EMC® NetWorker® and VMware

Release 8.1 SP1

Integration Guide

P/N 302-000-433
REV 10

Published September, 2014

CONTENTS

Chapter 3 VADP Backup and Recovery (legacy)

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 representative if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. New versions of this document might be released on the EMC online support website. Check the EMC online support website to ensure that you are using the latest version of this document.

Purpose

This document describes how to configure and use EMC 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.

Related documentation

The following EMC information products provide additional information:

- *EMC NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *EMC NetWorker Installation Guide*
  Explains how to install or update the NetWorker software for the clients, console, and server on all supported platforms.
- *EMC NetWorker Cluster Integration Guide*
  Explains how to set up and configure the NetWorker software in supported cluster environments.
- *EMC NetWorker Release Notes*
  Contain information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *EMC NetWorker and EMC 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 and VMware Integration Guide*
  Provides planning and configuration information on the use of VMware in a NetWorker environment.
- *EMC NetWorker Snapshot Management Integration Guide*
  Provides the ability to catalog and manage snapshot copies of production data that are created by using mirror technologies on EMC storage arrays.

- *EMC NetWorker and EMC Avamar Integration Guide*
  Provides planning and configuration information on the use of Avamar in a NetWorker environment.
- *EMC NetWorker Cloning Integration Guide*
  Contains planning, practices, and configuration information for using the NetWorker, NMM, and NMDA cloning feature.
- *EMC NetWorker Error Message Guide*
  Provides information on common NetWorker error messages.
- *EMC NetWorker Performance Optimization Planning Guide*
  Contains basic performance tuning information for NetWorker.
- *EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide*
  Explains how to design and plan for a NetWorker disaster recovery. However, it does not provide detailed disaster recovery instructions. The Disaster Recovery section of the NetWorker Procedure Generator (NPG) provides step-by-step disaster recovery instructions.
- *EMC NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.
- *EMC NetWorker Licensing Guide*
  Provides information about licensing NetWorker products and features.
- *EMC NetWorker License Manager 9th Edition Installation and Administration Guide*
  Provides installation, setup, and configuration information for the NetWorker License Manager product.
- *EMC NetWorker Software Compatibility Guide*
  Lists supported client, server, and storage node operating systems for NetWorker, NetWorker Modules, and options.
- 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. The NetWorker User Online Help 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.
- EMC NetWorker SolVe Desktop (also known as the NetWorker Procedure Generator (NPG)
  The NetWorker Procedure Generator (NPG) is a stand-alone Windows application used to generate precise user driven steps for high demand tasks carried out by customers, support, and the field. With the NPG, each procedure is tailored and generated based on user-selectable prompts.

  To access the NetWorker Procedure Generator, log on to https://support.emc.com/. and search for NetWorker Procedure Generator. You must have a service agreement to use this site.

- Technical Notes and White Papers
  Provides an in-depth technical perspective of a product or products as applied to critical business issues or requirements. Technical Notes and White paper types include technology and business considerations, applied technologies, detailed reviews, and best practices planning.

Conventions used in this document

EMC uses the following conventions for special notices:

NOTICE

NOTICE is used to address practices not related to personal injury.

Note: A note presents information that is important, but not hazard-related.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities • URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications
Bold	Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages Used in procedures for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • What the user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis, for example, a new term • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
`Courier bold`	Used for specific user input, such as commands
`Courier italic`	Used in procedures for: • Variables on the command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	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 nonessential 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, licensing, and service, go to the EMC Online Support website (registration required) at:

https://support.emc.com/

Technical support — For technical support, go to EMC online support and select Support. On the Support page, you will see several options, including one to create a service request. 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 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 covers these topics:

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.
- VADP (legacy solution) — This pre-NetWorker 8.1 solution uses vStorage APIs for Data Protection (VADP) technology to offload backup processing from the NetWorker server to a separate backup proxy host. This option provides automatic discovery of VMware environments, notifications when the environment changes, and a graphical map and tabular view of VMware environments. 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 since 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.
- NetWorker VMware Protection — A NetWorker-integrated VMware backup and monitoring solution introduced in NetWorker 8.1. In this solution, when you deploy an EMC Backup and Recovery appliance, also known as a VMware Backup Appliance, in the vSphere server and register the appliance with NetWorker and vCenter, you can create backup policies with the VMware Backup Appliance for VMs in NMC, and assign the backup policy to VMs using the EMC Backup and Recovery plug-in in the vSphere Web Client interface. After backing up the policy, you can then perform image-level recoveries of these backups from the vSphere Web Client, or file-level recoveries from the EMC Data Protection Restore Client interface.

Backup and recovery types

Table 1 on page 12 provides a quick comparison between Guest-based, VADP, and NetWorker VMware Protection backup and recovery.

Table 1 Comparing Guest based, VADP, and NetWorker VMware Protection (page 1 of 2)

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
Individual file backups	Yes	Yes for Windows guest OS only	Not required

Table 1 Comparing Guest based, VADP, and NetWorker VMware Protection (page 2 of 2)

Option	Guest-based	VADP (legacy)	NetWorker VMware Protection
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	Yes for Windows guest OS only	Yes for Windows and Linux
Deduplication supported	Yes	Yes — Direct backup to Data Domain	Yes — Direct backup to EMC Backup and Recovery 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 - dependant 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 Client Configuration wizard	EMC Backup and Recovery appliance registration through web interface
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

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

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

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

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.

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.

Note: The following types of VM disks are not supported when using VADP backup:
Virtual Machine OS containing GPT or dynamic disks
Virtual Machine OS containing uninitialized disks
Virtual Machine OS containing unformatted partitions
Virtual Machine OS containing partitions without drive letters
Virtual Machine configuration with Virtual IDE Disk Devices (only SCSI)
Virtual Machine configuration with independant disk mode

Advantages

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

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.

NetWorker VMware Protection

NetWorker VMware Protection provides an EMC Backup and Recovery appliance that, when deployed and configured, allows you to set up backup policies in NMC, and then assign VMs to those backup policies by using the EMC Backup and Recovery plug-in within the vSphere Web Client.

Advantages

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

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.

CHAPTER 2
NetWorker VMware Protection

This chapter includes the following topics:

NOTICE

Within this document, VMware Backup Appliance and EMC Backup and Recovery appliance refer to the same appliance.

NMC refers to this appliance as the VMware Backup Appliance for the purpose of VMware backup. Therefore, this document refers to VMware Backup Appliance when discussing the solution from NMC.

For the vCenter administrator, the vSphere Client refers to this appliance as the EMC Backup and Recovery appliance for the purpose of protecting the virtual machine (VM) environment. Therefore, this document refers to EMC Backup and Recovery when discussing the solution from a vCenter perspective.

Introduction to NetWorker VMware Protection

NetWorker VMware Protection is a NetWorker-integrated VMware backup and monitoring solution introduced with NetWorker 8.1. This solution allows you to create backup and cloning policies for a VMware Backup appliance using NMC. You can then assign those policies to VMs using the **EMC Backup and Recovery plug-in** user interface in the vSphere Web Client.

This solution becomes available when you deploy an EMC Backup and Recovery appliance in the vSphere server and register the appliance with NetWorker and vCenter. After performing VM 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.

Table 2 on page 20 compares tasks in NMC with tasks in the vSphere Web Client and the EMC Data Protection Restore client.

Table 2 NetWorker VMware Data Protection tasks

Program/Role	Task
VMware vSphere Web Client interface with EMC Backup and Recovery plug-in	Assign VMs to the backup policy created in NMC Start an adhoc VM backup Restore a full VM backup **Note:** When you start a policy from the vSphere Web client interface, you can only perform backups and not clones.
NMC	Create and edit Data Protection policies (backup, clone) Assign a backup policy to the VMware Backup Appliance Start or schedule a policy for backup **Note:** When you start a policy from NMC, you can perform both backups and clones, based on the actions defined in the policy.
EMC Data Protection Restore Client	Perform file-level restores **Note:** Supports both Windows and Linux platforms.

System requirements

Table 3 on page 21 lists the required components for NetWorker VMware Protection.

Note: NetWorker VMware Protection only supports the following NetWorker server architectures:
-Windows 64-bit
-Linux x86_64
-Solaris SPARC 64-bit

Also, the EMC Backup and Recovery appliance is available in 2 capacities — a 0.5 TB and 4 TB OVA. You only need to download one of these appliances, based on your system requirements. The section "Downloading the OVAs for EMC Backup and Recovery" on page 31 provides more information.

Table 3 NetWorker VMware Protection requirements

Component	Requirements
NetWorker	• 8.1 Server software with NMC
EMC Backup and Recovery appliance (0.5 TB OVA)	• CPU: 4 * 2 GHz • Memory: 8GB • Disks: 3* 250 GB • Backup storage capacity: 0.5 TB • OS: 250 GB
EMC Backup and Recovery appliance (4 TB OVA)	• CPU: 4 * 2 GHz • Memory: Refer to Table 9 on page 32 • Disks: 6 * 1 TB • Backup storage capacity: 4 TB • OS: 250 GB
Proxy Appliance	• CPU: 4 * 2 GHz • Memory: 4 GB • Disks: 2 disks (16 GB and 1 GB)
vCenter server	• version 5.1 and later • Linux or Windows platform, or VC appliance • vSphere Web Client (the VMware website provides information for supported web browsers) **Note:** You must enable web browsers with Adobe Flash Player version 11.3 or higher to access the vSphere Web Client, File-level recovery (FLR), and **EMC Backup and Recovery plug-in** user interface.
ESX/ESXi server	• version 4.1 and later • Changed Block Tracking (CBT) enabled
Data Domain	• Data Domain system OS at DDOS 5.3.0.6 or 5.4.0.4 and later • DDBoost user requires administrator privileges

Port requirements

The NetWorker VMware Protection solution requires the ports outlined in Table 4 on page 22 and Table 5 on page 22.

Table 4 Incoming port requirements

From	To	Port	Purpose
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 Configure	VMware Backup Appliance	8543	VMware Backup Appliance configuration
vCenter	VMware Backup Appliance	8543	EMC Backup and Recovery plug-in for vSphere Web Client

Table 5 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	111, 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) 28102 (NetWorker 8.2 and later)	MCS to proxy communications
External proxy	VMware Backup Appliance	28001, 27000, 29000	External proxy to MCS and GSAN

Limitations and unsupported features

Before you deploy the NetWorker VMware Protection solution, review the following limitations and unsupported features:

- The solution cannot detect if there is another EMC Backup and Recovery appliance in vCenter. This can lead to possible redundancy in VM backups.
- If you have multiple vCenters, you must deploy the EMC Backup and Recovery appliance to an ESX host that is managed by the same vCenter you register the appliance to. Otherwise, a connection error displays indicating "Unable to find this EBR in the vCenter inventory."
- You can only backup to the EMC Backup and Recovery appliance internal storage or Data Domain system.
- You cannot clone backups from a Data Domain system to EMC Backup and Recovery appliance internal storage.
- You cannot clone backups from EMC Backup and Recovery appliance internal storage to any other devices, including Data Domain systems.
- Backups to a Data Domain system can only be cloned to another Data Domain system, AFTD, or tape.
- NetWorker creates the default EMC Backup and Recovery appliance (identified as the VMware Backup Appliance in NMC) 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.
- An automatic migration tool to move from the previous VM backup solution to the NetWorker VMware Protection solution does not exist.
- The NetWorker VMware Protection solution supports only the hotadd and nbd transport modes. The hotadd mode is the default transport mode.
- The EMC Backup and Recovery plug-in in vCenter only supports English language keyboards.
- The NetWorker VMware Protection solution only supports image-level backup; you cannot perform individual folder or drive-level backup.

  Even though the NetWorker VMware Protection solution does not support the manual selection of individual VM disks (VMDKs) for backup, you can skip specific disks by marking each disk that you want to exclude as an Independent disk in the **Virtual Machine Properties** window on the vSphere Client.
- The NetWorker VMware Protection solution does not support Disaster recovery of data backed up to GSAN if the internal AFTD metadata is lost.

Performance and scalability

Performance and scalability of the NetWorker VMware Protection solution depends on several factors, including which OVA you deploy, the number of vCenters and number of proxies, and whether you perform a large number of concurrent VM backups. Observe the following performance statistics and where applicable use the recommendations and best practices as a guideline for achieving the best performance in your environment:

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

- Backups to a Data Domain system occur faster than backups to EMC Backup and Recovery appliance internal storage.
- To determine whether to use the 0.5 TB OVA or the 4 TB OVA:
  - If using a Data Domain system, select the 0.5 TB OVA
  - If not using Data Domain system, select the 4 TB OVA

  Note: EMC does not recommend using a mixed environment of Data Domain system and EMC Backup and Recovery appliance internal storage.

- An EMC Backup and Recovery appliance can backup up to 8 VMs in parallel. If you want to run up to 24 VM backups in parallel, then add up to 2 external proxies. Each external proxy can backup up to 8 VMs.
- For better performance, EMC recommends using a dedicated data store for the EMC Backup and Recovery appliance, especially for backups and recoveries performed from internal storage of the appliance.
- I/O contention may occur during snapshot creation and backup read operations when all VMs reside on a single data store.
- EMC recommends setting an appropriate NetWorker server parallelism value to reduce queuing on the NetWorker server.
- Each VM backup to a Data Domain system consumes one session on the Data Domain device. If you exceed the maximum limit of 60 sessions, EMC recommends that you configure additional devices.
- To achieve the best concurrent backup performance in a setup that requires additional vCenters, VBAs or proxies, EMC recommends using 1 EMC Backup and Recovery appliance + 2 External proxies per vCenter. Table 6 on page 24 and Table 7 on page 25 provide information on expected performance for different setups.

Table 6 Maximum concurrent sessions per EMC Backup and Recovery appliance

Deployed per vCenter	Maximum concurrent sessions
1 EMC Backup and Recovery appliance	8
1 EMC Backup and Recovery appliance + 1 external proxy	16
1 EMC Backup and Recovery appliance + 2 External proxies	24
1 EMC Backup and Recovery appliance + 3 External proxies	26

Table 7 Concurrency/parallelism

Component	Concurrency count	Notes
Proxies per vCenter	3	vCenter with the default configuration achieves good performance with 25 sessions. Each EMC Backup and Recovery appliance has 8 internal proxies, and the external proxy adds 8 more concurrent sessions. Therefore, use 1 EMC Backup and Recovery appliance and 2 external proxies.
VMs per policy	25	vCenter can process 25 VMs at a time. If a single policy contains more than 25 VMs, the remaining VMs will be queued during backup.
EMC Backup and Recovery appliance	26 concurrent VMs	The maximum concurrent sessions per EMC Backup and Recovery appliance is 26, irrespective of the target device.
External proxy	24 concurrent hotadd of VMDKs	External proxy has only 2 SCSI controllers which limits the concurrent hotadd sessions to 24. If you back up more than 24 VMDKs, the backup uses NBD mode.
vCenter	25 concurrent sessions	EMC recommends a maximum of 25 concurrent VM backups per vCenter. If vCenter runs on a standalone server with the vCenter database running on SQL, then a single vCenter can process more than 25 VMs at a time.
vCenter	2 external proxies (EMC Backup and Recovery appliance includes an internal proxy)	Due to the above recommendation, EMC recommends 2 external proxies per EMC Backup and Recovery appliance for concurrent backups.

Pre-installation requirements

Before you deploy the EMC Backup and Recovery appliance, follow the pre-installation requirements and review the best practices in the following sections:

- "DNS Configuration" on page 25
- "NTP Configuration" on page 26
- "EMC Backup and Recovery appliance best practices" on page 26

DNS Configuration

You must add an entry to the DNS Server for the appliance IP address and Fully Qualified Domain Names (FQDNs). The DNS server must support both forward and reverse lookup.

IMPORTANT

Failure to set up DNS properly can cause many runtime or configuration issues.

To confirm DNS configuration, open a command prompt and run the following commands from the vCenter Server:

1. To verify DNS configuration, type:

```
nslookup EMC_Backup_and_Recovery_appliance_IP_address
DNS_IP_address
```

The nslookup command returns the FQDN of the EMC Backup and Recovery appliance.

2. To verify that the FQDN of the EMC Backup and Recovery appliance resolves to the correct IP address, type:

```
nslookup FQDN_of_EMC_Backup_and_Recovery_Appliance 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:

```
nslookup FQDN_of_vCenter 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 lookups for the short names.

IMPORTANT

After deployment, check for DNS resolution (forward and reverse) from the EMC Backup and Recovery appliances and proxies for vCenter and the NetWorker hosts.

NTP Configuration

The EMC Backup and Recovery appliance leverages VMware Tools to synchronize time through NTP, using the **Sync guest OS time with host** option by default. All ESXi hosts, the vCenter server, and the NetWorker server should have NTP configured properly. The EMC Backup and Recovery appliance obtains the correct time through VMware Tools, and should not be configured with NTP.

Note: If you configure NTP directly on the **EMC Backup and Recovery plug-in** in the vSphere Web Client, then time synchronization errors occur.

ESXi and vCenter Server documentation provides more information about configuring NTP.

EMC Backup and Recovery appliance best practices

Observe the following best practices when deploying an EMC Backup and Recovery appliance:

- Deploy the EMC Backup and Recovery appliance on shared VMFS5 or higher to avoid block size limitations.
- Avoid deploying VMs with IDE virtual disks; using IDE virtual disks degrades backup performance.
- License the ESXi hosts for hotadd mode if using ESXi 4.1 or 5.0. ESXi 5.1 includes this feature by default.
- 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 EMC Backup and Recovery appliance on an ESXi host that has a path to the storage holding the virtual disk(s) being backed up.

Note: Hotadd mode will not work if the VMs backed up contain any independent virtual hard disks.

- When planning for backups, ensure that EMC Backup and Recovery supports the disk types. Currently, EMC Backup and Recovery does not support the following disk types:
  - Independent
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode
- In order to support 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.
- Install VMware Tools on each VM that you want to backup up using the **EMC Backup and Recovery plug-in** user interface. 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.

Create 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 EMC Backup and Recovery. 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

To create the user account:

1. From a web browser, connect to the vSphere Web Client:

   https://<*IP_address_vCenter_Server*>:9443/vSphere-client/
2. Navigate to **Home › Administration › SSO Users and Groups**.
3. In the **Users** tab, click on the Green **+**. The New User window appears.
4. In the **Username** field, specify a username (for example, EMC Backup and Recovery).
5. In the **Password** and **Confirm Password** fields, specify a password. You can leave the First name, last name and password fields blank.
6. In the **Permissions** field, select **Administrator User**.
7. Click **OK**.

Create a customized role

To customize a role with the required privileges:

1. In the vSphere Web Client, go to **Administration › Role Manager** and click on the green **+**.

   The **Create Role** dialog displays.

2. Type the name of this role (for example, Admin1).

3. Select all the privileges listed in Table 8 on page 28 and click **OK**. This vCenter user account must have these privileges at a minimum.

Table 8 Minimum required vCenter user account privileges (page 1 of 2)

Setting	vCenter 5.1 required privileges	vCenter 5.0 required privileges
Alarms	• Create alarm	• Create alarm
Datastore	• Allocate space • Browse datastore • Low level file operations • Move datastore • Remove datastore • Remove file • Rename datastore	• Allocate space • Browse datastore • Low level file operations • Move datastore • Remove datastore • Remove file • Rename datastore
Extension	• Register extension • Unregister extension • Update extension	
Folder	• Create folder	• Create folder
Global	• Cancel task • Disable method • Enable method • Licenses • Log event • Manage custom attributes • Settings	• Cancel task • Disable method • Enable method • License method • Log event • Manage custom attributes • Settings
Network	• Assign network • Configure	• Assign network • Configure
Resource	• Assign virtual machine to resource pool	• Assign virtual machine to resource pool
Sessions	• Validate session	• Validate session
Tasks	• Create task • Update task	• Create task • Update task
vApp	• Export • vApp application configuration	• Export • vApp application configuration

Table 8 Minimum required vCenter user account privileges (page 2 of 2)

Setting	vCenter 5.1 required privileges	vCenter 5.0 required privileges
Virtual machine		
Configuration	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Disk change tracking • Disk Lease • Host USB device • Memory • Modify device setting • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual hardware • Extend virtual disk	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Disk change tracking • Disk Lease • Host USB device • Memory • Modify device setting • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual hardware • Extend virtual disk
Guest Operations	• Guest operation modifications • Guest operation program execution • Guest operation queries	• Guest operation modifications • Guest operation program execution • Guest operation queries
Interaction	• Console interaction • Guest operating system management by VIX API • Power off • Power on • Reset • VMware Tools install	• Acquire guest control ticket • Console interaction • Power off • Power on • Reset • VMware Tools install
Inventory	• Create new • Register • Remove • Unregister	• Create new • Register • Remove • Unregister
Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Mark as Template	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Mark as Template
Snapshot Management	• Create snapshot • Remove Snapshot • Revert to snapshot	
State		• Create snapshot • Remove Snapshot • Revert to snapshot

vSphere Client user accounts

Before you can use the vCenter user account with the EMC Backup and Recovery appliance, or before you can use the Single Sign-on (SSO) admin user with the EMC Backup and Recovery 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 EMC Backup and Recovery appliance. Table 8 on page 28 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.

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.**

4. On the left side of the page, click on the vCenter Servers, as shown in Figure 1 on page 30. It is important this be selected from the root level of the tree structure (represented under Hosts and Clusters). If you select the vCenter VM, the configuration fails.

