Recovery. 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, running a VMware Backup Appliance scheduled backup job against a running VM creates the following task entries:

- 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 virtual center).
- Remove snapshot (virtual center 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 of the EMC Backup and Recovery user

interface in the **vSphere Web Client**, and enter `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 select Run integrity check.
EBR: [002] The VMware Backup appliance is nearly full.	The VMware Backup appliance is nearly out of space for additional backups. 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 time that backups are retained.
EBR: [003] The VMware Backup appliance is full.	The VMware Backup appliance has no more space for additional backups. The appliance will run in read-only (or restore-only) mode until additional space is made 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 time that backups are retained.
EBR: [004] The VMware Backup appliance datastore is approaching maximum capacity.	The datastore where the VMware Backup appliance provisioned its disks is approaching maximum capacity. When the maximum capacity of the datastore is reached, 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.	Start Core services using the EMC Backup and Recovery Configure window.

Table 20 EMC Backup and Recovery alarms (continued)

Alarm Name	Alarm Description
EBR: [006] Management services are not running.	Start Management services using the EMC Backup and Recovery Configure window.
EBR: [007] File system services are not running.	Start File system services using the EMC Backup and Recovery Configure window.
EBR: [008] File level restore services are not running.	Start File level restore services using the EMC Backup and Recovery Configure window.
EBR: [009] Maintenance services are not running.	Start Maintenance services using the EMC Backup and Recovery Configure window.
EBR: [010] Backup scheduler is not running.	Start Backup scheduler 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.

Selecting an event entry displays details of that event, which includes a link to Show related events.

Monitoring VMware Backup Appliance events from NMC

You can also monitor VMware Backup Appliance events, such as system errors, from the NMC Enterprise window.

Procedure

1. Log in to NMC.

   The **NMC Enterprise** window displays.

2. Right-click **Enterprise** from the left navigation tree and select **New** > **Host**.
3. Enter the VMware Backup Appliance hostname or IP and click **Next**.

   The **Select Host Type** dialog displays.

4. Select **Avamar** and click **Next**, and then click **Finish**.

Other options for monitoring sessions

In addition to using the EMC Backup and Recovery user interface in the vSphere Web Client to monitor recent tasks, you can use the following options to monitor sessions:

- In the **vSphere Client**, go to **Administration** and then select **Sessions**
- Open a web browser and enter https://<vcenter-IP>/mob/?moid=SessionManager
- Use proxycp by running `java -jar proxycp.jar --listvcsessions`
- Use the vSphere PowerCLI script.

Example 2 Using the vSphere PowerCLI script to monitor sessions

Figure 45 vSphere PowerCLI example output

```
Function Get-ViSession {
    <#          .SYNOPSIS            Lists vCenter Sessions.
        .DESCRIPTION            Lists all connected vCenter Sessions
        .EXAMPLE              PS C:\> Get-VISession
        .EXAMPLE              PS C:\> Get-VISession | Where { $_.IdleMinutes -gt 5 }     #>
    $SessionMgr = Get-View $DefaultViserver.ExtensionData.Client.ServiceContent.SessionManager
    $AllSessions = @()
    $SessionMgr.SessionList | Foreach {
        $Session = New-Object -TypeName PSObject -Property @{
            Key = $_.Key
        IPAddress = $_.IPAddress
        Agent = $_.userAgent
            LoginTime = ($_.LoginTime).ToLocalTime()
            LastActiveTime = ($_.LastActiveTime).ToLocalTime()
            }
            If ($_.Key -eq $SessionMgr.CurrentSession.Key) {
                $Session | Add-Member -MemberType NoteProperty -Name Status -Value "Current Session"
            } Else {
                $Session | Add-Member -MemberType NoteProperty -Name Status -Value "Idle"
            }
            $Session | Add-Member -MemberType NoteProperty -Name IdleMinutes -Value ([Math]::Round(((Get-Date) -
            ($_.LastActiveTime).ToLocalTime()).TotalMinutes))
    $AllSessions += $Session
    }
    $AllSessions
}
```

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 the appliance is powered off without 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 Power On to restart the appliance.

If the appliance does not shutdown properly, then rollback to the last validated checkpoint 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 be run 24x7 to support maintenance operations and to be available for restore operations. It should not be shutdown unless there is a specific reason for 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 108
- Save set lifecycle on page 108

Impact of selecting thin or thick provisioned disks

This section describes the advantages and disadvantages of selecting a thin or thick disk partitioning for the EMC Backup and Recovery datastore.

Thin provisioning uses virtualization technology to allow the appearance of more disk resources than what might be physically available. Use thin provisioning when an administrator actively monitors disk space and can allocate additional physical disk space as the thin disk grows. If you do not monitor and manage disk space and the EMC Backup and Recovery datastore is on a thin provisioned disk that cannot allocate space, the VMware Backup appliance fails. When this occurs, you can rollback to a validated checkpoint. Any backups and configuration changes that occurred after the checkpoint will be lost.

Thick provisioning allocates all of the required storage when the disk is created. The best practice for the EMC Backup and Recovery datastore is to create a thin provisioned disk when the EMC Backup and Recovery appliance is deployed (this allows for rapid deployment), and then convert the disk from thin provisioning to thick provisioning after deployment.

Note

See the VMware documentation for details on inflating thin provisioned disks to thick provisioned disks. This procedure requires that you shut down the VMware Backup appliance. This may take several hours to complete.

Save set lifecycle

The NetWorker server exclusively manages the lifecycle of save sets created by VMware Backup appliance nodes.

Deletion and expiration of save sets and metadata

The following sections describe deletion and expiration of save sets and metadata.

Expiring save sets from NetWorker

NetWorker manages the retention period for EMC Backup and Recovery appliance (VMware Backup appliance) backups. When a save set in the appliance expires in NetWorker, NetWorker deletes the corresponding backup from the appliance's storage.

Manual deletion of save sets from NetWorker

Delete EMC Backup and Recovery appliance backups from NetWorker by using the nsrmm command:

```
nsrmm -d -S ssid/cloneid
```

When you delete a backup from NetWorker, the corresponding backup will also be deleted 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 volume

You can delete a default VMware Backup appliance volume or user-defined Data Domain device volume that contains VMware Backup appliance backups after you unmount the devices. If the backups cannot be deleted from the VMware Backup appliance, then the volume deletion operation fails.

Volume relabeling

You can relabel a default VMware Backup appliance volume or 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 the backups cannot be deleted 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 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. For this reason, 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.

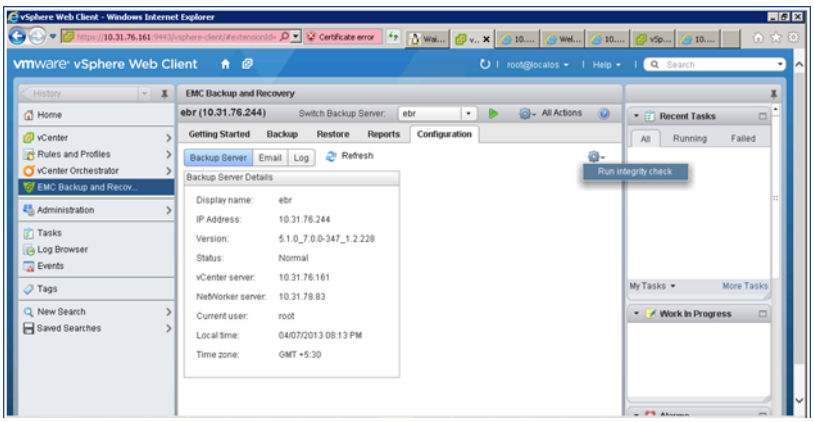
Creating a checkpoint using the EMC Backup and Recovery user interface

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 114 provides information on creating and validating checkpoints from the command line.

Procedure

1. Navigate to the **Configuration** tab.
2. Select the **Run integrity Check** option, as shown in the following figure.

Figure 46 Run Integrity Check button in EMC Backup and Recovery user interface



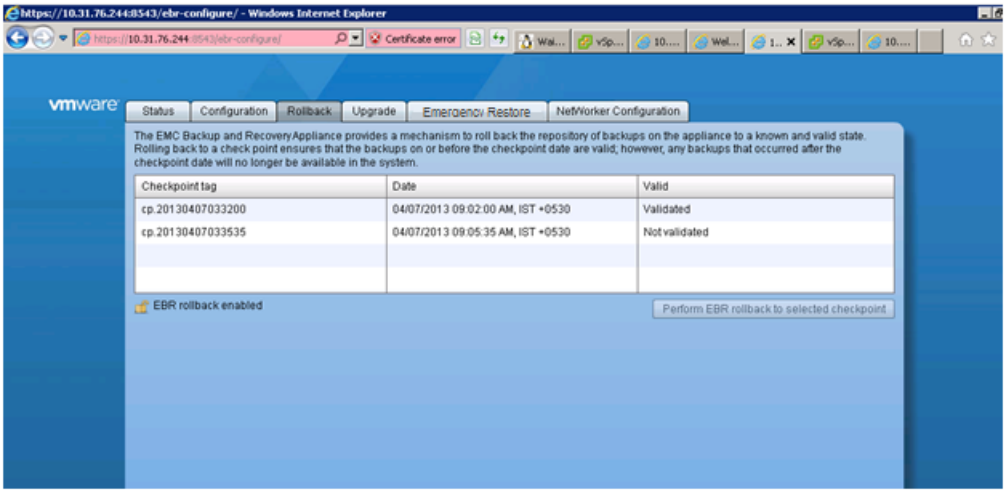
Rolling back to a checkpoint

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 and navigate to the **Rollback** tab.
2. Select **Unlock** to enable EMC Backup and Recovery rollback.
3. When prompted, specify the appliance password, then click **OK**.
4. Select a validated checkpoint, then click the **Perform EBR rollback to selected checkpoint** button.

Figure 47 Roll back in EMC Backup and Recovery Configure window



Note

NetWorker does not support disaster recovery from a checkpoint backup that was taken using an OVA earlier than the currently installed version. For example, if you upgrade to a NetWorker 8.2 server and OVA 1.1.09.147 from NetWorker 8.1 SP1 and OVA 1.0.1.9, you cannot perform a disaster recovery from a checkpoint backup created with OVA 1.0.1.9. Backup and restore operations will hang in "Waiting: Queued" state.

5. In the EBR Rollback window, click **OK**.

Protecting checkpoints for the VMware Backup appliance

In order to provide complete protection for the VMware Backup appliance, EMC recommends that you protect the checkpoints that you perform and store on the appliance.

You can accomplish this by adding VBA checkpoint discover and VBA checkpoint backup actions to a policy, as described in the section Setup and configure policies in NMC on page 71.

You should run backups once or twice daily, occurring a couple hours after the checkpoint gets created, to secure the checkpoint files to NetWorker media. Preparing the VMware Backup appliance for disaster recovery on page 114 provides a list of checkpoint locations.

