vSphere Data Protection Administration Guide

vSphere Data Protection 6.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001565-00

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1 Understanding VDP 13

Introduction to vSphere Data Protection 14

Benefits of vSphere Data Protection 14

VDP Functionality 15

Image-level Backup and Restore 16

Single VMDK Backup and Restore 16

Guest-level Backup and Restore 16

Replication 17

File Level Recovery 17

Customer Experience Improvement Program 17

vSphere Data Protection Architecture 17

2 VDP Installation and Configuration 19

vSphere Data Protection Capacity Requirements 20

Software Requirements 20

Hardware Versions and Migration 20

vSphere Hosts and vSphere Flash Read Cache Compatibility and Performance 20

Unsupported Disk Types 20

System Requirements 20

VDP System Requirements 21

IPv6 Requirements 21

Preinstallation Configuration 21

DNS Configuration 21

NTP Configuration 22

vCenter Hosts and Clusters View 22

User Account Configuration 22

VDP Best Practices 23

General Best Practices 23

HotAdd Best Practices 24

Storage Capacity for Initial VDP Deployment 24

Monitoring VDP Capacity 24

VDP Installation 25

Deploying the OVF Template 25

Initial Configuration 26

3 VDP Appliance Upgrades 31

Best Practices 32

Supported Upgrade Paths 32

Creating a Snapshot of the VDP Appliance 33

Mounting the Upgrade ISO Image on the Appliance 34

Installing the Upgrade 34

Freeing up space for the upgrade 36

Completing the Upgrade 36

Reverting Back to a Snapshot 37

Upgrading Proxy Software 38

4 Post-Installation Configuration of VDP Appliance 41

About the VDP Configure Utility 42

Viewing Status 42

Starting and Stopping Services 43

Collecting Logs 44

Modifying Configuration Settings 45

Network Settings 45

vCenter Server Registration 45

Rolling Back an Appliance 46

Emergency Restore 46

Automatic Host Detection 49

Refreshing Restore Points 49

Reconnecting the Host to the vCenter 49

5 Securing Communication between vCenter and VDP 51

Secure VDP Services Communication to vCenter 52

Secure External Proxy Communication with vCenter 53

6 Configuring VDP 55

Login Security 56

Configuring the Customer Experience Improvement Program 56

Configuration and Monitoring 57

Viewing Backup Appliance Configuration 57

Editing the Backup Window 58

Configuring Email 58

Viewing the User Interface Log 59

Running an Integrity Check 60

Monitoring VDP Activity 60

Viewing Recent Tasks 61

Viewing Alarms 61

Viewing the Event Console 62

VDP Shutdown and Startup Procedures 62

7 Proxies 63

Proxy Overview 64

Considerations Before Deploying an External Proxy 64

Deployment of External Proxies 64

Number of Proxies to Deploy and Proxy Throughputs per Proxy 64

Best Practices when Deploying a VDP Appliance 65

Managing Internal and External Proxies 66

External Proxy Support 66

Adding an External Proxy 68

Disabling the Internal Proxy 68

(Optional) Configuring Proxy Certificate Authentication 69

Monitoring External Proxy Health Status 69

Health Status Criteria 69

External Proxy Logs 69

8 Storage Management 71

Creating New Storage 72

Minimum Storage Performance 73

Attaching Existing VDP Disks 73

Detaching and Reattaching Storage 75

Viewing the Storage Configuration 76

9 Data Domain Integration 79

VDP and Data Domain System Integration 80
Architecture Overview 80
VDP Client Support 81
Best Practices 81
Data Domain Limitations 82
Backup 82
Restore 82
Security — Encryption 82
Data Migration 82
Pre-integration Requirements 82
Network Throughput 83
Network Configuration 83
NTP Configuration 83
Licensing 84
Port Usage and Firewall Requirements 84
Capacity 84
Data Domain System Streams 84
Existing Backup Products in Use with Data Domain 85
Preparing the Data Domain system for VDP Integration 85
Adding a Data Domain System 86
Changing the Max Streams Value 87
Editing the Data Domain System 87
Deleting the Data Domain System from the VDP Appliance 88
Backups with VDP and Data Domain 90
How Backups Work with VDP and Data Domain 90
Where Backup Data is Stored 90
How VDP Appliance Manages Backup Data 90
Supported Backup Types 90
Canceling and Deleting Backups 90
Selecting a Data Domain Target for Backups 91
Replication Control 91
Replication Data Flow 91
Replication Schedule 91
Replication Configuration 92
Replication Monitoring with VDP 92
Server Maintenance Activity Monitoring 92
Restoring Avamar Checkpoint backups from Data Domain systems 92
Assumptions for the Restore Operation 92
Performing the Checkpoint Restore 93
Monitoring Data Domain from the VDP Appliance 94
Monitoring Using the vSphere Web Client 94
Monitoring Using the VDP Configure UI 94
Data Domain Capacity Monitoring 95
Reclaiming Storage on a Full Data Domain System 95
Common Problems and Solutions 96
Backup Fails if the Data Domain System is Offline 96
Rolling Back after Deleting a Data Domain System 97

10 VDP Disk Expansion 99

Pre-Expansion Requirements 100
VMFS Heap Size Recommendations 100
Performing Disk Expansion 101

Viewing the Storage Configuration 102
Performance Analysis 103
Running the Performance Analysis Test 103
Disk Expansion with Essentials Plus 103

11 Using vSphere Data Protection 105
Accessing vSphere Data Protection 106
Accessing the VDP Appliance Command Line 106
Understanding the VDP User Interface 107
Switching VDP Appliances 107
VDP User Interface 108
Viewing Information from the Reports Tab 108
Refresh 108
Task Failures Tab 108
Job Details Tab 109
Unprotected Clients Tab 110