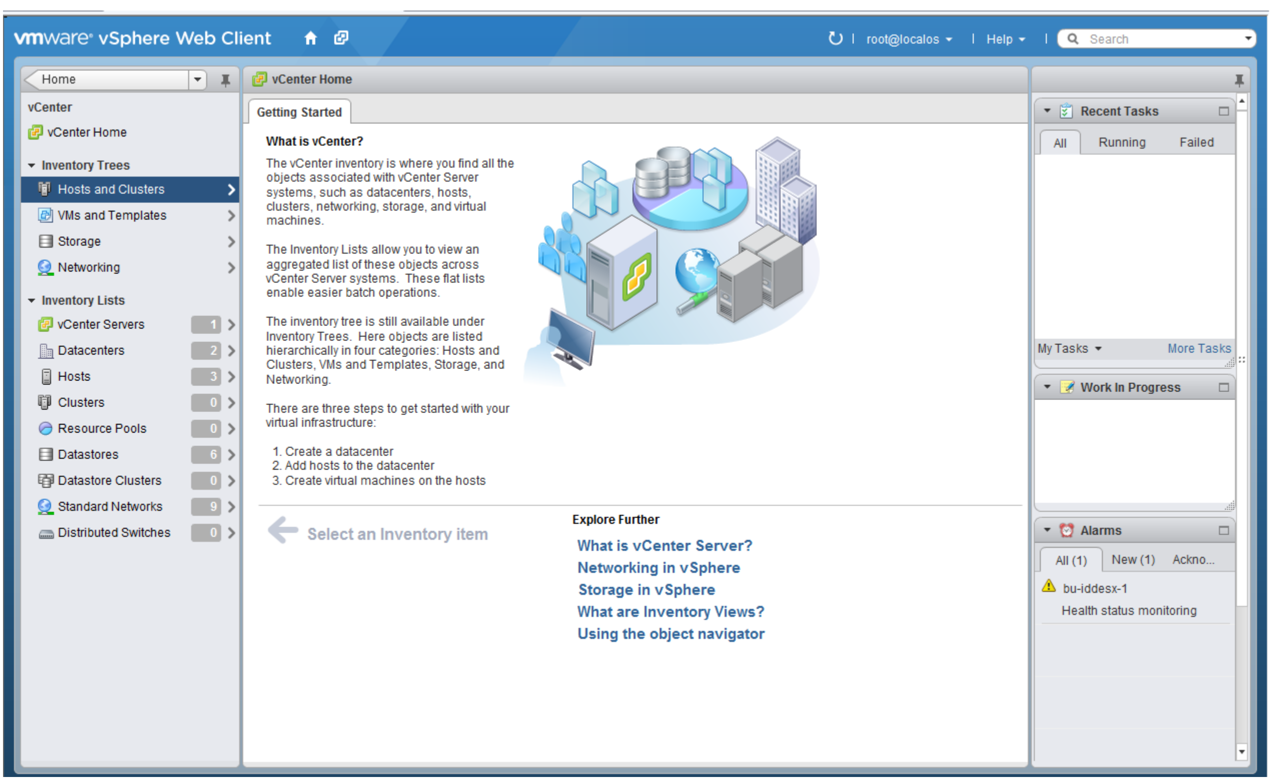


Figure 1 Selecting the vCenter server in the vSphere Web Client

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 displays.
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 displays in the format "SYSTEM-DOMAIN\admin" format. If the user name displays in the format "admin@SYSTEM-DOMAIN", then tasks related to the backup job may not appear in 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**.

Deploying the EMC Backup and Recovery appliance

This section describes how to download and deploy the EMC Backup and Recovery appliance to use NetWorker VMware Data Protection:

- "Downloading the OVAs for EMC Backup and Recovery" on page 31
- "Deploying the EMC Backup and Recovery appliance" on page 32
- "Upgrading the EMC Backup and Recovery appliance" on page 34

Downloading the OVAs for EMC Backup and Recovery

You can obtain the EMC Backup and Recovery 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. Only NetWorker 8.1 contains the OVA downloads.

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. Table 9 on page 32 provides recommendations on provisioning memory and swap space based on the storage space in use.

Table 9 Recommended memory and swap space based on storage space utilization

Utilization	Physical Memory	Swap Space
less than 25% (1.0 TB)	12 GB	16 GB
less than 65% (2.5 TB)	18 GB	16 GB
up to 100% (4.0 TB)	24 GB	16 GB

- 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.
- EBRUpgrade — download this ISO if you need to update the deployed EMC Backup and Recovery appliance to the latest version.

Other system requirements for the appliances are provided in "NetWorker VMware Protection requirements" on page 21. Download the desired OVA and place in shared storage.

Deploying the EMC Backup and Recovery 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.

To deploy the .ova:

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 Figure 2 on page 33.
4. In the filetype drop-down, select OVA Packages then navigate to the directory that contains the ova files. Select the file and then click **Open.**

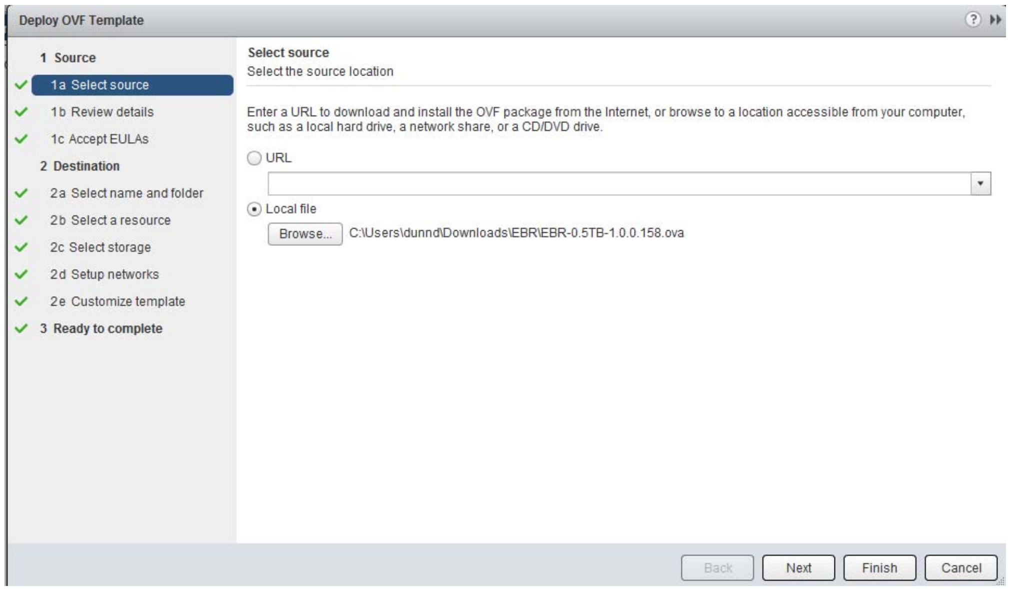


Figure 2 Selecting the OVA to deploy in vCenter/vSphere Web Client

5. On the **Deploy OVF Template** window, click **Next.**
6. In the **Review Details** window, click **Next.**
7. Accept the EULA and click **Next.**
8. Specify a name for the EMC Backup and Recovery 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 EMC Backup and Recovery 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.**

After a few minutes a screen similar to Figure 3 on page 34 appears in the console of the EMC Backup and Recovery appliance in vCenter.

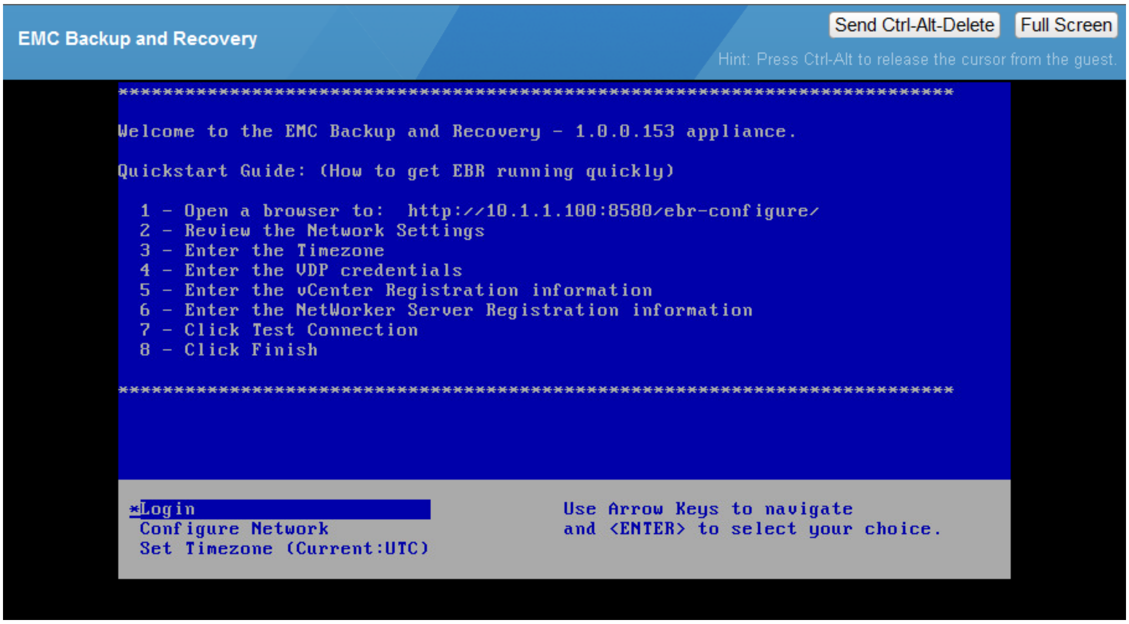


Figure 3 EMC Backup and Recovery appliance registration screen

Upgrading the EMC Backup and Recovery appliance

To upgrade the EMC Backup and Recovery appliance, perform the following steps:

1. Create and validate a checkpoint of the existing EMC Backup and Recovery appliance by running an integrity check:

   a. Navigate to the **Configuration** tab.

   b. Select the **Run integrity Check** option, as shown in Figure 33 on page 79.

2. Shut down the EMC Backup and Recovery 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 Figure 4 on page 34.

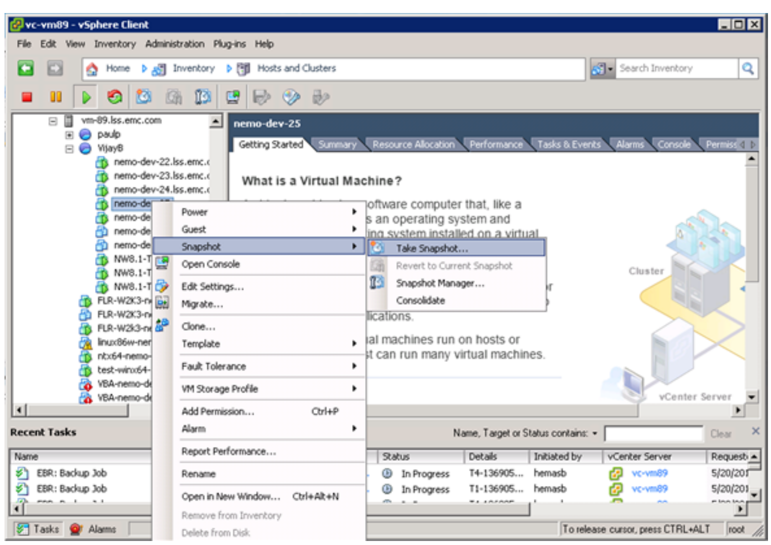


Figure 4 Take Snapshot in vSphere Client

3. Restart the appliance.
4. Attach the ISO to the EMC Backup and Recovery appliance by selecting **Connect to ISO image on local disk** in the vSphere Client, as shown in Figure 4 on page 34.

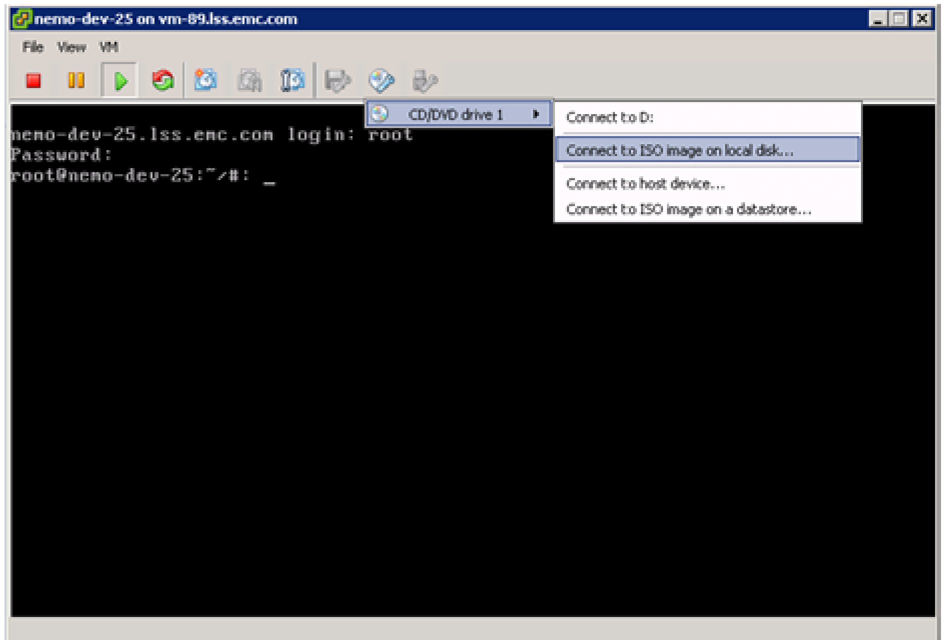


Figure 5 Connect to ISO in vSphere Client

5. Open the **EMC Backup and Recovery Configure** window. The section "Post-Installation configuration in the EMC Backup and Recovery Configure window" on page 44 provides information about the **EMC Backup and Recovery Configure** window.
6. Navigate to the **Upgrade** tab and click **Check Upgrades**. The available upgrade package appears.
7. Navigate to the **Status** tab to ensure all services are running.
8. Return to the **Upgrade** tab and click **Upgrade EBR**.
9. When the upgrade completes, the EMC Backup and Recovery appliance shuts down automatically.
10. Return to the vSphere Client to delete the snapshot taken in Step 2 on page 34.
11. Right-click the VM or container and select **Edit Settings...**.
12. Mark all the hard disks as **persistent-independent**.
13. Power on the EMC Backup and Recovery appliance.

When you open the **EMC Backup and Recovery** user interface in the vSphere Web Client and navigate to the **Configuration** tab, the new version displays.

NOTICE

Note that you cannot upgrade external proxies. If using a previous version of the external proxy and you want to upgrade, you must redeploy the external proxy.

If you deployed an external proxy prior to upgrading the EMC Backup and Recovery appliance, restart all external proxy VMs.

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 proxy OVA described in the section “Deploying the EMC Backup and Recovery appliance” on page 31 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. You assign a proxy for 1 backup or 1 recover of a VM at a point in time.

Selection of a Proxy for backup or recovery

EMC Backup and Recovery selects a proxy from the proxy pool based on its availability and periodically refreshes the Proxy to datastore association. If a Proxy is available and has access to the datastore of the VM that you want to back up, then the Proxy uses hotadd mode. If a Proxy is available but does not have access to the datastore of the VM that you want to back up, then the Proxy uses NBD mode, which is over LAN and typically slower than hotadd mode.

Note: Currently, the number of hotadd sessions that an external Proxy can establish depends on the total number of the VMDKs present on all the VMs being backed up. For example, a Proxy with one controller can only support 12 hotadd sessions, and if there are more than 12 VMDKs being backed up, then the proxy will fallback to nbd mode for the remaining VMDKs. This may lead to degraded backup performance.

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 that the VM runs on.
- 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.

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 this will result in the backup failing with an error indicating “No Proxy.”

To configure this mode of operation, perform the following steps from the Console on the EMC Backup and Recovery appliance:

1. Navigate to the /usr/local/vdr/etc directory.
2. Edit the vcenterinfo.cfg file by adding the following entry:

```
proxy-datastore-updater=local
```

3. Run emwebapp.sh --restart.

The external proxy has 2 SCSI controllers, and each SCSI controller allows a maximum 12 hotadd mode backups of disks (VMDKs). Therefore, the maximum hotadd mode backups of virtual disks per external proxy is limited to 24. Any backup operations that exceed this number will result in the backup falling back to nbd transport mode.

NetWorker backs up each virtual disk from the VM sequentially when the VM has more than 2 VMDK files. However, if you leverage CBT, backup speed increases with very little or no change rate of data on VMs.

Deploying external proxies

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 37, 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.

Deploy external proxy appliance in vCenter

Deploy the proxy appliance in the vCenter as follows:

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 EMC Backup and Recovery proxy OVA file that was previously downloaded in “Downloading the OVAs for EMC Backup and Recovery” on page 31.

   d. Select the 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 VM on which the proxy runs. This is also the name managed and visible within vCenter.

      – The DNS name assigned to the proxy VM.

      – The EMC Backup and Recovery appliance hostname after the proxy registers and activates with the server.

      NOTICE

      In order to avoid confusion and potential problems, 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 **Networking Properties** 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 the settings you type the correct settings in the **Networking Properties** 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 the EMC Backup and Recovery appliance is deployed, navigate to the console of the VM in the vSphere client.

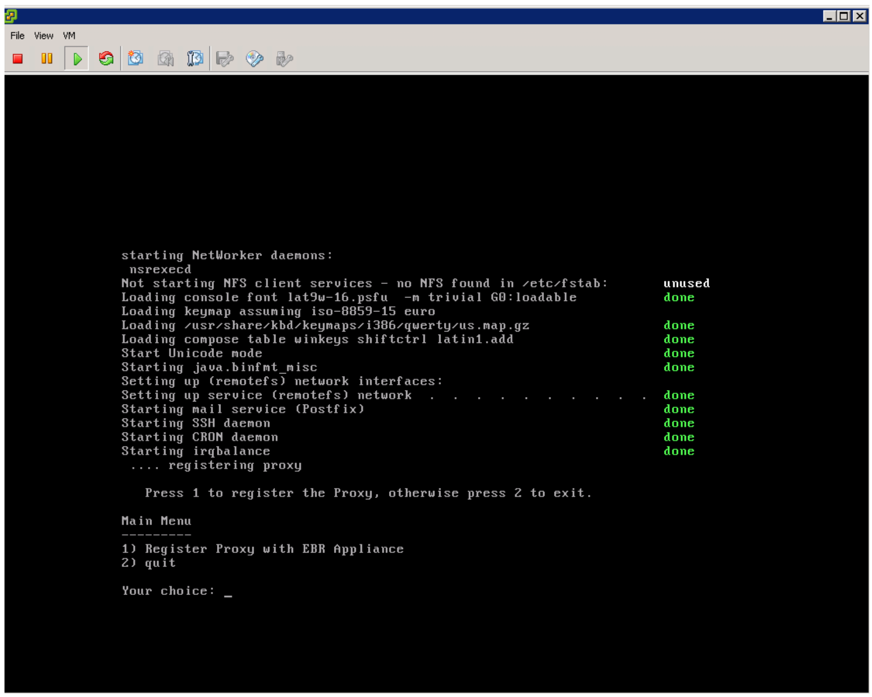


Figure 6 Registering proxy with EMC Backup and Recovery appliance

Follow the prompts to register the proxy, as shown in Figure 6 on page 40:

1. Press **1** to register the proxy.
2. At the **Enter the EMC Backup and Recovery Appliance address** prompt, type the FQDN of the EMC Backup and Recovery appliance server name.
3. At the **Enter the server domain [clients]:** prompt, press **enter** and do not modify.
4. Provide the EMC Backup and Recovery appliance password if using a non-default password.

   Wait for the **Attempting to connect to the EMC Backup and Recovery Appliance...Connection successful** message.

5. Validate the registration in NMC by ensuring that the external proxy host appears under the external proxy hosts column of the associated/linked proxy, as shown in Figure 7 on page 41.

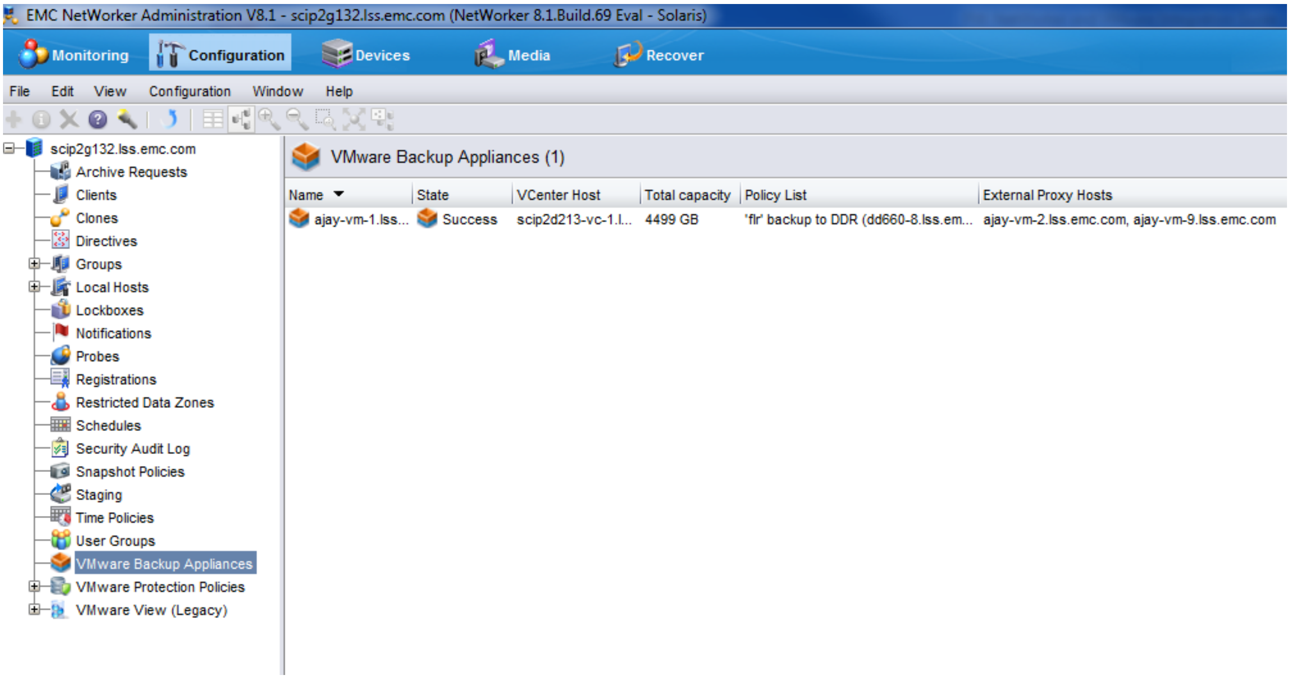


Figure 7 External proxy hosts in NMC

NOTICE

If you upgrade or reboot the EMC Backup and Recovery appliance after deploying an external proxy, restart all external proxy VMs.