Cross Sync

A Cross sync operation synchronizes the VMware Backup appliance and NetWorker databases for backups, triggered automatically upon VMware Backup appliance rollback. You can also perform 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.

Note

After running the scanner command to recover the media database, you must manually perform a cross sync in order to cross sync with the VMware Backup appliances and set primary clone IDs correctly.

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 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 cross sync on an entire database where the database is very large, it may take longer than normal to synchronize.

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."

Decommissioning the VMware Backup Appliance

NOTICE

Use caution when you completely remove references of a VMware Backup Appliance from the NetWorker Server as this erases all the backups, clones, and configuration information.

The decommissioning process deletes all backup metadata on the appliance node, if the operation is successful. If an error occurs, you will be provided with one of the following options:

- Abort the decommission.
- Continue without further contact with the VMware Backup Appliance, and decommission the appliance only from NetWorker.

If you confirm to continue decommission, this will:

- Remove all the save sets/clones from their respective volumes and the media database.
- Delete the NSR Client resource associated with the VMware Backup Appliance.
- Delete the NSR VMware Backup Appliance Server RAP resource.
- Remove the VMware Backup Appliance entry from all policies referencing it.

⚠ CAUTION

You should only decommission a VMware Backup Appliance node with EMC NetWorker Support's guidance. The knowledgebase article 204064, available at http://support.emc.com, provides more information.

Disaster Recovery to the same vCenter

NetWorker VMware Protection is robust in its ability to store and manage backups. In the event of a failure where you need to perform a disaster recovery to the same vCenter, as a first course of action rollback to a known validated checkpoint. To recover from a VMware Backup appliance failure, refer to the following disaster recovery guidelines.

Note

NetWorker VMware Protection does not support a disaster recovery of data backed up to Avamar storage when the internal AFTD metadata is lost.

Disaster Recovery Guidelines

Review these guidelines before performing a disaster recovery:

1. When setting save set browse and retention policies, ensure that the save sets in the media database are active and *not* expired and recycled.
2. Ensure that the checkpoint backup you plan to use was taken using the same version OVA as the currently installed version. NetWorker does not support disaster recovery from a checkpoint backup that was taken using a previously installed OVA. For example, if you upgrade to a NetWorker 8.2 server and OVA 1.1.09.147 from NetWorker 8.1 SP1 and OVA 1.0.1.9, you cannot perform a disaster recovery from a checkpoint backup created with OVA 1.0.1.9. Backup and restore operations will hang in "Waiting: Queued" state.
3. Before shutting down the VMware Backup appliance, verify that no backup or maintenance tasks are running. Depending on the backup method used and how long it takes, schedule your backup during a time where 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 schedule. This is an ideal time to shut down and backup the appliance.
4. In the vSphere Client, navigate to the appliance. Perform a Shut Down Guest OS on the VM. Do not use Power Off. A power off task is equivalent to pulling the plug on a physical server and may not result in a clean shut down process. Shutdown and Startup Procedures on page 107 provides more information.

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 or login to the EMC Backup and Recovery console, ensure that you login as admin instead of root. The section Log in to the EMC Backup and Recovery Console as admin instead of root on page 132 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. 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. Validate the checkpoint by running:

```
# 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. Add two actions for the VMware Protection Policy within NMC, in the following order:
   a. VMware checkpoint discover action.
   b. VMware checkpoint backup action.

   Note

   You can only perform a checkpoint backup to a Data Domain pool. The section Setup and configure policies in NMC on page 71 provides more information about configuring a policy with VMware Actions in NMC.

   Optionally, you can 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.

Note

Although the 0.5TB appliance contains 3 * 256 GB disks and the 4TB appliance contains 6 * 1TB disks, only one checkpoint save set gets created on NetWorker for all the disks. Ensure that you know which VMware Backup appliance (0.5 or 4TB) you deployed before performing disaster recovery. This information is not required when performing the checkpoint backup, but it will be required during re-deployment of the appliance as part of the disaster recovery.

To help identify the deployed appliance and verify the checkpoint backup, you can view log messages within NMC's daemon log file, and within the policy logs (located in /nsr/logs/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 55).

Procedure

1. Redeploy the VMware Backup appliance with the same network configuration, and use the **Override** button within the **EMC Backup and Recovery Configure** window.

Note

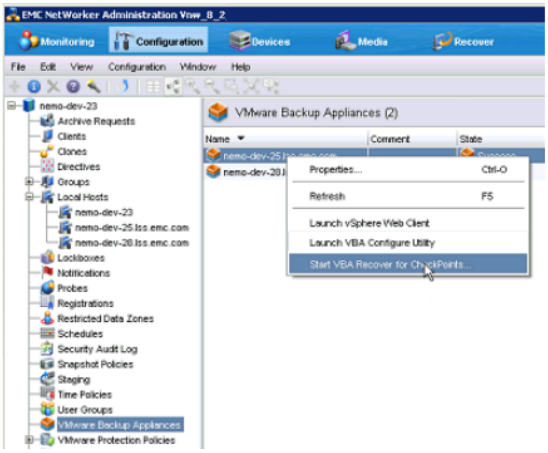
Ensure that the password for the system you plan to recover to matches the password for the system that the checkpoint was taken from.

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. Navigate to the **Configuration** tab in NMC and highlight VMware Backup Appliance in the lower left pane.
4. In the right pane, right-click the VMware Backup Appliance and select **Start VBA Recover for Checkpoints**, as shown in the following figure. A list of checkpoint backups display.

Figure 48 Start VBA Recover for Checkpoints in NMC



5. Select the checkpoint backup you want to rollback to, then click **OK**. After clicking OK, the following events occur:
   a. The status of the VMware Backup Appliance changes to **recover pending**, and the recovery takes 10-15 minutes to complete.
   b. Upon successful recovery, the status of the VMware Backup Appliance changes to **query pending**.
   c. 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.
```

Note

When you perform a disaster recovery after upgrading from a NetWorker 8.2 SP1 VMware Backup appliance to a NetWorker 8.2 SP2 version, you may be required to perform cross-sync manually. If cross-sync does not occur automatically, you can start the operation by running the command `nsrim -X -S -h` *VMware Backup appliance IP* on the NetWorker server. .

   d. The status of the VMware Backup Appliances changes to **Success**.
6. 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 section describes the steps required for a complete disaster recovery, where you need to restore both the connection to the VMware Backup appliance, and the device (Data Domain or tape device) that has completely failed:

- Prerequisites for performing a complete disaster recovery on page 117
- Performing a complete disaster recovery on page 117

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 114.
- Clone the backups to a secondary Data Domain and/or tape device.

Performing a complete disaster recovery

Perform the following steps if a complete disaster recovery of the VMware Backup appliance is required:

Procedure

1. Redeploy the VMware Backup appliance with the same network configuration, and use the **Override** button within the **EMC Backup and Recovery Configure** window.

   Note

   Ensure that the password for the system you plan to recover to matches the password for the system that the checkpoint was taken from.

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. Navigate to the **Configuration** tab in NMC and highlight VMware Backup Appliance in the lower left pane.
4. In the right pane, right-click the VMware Backup Appliance and select **Start VBA Recover for Checkpoints**, as shown in Figure 48 on page 116. A list of checkpoint backups display.
5. Select the checkpoint backup you want to rollback to, then click **OK**.
6. 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

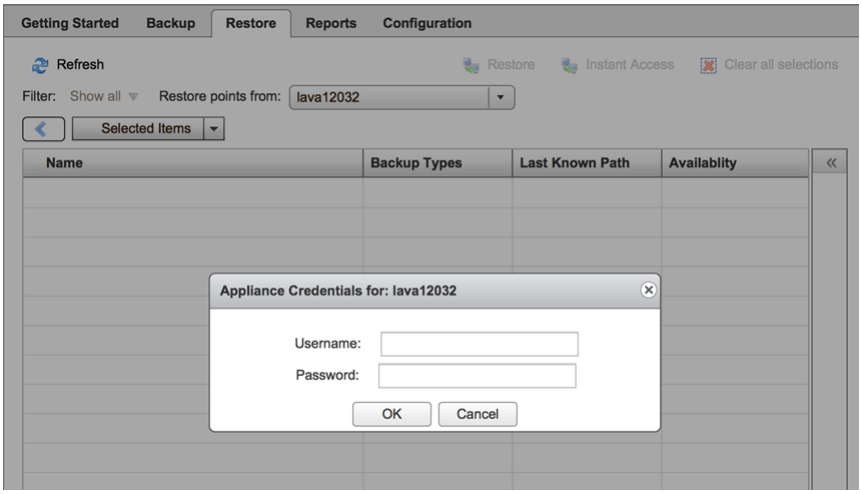
Starting in NetWorker 8.2 SP1, when you clone a VM or VMDK backup to a secondary site with its own vCenter and VMware Backup appliance, and the secondary site shares the same NetWorker server as the primary site, you can recover data from the secondary site. This procedure is particularly useful to recover 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.

To select this option:

1. Navigate to the **Restore** tab of the EMC Backup and Recovery user interface in the vSphere Web Client.
2. From the **Restore points from** field, select the VMware Backup appliance that contains the required backup(s). The Appliance Credentials dialog displays.
3. Provide the credentials for the VMware Backup appliance, and then click **OK**.

Figure 49 Recovery from a secondary site in the EMC Backup and Recovery user interface



4. Browse restores from the VMware Backup appliance and select the VMs/VMDKs you want to restore to the new location, as specified in the section Performing a FULLVM restore. Restore to the original location, Instant Access Restore and restore from GSAN will be disabled.

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 vCenters and number of proxies, and whether you perform a large number of concurrent VM backups. The following table provides these scalability factors.

Table 21 Scalability Factors

Component	Recommended count	Notes
VMs per VMware Backup appliance (internal storage)	Up to 48 VMs	
VMs per VMware Backup appliance (Data Domain backup, no external proxy)	800-1000 VMs	Given an average size of 20-30 GB per VM, the 0.5 TB OVA can accommodate a

Table 21 Scalability Factors (continued)

Component	Recommended count	Notes
		maximum of 800-1000 VMs when backing up to a Data Domain device. One VMware Backup appliance can run 8 sessions in parallel. Considering the VM size and data change rate, a VMware Backup appliance can complete a backup of 800-1000 VMs 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 VMs in approximately 8 hours.
VMware Backup appliance per vCenter	3 or lower	Better performance is observed with a single vCenter processing 48 concurrent sessions, so when performing backups from multiple VMware Backup appliances, EMC recommends staggering the backup to reduce the load on vCenter.
Proxies per vCenter	5	Each VMware Backup appliance has 8 internal proxies, and the external proxy adds 8 more concurrent sessions. Therefore, use 1 VMware Backup appliance and 5 external proxies. **Note** EMC recommends disabling the internal proxy for the VMware Backup Appliance if backing up more than 100 VMs.
VMs per policy	200 or lower	A single policy can scale up to 200 VMs. If more than 48 VMs per policy, the remaining VMs will be queued during backup.
VMs per restore	16	More than 16 VMs may result in NBD based restore due to VMware API limitations.