12 Managing Backups 111
Backup Jobs 112
Choosing the Virtual Machines 112
Identifying retired virtual machines 112
Specifying the Backup Schedule 113
Setting the Retention Policy 113
Creating a Full Image Backup Job 114
Creating a Backup Job on Individual Disks 115
Unsupported disk types 116
Limitation 116
Migration on Individual Disks 117
Viewing Status and Backup Job Details 117
Editing a Backup Job 117
Cloning a Backup Job 117
Deleting a Backup Job 118
Enabling or Disabling a Backup Job 118
Running Existing Backup Jobs Immediately 118
Locking and Unlocking a Backup 119

13 Automatic Backup Verification 121
About Automatic Backup Verification 122
Limitations 122
Best Practices 122
Creating a New Backup Verification Job 123
Editing a Backup Verification Job 124
Cloning a Backup Verification Job 125
Executing and Running a Backup Verification Job 125
Monitoring Backup Verification 126
Enabling and Disabling a Backup Verification Job 126
Deleting a Backup Verification Job 126

14 Managing Restores 127
Restore Operations 128
Limitations 128
Selecting Backups to Restore 128
Filtering for List of Backups 128

Restores when Snapshots Are Present 128
Restoring Image Backups to the Original Location 128
Restoring Image Backups to a New Location 130
Restoring Backups to Individual SCSI Disks 131
Deleting a Backup from the Restore Tab 132
Clearing all Selected Backups from the Restore Tab 132

15 Replication 133
Replication Jobs 134
Replication Compatibility 134
Replication and Data Domain 136
Best Practices when Replicating 136
Limitations 136
Defining Backup Types for a Replication Job 136
Creating a Replication Job 136
Managing Destinations 140
Editing a Replication Job 140
Cloning a Replication Job 141
Deleting a Replication Job 141
Enabling or Disabling a Replication Job 141
Viewing Status and Replication Job Details 141
Running Existing Replication Jobs Immediately 141
Replication Back to the Source 141
Node Structure for Recovered Backups 142
Node Structure of Backups Replicated Again 142
Replication Destinations 142
Replication Recovery Compatibility 142
Enabling or Disabling Replication Recovery 143
Replication Recovery 143
Multi-Tenancy 144

16 Using File Level Restore 147
Introduction to the VDP Restore Client 148
LVM / EXT Support 148
File Level Restore Limitations 148
Unsupported VMDK Configurations 148
Unsupported Windows Configurations 149
Logging in to the Restore Client 149
Basic Login 149
Advanced Login 150
Mounting Backups 150
Filtering Backups 150
Navigating Mounted Backups 151
Performing File Level Restores 151
Using the Restore Client in Basic Login Mode 151
Using the Restore Client in Advanced Login Mode 152
Monitoring Restores 152

17 VDP Application Support 153
VDP Application Support 154
Installing Application Agents 154
Checking the User Account Control Setting on Microsoft Windows 154
Installing VDP Clients when UAC is Enabled 154
Backing Up and Restoring Microsoft SQL Servers 155

Microsoft SQL Server Options 155
Hardware Requirements 155
Microsoft SQL Server Support 155
Installing VDP for SQL Server Client 156
Configuring the Cluster Client in a Failover Cluster 157
Configuring the Cluster Client for an AlwaysOn Availability Group 159
Creating Backup Jobs for Microsoft SQL Servers 160
Restoring Backups of Microsoft SQL Servers 163
Monitoring Client Activity 164
Uninstalling the VDP Plug-in for SQL Server 164
Backing Up and Restoring Microsoft Exchange Servers 164
Microsoft Exchange Server Options 164
Microsoft Exchange Server Support 165
Microsoft .NET Framework 4 Requirement 165
Hardware Requirements 165
Unsupported Microsoft Exchange Servers 165
Installing VDP for Exchange Server Client 165
Installing in a DAG or Cluster Environment 166
Configuring an Exchange DAG Client 167
Using the VMware Exchange Backup User Configuration Tool 168
Manually Configuring the VDP Backup Service 170
Creating Backup Jobs for Microsoft Exchange Servers 170
Restoring Backups of Microsoft Exchange Servers 172
Suspending Replication in a DAG or Cluster 173
Monitoring Client Activity 173
Uninstalling the Exchange Server Plug-in 174
Granular Level Recovery on Microsoft Exchange Servers 174
Backing Up and Restoring Microsoft SharePoint Servers 177
Hardware Requirements 177
Supported Microsoft SharePoint Servers 177
Installing VDP for SharePoint Server Client 178
Creating Backup Jobs for Microsoft SharePoint Servers 178
Restoring Backups of Microsoft SharePoint Servers 179
Monitoring Client Activity 180
Uninstalling the VDP Plug-in for SharePoint Server 180

18 VDP Disaster Recovery 181
Basic Disaster Recovery 182
Extended Data Protection 182
Best Practices for Archiving the VDP Appliance to Tape 182
Exporting the Replication Target 183
Configuring Backups for Tape-Out 183
Backing Up VDP Replication Target to Tape 183
Restoring the VDP Replication Target from Tape to the vCenter 184

A vSphere Data Protection Port Usage 187

B Minimum Required vCenter User Account Permissions 189

C vSphere Data Protection Troubleshooting 193
Troubleshooting VDP Appliance Installation 194
Troubleshooting the Installer Package 194
Troubleshooting Accessing the VDP Web Client 194
Troubleshooting VDP Backups 194

Troubleshooting VDP Restores 196
Troubleshooting VDP Replication Jobs 197
Troubleshooting VDP Integrity Check 197
Troubleshooting Automatic Backup Verification 197
Troubleshooting the Restore Client (File Level Recovery) 198
Troubleshooting VDP Advanced Licensing 199
Troubleshooting the VDP Appliance 201
Troubleshooting VDP Microsoft Exchange Server 201
Troubleshooting VDP Microsoft SQL Server 203
Troubleshooting VDP Microsoft SharePoint 203
Accessing VDP Knowledge Base Articles 203

Index 205

About This Book

The *vSphere Data Protection Administration Guide* describes how to install and manage backups for small and medium businesses. This guide also includes troubleshooting scenarios and recommendations for resolution.