Re-registering the proxy with a different server

To re-register the proxy with a different server:

1. Launch the Console, then log in to the proxy.
2. Run the following command:

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

EMC Backup and Recovery Configure window setup

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

1. Open an internet browser and type the URL to connect to the EMC Backup and Recovery appliance. The URL will be similar to the following:

   `http://`*`EMC Backup and Recovery appliance FQDN`*`:8580/ebr-configure`

   When connected, the **EMC Backup and Recovery Configure** window displays, as shown in Figure 8 on page 42.

Figure 8 EMC Backup and Recovery Configure window's Welcome page

NOTICE

The **EMC Backup and Recovery Configure** window requires Adobe Flash player. If you do not have the appropriate version of Adobe Flash Player installed, a message displays 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 EMC Backup and Recovery 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. The defaults are:
   - 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 vCenter appliance in the Configuration tab, then click **Test connection.** Ensure that **Use the FQDN of the vCenter server for the SSO** remains selected as shown in Figure 9 on page 43. Click **Next.**

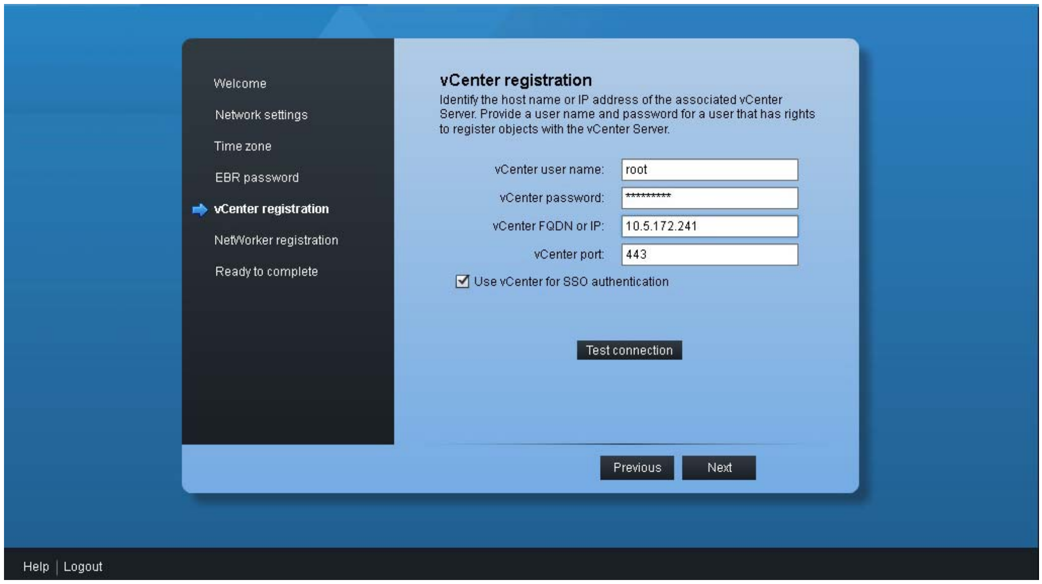


Figure 9 EMC Backup and Recovery Configure window during registration

---

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.

---

8. 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**.

   ---

9. Click Test NetWorker connection to test the connection. If performing a disaster recover, select the **Override NetWorker registration** option if the EMC Backup and Recovery appliance has registered to the NetWorker server.

10. Click **Finish.** A message appears indicating that configuration is complete and the EMC Backup and Recovery appliance will reboot.

Once the reboot completes, allow up to one hour for the deployed EMC Backup and Recovery appliance (displayed as 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 EMC Backup and Recovery appliance/VMware Backup Appliance in NetWorker:

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.

When you open the **EMC Backup and Recovery Configure** window after registration, the window in Figure 10 on page 44 displays, allowing you to verify information about your configuration and to ensure the required services are running.

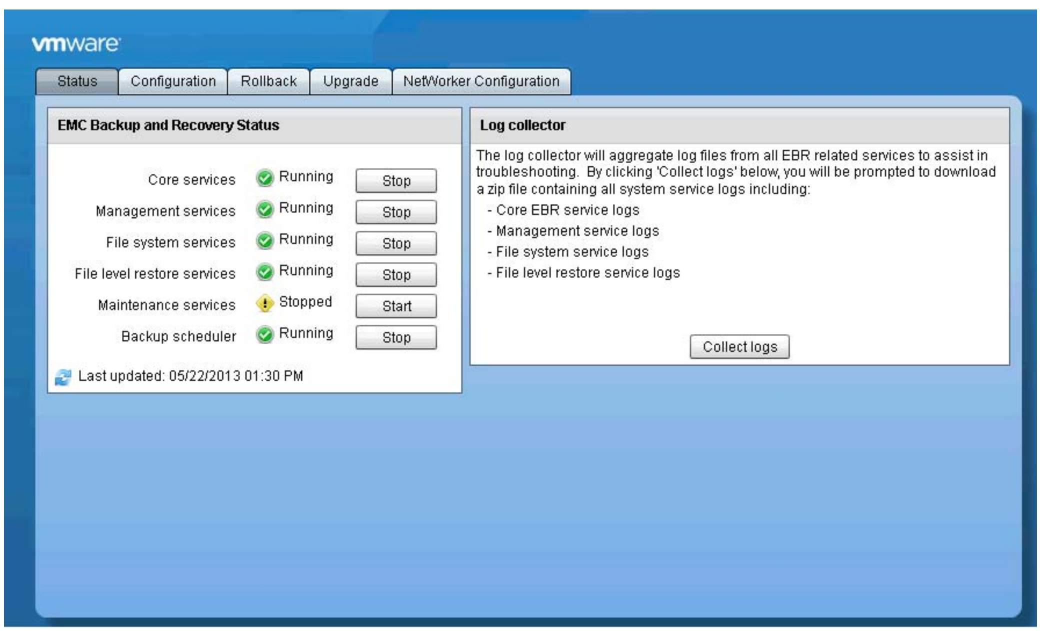


Figure 10 EMC Backup and Recovery Configure window after registration

EMC Backup and Recovery Status

The **Status** tab lists all of the services required by EMC Backup and Recovery and the current status of each service. Table 10 on page 45 describes these services.

Table 10 Description of services running on the EMC Backup and Recovery 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. You can make changes to the default maintenance window by using the command line. The section "Changing the Maintenance window" on page 47 provides more information. **Note:** 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.

EMC Backup and Recovery displays one of the following statuses for a service:

- Starting
- Start Failed
- Running
- Stopping
- Stop Failed
- Stopped
- Loading-getting state
- Unrecoverable (Core services only)
- Restoring (Management services only)
- Restore Failed (Management services only)

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

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.

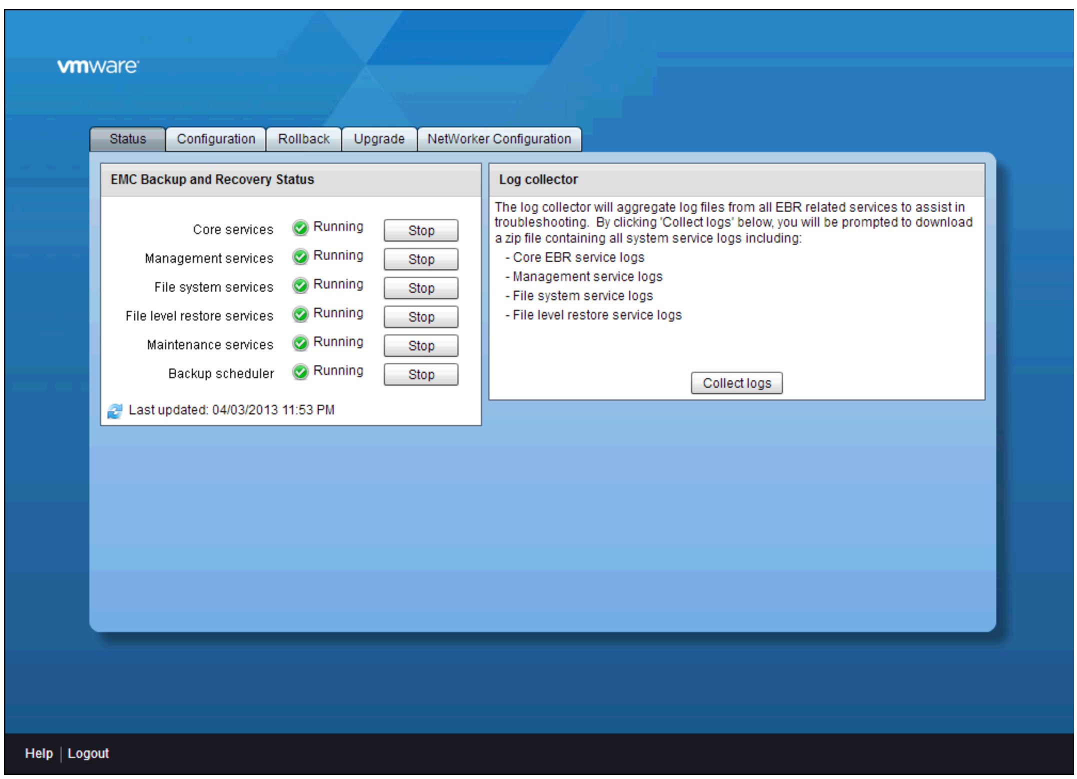


Figure 11 Collecting log files in the EMC Backup and Recovery Configure window

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):

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 VMs using NMC and the EMC Backup and Recovery plug-in

After a successful deployment, use the following two applications to set up and perform VM backups:

- "VMware Backup Appliance in the NetWorker Management Console" on page 48
- "EMC Backup and Recovery plug-in for vCenter" on page 57

VMware Backup Appliance in the NetWorker Management Console

NMC is the user interface for the NetWorker Console server, which manages all NetWorker servers and clients and provides reporting and monitoring capabilities for all NetWorker servers and clients.

NMC runs from any computer that has a supported web browser and Java Runtime Environment (JRE). The *NetWorker Installation Guide* provides information on supported web browsers and supported versions of the JRE.

The interface for NMC consists of two main windows:

- Console window
- Administration window

When you connect to the NMC server, the Console window appears as shown in Figure 12 on page 48.

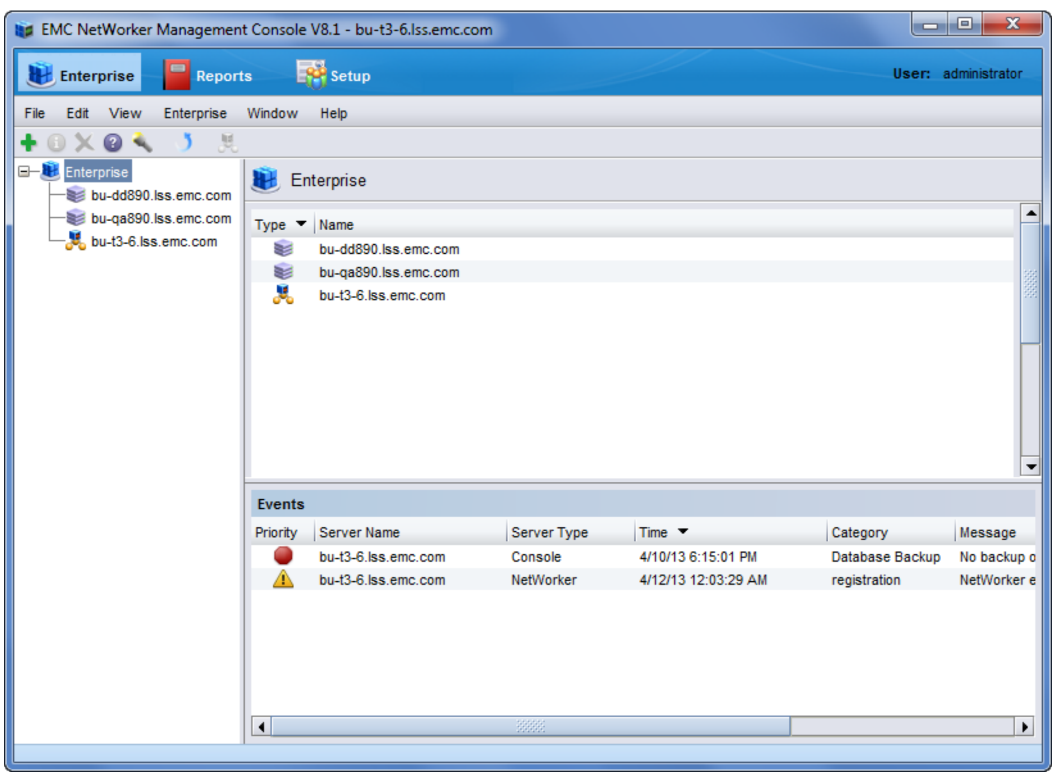


Figure 12 Console window

The **Console** window is the first point of access for NetWorker tasks. To manage and monitor a NetWorker server and clients:

1. Select the **Enterprise** button, then select a NetWorker server in the left pane.
2. Right-click on the server in the left pane of the Console window, and select **Launch Application**. The **Administration** window displays.
3. Select the **Configuration** tab. Figure 13 on page 49 displays.

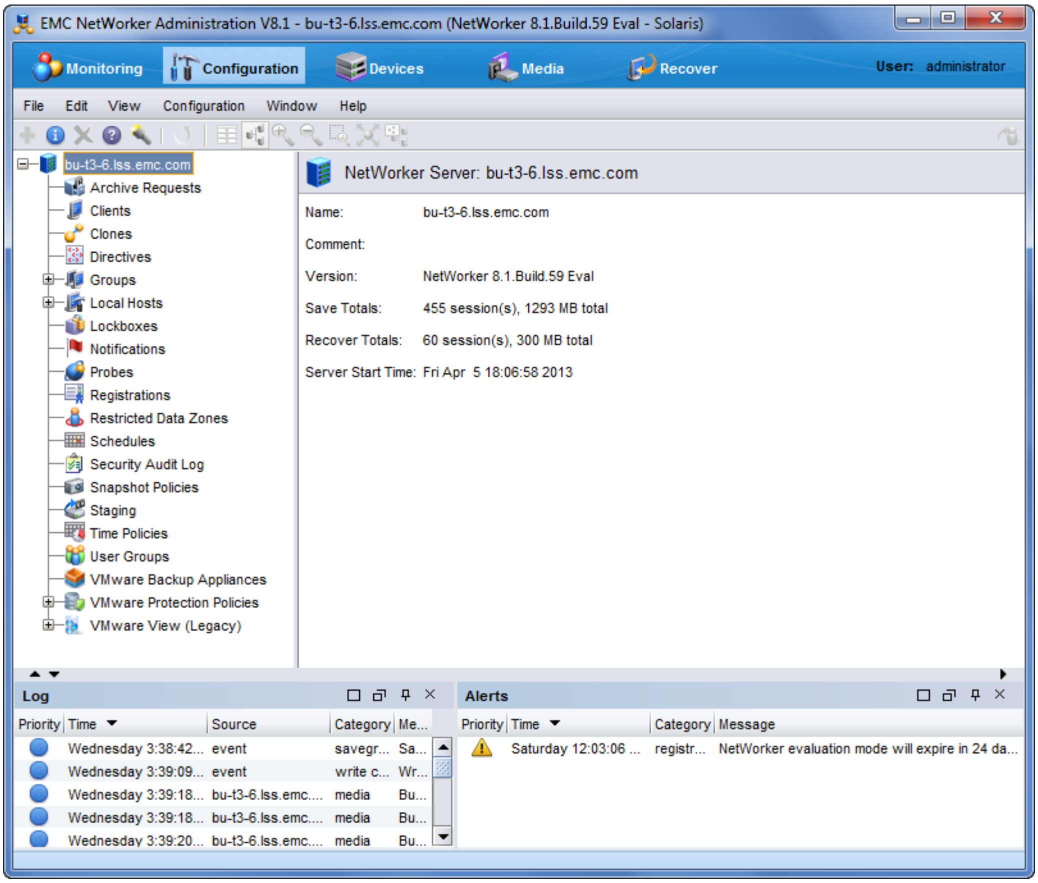


Figure 13 Configuration tab in the NMC Administration window

Two resource groups appear in the lower part of the left pane:

- VMware Backup Appliance — displays the registered VMware Backup Appliance(s)
- VMware Protection Policies — displays the default policy after NetWorker registers the first VMware Backup Appliance. NetWorker creates this default VMware protection policy and automatically assigns this policy to the appliance. Figure 14 on page 50 displays the Default VMware Protection policy.

Additionally, a new resource appears in the Devices window. 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.

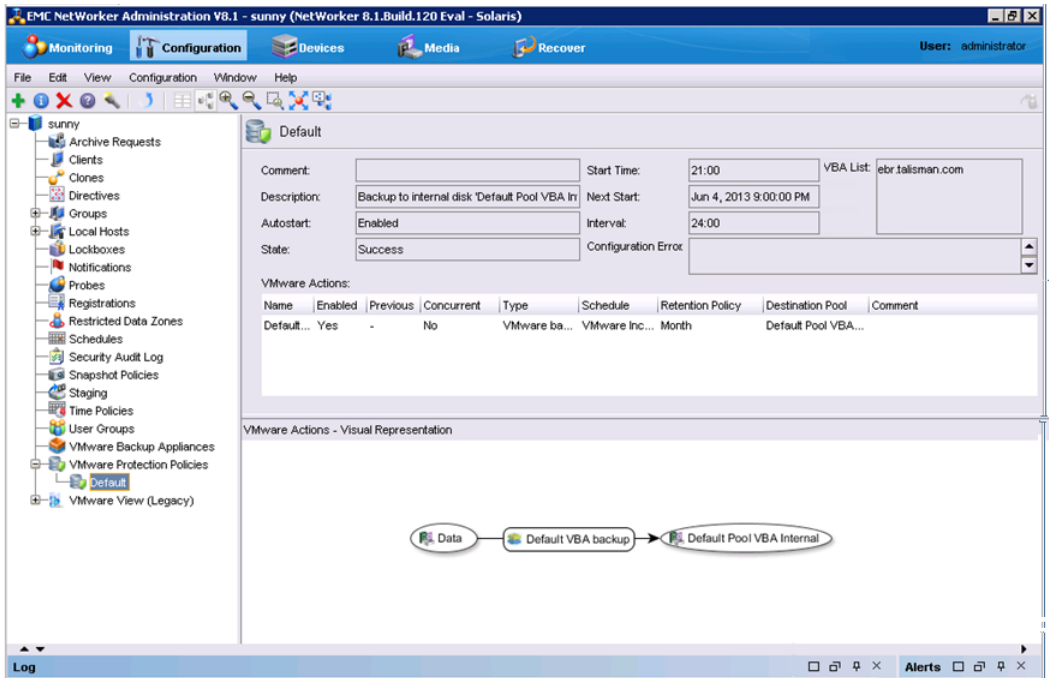


Figure 14 Default VMware Protection Policy in NMC

NetWorker enables the Default policy to run once every 24 hours starting at 21:00. The backup level used is determined by the levels defined in the Default schedule, and uses a one month data retention policy.

To add VMs to the protection policy, you do not create new client instances for each VM. Instead, you assign VMs to the VMware Protection Policies by using the EMC Backup and Recovery plug-in for the vSphere Web Client. The section "EMC Backup and Recovery plug-in for vCenter" on page 57 provides information. If you want to create new policies or modify the existing policy, continue with this section.

Note: If you do not add VMs to the policy, the backup runs as scheduled but without any contents.

Setup and configure policies

NetWorker automatically creates a policy named "Default" in NetWorker when you register the first VMware Backup Appliance. NetWorker applies this policy to all registered VMware Backup Appliances, and saves the backups created by this policy on the internal storage of the appliance.

You may require multiple policies to back up VMs. 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:

1. In the **Configuration** tab of the NMC **Administration** window, right-click **VMware Protection Policies** in the left pane and select **New**, as in Figure 15 on page 51.