Table 21 Scalability Factors (continued)

Component	Recommended count	Notes
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 VMs in parallel. If you want to run up to 48 VM backups in parallel, then add up to 5 external proxies. Each external proxy can backup up to 8 VMs.

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 disabling the internal proxy on the VMware Backup Appliance. The values calculated in the table above reflect 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 machine backups per vCenter.

Table 23 Concurrency/parallelism recommendations (continued)

Component	Concurrency count	Notes
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 8.2 SP1 with OVA 1.1.1.50.
- 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 holding the virtual disk(s) being backed up. In environments using 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 VMs being backed up are using VM hardware version 7 at a minimum.

  For sites that contain a large number of VMs 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:

  - Set up Management network redundancy
  - Set up backup network to ESXi for NBD

- Go to http://www.vmware.com/files/pdf/techpaper/vmw-vsphere-high-availability.pdf to learn how to set up storage heartbeats.

- 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 performing 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 NMC, as outlined in the section Setup and configure policies in NMC.
- When planning for backups, ensure that NetWorker VMware Protection supports the disk types. 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
- Enabling Change Block Tracking (CBT) allows you to 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 VM has changed more than 25% since the last backup, a level full backup is performed. In order to support Changed Block Tracking (CBT):
  - Ensure that all VMs run VMware hardware version 7 or higher.
  - If you add a disk or dynamically expand a disk on a VM, you must take a new full backup for CBT to function.

  For Incremental backups with CBT, remove any existing snapshots of a VM before adding to the VMware Backup Appliance.
- When backing up thin-provisioned VMs or disks for VMs on NFS datastores, note that thin provisioning is not preserved during recovery for NFS datastores. The VMware knowledgebase article 1035096 at http://kb.vmware.com/kb/1035096 provides more information.
- Install VMware Tools on each VM that you want to back up 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. VMware Tools is also required for some features used in File Level Restore.
- For VDDK backups, install the latest VDDK kit:
  - HF222276 for the NetWorker 8.1 VMware Backup Appliance
  - HF222268 for the NetWorker 8.1 SP1 and later VMware Backup Appliance
  - HF207384 for the NetWorker 8.2 and later VMware Backup Appliance
- 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. The knowledgebase

article at http://kb.vmware.com/kb/1025360 provides instructions to remove conflicting plugins.

- EMC recommends setting 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 VM 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.
- VMs with extremely high IO may face hangs during consolidation due to the ESXi forced operation called synchronous consolidate. Plan your backups of such VMs according to the amount of workload on the VM.
- When working with the vCenter database either directly or by using scripts, do not change the name attribute for the vmfolder object. The knowledgebase article at https://support.emc.com/kb/190755 provides more information.
- Setting up multiple devices locally on the NetWorker server can lead to resource contention. Large VMware environments are observed to have more stability when most backup devices are set up on a remote storage node.
  When you mount a backup or clone pool volumes on a remote storage node, then modify the properties for the VMware Backup Appliance to add these storage node names under the Globals (2 of 2) tab of the NetWorker Client Properties window in NMC.
- Resource contention can occur at various points during the backup cycle. Running larger savegroups and policies often cause issues due to contention of resources that impact all running operations. Adjust your resources and times for other larger savegroups/policies to avoid overlaps, thereby avoiding resource contention.
  For example, if you set up a policy where every day at 10pm two policies called 'Bronze1' and 'Bronze2' with 400 clients each start writing to a pool named 'Bronze' which is configured for just one device on NetWorker, 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

Actions cannot be added to workflows that have the same name in different policies

For traditional workflows, VMware allows the same workflow name to be used in different policies. However, if you add such a workflow to a policy, you will not be able to 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 a recovery is immediately required in the environment, temporarily shut down all of the external proxies while starting the restore for the VM. This will ensure that the recovery gets assigned to the VMware Backup Appliance internal proxy. Knowledgebase 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*. Knowledgebase 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 browse disks for FLR by using the EMC Data Protection Restore Client, 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.

Knowledgebase 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.

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 appears indicating "Unable to find this EBR in the vCenter inventory."

Backups to VMware Backup appliance and Data Domain system not supported
You can only backup to the VMware Backup appliance internal storage or a Data Domain system.

Cloning between Data Domain system and VMware Backup Appliance internal storage not supported
You cannot clone backups from a Data Domain system to VMware Backup appliance internal storage, nor can you clone backups from VMware Backup appliance internal storage to any other devices, including Data Domain systems. However, backups to a Data Domain system can be cloned to any device that NetWorker supports for cloning.

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 VM 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 VM.

NMC's VMware View map view does not display when configuration for VMs within the vCenter is incomplete
When using NMC's VMware View, the map view does not appear when the configuration for one or more VMs in the vCenter is incomplete. To avoid this issue, remove incomplete VM configurations from vCenter.

I/O contention when all VMs on a single data store
I/O contention may occur during snapshot creation and backup read operations when all VMs reside on a single data store.

No automatic migration tool to move from previous solution to NetWorker VMware Protection
An automatic migration tool to move from the previous VM 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

Each Data Domain system has a soft limit to the maximum number of connections and data streams that can be sustained simultaneously while maintaining performance. Different models of Data Domain systems have different stream counts as described at the following link:

https://support.emc.com/kb/180681

Each client VM backup creates two streams to Data Domain:

- One stream from the NetWorker server (or storage node) to Data Domain
- One stream from the VMware Backup Appliance node (or external proxy) to Data Domain

When planning the number of backup sessions, consider the following:

- To obtain the number of sessions, multiply the total number of VMware Backup Appliance sessions (all VMware Backup Appliances + all external proxies) by 8, and then multiply that total by 2.

  Note

  This does not include VMware Backup Appliance nodes with the internal proxy disabled

- You may need to make adjustments depending on whether you configured any other types of backups simultaneously to this Data Domain system.
- Note the maximum number of streams allowed by your particular Data Domain model/configuration. If the combination of the VMware Backup Appliance and other sessions exceeds the maximum streams allowed, then performance degradation or backup and cloning failures may occur. In such cases, you may benefit from staggering backups.

Additionally, note the following requirements:

- All Data Domain systems must use DDOS version 5.4 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 per Data Domain system pool when used in any Action

Monitoring Stream Counts (Advanced)

You can monitor changes to the stream by using an SSH connection to the Data Domain system.

1. Launch PuTTY and connect to Data Domain over SSH as sysadmin.
2. Run the `system show performance` command, as shown in the following example.

Example 3 Stream counts output

When you run the following command, the output displays stream counts over a period of 5 minutes, with a maximum of 15 streams.

```
system show performance custom-view throughput,streams duration
5 min interval 1 min
```

Figure 50 Monitoring stream counts output

```
-------------------------------------------------------------------------------
Time Stamp     |Throughput                                          |Streams
               |read     write    repl network    repl pre-comp     |
  Date    Time |                      in/out          in/out        | rd/ wr/ r+/ w+
MM/DD/YY HH:MM| MB/s     MB/s         MB/s            MB/s         |       #
-------- ----- ------- ------- -------------- -------------- ---------------
02/15/15 19:26     0.0     0.0        0.0/  0.0      0.0/  0.0   0/  0/  0/  0
02/15/15 19:27     0.0     0.0        0.0/  0.0      0.0/  0.0   4/  0/  0/  0
02/15/15 19:28     0.0     0.0        0.0/  0.0      0.0/  0.0   9/  0/  0/  0
02/15/15 19:29     0.0    11.0        0.0/  0.0      0.0/  0.0  15/  2/  0/  0
02/15/15 19:30     0.0    61.4        0.0/  0.0      0.0/  0.0  15/  0/  0/  0
```

Example 4 Exceeding max sessions

In this example, you notice a performance issue during backups to a Data Domain 670 system, which you set up with one VMware Backup Appliance node (with internal proxy disabled) and 12 external proxies. Additionally, you will run Exchange and UNIX backups for a total of 150 clients each day, with a maximum parallelism of 40.

Considerations:

- Maximum number of VMware Backup Appliance sessions ((node=0 + external proxy=12) * 8) *2 = 192
- Are any other types of backups configured? Yes. The max parallelism is set to 40
- Max number of streams allowed by this Data Domain model (mixed Total) = 140

Now, since the totals from the first two bullets (192+40=232) exceed 'Max stream allowed' (140), you should stagger the backups to run a lower session count. Some suggestions to achieve this include:

- Set up group start times to simultaneously work only through 6 clusters (VMware Backup Appliance external proxies (6 * 8 * 2)) = 96 streams.
- Reduce the parallelism for other backups to lower than 25.

The combined parallel stream count (VMware Backup Appliance + others) should now be lower than 140 at all times.

Example 4 Exceeding max sessions (continued)

If the number of clients required for backup continues to grow, you may want to set up a Data Domain system that allows for a higher stream count, such as a DD 7200, for these operations.

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
```

NetWorker configuration

- Ensure that NetWorker services are up before you configure the EMC Backup and Recovery appliance
- Leave “Source Storage Node” empty when you configure the “VM Backup” action
- Ensure that the relevant devices are mounted
- Wait until you successfully configure a policy before you run the policy.

VMware Backup appliance installation

If you have problems with the VMware Backup appliance installation:

- Confirm that all of the software meets the minimum software requirements (see System requirements on page 27).
- Confirm that the hardware meets the minimum hardware requirements (see System requirements on page 27).
- Confirm that DNS is properly configured for the VMware Backup appliance (see Pre-installation requirements on page 31).

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 backup scheduler are running. Note that maintenance services will start between 24 to 48 hours after booting up. You can also start maintenance services manually if desired.
- Do not add more than 500 VMs to a VMware Backup appliance to avoid slower recovery times
- Ensure that the VMware Backup appliance still has space left for backups
- VMware snapshot for backup is not supported for independent disks

Peer information issues

Peer information issues can occur for the VMware Backup Appliance and its external proxies when you redeploy an appliance or upgrade the proxy appliance.

To identify and correct peer information issues, perform the following.

Procedure

1. Render the logs:

   ```
   nsr_render_log /nsr/logs/daemon.raw | grep peer
   ```

2. If you notice errors, check the host names involved and remove peer information for the problem hosts.
3. Log in to the problem host and check the hostname. Ensure that the NetWorker nsrladb shows the correct host names on both affected machines.

You discover the following error message on your NetWorker server nwserver1:

```
nwserver1.example.com nsrexecd GSS critical An authentication
request from nwproxy1.example.com was denied. The 'NSR peer
information' provided did not match the one stored by
nwserver1.example.com. To accept this request, delete the 'NSR peer
information' resource with the following attributes from
nwserver1.example.com's NSRLA database: name: nwproxy1.example.com;
NW instance ID: e3d0db59-00000004-
abab1f2b-5498736c-00010000-00000000; peer hostname:
nwproxy1.example.com
```

To fix, you run the following commands on nwserver1:

```
nsradmin -p nsrexec
nsradmin> d type: nsr peer information; name: nwproxy1.example.com
Delete? Yes
nsradmin> quit
```

Then, you log in to nwproxy1 and check to ensure the host name is valid.

Connectivity between the VMware Backup Appliance and the ESXi/vCenter

Use the following procedure to validate basic connectivity between the VMware Backup Appliance (or external proxy) and ESXi hosts/vCenter.

1. Connect to the VMware Backup Appliance or external proxy using PuTTY.

   Note

   For NetWorker 8.2 or later VMware Backup Appliances, login as admin.

2. Run the following command to test connectivity to a particular host(port): `curl` *hostname-or-IP*`:port`

Example 5 Example command

Example 5 Example command (continued)

```
curl esxi.my.local:902
220 VMware Authentication Daemon Version 1.10: SSL Required,
ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS
supported
```

If you receive a response such as "curl: (7) couldn't connect to host", this may indicate that there is a host-based connectivity issue or network firewall software blocking connectivity.

Connectivity between the VMware Backup Appliance and the NetWorker server

Use the following test to validate connectivity between the VMware Backup Appliance node (or external proxy) and the NetWorker server.

Before you begin

Before running the test, log in to NMC and create a client for the external proxy.

Procedure

1. Connect to the VMware Backup Appliance or external proxy using PuTTY.

   For NetWorker 8.2 or later VMware Backup Appliances, login as admin.

2. Run the following command.

   ```
   save -J <storage-node> -s <nw-server> -b <pool> /etc/hosts
   ```

   ```
   save -J nw-sn1.my.local -s nw82sp1.my.local -b boostPool /etc/
   hosts
   libDDBoost version: major: 3, minor: 0, patch: 1,
   engineering: 1, build: 459919
   86704:save: Successfully established DDCL session for save-
   set ID '3974440777' (ebr82sp1.my.local:/etc/hosts).
   /etc/hosts
   /etc/
   /
   save: /etc/hosts  8 KB 00:00:03      3 files
   94694:save: The backup of save set '/etc/hosts' succeeded.
   ```

   If the output shows the backup was successful, you can skip the remaining steps.

3. If the backup fails, check the /etc/hosts file for the following entry:

   ```
   127.0.0.1  localhost.localdomain localhost
   ::1        localhost.localdomain localhost
   ```

   If not present, add these entries to the hosts file. If you see these entries, skip to the next step.

   Note

   If logged in as admin, switch to root by using the su - command.

4. Check for any peer information issues on the VMware Backup Appliance or external proxy host and the NetWorker server and clear up these issues.
5. Run a debug backup to check for other issues such as DNS errors:

   ```
   save -D2 -J <storage-node> -s <nw-server> -b <pool> /etc/hosts
   ```

6. Ensure that the *Network Portgroup* for the VM (VMware Backup Appliance or external proxy) is set on the correct port group.

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** inactivity timeout to allow for longer wait times, for example 7 to 8 minutes, using the following procedure.

1. Run the following command to verify the version.

   ```
   /usr/local/avamarclient/bin/avnwcomm --version
   ```

   This setting applies only to the following NetWorker and OVA versions for the VMware Backup appliance node or external proxy.

   Table 24 OVA versions by NetWorker release

NetWorker version	OVA version	Command output	Notes
8.1 SP1	1.0.1.9	7.0.161-7	Patch only
8.1 SP2	1.0.2.16	7.0.162-11	Patch only
8.2	1.1.0.149	7.0.160-13	Patch only
8.2 SP1	1.1.1.50	7.0.161-6	Built-in
8.2 SP2	1.1.2.8	7.1.62-4	Built-in

   Note

   You can obtain the patch for avnwcomm from https://support.emc.com/kb/195372.

2. Create a file on the VMware Backup appliance node and external proxy called **avnwcomm.cmd** under `/usr/local/avamarclient/var/` for NetWorker 8.2.x, or `/usr/local/avamarclient/var-proxy-?` for NetWorker 8.1.x.

3. Edit **avnwcomm.cmd** to add the following:

```
--nw_init_timeout=420
```

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.

After you ssh to the Console as admin, you can then switch to the root user, as shown in the following example:

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

If you connect to the EMC Backup and Recovery Console via the vSphere Client, you can log in as the root user.

Note

The password for the admin user is the same as the password that was specified in the EMC Backup and Recovery Configure window during the initial installation of the VMware Backup appliance.

Note

Modifying the ssh configuration file in /etc/ssh so that a user can ssh into the appliance directly as root is not recommended as it may result in future upgrade failures.

Unable to add VM to a policy in NMC's VMware View when you register multiple VMware Backup Appliance's with a combination of IP and FQDN

When you register multiple VMware Backup Appliances to the NetWorker server and vCenter, use only the IP or only the FQDN but do not use a combination.

When you use a mix of IP and FQDN, for example, Appliance 1 is registered using NetWorker server FQDN and vCenter IP, but Appliance 2 is registered using NetWorker server FQDN and vCenter FQDN, issues may occur when adding a VM to a policy, such as the option to add a VM to a policy not appearing in NMC's VMware View.

When you register the VMware Backup Appliance with the NetWorker server and vCenter using the EMC Backup and Recovery Configuration utility, EMC recommends that you always specify FQDN.

Launch of EMC Backup and Recovery Configure window fails when using Chrome or Firefox web browsers

242550

Google Chrome and Mozilla Firefox web browsers may fail to open the **EMC Backup and Recovery Configure** window.

Workaround

If the **EMC Backup and Recovery Configure** window does not open with Chrome or Firefox, use the following workaround procedure:

1. As the root user on UNIX, or Administrator on Windows, edit the `/usr/local/avamar-tomcat/conf/server.xml` file with the following modifications to the ciphers:
   Before:

   ```
   <Connector SSLEnabled="true" Server="Avamar"
   ciphers="TLS_DHE_RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_1
   28_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_128_CBC_SHA
   ,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_C
   BC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_E
   DE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_KRB5_WITH_R
   C4_128_SHA,TLS_KRB5_WITH_RC4_128_MD5,TLS_KRB5_WITH_3DES_EDE_
   CBC_SHA,TLS_KRB5_WITH_3DES_EDE_CBC_MD5"
   clientAuth="false" maxKeepAliveRequests="1" maxThreads="150"
   port="8543" maxHttpHeaderSize="32768"
   protocol="org.apache.coyote.http11.Http11NioProtocol"
   scheme="https" secure="true"
   sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2,SSLv2Hello"
   sslProtocol="TLS"/>
   ```

   After:

   ```
   <Connector SSLEnabled="true" Server="Avamar"
   ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA
   _WITH_AES_128_CBC_SHA,
   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES
   _256_CBC_SHA,TLS_ECDHE_RSA_WITH_RC4_128_SHA,
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
   ,TLS_RSA_WITH_AES_256_CBC_SHA256,
   TLS_RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA"
   clientAuth="false" maxKeepAliveRequests="1" maxThreads="150"
   port="8543" maxHttpHeaderSize="32768"
   protocol="org.apache.coyote.http11.Http11NioProtocol"
   scheme="https" secure="true"
   sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2,SSLv2Hello"
   sslProtocol="TLS"/>
   ```

2. Restart the browser. You should now be able to open the **EMC Backup and Recovery Configure** window.

Removing VMware Protection Policy when VMware Backup Appliance is offline

If you attempt to delete a VMware Protection Policy from NMC's **Administration** window for a VMware Backup Appliance that is offline, the following error appears:

```
Delete operation failed for the following VBA's Detailed logs:couldnt
not delete backup job on VBA <VBA_Name>,error: VBA returned status of
failure:details "NW_7007:Unable to locate backup job to delete <VBA
policy>
```

To remove the VMware Protection Policy:

1. Open the *<networker install directory>*/res directory and copy nsrdb to a safe location.
2. Stop the nsrd service.
3. Connect to nsrdb by using nsradmin:

   ```
   nsradmin -d <path to nsrdb>
   . type: NSR data protection policy
   Print
   ```

   The command returns multiple policies.
4. Select the policy you want to delete by specifying the name of the policy in the following syntax:

   ```
   . type: nsr data protection policy ; name: BadPolicy
   ```
5. Delete the policy. When prompted to confirm deletion, type **Yes**.
6. Restart the nsrd service.

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 Figure 14 on page 64.
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.

Inactivity timeout in NMC for VMware Protection Policies

Wait times for a backup session may vary and can increase for environments with a large amount of backups running and in queue.

Even though EMC recommends staggering backups to avoid long queues, setting the *Inactivity Timeout* variable in NMC's **Edit VMware Action** window to a lower value can cause queued policies to fail. However, setting this variable is very useful to avoid backups stalling for long durations. Before setting the *Inactivity Timeout*, confirm that the NetWorker server configuration is stable and does not show backups in queue for long durations.

VMware Protection Policy fails for manually created client resource with DataDomain backup attribute enabled

When you manually create a client resource and enable the DataDomain backup attribute (using nsradmin or the NMC Client Properties window), the default VMware Protection Policy fails with the following error:

```
NWP_LOG_OUTPUT: NW Client Plugin: ABORT session operation
successful. Reason for abort: nwp_start_backup_session_helper: no
matching IP interface data domain devices for save of client
clientname; check storage nodes, devices or pools
```

If this occurs, unselect/disable the DataDomain backup attribute on the manually created client resource.

“No proxies running on VBA {appliance name} for backing up VM {VM name}”

When the avagent is not running, or no proxies are running, this error appears in the VMware Protection Policy details window in NMC.

If you see this error, log in as root from the EMC Backup and Recovery Console in the vSphere Client and invoke service avagent restart:

```
/etc/init.d/avagent restart
```

System proxy configuration handling on SuSE

For NetWorker servers on the SuSE Linux platform where system proxy is enabled, you must remove or change the system proxy configuration to allow for connectivity to the VMware Backup Appliance.

Perform one of the following options.

- To disable the system proxy, open the /etc/sysconfig/proxy file in a text editor and set PROXY_ENABLED="no"
- To add an exception, modify the NO_PROXY line in the /etc/sysconfig/proxy file to include the IP address of each VMware Backup Appliance instance, for example:
  NO_PROXY="localhost, 127.0.0.1, <VMA IP1>[,<VBA IP2>[,…]]"

The knowledgebase article at http://www.novell.com/support/kb/doc.php?id=7006845 provides more information.

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. Login into 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.

After ESX upgrade to 6.0, EMC Backup and Recovery plug-in missing from vSphere Web Client

242527
After you upgrade ESX to vCenter 6.0 on NetWorker 8.2.x, the EMC Backup and Recovery plug-in disappears from the vSphere Web Client and the following error displays upon opening the vSphere Web Client:

```
ERROR "An internal error has occurred-Unable to load resource module from /EBR2/locales/EBR-en_US.swf"
```

Workaround

To avoid this issue, add port 9443 into the vSphere Web Client browse request, and then open the vCenter. Type the following address:

```
https://<vCenter_IP>:9443
```

where:

vsCenter_IP is the IP address of the vSphere Web Client.

Restart the Enterprise Manager Web Application (emwebapp)

Use the following steps to restart emwebapp.

Note

When you use ssh to connect or login to the EMC Backup and Recovery Console in the vSphere Client, ensure that you login as admin instead of root. The section Log in to the EMC Backup and Recovery Console as admin instead of root on page 132 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*
   ```

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 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 108.