Intended Audience

This book is for anyone who wants to provide backup solutions by using vSphere® Data Protection (VDP). The information in this book is for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Typographical conventions

VMware uses the following type style conventions in this document:

Bold	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: ■ System output, such as an error message or script ■ System code ■ Pathnames, filenames, prompts, and syntax ■ Commands and options
`Monospace italic`	Use for variables
`Monospace bold`	Use for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Document Feedback

VMware welcomes your suggestions for improving our documentation. Send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current versions of other VMware books, go to http://www.vmware.com/support/pubs.

Online Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Understanding VDP

1

This chapter includes the following topics:

- "Introduction to vSphere Data Protection" on page 14
- "Benefits of vSphere Data Protection" on page 14
- "VDP Functionality" on page 15
- "Replication" on page 17
- "File Level Recovery" on page 17
- "Customer Experience Improvement Program" on page 17
- "vSphere Data Protection Architecture" on page 17

Introduction to vSphere Data Protection

vSphere Data Protection (VDP) is a robust, simple to deploy, disk-based backup and recovery solution that is powered by EMC. VDP is fully integrated with the VMware vCenter Server and enables centralized and efficient management of backup jobs while storing backups in deduplicated destination storage locations.

The VMware vSphere Web Client interface is used to select, schedule, configure, and manage backups and recoveries of virtual machines.

During a backup, VDP creates a quiesced snapshot of the virtual machine. Deduplication is automatically performed with every backup operation.

The following terms are used throughout this document in the context of backup and recovery.

- A **datastore** is 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.
- **Changed Block Tracking (CBT)** is 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.
- **File Level Recovery (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 VDP Restore Client.
- **VMware 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 machine.
- **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.
- **VDP Appliance** is a purpose-built virtual appliance for VDP.

Benefits of vSphere Data Protection

The benefits of vSphere Data Protection (VDP) are as follows:

- Provides fast and efficient data protection for all of your virtual machines, even those powered off or migrated between vSphere hosts.
- Significantly reduces disk space consumed by backup data using patented variable-length deduplication across all backups.
- Reduces the cost of backing up virtual machines and minimizes the backup window by using Change Block Tracking (CBT) and VMware virtual machine snapshots.
- Allows for easy backups without the need for third-party agents installed in each virtual machine.
- Uses a simple, straight-forward installation as an integrated component within vSphere, which is managed by a web portal.
- Provides direct access to VDP 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.
- Through emergency restore, provides a method for restoring the vCenter Server when the vCenter Server is unavailable or the user is unable to access the VDP user interface with the vSphere Web Client.
- Through replication, enables you to avoid data loss if the source VDP Appliance fails because copies of the backups are available on a destination target.

- 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 over and over again. vSphere Data Protection uses 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 for determining segment size. Fixed-block or fixed-length segments are commonly employed by snapshot and some deduplication technologies. 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. vSphere Data Protection uses an intelligent variable-length method for determining segment size that examines the data to determine logical boundary points, which increases efficiency.

- Logical Segment Determination

  VDP uses a patented method for segment size determination designed to yield optimal efficiency across all systems. VDP's algorithm analyzes the binary structure of a dataset to determine segment boundaries that are context-dependent. Variable-length segments average 24 KB in size and are further compressed to an average of 12 KB. By analyzing the binary structure within the VMDK file, VDP works for all file types and sizes and deduplicates the data.

VDP Functionality

The vSphere Data Protection product, starting with version 6.0, includes all features that were previously included in VDP Advanced. VDP functionality is included as part of vSphere Essential+ and does not require a specific license key. The following table lists VDP functionality.

Table 1-1. VDP Functionality

Feature	VDP
Virtual machines supported per VDP Appliance	Up to 400
Number of appliances supported per vCenter	Up to 20
Available storage size	8 TB
Support for image-level backups	Yes
Support for individual disk backups	Yes
Support for image-level restore jobs	Yes
Support for image-level replication jobs	Yes
Support for direct to host recovery	Yes
Support for detachable/remountable data partitions	Yes
Support for file level recovery (FLR)	Yes — Supports LVM and EXT4 with external proxies
Support for guest-level backups and restores of Microsoft Exchange Servers, SQL Servers, and SharePoint Servers	Yes
Support for application-level replication	Yes
Ability to expand current datastore	Yes
Support for backing up to a Data Domain system	Yes
Ability to restore to a granular level on Microsoft Servers	Yes
Support for automatic backup verification (ABV)	Yes

Table 1-1. VDP Functionality (Continued)

Feature	VDP
Support for external proxies	Yes, up to 24 simultaneous virtual machines if the maximum number of 8 external proxies are deployed.
Support for Customer Experience Improvement Program	Yes

Image-level Backup and Restore

vSphere Data Protection creates image-level backups, which are integrated with the vStorage API for Data Protection, a feature set within vSphere to offload the backup processing overhead from the virtual machine to the VDP Appliance. The VDP Appliance communicates with the vCenter Server to make a snapshot of a virtual machine's .vmdk files. Deduplication takes place within the appliance by using a patented variable-length deduplication technology.