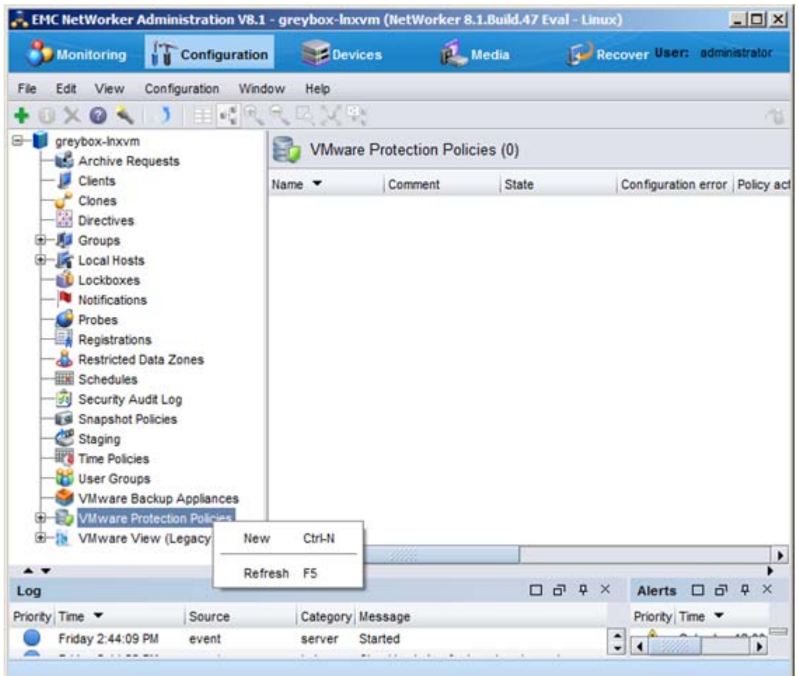


Figure 15 Create new policy in NMC

2. In 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 Figure 16 on page 51, a policy named **BackuptoDDRAndClone** is being created to backup and clone VMs to a Data Domain system.

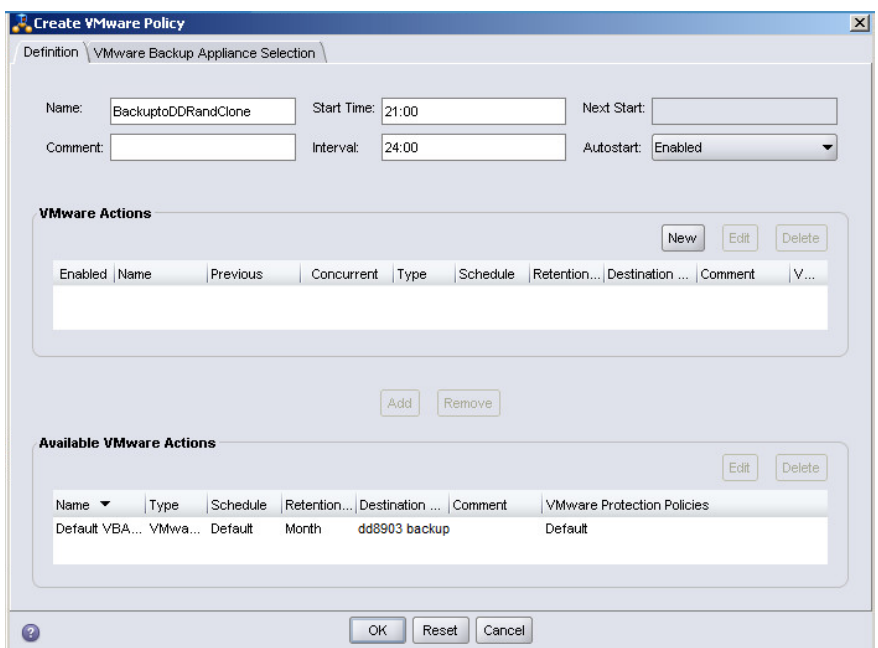


Figure 16 Create VMware policy window

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. Figure 17 on page 52 displays.

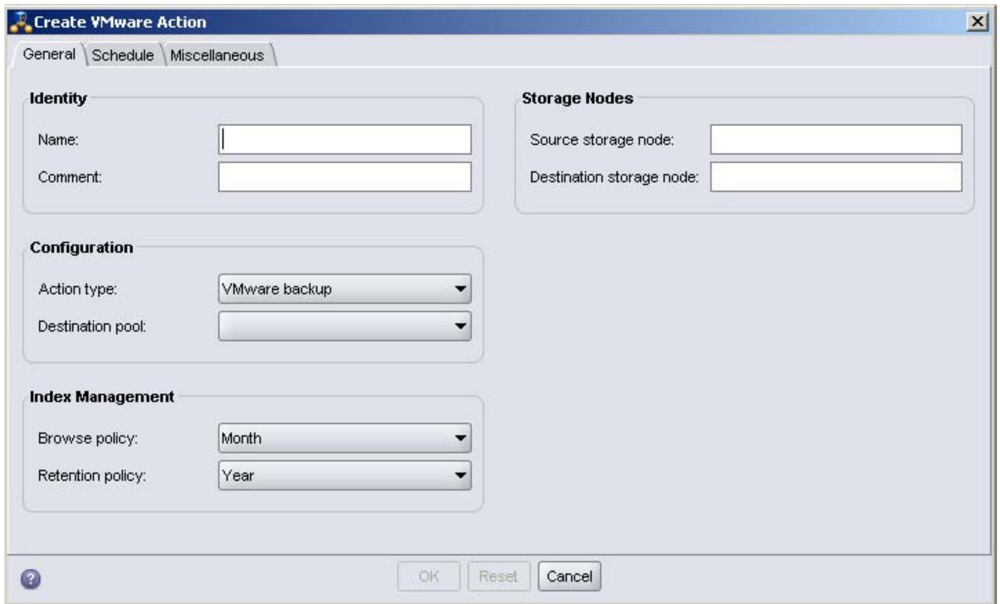


Figure 17 Create VMware Action window

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 *NetWorker 8.1 and Service Packs 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.

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. 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, since you cannot clone a backup to Default Pool VBA Internal.

   d. Select a browse and retention policy for Index Management, or use the default values.

   e. In 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: 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 in the **VMware Backup Appliance Selection** tab, as shown in Figure 18 on page 54, and then click **OK**.

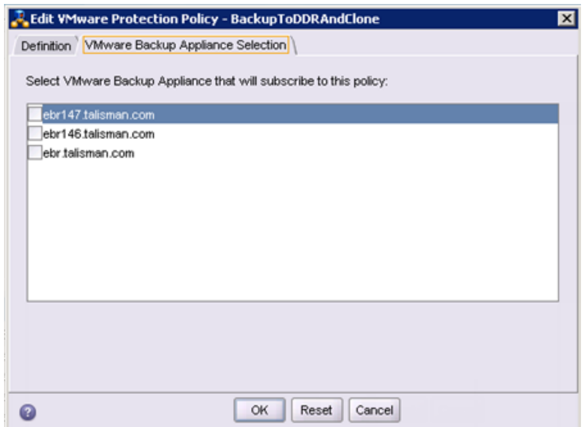


Figure 18 Select a VMware Backup Appliance in the Create/Edit VMware Protection Policy window

---

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.

When you complete these steps, Figure 19 on page 54 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.

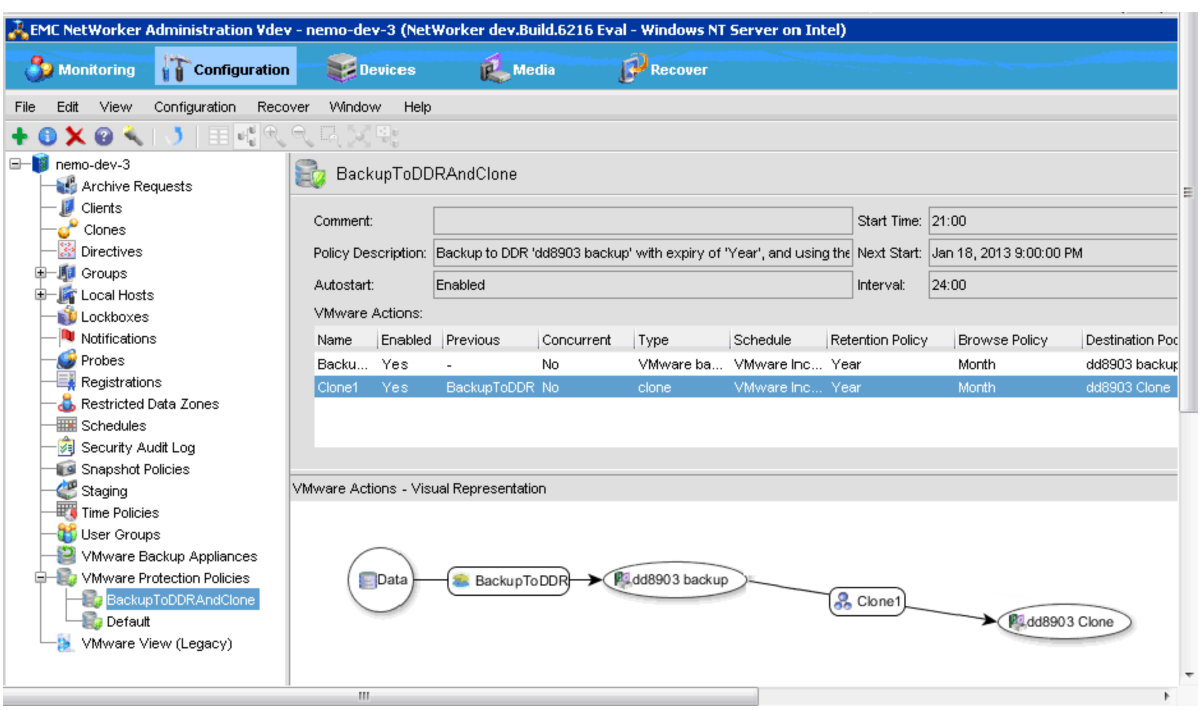


Figure 19 VMware Protection policy with associated actions

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:

1. Open the Create VMware Policy or Edit VMware Protection Policy window.
2. Select the appropriate checkboxes under the **Definition** tab, as shown in Figure 20 on page 55.

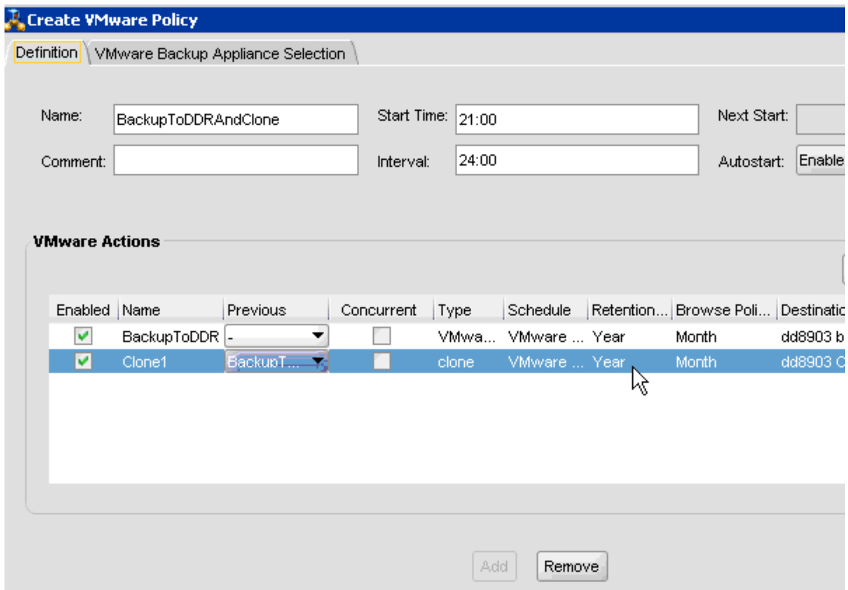


Figure 20 Enable and mark actions concurrent in Create VMware Policy window

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.

Note: Although you cannot use NetWorker to assign policies to specific VMs, you can assign a policy created in NMC to specific VMs in the vSphere Web Client interface. "Assigning VMs to a policy" on page 65 provides more information.

Starting the policy manually

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 the **Start** option. Otherwise, wait for NetWorker to start the backup policy based on the scheduled start time.

Viewing policy progress

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 in the Reports tab of the NMC Administration window by selecting **NetWorker Data Protection Policy** reports.

Stopping the policy from NMC

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.

VMware Backup Appliance health in NMC

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

You can monitor the state (offline/online) of the VMware Backup Appliance from NMC as shown in Figure 21 on page 56. To view more VMware Backup Appliance related properties, right-click on the appliance server resource and select **Properties**.

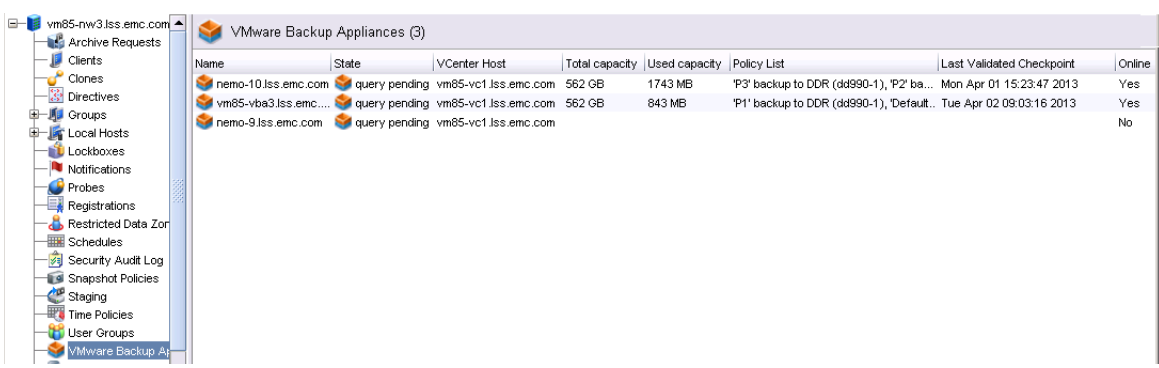


Figure 21 VMware Backup Appliance health monitoring in NMC

Decommissioning the VMware Backup Appliance

NMC includes the option to decommission a VMware Backup Appliance when problems occur. To decommission the appliance, right-click the appliance and select **Decommission** from the drop-down. The dialog shown in Figure 22 on page 57 displays.

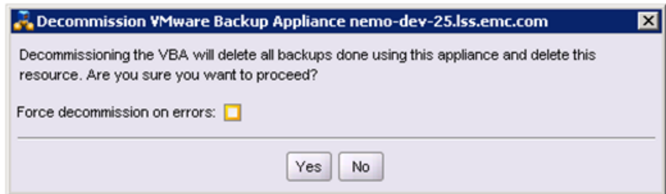


Figure 22 Decommissioning the VMware Backup Appliance in NMC

EMC Backup and Recovery plug-in for vCenter

The vSphere Web Client provides access to the **EMC Backup and Recovery** plug-in **user interface**. The **EMC Backup and Recovery plug-in** user interface functions as a plug-in within the vSphere Web Client to connect to the EMC Backup and Recovery appliance for VM backup storage. You can only manage EMC Backup and Recovery through the vSphere Web Client. Deduplication is automatically performed with every backup operation.

Note: You cannot use the EMC Backup and Recovery appliance without a vCenter Server. In linked mode, the EMC Backup and Recovery appliance works only with the vCenter to which it is associated.

Benefits of EMC Backup and Recovery

EMC Backup and Recovery provides the following benefits:

- Provides fast and efficient data protection for all of your VMs, even those powered off or migrated between ESX hosts.
- Significantly reduces disk space consumed by backup data by using patented variable-length deduplication across all backups.
- 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.

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

Accessing EMC Backup and Recovery in the vSphere Web Client

The **EMC Backup and Recovery plug-in** user interface appears in the vSphere Web Client and allows you to add VMs to the policies created in NMC. To access the **EMC Backup and Recovery plug-in** user interface in the vSphere Web Client:

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 a Backup Appliance from the drop-down. The drop-down lists all the EMC Backup and Recovery appliances registered in the vCenter.

Each vCenter Server supports up to 10 EMC Backup and Recovery appliances. The **Backup Appliances** field, as shown in Figure 23 on page 59, displays the appliance names alphabetically in a drop-down list.

In the **EMC Backup and Recovery plug-in** 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.

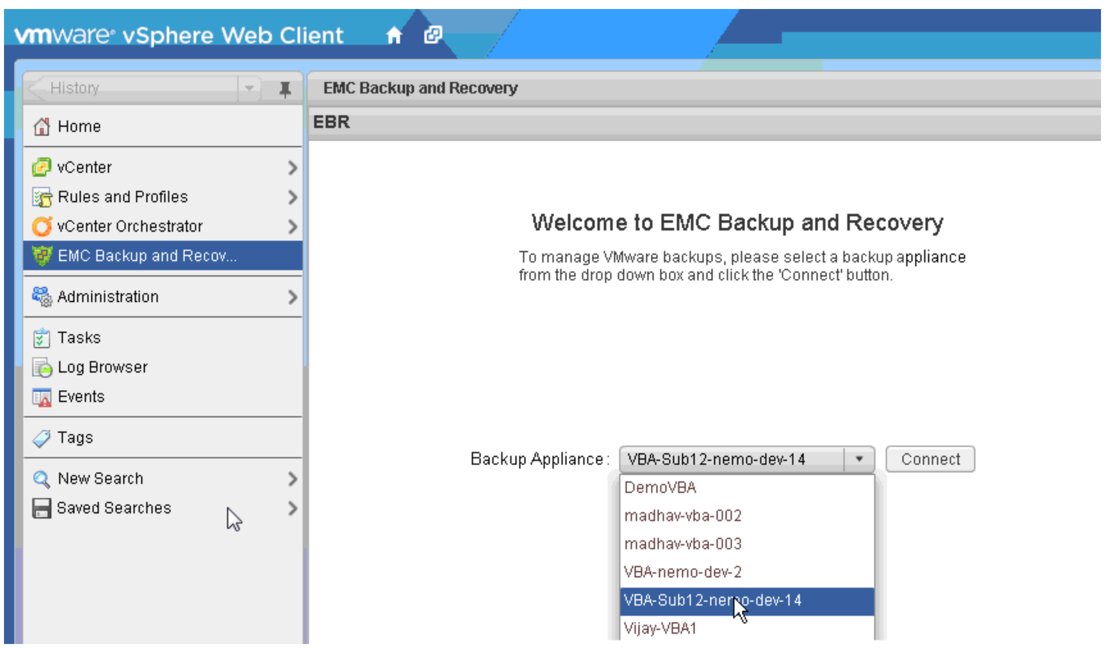


Figure 23 Selecting the Backup Appliance

5. Click **Connect**.

Note: The maximum retry attempts for the EMC Backup and Recovery appliance to connect to vCenter is two. Further attempts to connect to vCenter require you to restart the EMC Backup and Recovery server by typing the following command:

ebrserver.pl --restart.

Once connected, Figure 24 on page 60 displays.

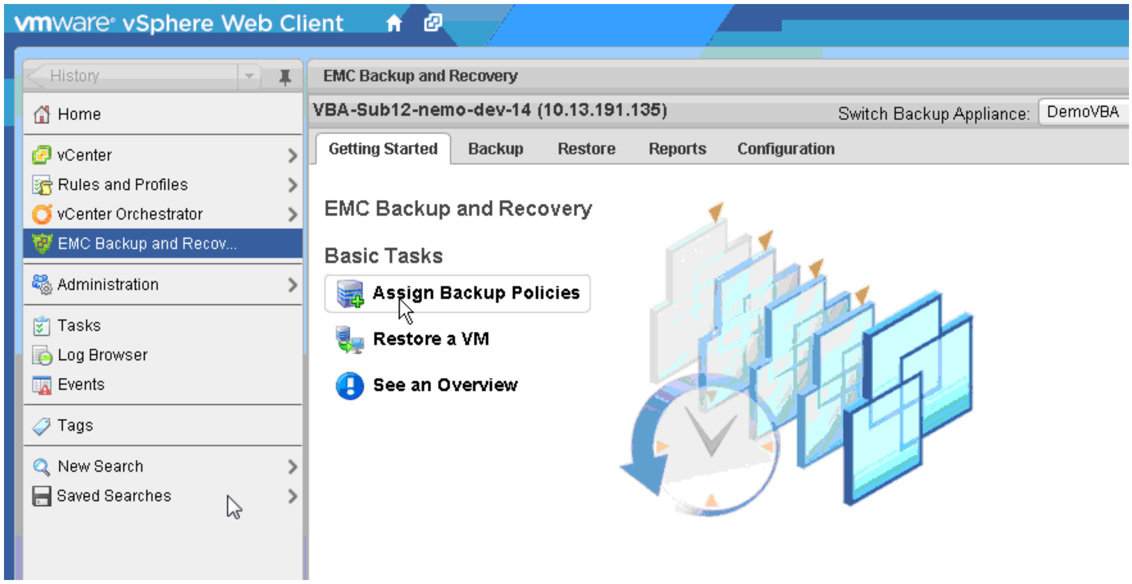


Figure 24 EMC Backup and Recovery plug-in user interface in the vSphere Web Client

The **EMC Backup and Recovery plug-in** user interface allows you to configure and manage the EMC Backup and Recovery appliance. The **EMC Backup and Recovery plug-in** user interface consists of five tabs:

- **Getting Started** — provides an overview of EMC Backup and Recovery functionality and 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 backup policy created in NMC. This window enables users to add VMs to protect to the backup policies, and to run backup policies on demand. "About the Backup Tab" on page 61 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 62 provides additional information.
- **Reports** — provides backup status reports for the VMs on the vCenter Server that you added to the backup policy. "About the Reports Tab" on page 62 provides additional information.
- **Configuration** — displays EMC Backup and Recovery 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 62 provides additional information.

The following sections describe the contents of the tabs.

About the Backup Tab

The Backup tab displays a tabular list of backup policies you deployed to this EMC Backup and Recovery appliance. The table contains the following information.

Table 11 Backup tab column descriptions

Column	Description
Name	The name of the backup policy.
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.

Figure 25 on page 61 displays two example backup policies.