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 38 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.

Network protection software exclusions

Some network protection software, such as Kaspersky Internet security, may block incoming connections on the NetWorker server, which can cause monitoring failures.

EMC recommends adding exclusions to the monitoring software to allow for communication with the VMware Backup Appliance and its external proxy hosts.

Ensure backup pool volumes mounted at all times

The DD Boost volumes on the NetWorker server may be impacted by network issues or resource contention, causing the volumes to unmount and triggering alerts "Waiting for # writable volume."

To fix this issue, EMC recommends mounting the volumes immediately.

Missing permissions for sites with LDAP configured

For sites with LDAP configured for NMC, missing permissions can cause backups for a VMware Backup Appliance or external proxy to fail with messages similar to the following in the avnwcomm (activity) log on the proxy:

```
avnwcomm Error <0000>: Received error from NetWorker connection
attempt:
Error Code 21: cannot get policy details, could not get Action for
Policy = test2. Hence, could not determine pool, browse,
retention.
```

To fix this issue, add the following user to the server administrators:

root@vba-name

root@proxy-name

Where *VBA-name* is the FQDN of the VMware Backup Appliance node, and *proxy-name* is the FQDN of the external proxy.

Alternatively, you can open access to all hosts/users by adding *@*. The knowledgebase article 174188, available at https://support.emc.com/kb/174188, provides more information.

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**.

Checkpoint discover timeout

When performing checkpoint discover actions in environments with a large datastore or more than 5 external proxies deployed, the VMware Backup Appliance may remain in "Query Pending" state for a period of time that exceeds the default timeout value before the status changes to "Success."

In the base NetWorker 8.1.x and 8.2.x releases, the default wait time is 2 minutes. In the latest cumulative releases for NetWorker 8.1 and 8.2, the default value is 5 minutes. When the timeout is reached, messages similar to the following appear in the NetWorker policy logs:

```
nsrdiscover: Configuration for VBA is in pending state. Retrying...
nsrdiscover: Cannot retrieve checkpoint tag. Timed out retrying.
```

To increase the timeout value for checkpoint discovery to 5 minutes, upgrade to the latest NetWorker cumulative release. If you require a timeout value greater than 5 minutes, you can then modify the timeout by setting the environment variable *NSR_VBA_CPTAG_REQUEST_TIMEOUT=<value>*, where value is in seconds. The maximum value permitted is 3600 seconds (one hour).

Note

EMC recommends that you only register required proxies. The section "Proxy Registrations" provides more information.

Regenerate SSL certificates on the VMware Backup Appliance

Use the following procedure to regenerate the SSL certificate on the VMware Backup Appliance.

Procedure

1. Run `emwebapp.sh --stop` to stop emwebapp.
2. Back up the existing keystore:

   ```
   cp /root/.keystore /root/.keystore.sav
   ```

3. Delete the tomcat certificate from the keystore:

   ```
   /usr/java/latest/bin/keytool -delete -alias tomcat -
   storepass changeit
   ```

4. Regenerate the SSL certificate using SHA256:

   ```
   /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"
```

5. Run `emwebapp.sh --start` to start emwebapp.
6. On the Networker server, stop the `nsrvmwsd` task/service.

   Allow 10-20 minutes for the changes to take effect. If you still experience issues after this time, re-register the VMware Backup Appliance to the vCenter server and Networker server and reboot the VBA when completed.

Note

At any time during this procedure, you can look up the SSL key by running the following command: `/usr/java/latest/bin/keytool -list -keystore /root/.keystore -storepass changeit -alias tomcat`

CHAPTER 3

VADP Backup and Recovery (legacy)

This chapter contains the following topics:

- Software and hardware requirements 148
- Limitations and unsupported features 149
- Transport modes 151
- Changed Block Tracking (CBT) 152
- Configuration options 152
- Configuring the VADP proxy host and Hypervisor resource 152
- Configuring a virtual client for backup 160
- Creating a VADP User role in vCenter 165
- Configuring Changed Block Tracking (CBT) 168
- Monitor VMs 170
- Launching the vSphere Web Client from the NetWorker Console (Windows only) 170
- Recovering VADP Backups 170
- VADP Planning and Best Practices 180
- Upgrading from VCB to VADP (pre-NetWorker 8.1) 196

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 6.0 and vCenter 6.0
  - vSphere 5.1 with ESX 5.1 and vCenter 5.1 U3
  - vSphere 5.5 with ESX 5.5 and vCenter 5.5
  - vSphere 5.0 with ESX 5.0 and vCenter 5.0

  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 195 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 149 and Limitation for VADP proxy host on non-English versions of Windows on page 150.
- 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 FibreChannel 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 179.

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 inConfiguring the VADP proxy host and Hypervisor resource on page 152. The transport modes are outlined in the table Table 25 on page 156.

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 168.

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.

Configuration options

There are two options for configuring NetWorker clients for VADP backup. The configuration can be performed automatically by using the Client Backup Configuration wizard, or manually by using the Client Properties window:

- If using the Client Backup Configuration wizard, refer to Configuring a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard on page 153.
- If using the Client Properties window, refer to Configuring a VADP proxy host and Hypervisor resource manually by using nsradmin on page 155.

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 by using one of the following methods:

- Configuring a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard on page 153
- Configuring a VADP proxy host and Hypervisor resource manually by using nsradmin on page 155

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.

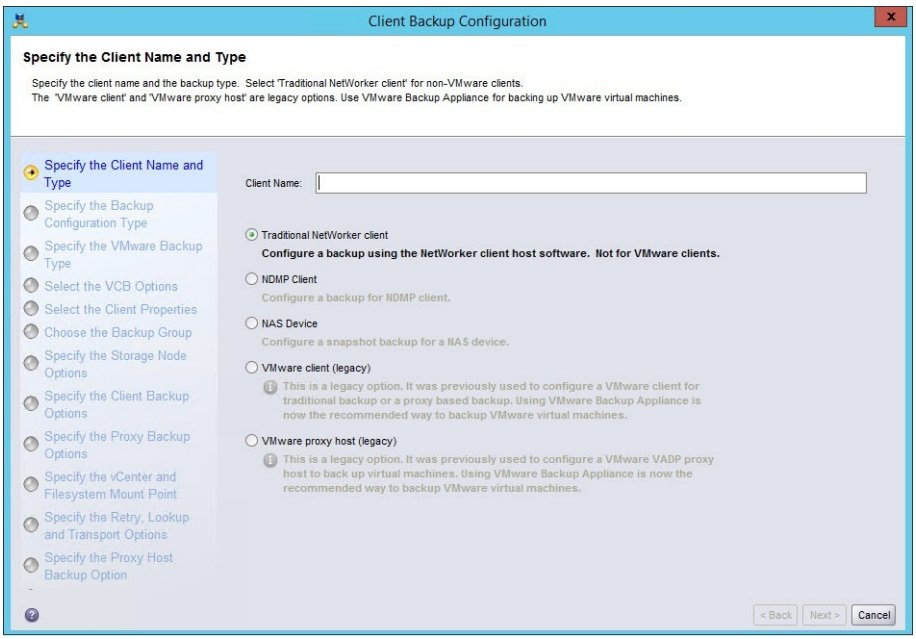
Configuring a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard

Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, right-click **Clients** and select **Client Backup Configuration** > **New**.

   The Specify Client Name and Type page displays, as shown in the following figure.

Figure 51 Specify Client name and type



3. Type the name of the host machine in the **Client Name** field and select **VMware proxy host** and click **Next**.
4. Select the vCenter server associated with the Proxy host if present, otherwise:
   a. In the vCenter section, click **New** to create a new Hypervisor resource.
   b. In the vCenter field, specify the hostname of the vCenter server.

Note

There is no limit to the number of vCenter servers supported; however, each vCenter server must be created in the Hypervisor resource and each must be associated with the appropriate proxy/proxies in the environment.

c. In the Username and Password field, type the username and password for an account with permission to perform backups, snapshots and registering/creating a new VM.

If the user has non-administrative privileges on the vCenter server, follow the steps in the section Creating a VADP User role in vCenter on page 165.

d. Click **OK**.

Note

This will set the **VADP_HOST** variable in the Application Information properties of the Proxy host client in NetWorker.

5. In the Filesystem Mount Point Options section, specify the directory where all the VM backup jobs are supposed to reside in. The default value is **c:\\mnt**. This option will set the **VADP_BACKUPROOT** variable in the Application Information properties of the Proxy host client in NetWorker.

   Consider the following when defining this option:

   - Ensure that the directory already exists, otherwise the 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 * backup type and the VM name will be created here.

6. In the Retry Option selection, set the desired number of time to retry failures and the wait time in between retries. These options will set the **VADP_MAX_RETRIES** and **VADP_MAX_BACKOFF_TIME** variables respectively in the Application Information properties of the Proxy host client in NetWorker.

   Consider the following:

   - **VADP_MAX_RETRIES** - 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 software retries.
   - **VADP_MAX_BACKOFF_TIME** - If you change this default, also change the default for MAX_RETRIES, because this setting only applies if MAX_RETRIES is larger than 0).

7. In the Transport Mode Options section, select all desired modes in the Available Modes section and click the button to add. Change the mode order if desired, the order in which modes are specified dictate the priority in which they are attempted. This option will set the **VADP_TRANSPORT_MODE** variable in the Application Information properties of the Proxy host client in NetWorker.

Note

Each transport mode will be separated by a | when the variable is defined.

8. Click **Next**.
9. Click **Next** in the Specify the Proxy Host Backup option as it is not necessary to backup the Proxy host.
10. Click **Next** and review the Backup Configuration Summary.
11. Click **Create**.
12. Click **Finish**.

Configuring a VADP proxy host and Hypervisor resource manually by using nsradmin

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 after upgrading by creating a NSR Hypervisor resource on page 49.