To support the large scale and continually expanding size of many VMware environments, each VDP Appliance can simultaneously back up to 8 virtual machines if the internal proxy is used, or back up to 24 virtual machines if the maximum number of 8 external proxies are deployed with the VDP Appliance.

To increase the efficiency of image-level backups, VDP utilizes the Changed Block Tracking (CBT) feature, which greatly reduces the backup time of a given virtual machine image and provides the ability to process a large number of virtual machines within a particular backup window.

By leveraging CBT during restores, VDP offers fast and efficient recoveries of virtual machines to their original location. During a restore process, VDP uses CBT to determine which blocks have changed since the last backup. The use of CBT reduces data transfer within the vSphere environment during a recovery operation and more importantly reduces the recovery time.

Additionally, VDP automatically evaluates the workload between both restore methods (full image restore or a recovery leveraging CBT) and performs the method resulting in the fastest restore time. This is useful in scenarios where the change rate since the last backup in a virtual machine being restored is very high and the overhead of a CBT analysis operation would be more costly than a direct full-image recovery. VDP determines which method results in the fastest image recovery times for virtual machines in the environment.

IMPORTANT VDP does not support backups of a vCenter Server Appliance (VCSA). The VDP virtual environment, however, can include a VCSA.

Single VMDK Backup and Restore

A full image backup job includes all disks in the entire virtual machine (VM) in a single image backup. Individual disk backup jobs allow you to select only the disks you need. An image-level backup of a VM with unsupported disk types does not include the unsupported disk types because of snapshot limitations.

When you restore a VM, the VDP Appliance restores the VM configuration file (.vmx), which results in the creation of all VMDKs from the original VM. If any of the original VMDKs were not backed up, the restore process creates them as provisional VMDKs. The VM may not be fully functional in this case. The protected VMDKs, however, can be accessed from the restore.

See "Creating a Backup Job on Individual Disks" on page 115 for instructions on backing up individual disks.

Guest-level Backup and Restore

VDP supports guest-level backups for Microsoft SQL Servers, Exchange Servers, and Share Point Servers. With guest-level backups, client agents (VMware VDP for SQL Server Client, VMware VDP for Exchange Server Client, or VMware VDP for SharePoint Server Client) are installed on the SQL Server, Exchange Server, or SharePoint Server in the same manner that backup agents are typically installed on physical servers.

The advantages of VMware guest-level backups are:

- Provides additional application support for Microsoft SQL Server, Microsoft Exchange Server, or SharePoint Server inside the virtual machines
- Support for backing up and restoring entire Microsoft SQL Server, Microsoft Exchange Server, or SharePoint Servers or selected databases
- Identical backup methods for physical and virtual machines

See "VDP Application Support" on page 151 for additional information on guest-level backup and restore.

Replication

Replication enables you to avoid data loss if the source VDP Appliance fails because copies of the backups are available on the destination target.

Replication jobs determine which backups are replicated, and when and to where the backups are replicated. With scheduled or ad hoc replication jobs for clients that have no restore points, only the client is replicated on the destination server. Backups created with VDP 6.0 or later can be replicated to another VDP Appliance, to an EMC Avamar server, or to a Data Domain system. If the target VDP Appliance is 5.8 or earlier, then the target must be VDP Advanced or Replication Target Identity.

See Chapter 15, "Replication," on page 133 for additional information on Replication.

File Level Recovery

File Level Recovery (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 by using the VDP Restore Client.

See Chapter 16, "Using File Level Restore," on page 147 for additional information on FLR.

Customer Experience Improvement Program

The Customer Experience Improvement Program is an option that enables you to send encrypted configuration and usage information about the VDP environment to VMware servers for analysis. The purpose of the Customer Experience Improvement Program is to help VDP improve the quality, reliability, and functionality of the VDP product. The Customer Experience Improvement Program is not enabled by default. During installation, you can enable the Customer Experience Improvement Program from the Product Improvement page in the VDP Configure Utility. You can also enable or disable this option any time after the installation of VDP from the post-installation UI. Refer to "Configuring the Customer Experience Improvement Program" on page 56 for more information.

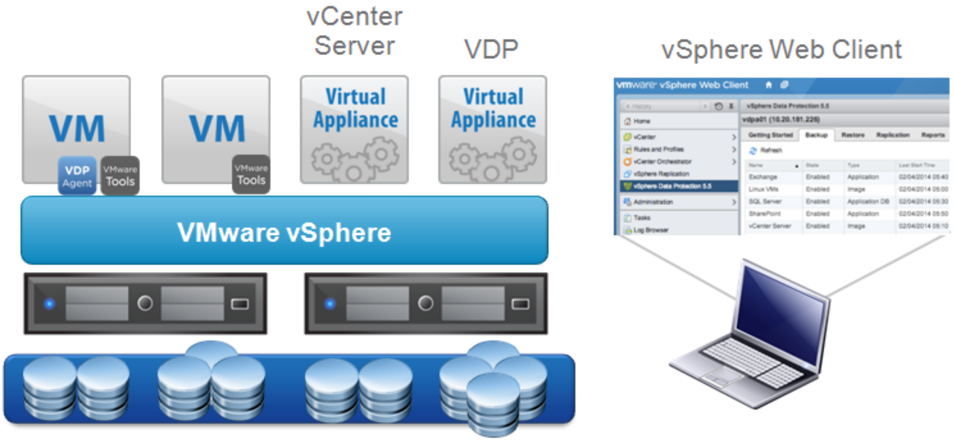
vSphere Data Protection Architecture

VDP can be deployed to any storage supported by vSphere. Supported storage includes VMFS, NFS, and VSAN datastores. Management of VDP is performed by using the vSphere Web Client.