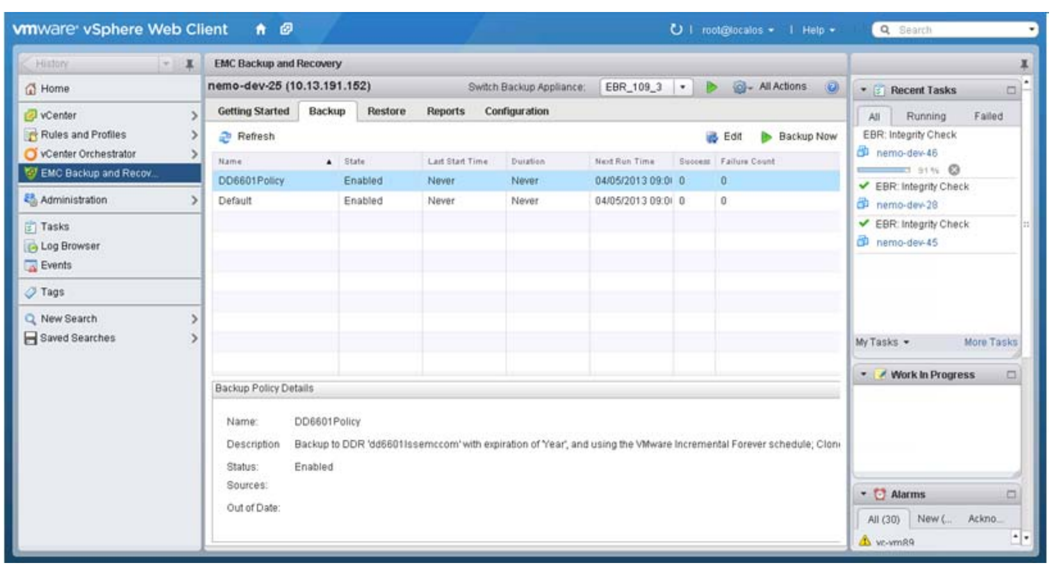


Figure 25 Backup policies in the EMC Backup and Recovery plug-in user interface in the vSphere Web Client

About the Restore Tab

The **Restore** tab displays a list of VMs that you backed up by using the EMC Backup and Recovery 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 VM backups" on page 68.

About the Reports Tab

The top half of the **Reports** tab lists each of the VMs associated with the vCenter Server. For each VM, you can view the following information:

- VM name
- State (EMC Backup and Recovery uses standard VMware state information).
- Backup Policies
- Last Successful Backup
- Status
- Date
- Backup Policy Name

From the bottom section of the **Reports** tab, you can select a VM and view detailed information about the selected client, which includes:

- VM Information
  - Name
  - Guest OS
  - Host
  - IP Address
  - State
  - Last Successful Backup
  - Backup Policies (associated with the selected VM)
- Last Backup Policy
  - Status
  - Date
  - Backup Policy

The left pane of 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 EMC Backup and Recovery appliance. You can perform the following tasks on this tab:

- "Viewing backup appliance configuration" on page 63
- "Configuring Email" on page 63

- "Viewing the Log" on page 65

Viewing backup appliance configuration

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

Backup Appliance Details include:

- Display name
- IP Address
- Status
- vCenter Server
- NetWorker Server
- Local time
- Current user
- Version
- Time zone

You can configure these options during the EMC Backup and Recovery 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 44 provides additional details.

Configuring Email

You can configure EMC Backup and Recovery to send SMTP email reports to specified recipients. When you enable email notification, the email includes the following information:

- EMC Backup and Recovery appliance status
- Backup jobs summary
- Virtual machines summary

Email configuration requires the information defined in the following table.

Table 12 Email configuration fields (page 1 of 2)

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 EMC Backup and Recovery appliance needs to be able to resolve the name entered. The default port for non-authenticated email servers is 25. The default port of authenticated mail servers is 587. You can specify a different port by appending a port number to the server name. For example, to specify the use of port 8025 on server "emailserver" enter: emailserver:8025
My server requires me to log in	Check this box if your SMTP server requires authentication.

Table 12 Email configuration fields (page 2 of 2)

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.

To configure email:

1. From the **EMC Backup and Recovery plug-in** 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.

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, shown in Figure 26 on page 65.

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.

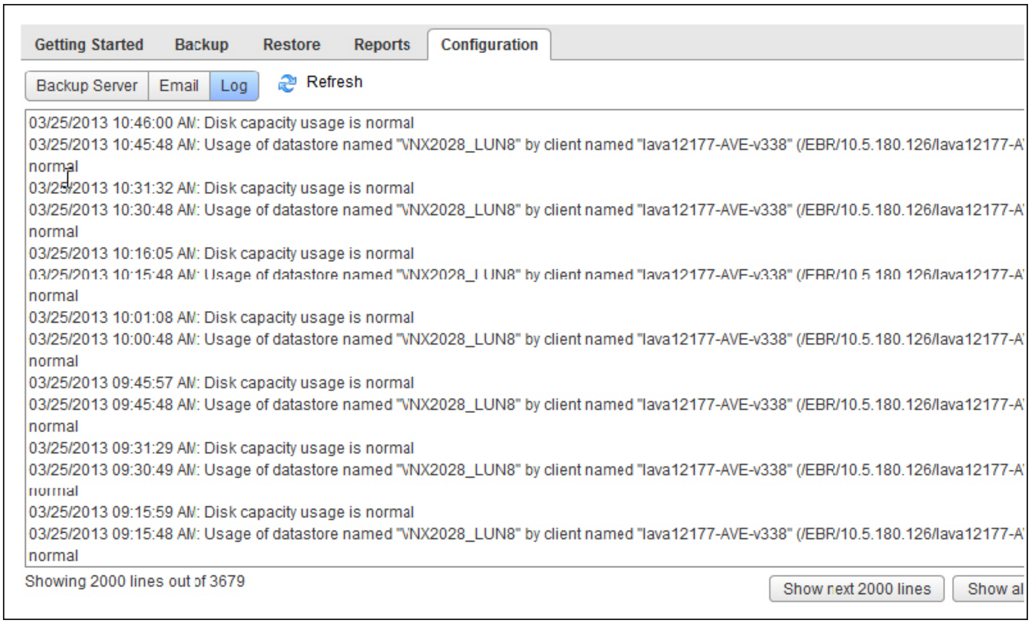


Figure 26 Viewing the log in the Configuration tab

Assigning VMs to a policy

You can assign a VM to a policy by using the **EMC Backup and Recovery plug-in** user interface in the vSphere web client:

1. Select **EMC Backup and Recovery** in the vSphere Web Client.

1. On the **Getting Started** tab, select **Assign Backup Policies**. The **Backup** tab displays, which shows the available policies.

   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 EMC Backup and Recovery appliance. When you perform backups to the internal storage of an EMC Backup and Recovery appliance, these details appear in NMC and as part of the policy description in EMC Backup and Recovery in vCenter.

2. Click **Edit**. All the VMs in the vCenter display.

3. Use the checkboxes next to the VMs to select the VMs that you want to include in the selected policy, as shown in Figure 27 on page 66. You can also select other inventory objects such as Resource Pools or Clusters in addition to specific VMs.

Note: You can only assign VMs to the policies that you create in NMC.

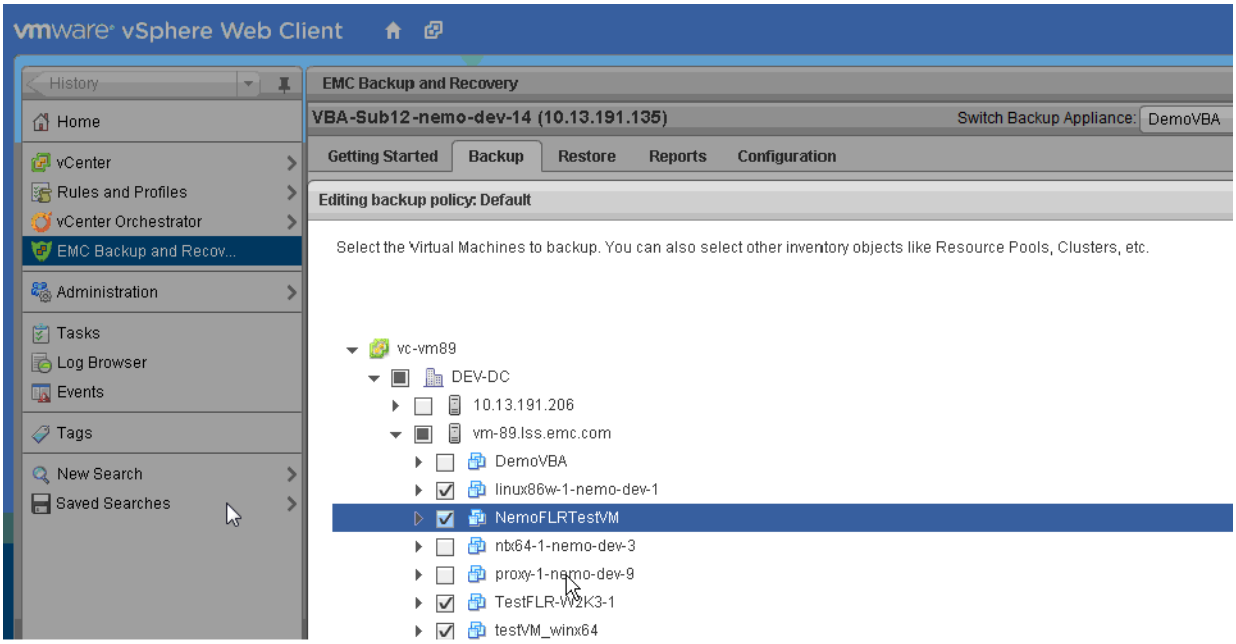


Figure 27 Selecting VMs for backup

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

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 under the **Sources** field.

Manually starting the backup policy

You can manually start the backup policy in the **EMC Backup and Recovery plug-in** user interface in one of the following ways:

- Click the **Backup Now** button in the **EMC Backup and Recovery plug-in** user interface's **Backup** tab
- Right-click individual VMs in vCenter and select **Backup Now.** Clicking **Backup Now** provides two options:
  - Backup all sources
  - Backup only out of date sources

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

Note: When you start the policy from the **EMC Backup and Recovery plug-in** user interface in the vSphere Web Client, the clone actions associated with the policies will not run. Only when you run the policies from NetWorker (NMC) will the clone actions also run.

Stopping a policy

To stop a policy in the **EMC Backup and Recovery plug-in** user interface:

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

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 Figure 28 on page 67.

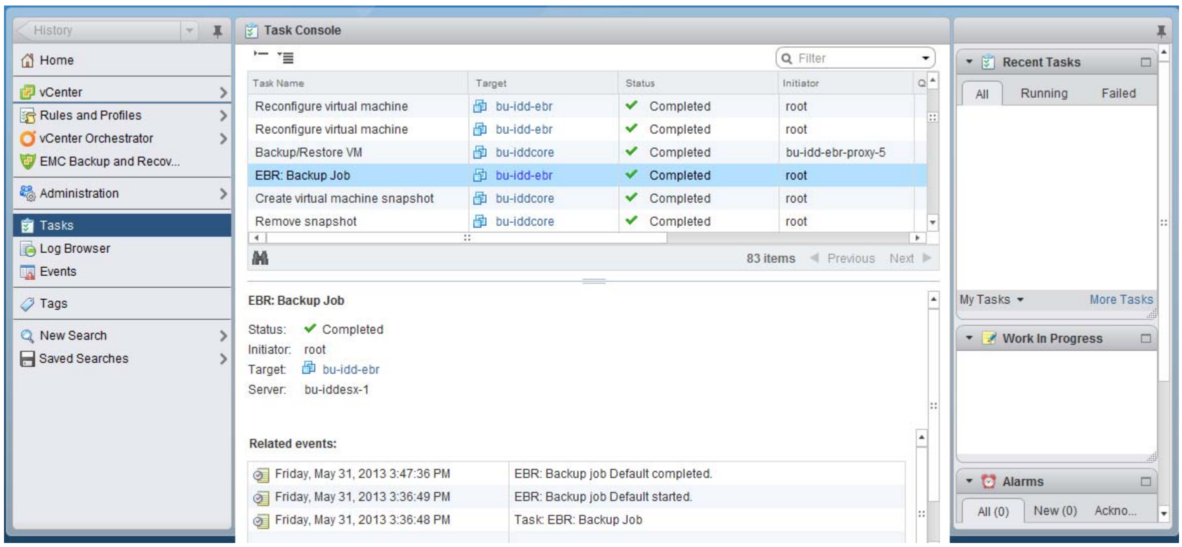


Figure 28 Viewing policy progress in the Task Console

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.

Choosing the VMs

You can specify collections of VMs, such as all VMs in a datacenter or select individual VMs. If an entire resource pool, host, datacenter, or folder is selected, 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 manually select a VM to be backed up, which ensures that NetWorker backs up the VM, even when you move the VM.

EMC Backup and Recovery will not back up the following specialized VMs:

- EMC Backup and Recovery appliances
- VMware Data Protection (VDP) Appliances
- Templates
- Secondary fault tolerant nodes
- Proxies
- Avamar Virtual Edition (AVE) Servers

Note: The Wizard will let you select these VMs; however, when you click **Finish** the Wizard displays a warning that the job does not contain these special VMs.

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.

Restoring VM backups

NetWorker offers two levels of restore functionality:

- Image-level restore — restores an entire backup image or selected drives to the original VM, another existing VM, or a new VM.
- File-level restore — restores specific folders or files from an image backup.

The following section provides details about both types.

Guidelines for performing image-level restores versus file-level restores

EMC Backup and Recovery provides two distinct mechanisms to restore VM data.

Image-level restores are less resource intensive and are best used for restoring large amounts of data quickly.

File-level 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.

Therefore, if you must restore or browse large numbers of folders or files, then you will experience better performance if you restore an entire image or selected drives to a temporary location, for example, a new temporary VM, then copy those files to the desired location following the restore.

FULLVM (Image-level) Restore

When the backup completes, you can restore full VMs by using the **Restore a backup** wizard, available from the **EMC Backup and Recovery plug-in** user interface in the vSphere Web Client. Select either of the following options in the **EMC Backup and Recovery plug-in** user interface:

- Click **Restore a VM** on the **Getting Started** tab.
- Select the **Restore** tab, select a restore point, and then click **Restore**.

When you select the **Restore** tab, available VMs appear, as shown in Figure 29 on page 69. For every clone, a backup is listed under the restore point.

Note: Restores from non-DD type devices will be slow due to a process called resurrection.

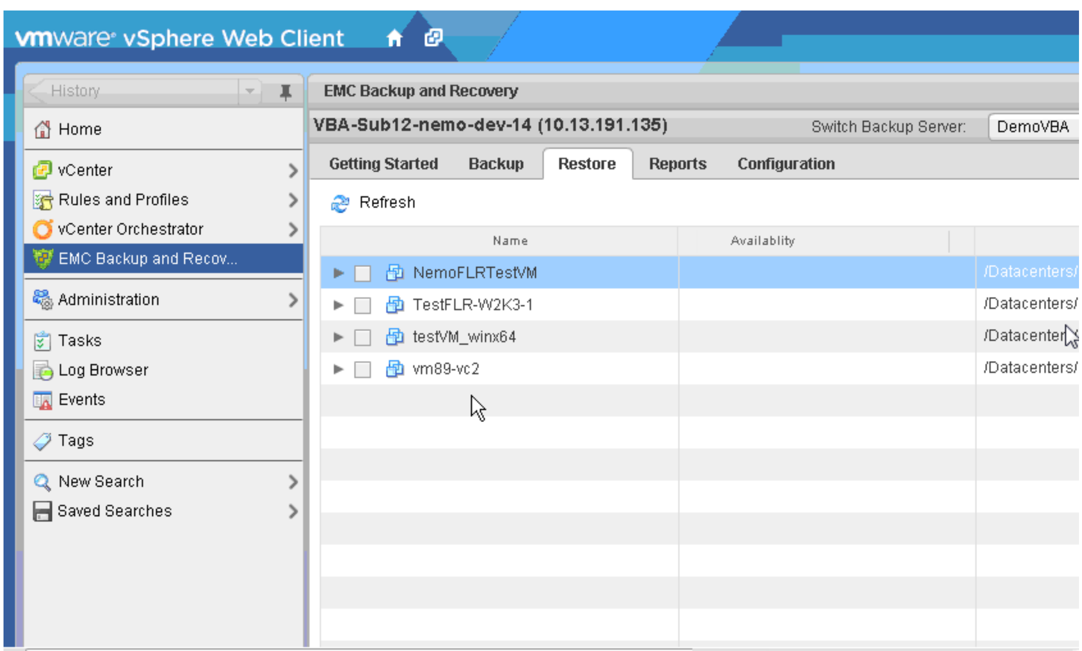


Figure 29 Restore tab in EMC Backup and Recovery plug-in user interface

To perform a full restore:

1. Power off each VM that you want to restore.
2. On the **Restore** tab, expand the VM that you want to restore.

3. Select a restore point and click **Restore**. The wizard launches.
4. 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**.
5. 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**, then you can specify a new location (new Name, destination, and datastore) where the backup 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.

   ---

6. 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).

   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.

Restore from last backup

The vSphere Web Client also provides an option to perform an EMC Backup and Recovery 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 EMC Backup and Recovery appliance by selecting the **EMC Backup and Recovery** user interface.

Cancelling a FULLVM restore

To cancel a restore at any time during setup, click the **Cancel** button in the Restore wizard.

File-level restore

Use the **EMC Data Protection Restore Client** interface to perform file-level restore (FLR).

Before you start a file-level restore, review the limitations specified in the section "FLR limitations" on page 73 to ensure that you can perform FLR in your configuration, and then review the following topics:

- "Restoring specific folders or files to the original VM" on page 71
- "Restoring specific folders or files from a different VM" on page 73

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.

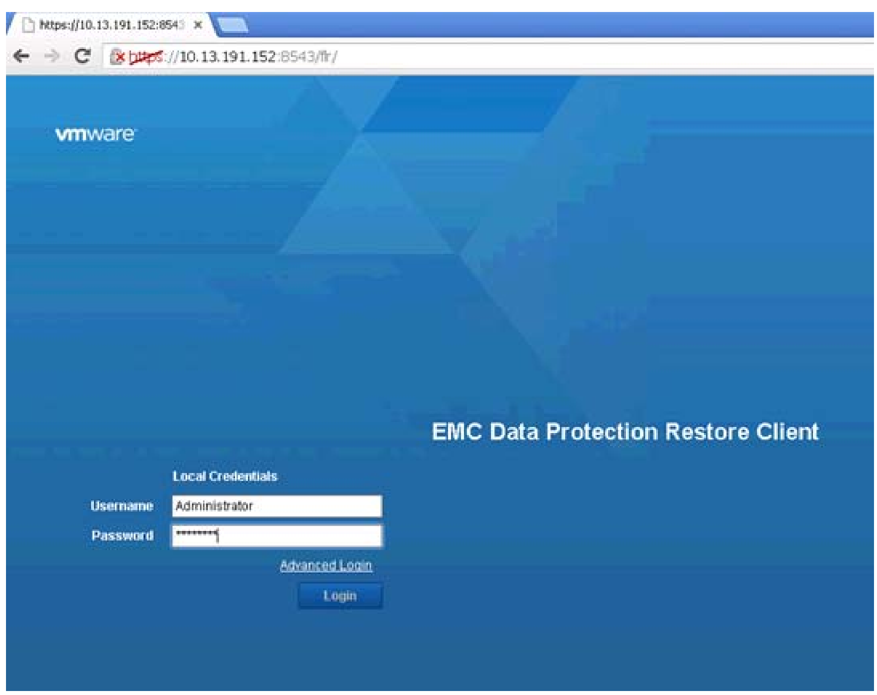
NOTICE

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. "Guidelines for performing image-level restores versus file-level restores" on page 68 provides details.

To restore backup data to the original VM location:

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

   http://*EMC_Backup_and_Recovery_appliance_host*:8580/flr



Note: The browser must point to an EMC Backup and Recovery 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 Figure 30 on page 72. Click **Mount** to mount a restore point.

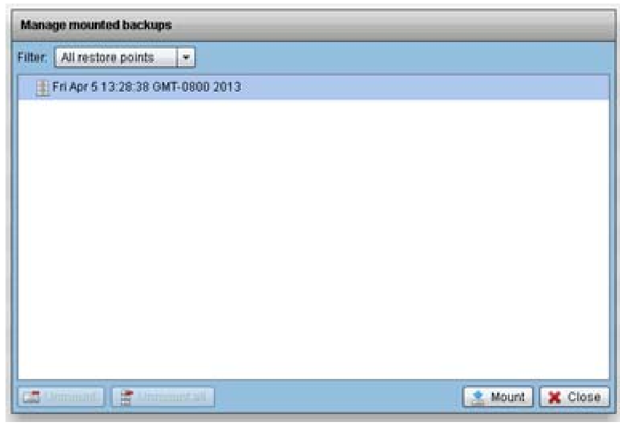


Figure 30 Manage Mounted Backups in EMC Data Protection Restore client

> **Note:** When you click **Mount,** if a folder hierarchy does not appear as shown in Figure 31 on page 72, the file system in use on the VM may not be supported. The section "FLR limitations" on page 73 provides more information.