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 25 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 * backup type and the VM name will be created here. • "If omitted, BACKUPROOT defaults to c:\\mnt. Example: VADP_BACKUPROOT=C:\\mnt"	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	No

Table 25 Application information values (continued)

Attribute name	Description	Default value
	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	
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 software retries. For example: Example VADP_MAX_RETRIES=1	0
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:	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

Table 25 Application information values (continued)

Attribute name	Description	Default value
	• 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 179 . • 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	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 25 Application information values (continued)

Attribute name	Description	Default value
	does not require shared storage and also enables VADP to be run inside a VM.	

Example: Attribute values used for VADP configuration

The following example displays all the possible attribute values used for a VADP configuration:

```
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
```

Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Clients**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type the hostname of the Proxy client.
5. The browse and retention policy fields can remain empty, as they are set for the virtual clients.
6. If the Proxy client must be backed up, ensure that **Scheduled Backups** is selected.

   Note

   It is not mandatory to backup the Proxy client.

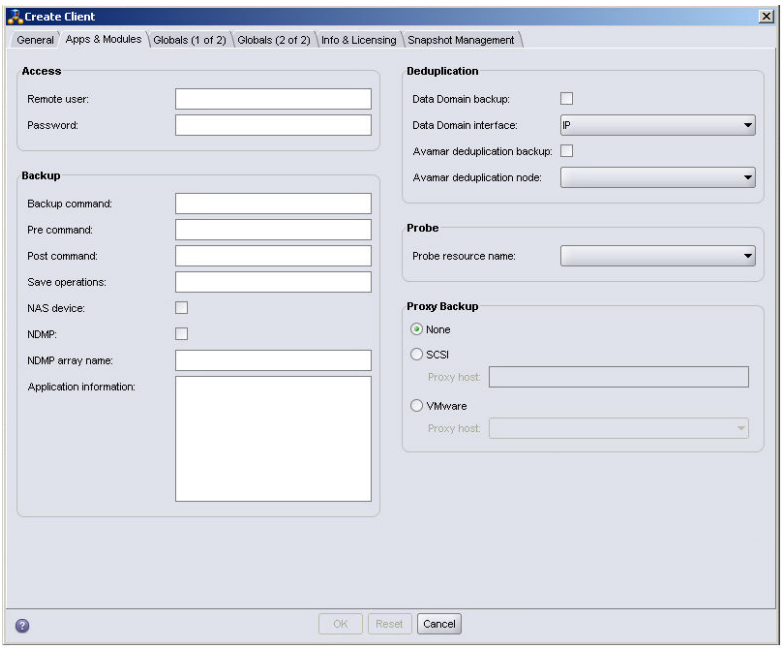
7. In the **Save Set** attribute, type the name of the files or directories to be backed up:
   a. To specify a file or directory for backup such as C drive, type **c:**.
   b. To back up a specific directory such as Documents and Settings, type **c:\Documents and Settings**.
   c. To backup all file systems and VSS/System save sets, type **ALL**.

   Note

   If the Proxy client will not be backed up use the default selection.

8. Click **Apps and Modules**. The Create Client dialog displays, as shown in the following figure.

Figure 52 Apps and Modules tab in NMC



9. In the Application Information field, add one line for each VC server hostname that is configured as part of the NSR Hypervisor resource:

   ```
   VADP_HOST=any.vc
   ```

   where any.vc is the hostname of the vCenter server configured as the NSR Hypervisor resource.

10. The variables, described in the following table, can also be specified in the Application Information section.

Configuring a virtual client for backup

You can configure a virtual client by using the Client Backup Configuration Wizard or by using the Client Properties window. Using either method, you can create a new Client resource or modify an existing one.

Complete the steps in one of the following topics depending on your environment:

- Configuring a virtual client by using the Client Backup Configuration wizard on page 162
- Configuring a virtual client manually by using the Client Properties window on page 164

VMware clients can also be configured as deduplication clients. After creating a VMware client, follow the instructions in the *NetWorker Data Domain Deduplication Devices Integration Guide* or the *NetWorker 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 170.

Table 26 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 backups) and the `VADP_DISABLE_FLR` APPINFO variable is set to Yes.*	No	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 by using the Client Backup Configuration wizard

To configure a virtual client if vCenter is configured:

Procedure

1. Right-click on the VM and select **Client Backup Configuration** > **New**.
2. In the Specify the Client Name page, confirm that the **client name** field is populated and **VMware client** is enabled. Click **Next**.

   Note

   The specified client name should be a recognized hostname/alias in a name service and/or FQDN. If the VM display name appears in the field, this entry must be changed to the hostname or FQDN or client creation will fail.

3. In the Specify the VMware Physical Host and Backup Type page, the Physical Host field will be populated with the Physical Host for the VM.
4. Select **VMware Proxy backup** and from the **Proxy host** list, select the name of the Proxy Host VC Server. The VC names are taken from the multiple VADP_HOST values set on the Application Information section of the proxy Client resource. Click **Next**.
5. In the Specify the Backup Options page, complete the following optional sections if required:
   - **Deduplication** — Select **Data Domain** if this client is being used with the DD Boost option that is available in NetWorker 7.6 SP1 and later. Select **Avamar deduplication backup** and the corresponding Avamar server from the list if this client is using Avamar deduplication. Select **None** if no deduplication is being used.
   - **Target Pool** — Select a pool, from the list, to which data from this client's backup will be directed. If a pool is selected, this value will override any other pool selection criteria that is associated with the client's backup group or the client's save sets. This field is most often used when backing up to a NetWorker 7.6 SP1 or higher Data Domain device.
6. Click **Next** to display the Specify the Proxy Backup Options page.
7. (Optional) In the **Virtual Machine Name** field, type the display name of the VM used in the vCenter. If a value is not entered, backups for this VM will be done by IP address.

   If a name is entered in this field, the name must match the display name as seen in vCenter Administrator, otherwise the backup will fail.

   Note

   This name is case-sensitive. Also, if the name of the VM contains spaces, then the name should be enclosed in double quotes "".

8. In the Backup Type section, specify the desired backup:
   - Image level backup (this is equivalent to saveset *FULL*).

- Backup all files (this is equivalent to saveset ALLVMFS).
- Backup Specific files and folders.
  - To specify a file or directory for backup such as C: drive, enter c:\ or c:.
  - To back up a specified directory, such as Documents and Settings, enter c:\Documents and Settings.

  Note

  Due to limits with VADP, only one entry is allowed for the Save Set attribute.

9. Click **Next**.
10. In the Select NetWorker Client Properties section, select the **Browse** and **Retention** policies from the drop down menus.
11. If desired, select the **Backup Schedule** for this client.

    Note

    If a backup schedule is also defined for the backup group that this client will be added to, the group schedule will override the client schedule.

12. Type a description of the client in the **Client Comment** field, if desired.
13. If the NetWorker server and VADP proxy client are two different machines, in the **Remote access** field specify:

    ```
    user=system, host=VADP proxy host
    ```

    Where *system* is the system account of the Windows VADP proxy and *VADP proxy host* is the name of the Proxy host.

14. Click **Next**.
15. In Specify the NetWorker Backup Group, choose the desired group or select **Create a new group** and provide a group name and desired number of client retries.
16. If a new group is created, in the Schedule Options section, specify the desired time for the group to start in the **Schedule backup start time** field and enable **Automatically start the backup at the scheduled time**.
17. Click **Next**.
18. In the **Backup Storage Nodes** section, select the storage nodes that contain the devices to which the backups will be directed.
19. In the **Recovery Storage Nodes** section, select the storage nodes whose available devices will be used for recovery operations.
20. Click **Next**.
21. Review the backup configuration summary and click **Create**.

    You can now enable a directive on the VM.

22. Click **Clients**, right-click the newly created VM client, and select **Properties**.
23. From the **Directive** list, select **Encryption directive** or **NT with compression** directive.

24. Click the **Apps and Modules** tab and ensure that **nsrvadp_save** is in the **Backup command** field.
25. Click **OK**.

Results

More information on directives is provided in the *NetWorker Administration Guide*.

Configuring a virtual client manually by using the Client Properties window

To configure a virtual client by using the Client Properties window:

Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Clients**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type the hostname of the client.
5. In the **Browse Policy** field, select a browse policy from the list.

   Note

   If the browse policy is set at the client level, it will override the browse policy specified for any groups to which this client is a member.

6. In the **Retention Policy** field, select a retention policy from the list.

   Note

   If the retention policy is set at the client level, it will override the retention policy specified for any groups to which this client is a member.

7. Ensure **Scheduled Backups** is selected.
8. In the **Save Set** attribute, type the name of the files or directories to be backed up.

   Note

   Due to limitations with VADP, only one entry is allowed for the Save Set attribute.

   a. To specify a file or directory for backup such as C drive, type **c:**.
   b. To back up a specific directory such as Documents and Settings, type **c:\Documents and Settings**.
   c. To backup all VM file systems, type **ALLVMFS**.
   d. To backup up the entire VM image, type ***FULL***.
9. From the **Directive** attribute, select a directive from the list, if desired.
10. Click the **Apps and Modules** tab.
11. In the **Backup Command** field, type **nsrvadp_save**.
12. In the **Application Information** field add a value **VADP_HYPERVISOR** to indicate which vCenter server to use for communication. For example:

    VADP_HYPERVISOR=*vCenter1*

Where *vCenter1* is the name of the vCenter server.

Also add this value for the VADP_VM_NAME attribute.

Note

VADP_VM_NAME is case-sensitive, so the VM host name must be entered as it is displayed (for example, SUSE11-X86). Also, if the name of the VM contains spaces, then the **VADP_VM_NAME** should be enclosed in double quotes "".

13. Select **VADP** for the **Proxy backup type** field.
14. If the NetWorker Server and VADP proxy client are on two different machines:
    a. Click on the **Globals (2 of 2)** tab.
    b. In the **Remote access** field specify:

```
user=system, host=VADP proxy host
```

    Where *system* is the system account of the Windows VADP proxy and *VADP proxy host* is the name of the Proxy host.
15. 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 166 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 27 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

Table 27 VADP backup privileges (continued)

Setting	Privileges
	• Update task

The following table provides VADP recovery privileges.

Table 28 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

Table 28 VADP recovery privileges (continued)

Setting	Privileges
	• Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility
Virtual machine > Interaction	• Power Off • Power On • Reset
Virtual machine > Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download
Virtual machine > State	• Create snapshot • Remove snapshot • Revert to snapshot
Network	• Assign network • Configure
Session	• Validate session
Tasks	• Create task • 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.

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.

Launching the vSphere Web Client from the NetWorker Console (Windows only)

On supported Windows platforms, you can launch the vSphere Web Client from the NetWorker Console's Configuration window using the main menu.