VDP consists of the following components:

- vCenter Server 5.1 or later (5.5 or later recommended)
- VDP virtual appliance (installed on vSphere hosts; versions 5.0, 5.1, and 5.5 are supported)
- vSphere Web Client
- Application backup agents

Backup data is deduplicated and stored in the .vmdk files that make up the VDP virtual appliance or a supported Data Domain appliance.



Name	State	Type	Last Start Time
Exchange	Enabled	Application	02/04/2014 05:40
Linux VMs	Enabled	Image	02/04/2014 05:00
SQL Server	Enabled	Application DB	02/04/2014 05:30
SharePoint	Enabled	Application	02/04/2014 05:50
vCenter Server	Enabled	Image	02/04/2014 05:10

Figure 1-1. vSphere Data Protection architecture

VDP Installation and Configuration 2

This chapter includes the following topics:

- "vSphere Data Protection Capacity Requirements" on page 20
- "Software Requirements" on page 20
- "System Requirements" on page 20
- "Preinstallation Configuration" on page 21
- "VDP Best Practices" on page 23
- "VDP Installation" on page 25
- "Initial Configuration" on page 26

vSphere Data Protection Capacity Requirements

vSphere Data Protection (VDP) capacity requirements depend on a number of factors including:

- Number of protected virtual machines
- Amount of data contained in each protected virtual machine
- Types of data being backed up (OS files, documents, and databases, for example)
- Backup data retention period (daily, weekly, monthly, or yearly)
- Data change rates

NOTE Assuming average virtual machine sizes, data types, data change rates, and a retention policy of 30 days, 1 TB of VDP backup data capacity supports approximately 25 virtual machines.

Software Requirements

Using the latest version (6.0) of VDP is recommended. VDP 6.0 requires the following software:

- The minimum requirement is vCenter Server 5.1, while vCenter Server 5.5 or later is recommended. VDP version 6.0 supports the Linux-based vCenter Server Virtual Appliance and the Windows-based vCenter Server.

NOTE VDP 5.1 is not compatible with vCenter 5.5 or later.

  - vSphere Web Client (see the VMware web site for current vSphere web browser support)
  - Web browsers must be enabled with Adobe Flash Player 11.3 or later to access the vSphere Web Client and VDP functionality

- vSphere host versions 5.0, 5.1, or 5.5

Hardware Versions and Migration

The virtual machine's hardware version limits virtual machines from migrating to the older versions that are configured on the newer versions of vSphere hosts. If the VDP Appliance was migrated to a vSphere host that was version 5.1 or lower, it would not be functional.

vSphere Hosts and vSphere Flash Read Cache Compatibility and Performance

The VDP Appliance is deployed as a virtual machine with hardware version 7, which enables backward compatibility with vSphere 4.*x* hosts. The vSphere Flash Read Cache-backed disks are only available on vSphere 5.*x* hosts, which expect a VM to have hardware version 10. As a result, if you attempt to perform an image-level backup of a vSphere Flash Read Cache-backed disk by using the VDP Appliance, then the current configuration causes the appliance to use the network block device (NBD) protocol (instead of HotAdd) as the transport mode, which adversely affects performance.

Unsupported Disk Types

- When planning for backups, make sure the disks are supported by VDP. Currently, VDP does not support the following virtual hardware disk types:
  - Independent
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode

System Requirements

The following section lists the system requirements for VDP.

VDP System Requirements

VDP is available in the following configurations:

- 0.5 TB
- 1 TB
- 2 TB
- 4 TB
- 6 TB
- 8 TB

IMPORTANT AfterVDP is deployed the size can be increased.

VDP requires the following minimum system requirements:

Table 2-2. Minimum system requirements for VDP

	0.5 TB	1 TB	2 TB	4 TB	6 TB	8 TB
Processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors
Memory	4 GB	4 GB	4 GB	8 GB	10 GB	12 GB
Disk space	873 GB	1,600 GB	3 TB	6 TB	9 TB	12 TB

IPv6 Requirements

DNS servers that VDP uses in an IPv6 environment must only contain AAAA records for hostnames. The DNS server must not contain both an A and an AAAA record with the same hostname.

Preinstallation Configuration

Before the VDP installation, complete the following preinstallation steps:

- "DNS Configuration" on page 21
- "NTP Configuration" on page 22
- "User Account Configuration" on page 22
- "VDP Best Practices" on page 23

DNS Configuration

The DNS server must support both forward and reverse lookup on the VDP and the vCenter.

Before you deploy VDP, you must add an entry to the DNS server for the VDP Appliance's IP address and Fully Qualified Domain Names (FQDN). In addition, communication to DNS is required by VMware proxy nodes (port 53) over both TCP and UDP protocols. Failure to set up DNS properly can cause many runtime or configuration issues.

To confirm that DNS is configured properly, run the following commands from the command prompt on the vCenter Server:

- `nslookup` <*FQDN_of_VDP*>

  The `nslookup` command returns the FQDN of the VDP Appliance.

- `nslookup` <*FQDN_of_vCenter*>

  The `nslookup` command returns the FQDN of the vCenter Server.

If the `nslookup` commands return the proper information, close the command prompt. If the `nslookup` commands do not return the information you seek, you can manually add the VDP name and address to the `/etc/hosts` file in the vCenter.