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

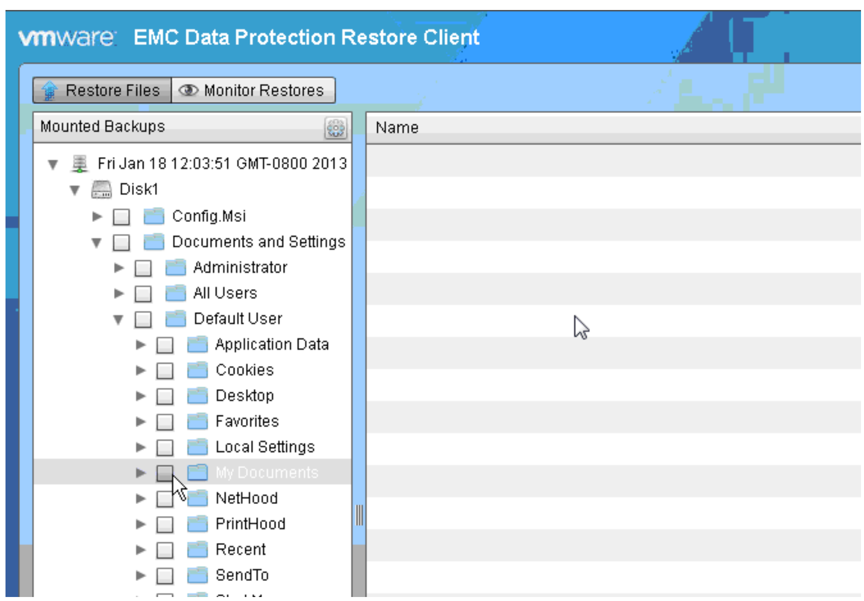


Figure 31 Browse and select files to recover

4. In the **Select Destination** window, select the folder to which you want to restore the VM, as shown in Figure 32 on page 73.

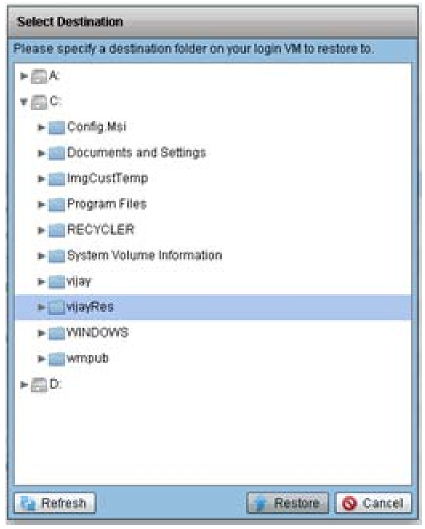


Figure 32 Select Destination window

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

Restoring specific folders or files from a different VM

EMC Backup and Recovery does not support restoring specific folders or files to a different VM. However, restoring specific folders or files *from* a different VM is supported. 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 EMC Backup and Recovery 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 in "Create dedicated vCenter user account and EMC Backup and Recovery role" on page 27.

Cancelling a File Level restore

When you select the **Recent Tasks** window in the **EMC Backup and Recovery plug-in** user interface, current task activity such as restores appear. You can also display Task details by clicking the link next to the VM icon on the **Running** tab under **Recent Tasks**.

To cancel tasks, from the Tasks pane click the **delete** icon.

FLR limitations

The following limitations apply to file-level restores:

- 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
  - GUID Partition Table (GPT) 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
- FLR restore of ext4 filesystems is supported only with external proxies. To perform FLR of ext4 filesystems, you must shut down the internal proxies. To shut down the internal proxies, log into the EMC Backup and Recovery appliance and run **/etc/init.d/avagent stop**.
- 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 EMC Backup and Recovery activity

You can monitor the activities of the **EMC Backup and Recovery plug-in** user interface:

- "Viewing Recent Tasks" on page 75
- "Viewing Alarms" on page 75
- "Viewing the Event Console" on page 76

Most EMC Backup and Recovery tasks, events, and alarms are prefaced by "EBR:" Note that some of the tasks and events that occur as part of EMC Backup and Recovery processes are performed by the vCenter Server and do not have this prefix.

For example, if EMC Backup and Recovery runs a scheduled backup job against a running VM, the following task entries are created:

1. Create a VM snapshot (vCenter acting on the VM to be backed up)
2. EMC Backup and Recovery: Scheduled Backup Job (EMC Backup and Recovery starting the backup job)
3. Reconfigure the VM (the EMC Backup and Recovery appliance requesting services from virtual center)
4. 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, and enter “EMC Backup and Recovery**:**” in the **Filter** field.

Viewing Recent Tasks

EMC Backup and Recovery generates task entries in the **Recent Tasks** windows when it performs the following operations:

- Backups
- Restores
- Integrity Checks

Clicking on a task entry in the Recent Tasks window displays task details in the pane at the bottom of the screen. Task details can also be displayed by clicking the link next to the VM icon in the **Running** tab under **Recent Tasks.**

Tasks can also be cancelled from the **Running** tasks pane by clicking the delete icon.

Viewing Alarms

The EMC Backup and Recovery appliance can trigger the following alarms:

Table 13 EMC Backup and Recovery alarms (page 1 of 2)

Alarm Name	Alarm Description
EBR: [001] The most recent checkpoint for the EMC Backup and Recovery appliance is outdated.	From the **Configuration** tab of the **EMC Backup and Recovery plug-in** user interface, click the **All Actions** icon and select **Run integrity check.**
EBR: [002] The EMC Backup and Recovery Appliance is nearly full.	The EMC Backup and Recovery 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 EMC Backup and Recovery Appliance is full.	The EMC Backup and Recovery 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.

Table 13 EMC Backup and Recovery alarms (page 2 of 2) (continued)

Alarm Name	Alarm Description
EBR: [004] The EMC Backup and Recovery Appliance datastore is approaching maximum capacity.	The datastore where the EMC Backup and Recovery appliance provisioned its disks is approaching maximum capacity. When the maximum capacity of the datastore is reached, the EMC Backup and Recovery 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.
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.

EMC Backup and Recovery Shutdown and Startup Procedures

If you need to shutdown the EMC Backup and Recovery 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 shutdown and restart the EMC Backup and Recovery appliance. You can monitor the status through the VM console. After vSphere shuts down the appliance, use **Power On** to restart the appliance.

If the appliance does not shutdown properly, then during the restart operation the EMC Backup and Recovery rolls back to the last validated checkpoint. 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 EMC Backup and Recovery 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 77
- "Save set lifecycle" on page 77

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 EMC Backup and Recovery 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 EMC Backup and Recovery appliance. This may take several hours to complete.

Save set lifecycle

The NetWorker server exclusively manages the lifecycle of save sets created by EMC Backup and Recovery appliance (VMware Backup appliance) nodes.

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 EMC Backup and Recovery appliance volume or user-defined Data Domain device volume that contains EMC Backup and Recovery appliance backups after you unmount the devices. If the backups cannot be deleted from the EMC Backup and Recovery appliance, then the volume deletion operation fails.

Volume relabelling

You can relabel a default EMC Backup and Recover appliance volume or user-defined Data Domain volume that the EMC Backup and Recovery 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 EMC Backup and Recovery appliance rollback

A checkpoint is 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. In the event you need to recover the EMC Backup and Recovery appliance, a rollback setting within the **EMC Backup and Recovery plug-in** user interface 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 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 be 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

You can only create a validated checkpoint by using the **EMC Backup and Recovery plug-in** user interface in the vSphere Web Client. To create a checkpoint:

1. Navigate to the **Configuration** tab.

2. Select the **Run integrity Check** option, as shown in Figure 33 on page 79.

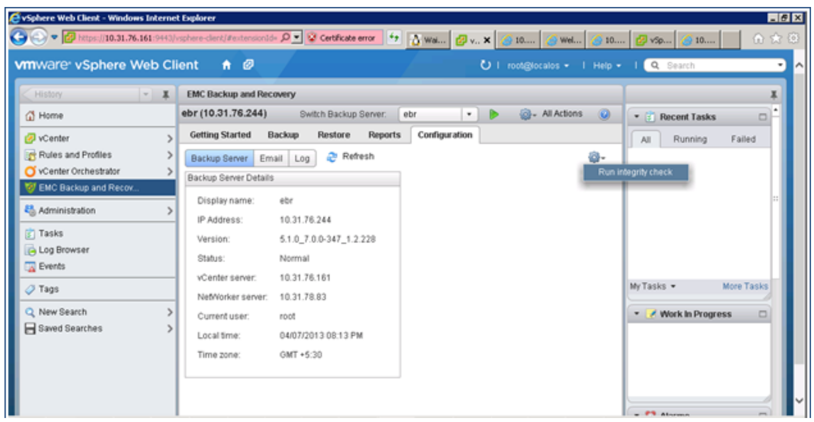


Figure 33 Run Integrity Check button in EMC Backup and Recovery plug-in user interface

Rolling back to a checkpoint

EMC Backup and Recovery appliance 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.

To roll back to a checkpoint from the **EMC Backup and Recovery Configure** window:

1. Log in to the appliance at http://*EMC Backup and Recovery 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, as shown in Figure 34 on page 80.

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

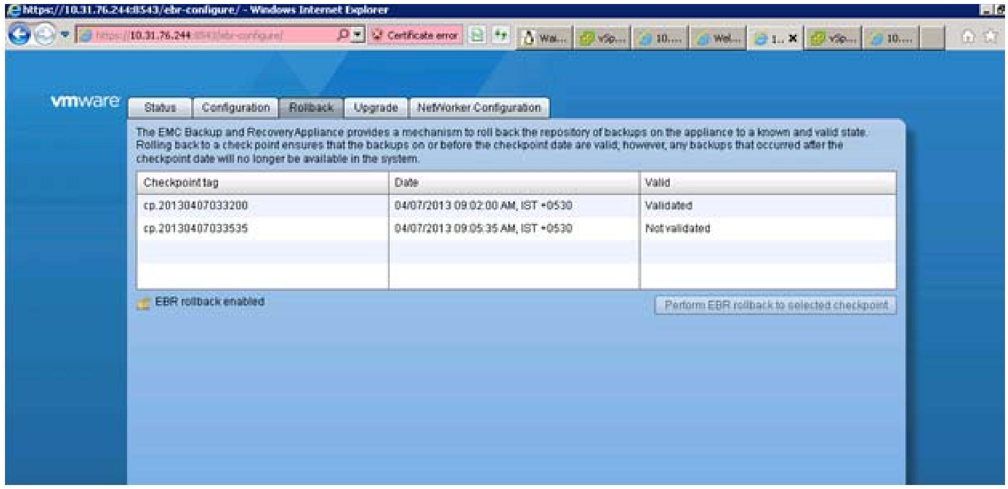


Figure 34 Roll back in EMC Backup and Recovery Configure window

Protecting the EMC Backup and Recovery appliance

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

You can protect these checkpoints by creating a NetWorker client and performing regular full backups — the schedule should be once or twice daily, occurring a couple hours after the checkpoint gets created — to secure the checkpoint files to NetWorker media. "Preparing the EMC Backup and Recovery appliance for disaster recovery" on page 82 provides a list of checkpoint locations.

Cross Sync

A Cross sync operation synchronizes the EMC Backup and Recovery appliance and NetWorker databases for backups, triggered automatically upon EMC Backup and Recovery 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 EMC Backup and Recovery 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 EMC Backup and Recovery 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 EMC Backup and Recovery appliance cross sync
- -h specifies the EMC Backup and Recovery 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 EMC Backup and Recovery 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 EMC Backup and Recovery 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, kit 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 EMC Backup and Recovery appliance

NOTICE

Use caution when you completely remove references of an EMC Backup and Recovery appliance/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 EMC Backup and Recovery appliance/VMware Backup Appliance, and decommission the appliance only from NetWorker.

If you confirm to continue decommission, then:

- 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.

Disaster Recovery

EMC Backup and Recovery is robust in its ability to store and manage backups. In the event of failure, as a first course of action, rollback to a known validated checkpoint. To recover from an EMC Backup and Recovery appliance failure, refer to the following disaster recovery guidelines.

Note: EMC Backup and Recovery does not support a disaster recovery of data backed up to Avamar storage when the internal AFTD metadata is lost.

Disaster Recovery Guidelines

Use these guidelines to perform an EMC Backup and Recovery 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. Before shutting down the EMC Backup and Recovery appliance, verify that no backup or maintenance tasks are running. Depending on the backup method used and how long it takes, schedule your EMC Backup and Recovery 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.
3. 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. "EMC Backup and Recovery Shutdown and Startup Procedures" on page 76 provides more information.
4. Once you have confirmed that the appliance has been shut down, proceed with your preferred method of protection.
5. Verify that the backup of EMC Backup and Recovery is complete and that no backup/snapshot/copy jobs are being performed against EMC Backup and Recovery.
6. From the vSphere Client, perform a Power On for the appliance.

Preparing the EMC Backup and Recovery appliance for disaster recovery

Perform the following steps to prepare for a disaster recovery of the EMC Backup and Recovery appliance:

1. Choose an existing checkpoint. If you have a recent checkpoint already created, verify that the checkpoint is validated.
   a. Run the following command to check whether you have a recent checkpoint:-

      ```
      # 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
      cp.20130206170913 2013-02-06 09:09:13 PST           No
      cp.20130206210904 2013-02-06 13:09:04 PST Validated No
      ```

b. If the selected checkpoint is not validated (the second line in the example output as shown above), validate it by running the following:

```
# mccli checkpoint validate --cptag=cp.20130206170913
--override_maintenance_scheduler
```

Validation takes some time to complete. Keep checking the status by running **mccli checkpoint show**.

2. To create a checkpoint if you do not have a recent checkpoint, or want to create a new checkpoint, then run the following commands.

   To create the checkpoint:

```
# mccli checkpoint create --override_maintenance_scheduler
```

   To verify the checkpoint was created successfully, run:

```
# mccli checkpoint show
```

   Then, validate the checkpoint:

```
# mccli checkpoint validate --cptag=cp.20130206170913
--override_maintenance_scheduler
```

   To verify the checkpoint was successfully validated:

```
# mccli checkpoint show
```

3. To perform a checkpoint backup of the VMware Backup appliance, 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 "VMware Backup Appliance in the NetWorker Management Console" on page 48 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.

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).

Disaster recovery of the EMC Backup and Recovery appliance

To perform disaster recovery of the EMC Backup and Recovery appliance:

1. Redeploy the EMC Backup and Recovery appliance with the same network configuration, and use the **Override** button with EMC Backup and Recovery configure.

   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:

   Re-register the VBA internal proxy agents by running:

   ```
   #/usr/local/avamarclient/etc/avagent.d register
   ```

   Re-register the proxies with the redeployed EMC Backup and Recovery appliance by running the following command from each external proxy, or reboot the external proxy:

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

3. Perform a save set recovery of all of the checkpoint files backed up using NetWorker. For example, the disks for the 0.5 TB and 4.0 TB OVAs specified in step 3 on page 83.
4. Perform a rollback:

   a. In a command prompt, cd to /usr/local/vdr/configure/bin.

   b. Run the following:

   ```
   ./ebr-rollback-util.sh -forcerollback checkpoint
   ```

   where *checkpoint* is the cp.#### that you recovered from NetWorker.

5. Check for restores of old backups and ensure that the policies are intact as per the checkpoint.
6. Any changes to the configuration files will need to be repeated (for example, the changes performed in the section “Restrict mapping of datastores” on page 36).

Complete disaster recovery of the EMC Backup and Recovery 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 EMC Backup and Recovery appliance, and the device (Data Domain or tape device) that has completely failed:

- “Prerequisites for performing a complete disaster recovery” on page 84
- “Performing a complete disaster recovery” on page 85

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 EMC Backup and Recovery appliance, as described in step 2 in the section “Preparing the EMC Backup and Recovery appliance for disaster recovery” on page 82.
- 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 EMC Backup and Recovery appliance is required:

1. Redeploy the EMC Backup and Recovery appliance with the same network configuration, and use the **Override** button with EMC Backup and Recovery configure.

   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 EMC Backup and Recovery appliance by running the following command from each external proxy, or reboot the external proxy:

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

3. Perform a save set recovery of all of the checkpoint files backed up using NetWorker. For example, the disks for the 0.5 TB and 4.0 TB OVAs specified in step 3 on page 83.
4. Perform a rollback:

   a. In a command prompt, cd to /usr/local/vdr/configure/bin.

   b. Run the following:

   ```
   ./ebr-rollback-util.sh -forcerollback checkpoint
   ```

   where *checkpoint* is the cp.#### that you recovered from NetWorker.

5. Unmount the volumes pointing to the primary Data Domain device that has failed.
6. Run the **nsrim** command to synchronize NetWorker and the EMC Backup and Recovery appliance, as described in the section "Cross Sync" on page 80.

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.

Troubleshooting

This section provides troubleshooting information for the NetWorker VMware Protection solution:

- "Configuration checklist" on page 86
- "Log file locations" on page 87
- "Enabling low-level logging of NetWorker web server on Windows systems" on page 87
- "Time synchronization error" on page 88
- "Create and analyze crashes on Windows 2008 R2" on page 88
- "Adding external proxies" on page 88
- "NetWorker operations" on page 89
- "vCenter server operations" on page 89

- "vSphere Web Client operations" on page 89
- "EMC Backup and Recovery appliance installation" on page 90
- "EMC Backup and Recovery appliance operations" on page 91
- "EMC Backup and Recovery backup operations" on page 91
- "EMC Backup and Recovery restore operations" on page 94
- "EMC Backup and Recovery Integrity Check" on page 94
- "Changing the Data Domain Boost password" on page 94
- "Accessing Knowledge Base Articles" on page 95

Configuration checklist

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

Basic configuration

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

Data Domain system configuration

- Upgrade all Data Domain systems to use DDOS version 5.3.0.6 or 5.4.0.4 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

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

EMC Backup and Recovery appliance configuration

- Supports configuration on thin disks

- Use the **EMC Backup and Recovery Configure** window to confirm that all services on the EMC Backup and Recovery 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 an EMC Backup and Recovery appliance to avoid slower recovery times
- Ensure that the EMC Backup and Recovery appliance still has space left for backups
- VMs with independent disks cannot be snapshot for back up

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/

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 10 on page 44.
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**.

Time synchronization error

A time synchronization error can occur when launching the EMC Backup and Recovery plug-in in vCenter in the following scenarios:

- When you configure the EMC Backup and Recovery appliance to synchronize its time with the ESX server that the appliance runs on
- 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.
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 plug-in** user interface, the times have been synchronized successfully.

Create and analyze 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. Type **analyze --v** in the bottom command window to retrieve full information.

Adding external proxies

The EMC Backup and Recovery 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 36 provides information.

NetWorker operations

The following troubleshooting items provide some direction on how to identify and resolve common issues with NetWorker and VMware Protection Policies.

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

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

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

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

"No proxies running on VBA {EMC Backup and Recovery 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 to the vSphere Web Client and invoke **service avagent start** or **service avagent restart** from the EMC Backup and Recovery appliance Console.

vCenter server operations

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 Web Client operations

The following troubleshooting items describe how to identify and resolve common issues that occur with EMC Backup and Recovery in the vSphere Web Client.

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 25 provides additional information.

EMC Backup and Recovery appliance installation

If you have problems with the EMC Backup and Recovery appliance installation:

- Confirm that all of the software meets the minimum software requirements (see "System requirements" on page 21).
- Confirm that the hardware meets the minimum hardware requirements (see "System requirements" on page 21).
- Confirm that DNS is properly configured for the EMC Backup and Recovery appliance. (see "Pre-installation requirements" on page 25).