Procedure

1. Start the Console, then click the **Configuration** tab.
2. Highlight the desired client in the left panel.
3. Launch the vSphere client by selecting **Configuration** > **Launch vSphere Web Client**.

Recovering VADP Backups

This section covers these topics:

- File based recovery of a VM on page 170
- Image level (single step) recovery of a full VM on page 172
- Recovery of pre-NetWorker 7.6 SP2 VM backups on page 180

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 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.

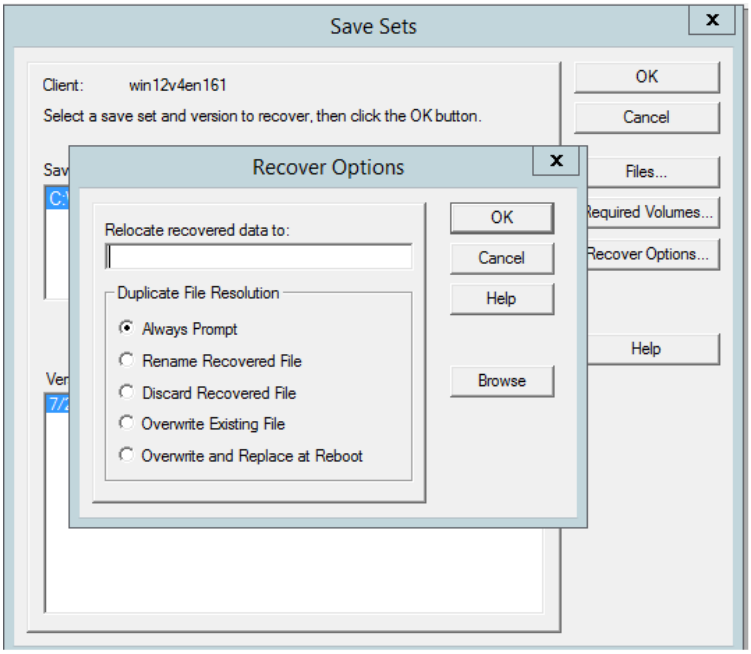
To perform a file based recovery on the local host:

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 53 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 173
- Performing an image level recovery from the command line on page 175

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 2003 (with at least SP1 installed)
  - Microsoft Windows 2003 R2
  - 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. The section Image level recovery to a different FARM or vCenter on page 178 provides more details. 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

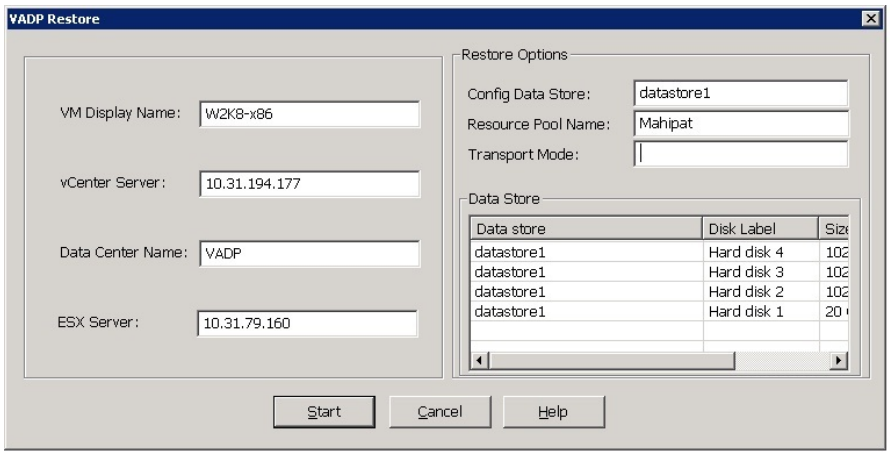
     NBDSSL mode fails for recovery of VMs in NetWorker. The transport mode Hotadd fails for ESX 5.0 and with VC 5.0. Recovering a VM using NBDSSL, SAN, or Hotadd transport mode on page 179 provides a workaround to this issue.

   - **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 54 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 176
  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 177
  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 *NetWorker Command Reference Guide* provides more information about using the recover command to mark (select) files and to perform the recovery.

Image level recovery to a different FARM or vCenter

When recovering to a different server within the same vCenter environment, or when recovering to a different server within a different vCenter environment, you must select whether to keep the same UUID, or create a new UUID.

When you start a VM that was restored to a new location, the following message displays:

In ESX/ESXi 3.x:

```
The virtual machine's configuration file has changed its location
since its last poweron. Do you want to create a new unique
identifier (UUID) for the virtual machine or keep the old one?
* Create
* Keep
* Always Create
* Always Keep
```

If you choose to keep the UUID, select Keep, then click **OK** to continue starting the VM.

If you choose to create a new UUID, Select Create, then click **OK** to continue powering on the VM.

In ESX/ESXi 4.x:

```
Question (id = 0) : msg.uuid.altered:This virtual machine might
have been moved or copied.
In order to configure certain management and networking features,
VMware ESX needs to know if this virtual machine was moved or
copied.
* Cancel
* I moved it
* I copied it
```

If you choose to keep the UUID, select **I moved it**, then click **OK** to continue starting the VM.

If you choose to create a new UUID, select **I copied it**, then click **OK** to continue powering on the VM.

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

Note

Windows 2008 32-bit can only be used as VADP proxy, not as the NetWorker server.

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.

Recovery of pre-NetWorker 7.6 SP2 VM backups

To recover backups of VMs that were performed via VCB, install VMware Converter 4.0.1 on the machine where the restore will be initiated. This allows you to perform a 2-step recovery, for example, first to a staging location, and then manually through the VMware Converter 4.0.1.

Note

You can only perform single Step recovery of VCB backups when VMware Converter 3.0.3 is installed, however, due to the incompatibility of this version with vSphere 4.0/4.1, EMC recommends *not* using Single Step recovery when recovering old VCB backups to a vSphere host. Note also that VMware Converter 4.0.1 is the last version that supports VCB. The knowledgebase article at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1026944provides more information.

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 148 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 187
- 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 191 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.
- In previous NetWorker releases using VCB, extra space was required for the mount point on the VCB proxy for copy operations during backup and recovery. NetWorker releases using the VADP proxy require significantly less space. The section VADP mount point recommendations and space considerations on page 189 provides more information.
- 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 190.

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

- The maximum number of concurrent sessions when using a physical proxy is higher than that of a virtual proxy. The section Recommendations and considerations for transport modes on page 191 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 29 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 30 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 188.

- 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 191 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 188.
  - 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 191.
  - 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 a VADP proxy host and Hypervisor resource manually by using nsradmin on page 155 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 fiber 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 fiber 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 196.
- 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 196.
- 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 179.
- 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
   ```

Upgrading from VCB to VADP (pre-NetWorker 8.1)

This section applies to upgrades from a NetWorker 7.6 SP1 or earlier release that uses the VMware Consolidated Backup (VCB) solution to protect virtual NetWorker clients, to a NetWorker 7.6 SP2 or later release that provides backup and recovery of VMware virtual clients using vStorage APIs for Data Protection (VADP), up to NetWorker release 8.1.

NetWorker 7.6 SP2 and later releases up to NetWorker 8.1 still support VCB-based backups with NetWorker 7.6 SP1 proxy servers. However, VADP-based backups must use a NetWorker 7.6 SP2 or later proxy server. A NetWorker 7.6 SP2 or later proxy cannot be used for VCB backups.

When upgrading the NetWorker software from any release previous to NetWorker 7.6 SP2, if VCB was used for backups in the previous release (for example, NetWorker 7.6 SP1) then the upgrade tool must be run on the NetWorker server to transition to VADP backups. The following chapter provides information on upgrading the NetWorker software to release 7.6 Service Pack 2 or later to use VADP.

Upgrading an existing NetWorker server and VCB proxy

After installing the NetWorker Release 7.6 SP2 or later software on the NetWorker server and the VADP proxy server, run the nsrvadpserv_tool command on the NetWorker server. The nsrvadpserv_tool command updates pre-7.6 Service Pack 2 NetWorker virtual clients to use VADP for backup and recovery, converting all clients on a specified proxy. The nsrvadpserv_tool replaces the nsrvcbserv_tool that was used in NetWorker 7.6 SP1.

Be aware of the following when running this command:

- If you are upgrading from a pre-7.6 NetWorker installation, the Proxy Host client must be configured with Administrator privileges for the operating system. To ensure the Proxy Host is configured with Administrator rights:
  1. Connect to the NetWorker server by using NMC.
  2. Click **Configuration**.
  3. On the left pane, click **Clients**.
  4. Right mouse click on the Proxy client and select **Properties**.
  5. Click on the **Apps & Modules** tab.
  6. In the Remote User and Password fields, specify a user name and password for an account with Administrator rights on the Proxy server.
- By default, the nsrvadpserv_tool is located C:\program files\legato\nsr\bin.
- The NetWorker server and VCB Proxy host must be at NetWorker Release 7.6 Service Pack 2 and later.
- If the VCB_LOOKUP_METHOD is set to **name**, refer to the notes below. Special consideration needs to be given if the VCB_LOOKUP_METHOD defined is set to IP rather than name.

  To determine the Lookup Method on the Proxy Client resource, in the Application Information section, make note of the value for VCB_LOOKUP_METHOD. If the value is not set to name, manual steps detailed later in this procedure will need to be performed after the nsrvadpserv_tool is executed.

To update pre-7.6 Service Pack 2 NetWorker VMware virtual clients, type this command on the NetWorker server:

```
nsrvadpserv_tool -p VM_proxy_hostname_or_IP_address
```

The nsrvadpserv_tool does the following:

- For pre-7.6 clients:
  - Identifies the NetWorker clients that are VMs configured for the specified VADP proxy server.
  - Executes the **nsrvadpclnt_tool** on the NetWorker client configured as the VADP proxy server.
  - Reads the configuration file (config.js) and sends the information to the NetWorker server.

- Updates the Application Information attribute of the NetWorker Client resource acting as the VADP proxy server with information from the config.js file.
- Sets the backup command attribute in the NetWorker Client resource of all VMs configured for the specified VADP proxy server to **nsrvadp_save**.
- Creates the vCenter resource.

- For 7.6 and 7.6 Service Pack 1 clients:
  - Changes the backup command attribute in the NetWorker Client resource of all VMs from **nsrvcb_save** to **nsrvadp_save**.
  - Updates the Application Information (APPINFO) attribute of the virtual Client resources so that "VCB" is replaced with "VADP" in all APPINFO variables. Examples are shown in the following table.

Note

After upgrading the NetWorker server from 7.6 SP1 to 7.6 SP2 or later, the VM Client resource associated with the VCB proxy does not display the correct information in NMC. For example, if you are using both VADP and VCB proxies, VM Client resources that are still associated with VCB proxies will display the VADP proxy when viewing the VM resource in NMC. The correct information displays in the nsradmin output for the Client resource.

This issue is documented in the Release Notes under NW129735.

Table 31 APPINFO variable replacements

Old APPINFO variable name	New APPINFO variable name
VCB_MAX_BACKOFF_TIME=20	VADP_MAX_BACKOFF_TIME=20
VCB_TRANSPORT_MODE=nbd	VADP_TRANSPORT_MODE=nbd
VCB_HOST=10.31.78.120	VADP_HOST=10.31.78.120
VCB_BACKUPROOT=F:\mnt	VADP_BACKUPROOT=F:\mnt
VCB_MAX_RETRIES=10	VADP_MAX_RETRIES=10
VCB_LOOKUP_METHOD=name	removed

The VADP_MAX_BACKOFF_TIME and VADP_MAX_RETRIES variables are removed if their values were set to 10 and 0 respectively, which are their default values.
The VADP_HYPERVISOR=*VC_name* variable is added to the APPINFO list of variables. This variable value is based on the VADP_HOST variable that is specified in the VADP proxy server's Client resource.
If VM lookups are done by name instead of IP address, you must add the VADP_VM_NAME variable in the Application Information attribute of each NetWorker virtual Client resource. The variable format is entered as VADP_VM_NAME=*vm1* where *vm1* is the display name of the VM used in the vCenter.
VADP_VM_NAME is case-sensitive. For example, if the VM host name is upper-case (such as SUSE11-X86), the value of VADP_VM_NAME must be set to SUSE11-X86.

Also, if the name entered for VADP_VM_NAME contains spaces, the name must be contained within quotation marks (for example, VADP_VM_NAME="this is my vm name").

Change vCenter role privileges after upgrading

The following steps are required if VCB backup/recovery was previously performed through NetWorker using a non-Administrator vCenter role.

In order to perform backups using VADP, the permissions associated with the non-Administrator role need to be modified in vCenter.

Creating a VADP User role

Procedure

1. Log in to the vCenter server with Administrator privileges using vSphere Client.
2. From the vCenter server, select **View** > **Administration** > **Roles**.
3. Right-click the existing non-Administrator role that was previously used by NetWorker and select **Clone**. A new cloned role is created.
4. Rename the cloned role to **VADP User**.
5. Right-click the VADP User role and select **Edit Role**.
6. Assign the required permissions to the VADP User role. The section Minimum vCenter permissions needed to back up and recover using VADP on page 166 provides more information.

Assigning the VADP User role to the user specified in the NetWorker Hypervisor resource

Note

The VMware Basic System Administration documentation and the Datacenter Administration Guide provide more information on assigning a role to a user. The VMware documentation is available at http://www.vmware.com/support/pubs/.

Procedure

1. Log in to the vCenter Server with Administrator privileges using vSphere Client.
2. In the left pane, select the vCenter server.
3. In the right pane, click the **Permissions** tab.
4. Right-click anywhere in the right pane and select **Add Permission** from the drop-down.
5. Add the NetWorker Hypervisor user and assign the **VADP User** role.
6. Ensure that **Propagate to Child Objects** is enabled, then click **OK**.

Upgrading only the proxy client to NetWorker 7.6 SP2 or later

If you only want to upgrade the NetWorker proxy client to 7.6 SP2 or later and do not want to upgrade the NetWorker server, a manual upgrade can be performed by using the following steps.

Note

The NetWorker server must be at a minimum of version 7.6. If the NetWorker server is not version 7.6 or 7.6 SP1, it will need to be upgraded prior to performing the proxy client upgrade.

A NetWorker 7.6 SP2 or later proxy can only be used for VADP based backups and should be used with a NetWorker 7.6 SP2 or later server.

Make the following changes to the APPINFO attribute of the Client resource for the proxy:

Procedure

1. Change **VCB_BACKUPROOT** to **VADP_BACKUP_ROOT**.
2. Change **VCB_HOST** to **VADP_HOST**.
3. Change **VCB_TRANSPORT_MODE** to **VADP_TRANSPORT_MODE**.
4. If **VCB_VM_LOOKUP_METHOD** is set to **ipdddr**, remove that entry; if it is set to **name**, the Client resource of the virtual client must be changed, as indicated in step 9.
5. Remove **VCB_PREEXISTING_MOUNTPOINT** and **VCB_PREEXISTING_VCB_SNAPSHOT**.
6. Change **VCB_MAX_RETRIES** to **VADP_MAX_RETRIES**.
7. Change **VCB_BACKOFF_TIME** to **VADP_BACKOFF_TIME**.
8. In the Client resource for the virtual client associated with the proxy, change the Backup command from **nsrvcb_save** to **nsrvadp_save**.
9. If **VCB_VM_LOOKUP_METHOD** was set to **name** in the proxy Client resource, add **VADP_VM_NAME** to the virtual Client resource's **APPINFO** attribute with the value of the VM Name that is known to the Virtual Center.

   Note

   The NMC Configuration wizards for NetWorker 7.6 SP2 or later will not work with a pre-7.6 SP2 server. Information must be entered manually in the Client resource, even for new proxy clients, until the server is upgraded to NetWorker 7.6 SP2 or later.

Upgrade to use vCenter if ESX/ESXi server was previously used for VM backups

The following upgrade steps must be performed if VM backups were previously configured directly to the ESX/ESXi server instead of going through the vCenter server.

Using a manual upgrade

If the nsrvadpserv_tool cannot be run (for example, if using a 7.6.1 or 7.6.0 NetWorker server instead of upgrading the server to 7.6 SP2), perform the following steps:

Procedure

1. Follow the manual upgrade steps provided in the section Upgrading only the proxy client to NetWorker 7.6 SP2 or later on page 200.
2. Manually create a new Hypervisor resource for vCenter.
3. Update the proxy host with the appropriate VADP_HOST values.

Using the nsrvadpserv_tool

If the NetWorker server is being upgraded to 7.6 SP2 or later, perform the following steps:

Procedure

1. Run the upgrade tool as outlined in the section Upgrading an existing NetWorker server and VCB proxy on page 197.
2. Manually create a new Hypervisor resource for vCenter.
3. Update the proxy host with the appropriate VADP_HOST values.

Space requirement changes on proxy for VADP vs VCB

In NetWorker releases using VCB, extra space was required for the mount point on the VCB proxy for copy operations during backup and recovery. NetWorker releases using the VADP proxy require significantly less space (typically, around 10% of the VM data size).

Post-upgrading steps for Virtual Center on a 64-bit Windows host

The procedure described in this section is optional and applies only if your pre-7.6 Service Pack 2 VMware integration with NetWorker had a Virtual Center server installed on a 64-bit Windows host.

Prior to NetWorker 7.6 Service Pack 2, if the Virtual Center server was installed on a 64-bit Windows host, you had to create a "command host" on a 32-bit Windows host and then reference the command host in the Hypervisor resource that was set up for Virtual Center. In NetWorker 7.6 Service Pack 2 and later, these additional steps are not required.

To eliminate the need for a 32-bit command host when the Virtual Center is installed on a 64-bit host:

Procedure

1. Install the NetWorker 7.6 Service Pack 2 or later client software on the 64-bit Virtual Center host.
2. Modify the Command Host attribute in the Hypervisor resource to specify the 64-bit Virtual Center server name.
   a. From the **Administration** window, click **Configuration**.
   b. In the expanded left pane, right-click **Virtualization** and then select **Enable Auto-Discovery**.
   c. In the Auto-Discovery dialog box, click **Advanced**.

d. Delete the name of the 32-bit Windows computer that was in the **Command Host** field. When this field is empty, the name of the Virtual Center server is used as the Command Host.

e. Ensure that the value in the **Command Name** field is **nsrvim**, then click **OK**.

CHAPTER 4

Licensing

This chapter contains the following topics:

- Virtual environments simplified licensing 204
- Physical ESX hosts in non-VADP configurations 204
- Guest-based licensing 204
- NetWorker VMware Protection licensing 205
- VADP licensing 205

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 *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 VCB/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 non-VCB/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 An operation that saves data to a volume.

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 A computer, workstation, or fileserver whose data can be backed up or recovered.

client file index A database that tracks every database object, file, or file system that is backed up. The NetWorker server maintains a single client index file for each client.

Console Server NetWorker servers and clients are managed from the NetWorker Console server. The Console server also provides reporting and monitoring capabilities for all NetWorker servers and clients.

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 The number of 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 A NetWorker assigned label that uniquely identifies a volume. Templates can be used to define label parameters.

M

managed application A program that can be monitored and/or administered from the Console server.

media database Indexed entries about the location and the life cycle status of all data and volumes that the NetWorker server manages.

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 A default NetWorker server user group that can add, change, or delete NetWorker server user groups.

NetWorker client **See** client

NetWorker Console server **See** Console Server

NetWorker Management Console **See** Console Server

NetWorker server The host running the NetWorker server software, which contains the online indexes and provides backup and recovery services to the clients on the same network. **See** online indexes

NetWorker storage node **See** storage node

O

online indexes Databases on the NetWorker server that contain information about client backups and backup volumes. **See** client file index **See** media database

R

recover To restore files from a backup volume to a client disk.

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 The command that backs up client files and makes entries in the online index.

save set A group of files or a file system that is backed up on storage media.

single step backup and recovery **See** image level backup and recovery

storage node A storage device physically attached to another computer whose backup operations are controlled by the NetWorker server.

U

update enabler A code that updates software from a previous release. Like other temporary enabler codes, it expires after 45 days.

V

VADP An acronym for vStorage APIs for Data Protection. VADP enables backup software to perform centralized virtual machine backups without the disruption and overhead of running backup tasks from inside each virtual machineVADP supersedes the VCB framework for VMware backups.

vCenter An infrastructure management tool that provides a central point for configuring, provisioning, and managing virtualized IT environments, and is part of the VMware Virtual Infrastructure package.

Virtual machine Software that creates a virtualized environment between the computer platform and its operating system, so that the end user can install and operate software on an abstract machine.

VM An acronym for virtual machine.

VMDK Virtual Machine Disk (VMDK) is a file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. These files are commonly called VMDK files because of the .vmdk extension that VMware adds to these files.

VMWare Backup Appliance) The VMware Backup Appliance (or EMC Backup and Recovery appliance) is an appliance that, when deployed, enables VMware backup and clone policy creation in NMC, and enables the EMC Backup and Recovery plug-in in the vSphere Web Client to assign VMs to those policies.

VMware Tools Installed inside each virtual machine, VMware Tools enhance virtual machine performance and add additional backup-related functionality.

VSS (Volume Shadow Copy Service) Microsoft technology that creates a point-in-time snapshot of a disk volume. NetWorker software backs up data from the snapshot. This allows applications to continue to write data during the backup operation, and ensures that open files are not omitted

VSS component A subordinate unit of a writer. **See** writer

W

writer A 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** metadata and **See** VSS component