NTP Configuration

VDP leverages VMware Tools to synchronize time through NTP. All vSphere hosts and the vCenter Server must have NTP configured properly. The VDP Appliance gets the correct time through vSphere and must not be configured with NTP.

CAUTION Configuring NTP directly on the VDP Appliance causes time synchronization errors.

See the ESXi and vCenter Server documentation for more information about configuring NTP.

vCenter Hosts and Clusters View

The VDP Appliance can work with folders and resource views that are created under the Hosts and Clusters view. The Hosts and Clusters view in the vSphere Web Client allow you to perform the following tasks:

- Configure user accounts
- Create a snapshot
- Mount the ISO image
- Remove a snapshot
- Revert back to a snapshot
- Expand disks
- Configure the VDP Appliance system settings.
- Remove the VDP Appliance from the vCenter inventory.

Accessing the Host and Clusters view

1 From a web browser, access the vSphere Web Client:

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

2 Log in with administrative privileges.

3 Select **vCenter** > **Hosts and Clusters**.

User Account Configuration

Before the vCenter user account can be used with VDP, or before the SSO admin user can be used with VDP, you must add these users as administrator on the vCenter root node. Users who inherit permissions from group roles are not valid.

NOTE In high-security environments, you can restrict the vCenter user account permissions required to configure and administer the VDP Appliance. The account permission categories are listed in "Minimum Required vCenter User Account Permissions" on page 189.

The following steps are used to configure the VDP user or SSO admin user using the vSphere Web Client.

1 From a web browser, access the vSphere Web Client:

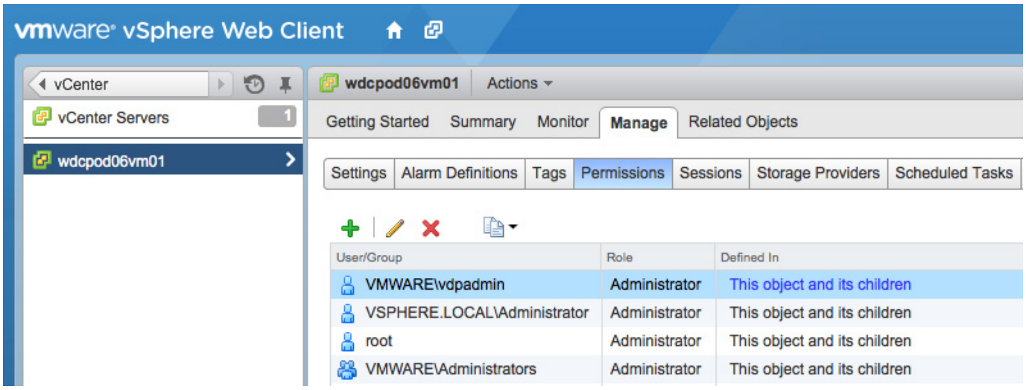
https://<*IP_address_vCenter_Server*>:9443/vsphere-client/

2 Log in with administrative privileges.

3 Select **vCenter** > **Hosts and Clusters**.

4 On the left side of the page, click the vCenter Server.

IMPORTANT Ensure that you select the vCenter from the root level of the tree structure (represented under Hosts and Clusters). If you select the vCenter VM, the configuration fails.



User/Group	Role	Defined In
VMWARE\vdpadmin	Administrator	This object and its children
VSPHERE.LOCAL\Administrator	Administrator	This object and its children
root	Administrator	This object and its children
VMWARE\Administrators	Administrator	This object and its children

5 Click the **Manage** tab, and then select **Permissions**.

6 Click the **Add permission (+)** icon.

7 Click **Add**.

8 From the Domain drop-down list, select domain, server, or VSPHERE.LOCAL.

NOTE: For vCenter versions 5.1 and earlier, the default domain is SYSTEM-DOMAIN.

9 Select the user who will administer VDP or be the SSO admin user, and then click **Add**.

10 Click **OK**.

11 From the **Assigned Role** list, select **Administrator**.

12 Confirm that the **Propagate to child objects** box is selected.

13 Click **OK**.

To verify that user is listed under Administrators, go to **Home > Administration > Role Manager** and click the **Administrator** role. The user you just added should be listed to the right of that role.

IMPORTANT If the VDP backup user using the VDP Configure utility belongs to a domain account, use the "SYSTEM-DOMAIN\admin" format in VDP-configure. If the username is entered in the format "admin@SYSTEM-DOMAIN" format, tasks related to the backup job may not show up on the Recent Running tasks.

IMPORTANT The domain account password cannot contain spaces.

VDP Best Practices

The following best practices should be used when deploying, using, and monitoring a vSphere Data Protection (VDP) Appliance.

General Best Practices

- Deploy the VDP Appliance on shared VMFS5 or later to avoid block size limitations.
- Make sure that all virtual machines are running hardware version 7 or later to support Change Block Tracking (CBT).
- Install VMware Tools on each virtual machine that VDP will back up. VMware Tools add additional backup capability that quiesces certain processes on the guest OS before the backup. VMware Tools are also required for some features used in File Level Restore.

- When configuring the network for the VDP Appliance and the vCenter, do not modify network address information by using NAT or other configuration methods (firewall, IDS, or TSNR). When these unsupported methods are deployed as part of the virtual network, some VDP functionality may not work as designed.

HotAdd Best Practices

The HotAdd transport mechanism is recommended for faster backups and restores and less exposure to network routing, firewall and SSL certificate issues. If you use the network block device (NBD) transport mechanism instead of HotAdd, backup performance will be degraded.