EMC Backup and Recovery appliance operations

Restart the Enterprise Manager Web Application (emwebapp)

To restart emwebapp:

1. Log into the EMC Backup and Recovery appliance 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*
```

EMC Backup and Recovery backup operations

The following troubleshooting items provide some direction on how to identify and resolve common issues with EMC Backup and Recovery 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 is configured with thick provisioning and is at capacity, see “EMC Backup and Recovery Capacity Management” on page 77.

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 EMC Backup and Recovery 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 EMC Backup and Recovery 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 EMC Backup and Recovery 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

EMC Backup and Recovery restore operations

The following troubleshooting items describe how to identify and resolve some common issues with restores.

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 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 VMware Tools is not installed, a message appears indicating the EBR 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 EMC Backup and Recovery appliance.

Log into a VM that has been backed up by EMC Backup and Recovery 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.

EMC Backup and Recovery 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 **Running** tasks tab under **Recent Tasks**. 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.

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 EMC Backup and Recovery 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 appliance console:

```
mccli dd edit --name=fqdn --password=newpassword
--password-confirm=newpassword --user-name=boostuser
```

Accessing Knowledge Base Articles

Additional troubleshooting information is available through the Featured VMware Documentation Sets website. Select **Products › VMware vSphere › Troubleshooting**.

CHAPTER 3
VADP Backup and Recovery (legacy)

This chapter includes the following topics:

Software and hardware requirements

The software and hardware requirements for VADP include:

- One or more VADP proxy systems running any of the following operating systems (English versions only):
  - Windows Server 2003 SP1 (64-bit)
  - Windows Server 2003 R2 (64-bit)
  - Windows Server 2003 SP2 (64-bit)
  - Windows 2008 R2
  - Windows 2008 (64-bit)
  - Windows 2012
- One or more vCenter/Virtual Center servers running any of the following versions:
  - vSphere 5.5 with vCenter 5.5
  - vSphere 5 or 5.1
  - VirtualCenter version 2.5 managing ESX/ESXi 3.
  - vCenter server versions 4.1 or 4.0, managing ESX/ESXi 4.1, 4.0, and 3.5

  Note: NetWorker supports VMware Vcenter appliance versions 5.0 and 5.1.

- You must perform the following prerequisites on the NetWorker server/proxy machine in order to run vSphere 5.5:
  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 support" on page 100 provides information on limitations when using vSphere 5.5 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 7.6 Service Pack 2 or later client software on the VADP Proxy host.
- You must install the NetWorker 7.6 Service Pack 2 or later client software on the vCenter server to enable autodiscovery.
- The NetWorker server requires NetWorker 7.6 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 153 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 99 and "Limitation for VADP proxy host on non-English versions of Windows" on page 100.
- 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 support

The following limitations apply to vSphere 5.5 support with NetWorker 8.1 SP1:

◆ 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, 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 (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 “Recovery of a VM using NBDSSL, SAN, or hotadd transport mode” on page 136.

You can set multiple transport modes to be used by the VADP proxy host using the pipe symbol “|” (for example, **san|nbd|nbdssl**).

By default, the transport mode field in the **NetWorker User** program is blank. Specify one transport mode to use for recovery.

More information on configuring transport modes is provided in"Task 1: Configuring the VADP proxy host and Hypervisor resource" on page 103. The transport modes are outlined in the table "Application information values" on page 108.

Support for directives

All local directives (.nsr file) are supported for ALLVMFS backups and specific save set backups.

VADP supports the following global directives:

- **Encryption directive** (for VADP enabled image level backups)
- **NT with Compression** (for VADP enabled image level backups)

Encryption directive

The Encryption directive is supported only for Windows VMs with all attached disks having NTFS filesystem.

For the backup, the directive can be specified in the VM client properties.

- Encryption- "Encryption directive"

For the recovery of files or the entire VM from Encryption image backups with a pass phrase that is different than the current pass phrase (the current pass phrase is listed in the Datazone Pass Phrase attribute of the NetWorker server), use the following procedure:

- To recover AES encrypted data that was not encrypted with the current pass phrase, use the **-p** option with the command that is being used to recover data. For example:
  - **recover -p** *pass_phrase*
  - **winworkr -p** *pass_phrase*
- To enter multiple pass phrases with the -p option, type:

  recover -p *pass_phrase1 -p pass_phrase2 -p pass_phrase3*

  Note: If an incorrect pass phrase or no pass phrase is entered, encrypted data is not recovered. Instead, the filenames will be created without data. However, if unencrypted data is also selected for recovery, it will be recovered.

Compression directive

The Compression directive is supported only for Windows VMs with all attached disks having NTFS filesystem.

For the backup, the directive **Compression-"NT with compression directives"** can be specified in the VM client properties.

For the recovery of files or recovery of the entire VM from **Compression** image backups, there is no change from the normal workflow.

Incremental backups with image level backups

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.

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, the virtual disk block changes are tracked from outside of the virtual machine 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 virtual machine has CBT enabled, or enable CBT, by performing the steps outlined in "Task 4: Configuring Changed Block Tracking (CBT)" on page 118.

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 "Configure a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard" on page 104.
- If using the Client Properties window, refer to "Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows" on page 106

Task 1: 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:

- "Configure a VADP proxy host and Hypervisor resource automatically by using the Client Backup Configuration Wizard" on page 104
- "Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows" on page 106

Note: The VADP proxy host cannot 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.

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

To create a NetWorker client for the VADP Proxy host by using the Client Backup Configuration Wizard:

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 in Figure 35 on page 104.

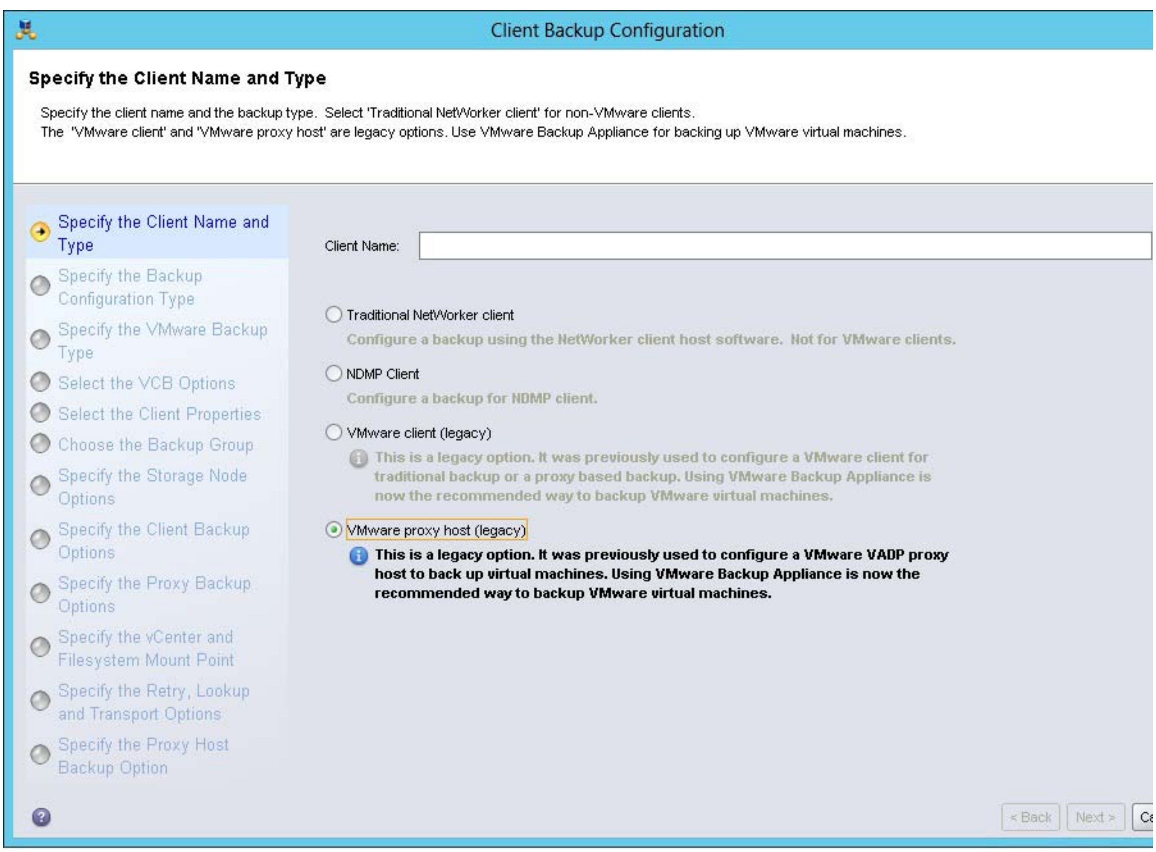


Figure 35 Specify Client name and type

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 "Task 3: Creating a VADP User role in vCenter" on page 115.
   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**.

Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows

If vCenter is configured in the environment, there must be a Hypervisor resource for the vCenter server hosting the VMs that use VADP. Before creating a Hypervisor resource for vCenter, ensure that the NetWorker client software is installed on the vCenter server to allow the Virtual Map of the environment to be generated with the auto-discovery feature.

Note: The NetWorker software supports auto-discovery of VMware environments with VMware vCenter only. It does not support auto-discovery with an ESX server.

If vCenter is not configured in the environment, there must be a Hypervisor resource created for each server in the environment. The NetWorker client on vCenter is only required if using the auto-discovery feature or the virtualization map feature.

VADP backups will work without the NetWorker client being installed on vCenter or VirtualCenter, however, the corresponding Hypervisor resource has to be created in the NetWorker server prior to starting the VADP backups.

To configure a Hypervisor resource:

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Virtualization**.
3. In the right pane, click **Enable Auto-Discovery**.
4. In the Auto-Discovery dialog box:
   a. In the **Hostname** field, enter the fully qualified domain name (FQDN) or IP address of the vCenter server.
   b. In the **Username** and **Password** fields, enter the credentials required to log onto the server. The username and password must belong to an account that has permission to perform VADP backups, snapshots and registering/creating a new VM. The user specified in the Hypervisor resource must also have administrative privileges on vCenter.

If the user has non-administrative privileges on the vCenter server, follow the steps in the section "Task 3: Creating a VADP User role in vCenter" on page 115.

c. To configure the vCenter server to use a port other than the default port for communications, click the **Advanced** tab and specify the correct port in the **endpoint attribute of NSRhypervisor** field.

   For example, if vCenter uses port 2000, define the endpoint attribute of NSRhypervisor attribute as:

   `https://server_hostname:2000/sdk`

   where *server_hostname* is the FQDN name of the vCenter host.

d. When the vCenter server configuration is complete, right-click **Virtualization** and select **Run Autodiscovery** to generate the topology map.

   Note: If auto discovery fails with the error "Falling back to rsh, but RUSER not provided," ensure that the NetWorker server and the vCenter server can resolve each other's IP / FQDN name.

   ---

e. Click **OK**.

To create a NetWorker client for the VADP Proxy host by using the Client properties windows:

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 Figure 36 on page 108.

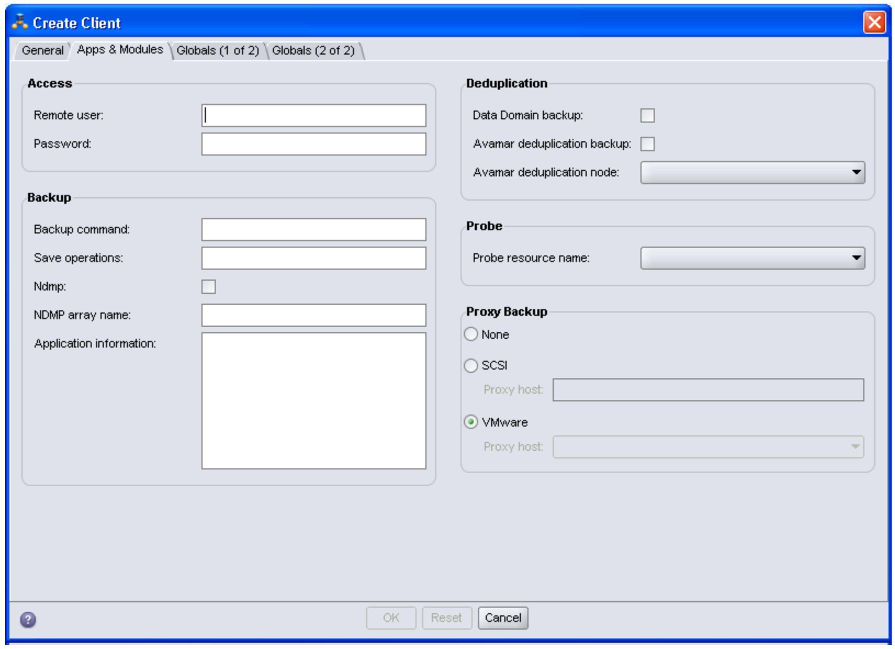


Figure 36 Apps and Modules tab in NMC

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 Table 14 on page 108, can also be specified in the Application Information section.

Table 14 Application information values (page 1 of 3)

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

Table 14 Application information values (page 2 of 3)

Attribute name	Description	Default value
VADP_DISABLE_FLR	If a virtual client is set up for image level backup and image level recovery (single step), setting this variable to YES will disable file level recoveries from the image backup. This variable only takes effect if the virtual client's backup saveset is specified as *FULL*, which indicates an image level backup, and the backup level is full (0) with no incremental backup levels selected. VADP_DISABLE_FLR=Yes **Note:** Setting this variable in the proxy application information and not specifying it at the virtual client level will disable file level recovery from all subsequent image backups done via the proxy	No
VADP_HOST **Note:** 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. 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 applys if MAX_RETRIES is larger than 0). VADP_BACKOFF_TIME=20	10

Table 14 Application information values (page 3 of 3)

Attribute name	Description	Default value
VADP_TRANSPORT_MODE	Specify the transport mode to transfer data from a VMFS data store to a VADP proxy server. The following options are supported: • SAN – Virtual disk data is read directly off a shared storage device that the virtual disk resides on. This requires VMFS storage on SAN or iSCSI and the storage device has to be accessible from both ESX and the VADP proxy. • hotadd – This mode can be used when VADP is used in a virtual proxy. Because it uses the ESX I/O stack to move data, hotadd is more efficient than the transport mode NBD. • NBDSSL – This mode is the same as nbd except that the data transferred over the network is encrypted. The data transfer in nbdssl mode can be slower and use more CPU than in the nbd transport mode. Also, For recovery of VMs using NBDSSL mode, refer to the section "Recovery of a VM using NBDSSL, SAN, or hotadd transport mode" on page 136. • 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 (since data is still transferred from the ESX host across the network). However, nbd does not require shared storage and also enables VADP to be run inside a virtual machine.	blank If left blank, the default values are selected in the order of the description list. You can specify multiple modes by inserting a pipe (|) symbol between each value as shown in the following: Example: `VADP_TRANSPORT_MODE= san | hotadd | nbdssl | nbd` The order in which modes are specified dictate the priority in which they are attempted. In the above example, the san mode is attempted first; if that fails the hotadd mode is attempted, and so on.

Example 1 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
```

Task 2: 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:

- "Configure a virtual client if vCenter is configured and auto-discovery has been run" on page 112
- "Configure a virtual client manually by using the Client Properties window" on page 114

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 virtual machine 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.

Table 15 on page 111 lists the recovery options that are available based on the virtual client's configuration. Recovery steps are described in "Recovering VADP Backups" on page 126.

Table 15 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 saveset is selected.	Yes	No
Virtual client with NTFS** OS and the *FULL* saveset is selected.	Yes	Yes
Virtual client with NTFS** OS and the *FULL* saveset 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* saveset selected.	No	Yes

* The VADP_DISABLE_FLR variable does not apply to virtual clients that have the ALLVMFS saveset 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

Configure a virtual client if vCenter is configured and auto-discovery has been run

To configure a virtual client if vCenter is configured:

1. In the Virtualization map, right click on the Virtual Machine 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 Virtual Machine.
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 virtual machine 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**.

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

Configure a virtual client manually by using the Client Properties window

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

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 virtual machine 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**.

Task 3: 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.

Create a VADP Proxy role

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**.

The section "Minimum vCenter permissions needed to back up and recover using VADP" on page 116 provides more information.

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

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.**

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/

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.

Table 16 on page 116 provides VADP backup privileges.

Table 16 VADP backup privileges

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

Table 17 on page 117 provides VADP recovery privileges.

Table 17 VADP recovery privileges (page 1 of 2)

Setting	Privileges
Global	• Cancel task • Licenses • Log Event • Settings
Resource	• Assign virtual machine to resource pool
Datastore	• Allocate space • Browse datastore • Low level file operations • Remove file • Update virtual machine files (only found in 4.1 and later)
Virtual machine › Inventory	• Create new • Register • Remove • Unregister
Virtual machine › Configuration	• Add existing disk • Add new disk • Add or Remove device • Advanced • Change CPU count • Change Resource • Disk change Tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device setting • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility
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

Table 17 VADP recovery privileges (page 2 of 2)

Setting	Privileges
Network	• Assign network • Configure
Session	• Validate session
Tasks	• Create task • Update task

Task 4: Configuring Changed Block Tracking (CBT)