The following mandatory requirements must be met for a disk to be mounted with HotAdd:

- If you are using vSphere Host version 5.0, the host must be licensed for HotAdd. vSphere Host version 5.1 and later include this feature by default.
- The VDP Appliance is deployed on a vSphere host that has a path to the storage that contains the virtual disks being backed up.
- HotAdd is not used on IDE-configured virtual disks. I/O over the network negatively impacts performance. Use SCSI virtual disks instead.
- The total capacity of the VMFS volume where VDP resides is equal to the size of the largest virtual disk being backed up (free space can be less than this amount).
- The block size of the VMFS volume where VDP resides is the same or larger than the size of the largest virtual disk being backed up.
- The virtual machine being backed up has no virtual hard disks designated as Independent.
- The virtual machine being backed up is in the same datacenter (vCenter Server container object) as the VDP Appliance. HotAdd transport cannot cross the datacenter boundary.
- The virtual machines and VMDKs in the vCenter Server have the same name as those associated with the virtual machine being backed up.
- HotAdd does not work with virtual machines that use vSphere Flash Read Cache (vFlash).

For more information about HotAdd best practices, refer to the following Knowledge Base article:

http://kb.vmware.com/kb/2048138

Storage Capacity for Initial VDP Deployment

When a new vSphere Data Protection (VDP) Appliance is deployed, the appliance typically fills rapidly for the first few weeks. This is because nearly every client that is backed up contains unique data. VDP deduplication is most effective when other similar clients have been backed up, or the same clients have been backed up at least once.

After the initial backup, the appliance backs up less unique data during subsequent backups. When initial backups are complete and the maximum retention periods are exceeded, it is possible to consider and measure the ability of the system to store about as much new data as it frees each day. This is referred to as achieving steady state capacity utilization. Ideal steady state capacity should be 80%.

Monitoring VDP Capacity

You should proactively monitor VDP capacity. You can view VDP capacity through the **VDP Reports** tab, Used Capacity (which is used to determine steady state). Refer to "Viewing Information from the Reports Tab" on page 108 for more information.

Table 2-3 describes VDP behavior for key capacity thresholds:

Table 2-3. Capacity thresholds

Threshold	Value	Behavior
Capacity warning	80%	VDP issues a warning event.
Capacity warning	95%	Tasks are not generated on vCenter for backup jobs when capacity is greater than 95% full.
Healthcheck limit	95%	Existing backups are allowed to complete but new backup activities are suspended. VDP issues warning events.
Server read-only limit	100%	VDP transitions to read-only mode and no new data is allowed.

Once you exceed 80% capacity, use the following guidelines for capacity management:

- Stop adding new virtual machines as backup clients.
- Remove unnecessary restore points.
- Delete jobs that are no longer needed.
- Reassess retention policies to see if you can decrease retention policies
- Consider adding additional VDP Appliances and balance backup jobs between multiple appliances

VDP Installation

The vSphere Data Protection (VDP) installation is completed through two steps:

- "Deploying the OVF Template" on page 25
- "Initial Configuration" on page 26

Deploying the OVF Template

Prerequisites

- The VDP Appliance requires one of the following vSphere host versions: 5.0, 5.1, or 5.5.
- The minimum requirement is vCenter Server 5.1. vCenter Server 5.5 or later is recommended.
- Log in to the vCenter Server from a vSphere Web Client to deploy the OVF template. If you are unable to connect to the vSphere Web Client, confirm that the vSphere Web Client service is started.
- The VDP Appliance connects to a vSphere host using port 902. If there is a firewall between the VDP Appliance and the vSphere Host, port 902 must be open. See Chapter A, "vSphere Data Protection Port Usage," on page 187, for additional information on port usage.
- The VMware Client Integration Plug-in must be installed on your browser. If it is not already installed, it can be installed during the following procedure.

Procedure

1 From a web browser, access the vSphere Web Client:

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

2 Log in with administrative privileges.

3 Select **vCenter > Datacenters.**

4 On the **Objects** tab, click **Actions > Deploy OVF Template.**

5 If prompted, allow and install the VMware Client Integration Plug-in.

6 Select the source where the VDP Appliance is located. By default the File name dialog is set to OVF Packages (*.ovf). From the drop-down box to the right of File name, select **OVA Packages (*.ova)**.

7 Navigate to the location of the VDP Appliance .ova file. Confirm that you select the appropriate file for the datastore. Click **Open**.

8 After the VDP Appliance .ova file is selected, click **Next**.

9 Review the template details and click **Next**.

10 On the Accept EULAs screen, read the license agreement, click **Accept**, and then click **Next**.

11 On the Select name and folder screen, type the name for the VDP Appliance. When typing the name, use the fully qualified domain name (FQDN), which the VDP configuration uses to find the VDP Appliance in the vCenter inventory. Do not change the VDP Appliance name after installation.

12 Click the folder or datacenter where you want to deploy the VDP Appliance, and then click **Next.**

13 On the Select a resource screen, select the host for the VDP Appliance and click **Next**.

14 On the Select Storage screen, select the virtual disk format and select the location of the storage for the VDP Appliance. Click **Next**.

15 On the Setup networks screen, select the Destination Network for the VDP Appliance and click **Next**.

16 In the Customize template screen, specify the **Default Gateway**, **DNS**, **Network 1 IP Address**, and **Network 1 Netmask**. Confirm that the IP addresses are correct and match the entry in the DNS server. Setting incorrect IP addresses in this dialog box will require the .ova to be redeployed. Click **Next**.

NOTE The VDP Appliance does not support DHCP. A static IP address is required.