You can check if your virtual machine 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
```

Enable 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.

Managing and Monitoring VMs in the VADP solution

This section covers these topics:

- "Performing on-demand auto-discovery of VMware environments" on page 121
- "Notifications of changes to VMware environments" on page 121
- "Visual representation of VMware environments" on page 122

Automatic discovery of VMware environments

The NetWorker software provides automatic discovery of VMware environments and notification of changes to those environments, and provides both a graphical map and tabular view of VMware environments.

Automatic discovery is performed by contacting one or more VMware vCenters that host a Web Services server. VMware vCenter is 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.

Auto-discovery of VMware environments within NetWorker requires VMware vCenter, and the NetWorker client software installed on a Windows system. VMware vCenter and the NetWorker client do not need to be installed on the same system to perform auto-discovery. The VMware Infrastructure documentation provides information about configuring VMware vCenter.

Note: NetWorker software supports auto-discovery via VMware vCenter only. It does not support auto-discovery via an ESX server. "Task 1: Configuring the VADP proxy host and Hypervisor resource" on page 103 describes how to enable auto-discovery.

A binary, nsrvim, is used to facilitate communication between the NetWorker software and the VMware vCenter. The nsrvim binary can communicate with the Web Services server on the VMware vCenter using the secure HTTPS protocol. The nsrvim binary is supported on NetWorker for Windows 32-bit and 64-bit installations. The nsrvim binary is also included in these installation packages.

All NetWorker servers regardless of platform must contact a NetWorker client running in a Windows environment for auto-discovery. By default, the NetWorker server contacts the NetWorker client running on the VMware vCenter.

The NetWorker software uses auto-discovery for two purposes:

- Notification of changes to the VMware environment.
- Creating and updating the visual view of the VMware environment.

The output of the daemon.raw file, located in the \Program Files\EMC NetWorker\nsr\logs directory, contains any errors that occur during auto-discovery.

Note: The NetWorker client must be installed on the vCenter Server in order to run auto-discovery in the default configuration.

Performing on-demand auto-discovery of VMware environments

To perform an auto-discovery of VMware environments at any time, right-click **VMware View (legacy)** in the left pane of the **Configuration** window and select **Run Auto-Discovery**. Individual elements under **VMware View (legacy)** can be selected to limit the auto-discovery task to the selected element.

After selecting **Run Auto-Discovery**, either from the right-click menu or from the Auto-Discovery dialog, the Running auto-discovery Now window allows you to monitor the auto-discovery process. Clicking the Stop Monitoring button will close the Running Auto-discovery Now window, but the auto-discovery process will continue.

Note: If auto discovery fails with the error, "Falling back to rsh, but RUSER not provided", ensure that the NetWorker server can resolve the IP/FQDN of the Virtual Centre server, and that the Virtual Centre server can resolve the NetWorker server.

Notifications of changes to VMware environments

After auto-discovery has been performed, if there are any new unprotected VMs, identified by vCenter, that do not have NetWorker Client resources associated with them, a notification will be triggered. A notification is also sent if auto-discovery fails.

Set up notifications

A default Notification resource, named New Virtual Machine, is included with the NetWorker installation. You must modify the Action attribute of this Notification resource to specify the mailserver and email accounts to which these notifications will be sent. You can also create custom Notification resources by selecting Hypervisor for the Event attribute of the custom Notification resource.

1. Connect to the NetWorker server via NMC.
2. Click **Configuration**.
3. In the left hand side navigation pane, select **Notifications**.
4. Right click **New Virtual Machine** and select **Properties**.
5. In the Action field, remove nsrlog and specify the command appropriate for your NetWorker server's operating system.
   a. For UNIX servers, the native mailer program will be used, refer to the appropriate operating system documentation for configuration details.
   b. For Windows servers, smtpmail, included with NetWorker can be specified. The action field would be:

      ```
      smtpmail -s subject -h mailhost recipient1@host.com
      recipient2@host.com
      ```

      Where:

      subject is the subject line of the email notification

      mailhost is the FQDN of an email server which allows SMTP relaying

      receipient1@host.com is the email address that will receive the emails.

Note: For details regarding additional switches for the smtpmail command refer to esg116292 on http://powerlink.emc.com.

Monitor VMs

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

Visual representation of VMware environments

After performing auto-discovery of VMware environments, the NetWorker console provides a graphical or tabular view of your VMware environments. This view displays in the right pane when you select **VMware View (legacy)** in the left pane of the NMC Configuration window.

If auto-discovery has not been configured and you select **VMware View (legacy)**, the right pane displays the **Enable Auto-Discovery** button. If auto-discovery has been configured and an auto-discovery has been performed, the right pane will display a graphical map of the VMware environment that was in place during the last auto-discovery. Automatic discovery is performed by contacting one or more VMware vCenters which host a Web Services server. VMware vCenter is an infrastructure management tool that provides a central point for configuring, provisioning, and managing virtualized IT environments, and is part of VMware Virtual Infrastructure package. For auto-discovery of VMware environments within NetWorker, VMware vCenters must also have NetWorker client software installed. See the VMware Infrastructure documentation for information about configuring VMware vCenter.

VMware View hierarchical display of the VMware environment

After an auto-discovery has been performed, **VMware View (legacy)** in the left pane of the Configuration window can be expanded to provide a hierarchical display of the VMware environment. Four elements are displayed, in hierarchical view:

1. vCenters
2. DataCenters within the vCenter
3. Clusters within the DataCenter
4. ESX servers

VMs, NetWorker clients associated with those VMs, and NetWorker groups performing backups of those clients are not displayed in the VMware View hierarchical display. They are displayed in the right pane only.

Clicking on any element in the hierarchical tree will provide a detailed map view of that element and all of its children in the right pane. For example, selecting the top level **VMware View (legacy)** will display a complete view of your VMware environment across all vCenters that are configured for auto-discovery, while selecting an individual ESX server in the hierarchy will display all child elements associated with that ESX server including VMs, NetWorker clients associated with those VMs, NetWorker groups performing backups of those clients, and the proxy node for VMware clients.

Two right-click menu operations are available from **VMware View (legacy)**:

- Enable Auto-Discovery will open the Auto-Discovery dialog to configure auto-discovery, as described in "Performing on-demand auto-discovery of VMware environments" on page 121.
- Run Auto-Discovery will perform an on-demand auto-discovery of your VMware environment. Individual elements in **VMware View (legacy)** can be selected to limit the auto-discovery task to the selected element.

Graphical display of the VMware environment

After an auto-discovery has been performed, elements of the VMware environment are displayed in the right "details" pane of the NetWorker Console. Objects displayed in the details pane vary depending on what is selected in **VMware View (legacy)** in the left pane. Several operations are available from the details pane, such as configuring new NetWorker clients to protect VMs.

Note: In order for a NetWorker Client resource to appear in the details pane, the name of the virtual machine and the name of the NetWorker Client resource must be identical.

Two views are available:

- Map view
- Tabular view

Map view of the VMware environment

Items displayed in the map view of the VMware environment will vary depending on what is selected in **VMware View (legacy)** in the left pane.

If **VMware View (legacy)** is selected, the map view displays all vCenters that have had an auto-discovery performed and all child elements of those vCenters, beginning with vCenters on the left side of the pane. Lines connect each child element to its parent, with child elements proceeding hierarchically from left to right in the display, as illustrated in Figure 37 on page 124.

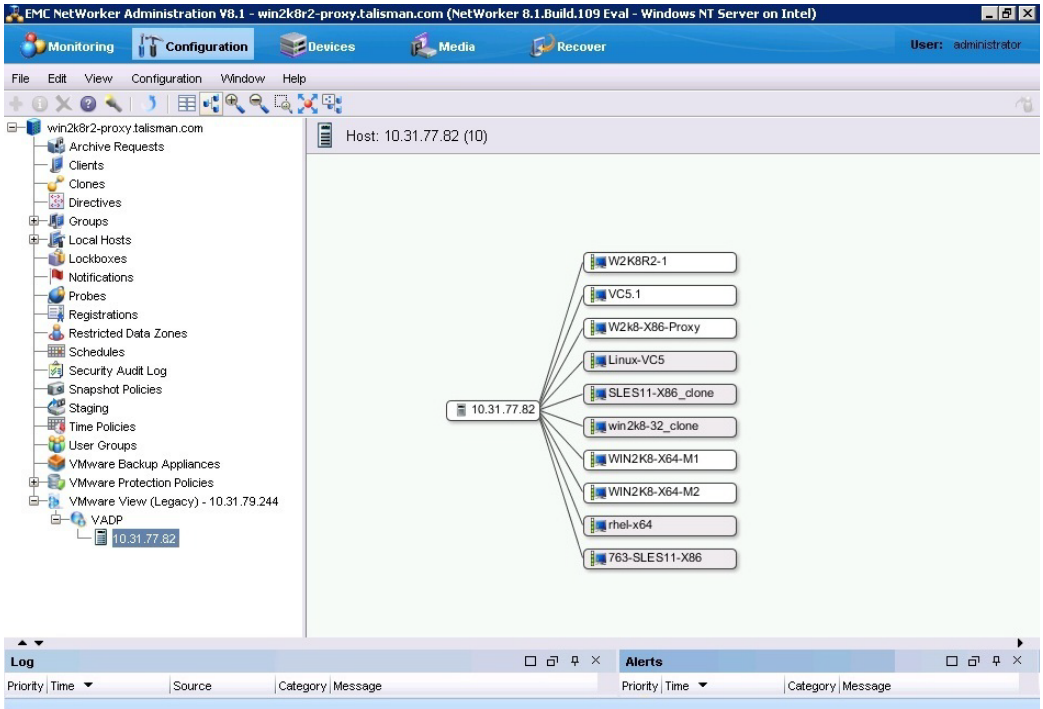


Figure 37 Map view of the NetWorker Console

Items displayed in the right details pane can be refined by selecting child elements in the Virtualization node hierarchy in the left pane. For example, if an individual ESX server is selected in the Virtualization node, only child elements associated with that ESX server are displayed.

Displaying NetWorker clients associated with VMs

By default, NetWorker clients associated with individual VMs are displayed. Rather, a Client icon will indicate whether the virtual machine has one or more NetWorker clients configured to protect it. NetWorker groups performing backups of those clients will be displayed with lines connecting the groups to the virtual machine.

If the virtual machine is being protected by the NetWorker software, you can double-click on the virtual machine to expand the display to view NetWorker clients configured to protect the virtual machine, with a line connecting the client to the NetWorker group that performs the backup of that client. You can also expand all VMs in the display by right-clicking anywhere in the right pane and selecting **Expand›All VMs**.

Creating new NetWorker clients for unprotected VMs

If a virtual machine displayed in the right details pane is unprotected, this is indicated by the lack of a Client icon for that virtual machine. You can create a new NetWorker client for that virtual machine by right-clicking on the virtual machine and selecting **Client Backup Configuration›New** to open the Client Backup Configuration Wizard, or by selecting **New** to manually create a new client. “Task 2: Configuring a virtual client for backup” on page 111 provides information about creating clients to protect VMs.

Other operations available from the map view

You can also perform typical NetWorker operations on clients and groups from the map view. For example, by right-clicking on an existing NetWorker client, you can edit, delete, and copy clients, as well as initiating a recovery. You can also right-click on a NetWorker group displayed in the map view and perform typical group operations, such as editing or copying the group with all clients.

Unscheduled clients for backup are displayed in dotted-line within the configuration. Multiple instances of the same client within the savegroup are represented by their backup type, client name, and saveset name.

Navigating within the Map view

Several operations are available to facilitate navigation within the map view:

- Zoom: 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 middle 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 from the right-click menu 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 elements: You can expand or collapse any element in the map view to display or hide the child elements associated with the element by double-clicking the element. Additionally, you can expand or collapse all elements of a certain type by right-clicking anywhere in the details pane and selecting **Expand** or **Collapse**, and then selecting the element type.
- Overview: You can open the Overview dialog by selecting the Overview icon on the map view icon bar or by right-clicking anywhere in the details pane and selecting Overview. The Overview dialog is particularly useful for large maps and allows you to quickly drill down to specific areas in the map.
- Show and Find: The Show and Find functions allow you to limit items displayed in the map, and to search for specific items.
- Tabular view: You can also switch to viewing the VMware environment in tabular view, rather than map view, by selecting the Table icon on the map view icon bar or by right-clicking anywhere in the details pane and selecting Table.

Tabular view of the VMware environment

The right details pane can display the VMware environment in tabular form, rather than map form, by selecting the Table icon on the map view icon bar or by right-clicking anywhere in the details pane and selecting Table. The tabular view functions like other tabular views in the NetWorker Console.

The NetWorker *Administration Guide* provides general information on using tables in the NetWorker Console.

Launch vSphere client from the NetWorker Console (Windows only)

On supported Windows platforms, the vSphere client can be launched from the NetWorker Console's Configuration window, using the main menu or the map view.

To launch the vSphere client from the Console:

1. Start the Console, then click the **Configuration** tab.
2. Highlight the desired client in the left panel.
3. Launch the vSphere client by performing one of the following:
   - From the menu, select **Configuration › Launch vSphere Client**.
   - From the map view, right-click the client and select **Launch vSphere Client** from the drop-down, as shown in Figure 38 on page 126.

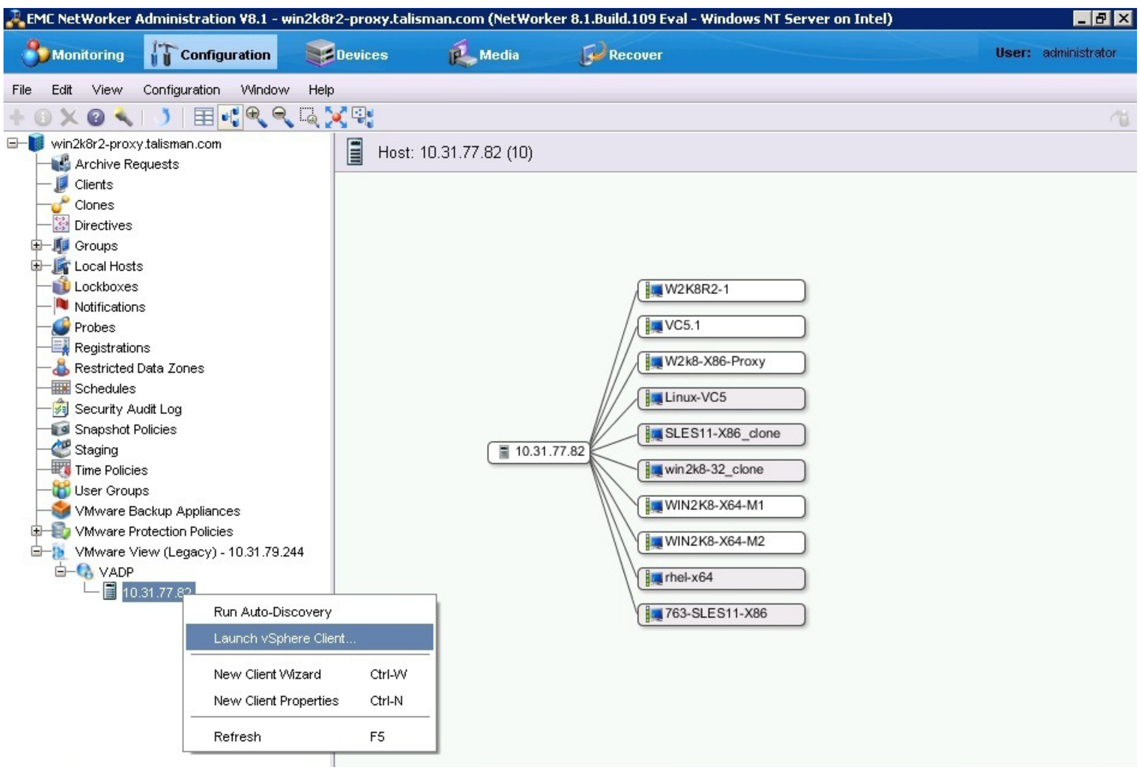


Figure 38 Launching the vSphere client from the Console (Windows only)

Recovering VADP Backups

This section covers these topics:

- "File-level recovery of a VM" on page 127
- "Image level (single step) recovery of a full VM" on page 129
- "Recovery of pre-NetWorker 7.6 SP2 VM backups" on page 137

File-level recovery of a VM

The following sections provide information on file-level recovery (FLR) of a VM, which is supported only on VMs that have a Windows operating system with the NTFS file system.

- "FLR on the local host" on page 127
- "FLR using the CIFS share" on page 128
- "FLR using directed recovery" on page 128
- "FLR unsupported configurations" on page 128

FLR on the local host

FLR on the local host running a VM client requires that the NetWorker client is installed on the VADP proxy.

To perform FLR on the local host:

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 Figure 39 on page 127.

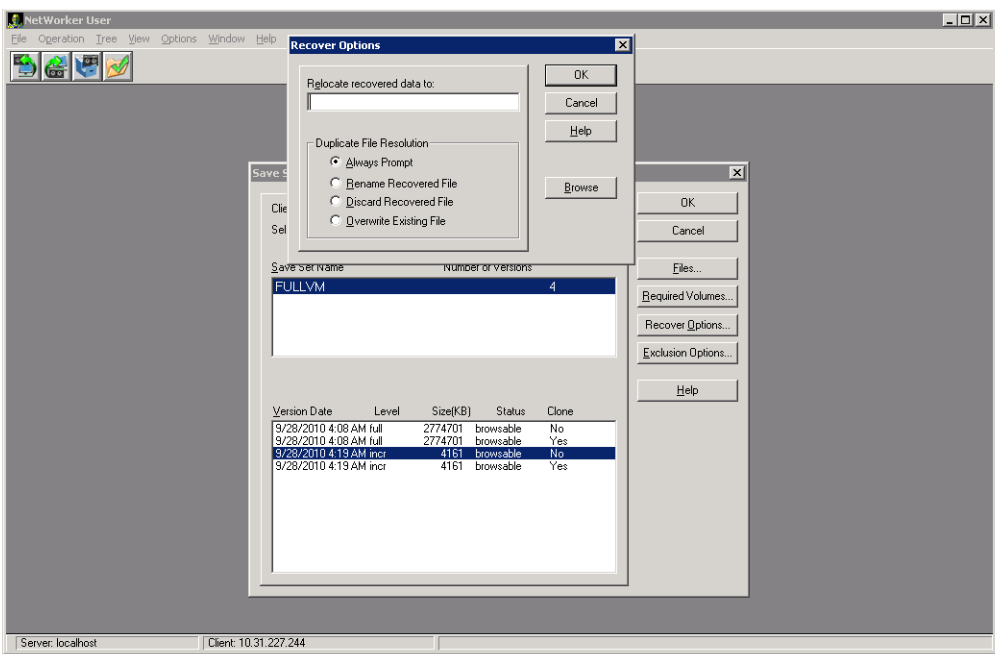


Figure 39 Recover Options dialog

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.

FLR using the CIFS share

To perform FLR using the CIFS share:

1. Launch the NetWorker User program on the NetWorker server or VADP proxy.

   Note: The remote access list of the VM client must include either user@server or user@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.

FLR using directed recovery

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

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.

FLR unsupported configurations

FLR is not supported in the following configurations:

- Windows 8 and Windows Server 2012 VMs with Resilient File System (ReFS)
- VM operating system containing GPT or dynamic disks
- VM operating system containing uninitialized disks
- VM operating system containing unformatted partitions
- VM operating system containing partitions without drive letters
- VM configuration with Virtual IDE Disk Devices (only SCSI)
- VM configuration with independent disk mode

Image level (single step) recovery of a full VM

This section describes how to perform an image level recovery (disaster recovery) of the full virtual machine. There are two methods of recovering a full virtual machine:

- "Perform an image level recovery from the NetWorker User program" on page 131
- "Perform an image level recovery from the command line" on page 132

Recommendations and considerations

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

- For a remote VADP proxy client, image level recovery requires the members of the VADP proxy client's administrator group to be part of the remote access list of the VM clients or the member should have the "Remote access all clients" privilege.
- The user must have VMware privileges to register or create VMs.
- Recovery of the full virtual machine 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 virtual machine (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 virtual machine, you must perform a level full backup before you can perform an image level recovery of the full virtual machine.
- The virtual machine 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 virtual machine (FULLVM save set), the recovered virtual machine 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 135 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.

Perform an image level recovery from an encrypted backup

If the image level backup of the VM being recovered was performed with the Encryption directive, the following step applies:

By default, the current Datazone pass phrase 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.

Perform 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 VMware virtual machine (VM) to the VMware ESX server or VMware vCenter server:

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 virtual machine 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 virtual machine 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. “Recovery of a VM using NBDSSL, SAN, or hotadd transport mode” on page 136 provides a workaround to this issue.

   - **Data Store** — Specify the name of the datastore for each disk on the VM.

Figure 40 on page 132 depicts a VADP Restore dialog box that is set up for a VMware vCenter restore.

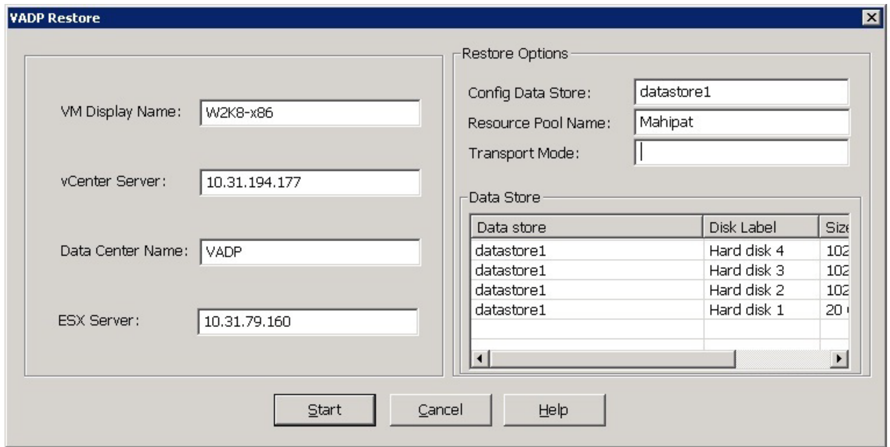


Figure 40 VMware vCenter restore

Note: During an image level recovery operation, multiple browse sessions will be displayed in the NetWorker Console Monitoring window. This is expected behavior.

Perform an image level recovery from the command line

To perform a command line recover of a full VMware virtual machine to the VMware ESX server or VMware vCenter (VC) server:

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 VMware virtual machine 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 release 7.6 Service Pack 2.
   - *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 name that the VM restored is connected to.
- *ESX hostname* is the VMware ESX server machine name where the VMware virtual machine needs to be restored.
- *datastores* is the list of datastores that need to be associated with the configuration and the disks of the virtual machine 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 133
  This issue applies only to NetWorker 7.6.2 build 631 or earlier.
- "Unable to browse guest based backups on non NTFS filesystems" on page 134
  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 virtual machine, 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 dependant 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.

Example 2 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"
volumetypeclient 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, since 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 once the respective indices are removed. If the traditional backup indices are still needed, they can be restored once 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 filesystems

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 filesystem 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.ROData 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 virtual machine.

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

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 virtual machine.

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

Recovery of 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.

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.

Recovery of 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:

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.

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=1026944 provides more information.

VADP Planning and Best Practices

This section covers these topics:

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"NetWorker VMware Protection" on page 17 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 144

- 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 149 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 146 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 virtual machine 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 in the Application Information tab in NMC

An option in 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 in 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 virtual machine 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 147.

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

Proxy node sizing and performance considerations

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

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

- The maximum number of concurrent sessions when using a physical proxy is higher than that of a virtual proxy. The section "Recommendations and considerations for transport modes" on page 149 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 virtual machine 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 virtual machine. 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 virtual machine configuration files, or change the working directory to a datastore with enough block size.

To move the virtual machine 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

Table 18 on page 143 indicates the maximum virtual disk file size corresponding to block sizes on a datastore in ESX/ESXi 4.0:

Table 18 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

Table 19 on page 143 identifies the maximum virtual disk file size corresponding to block sizes on a datastore in ESX/ESXi 4.1:

Table 19 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 virtual machine 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 virtual machine:

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 virtual machine. VMware recommends scheduling downtime before performing this action:

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 virtual machine.
- For DD Boost enabled VADP backups:

- The best CPU load and performance is observed with 4 concurrent backups per device. However, a NetWorker 8.x DD Boost library supports a greater number of concurrent backups (target sessions).
- Setting a lower number of parallel sessions to a single device does not result in optimal performance.
- Setting a higher number of parallel sessions to a single device increases the CPU load without any improvements to performance.
- It is recommended to have at least 400MB to 500MB of RAM for each 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 145.

- 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 149 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 145.
  - 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 149.
  - 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. "Configure a VADP proxy host and Hypervisor resource manually by using the Client properties windows" on page 106 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 above 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 of 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

Example 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 virtual machine configuration.

VMDirectPath requirements and recommendations

The following requirements and recommendations apply when using VMDirectPath:

- VMDirectPath requires Intel Virtualization Technology for Directed I/O (VT-d) or AMD IP Virtualization Technology (IOMMU). You may need to enable this option in the BIOS of the ESX/ESXi system.
- The 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 virtual machine 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 esg1010789 provides information on configuring VMDirectPath:

http://kb.vmware.com/kb/1010789

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 virtual machine:

- 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

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 153.
- 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

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 153.
- 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 virtual machine 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 virtual machine to back up and the virtual machine that contains the hotadd VADP proxy host must reside in the same VMware datacenter. This requirement also applies to virtual machine restore — the virtual machine to restore and the virtual machine 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 hotadded disks. In such cases, you must manually unmount the hotadded 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 hotadded disks and choose **Remove**.

Note: Ensure that you select **Remove from virtual machine** and *not* **Remove and delete...** when unmounting.

NBD/NBDSSL transport mode

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 "Recovery of a VM using NBDSSL, SAN, or hotadd transport mode" on page 136.
- 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.

Example 3 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.

Example 4 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.

Example 5 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

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

NBD/NBDSSL transport modes

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

Diskpart utility for SAN and hotadd transport modes

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

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

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

---

1. Shut down the Windows proxy.
2. Disconnect the Windows proxy from the SAN or mask all the LUNs containing VMFS volumes or RDM for VMs.
3. Start the proxy and log into an account with administrator privileges.
4. Open a command prompt and run the diskpart utility by entering the following:

   ```
   diskpart
   ```

   The diskpart utility starts and prints its own command prompt.
5. Disable automatic drive letter assignment to newly discovered volumes by entering the following in the diskpart command prompt:

   ```
   automount disable
   ```

6. Clean out entries of previously mounted volumes in the registry by entering the following in the diskpart command prompt:

   ```
   automount scrub
   ```

CHAPTER 4
Licensing

This chapter covers these topics:

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

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 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.

AMP virtual appliance

The EMC Asset Management and Planning (AMP) appliance is a free, virtual appliance that can be downloaded from EMC Online Support site and installed on any VMware ESX server. The AMP appliance can be used to understand your software usage, measure the source capacity usage for the Networker software, plan future software investments and ensure license compliance. NetWorker leverages the EMC AMP to provide an estimate of the source capacity usage in a customer environment. Information on how to download, install and configure the EMC AMP appliance is provided in the NetWorker *Licensing Guide.*

CHAPTER 5
Upgrading to the VADP solution (pre-NetWorker 8.1)

This chapter covers these topics:

Upgrading to 7.6 Service Pack 2 and later for VMware VADP backups

NetWorker Release 7.6 Service Pack 2 introduced support for backup and recovery of VMware virtual clients using vStorage APIs for Data Protection (VADP). Prior to this release, virtual NetWorker clients were protected with VMware Consolidated Backups (VCB).

NetWorker 7.6 SP2 and later releases 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.

Upgrade 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 on page 162.

  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 Table 20 on page 161.

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 20 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

Note:
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.

Task 1: Create a VADP User role

To create a **VADP User** role:

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 116 provides more information.

Task 2: Assign the VADP User role to the user specified in the NetWorker Hypervisor resource

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**.

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/.

Upgrade 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:

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. step 2 provides more information.
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**.

The following attributes of the Client resource for the virtual client associated with the proxy need to be changed:

1. The Backup command needs to be changed from **nsrvcb_save** to **nsrvadp_save**.
2. 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:

1. Follow the manual upgrade steps provided in the section "Upgrade only the proxy client to NetWorker 7.6 SP2 or later" on page 163.
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:

1. Run the upgrade tool as outlined in the section "Upgrade existing NetWorker server and VCB proxy" on page 160.
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. This was required so that NetWorker could support automatic discovery of VMware environments. In NetWorker 7.6 Service Pack 2 and later, these additional steps are not required because NetWorker now supports automatic discovery directly on the 64-bit Virtual Center server.

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

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.**

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." 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 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 also "online indexes."

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

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.

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.

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 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 “VSS component.”

INDEX