17 On the Ready to complete screen, confirm that all of the deployment options are correct. Check **Power on** after deployment and click **Finish**.

vCenter deploys the VDP Appliance and boots into the install mode. You can monitor **Recent Tasks** to determine when the deployment completes.

Initial Configuration

Prerequisites

- Ensure that the VDP `.ovf` template was deployed successfully. See “Deploying the OVF Template” on page 25 for more information.
- You must be logged into the vCenter Server from the vSphere Web Client.
- Enough free disk space exists on the datastore. When an optional performance analysis test is run during initial configuration of the appliance, 41 GB per disk per datastore is required (for example, if three disks are placed on the same datastore, 123 GB of free space is required). If there is not enough space available, the test reports a value of 0 for all of the read, write, and seek tests and gives a final status of insufficient space.

Procedure

1 From a web browser, access the vSphere Web Client:

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

2 Log in with administrative privileges.

3 Select **vCenter Home > vCenter > VMs and Templates**. Expand the vCenter tree and select the VDP Appliance.

4 Open a console session into the VDP Appliance by right-clicking the VDP Appliance and selecting **Open Console**.

5 After the installation files load, the Welcome screen for the VDP menu appears. Open a web browser and type:

https://<IP_address_VDP_Appliance>**:8543/vdp-configure/**

The VMware Login screen appears.

6 Type **root** in the **User** field and **changeme** in the **Password** field, and then click **Login**.

The VDP Welcome screen appears.

7 Click **Next**.

The Network Settings dialog box appears by default.

8 Specify (or confirm) the following network and server information for your VDP Appliance. Ensure that the values are populated correctly, otherwise the installation will fail.

a IPv4 Static address

b Netmask

c Gateway

d Primary DNS

e Secondary DNS

f Hostname

g Domain

9 Click **Next**.

The Time Zone dialog box appears.

10 Select the appropriate time zone for your VDP Appliance, and click **Next**.

The VDP Credentials dialog box appears.

11 In the **Password** field, type in the VDP Appliance password by using the following criteria, and then verify the password by retyping it in the **Verify password** field. This passwordis the universal configuration password.

The four-character classes are as follows:

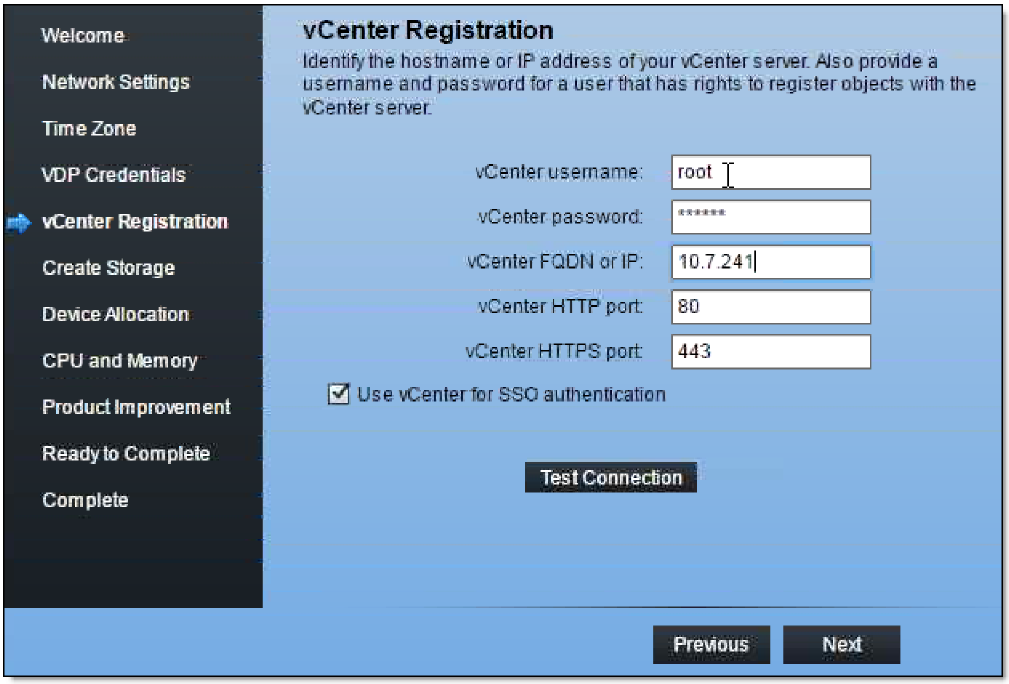
- Upper case letters A-Z
- Lower case letters a-z
- Numbers 0-9
- Special characters (for example: ~!@#,.)

Create the password using the following criteria:

- If all four character classes are used, the password must be at least 6 characters.
- If three character classes are used, the password must be at least 7 characters.
- If one or two character classes are used, the password must be at least 8 characters.

12 Click **Next**.

The vCenter Registration page appears.



vCenter Registration

Identify the hostname or IP address of your vCenter server. Also provide a username and password for a user that has rights to register objects with the vCenter server.

vCenter username: root

vCenter password: ******

vCenter FQDN or IP: 10.7.241

vCenter HTTP port: 80

vCenter HTTPS port: 443

☑ Use vCenter for SSO authentication

13 Specify the following values:

a vCenter username

If the user belongs to a domain account, enter the name by using the “SYSTEM-DOMAIN\admin” format.

CAUTION If an SSO admin user is specified as the vCenter username in the format <username@vsphere.local>, tasks related to VDP operations do not appear in the vCenter Recent Tasks pane of the vSphere Web Client. For tasks to appear in the Recent Tasks pane, specify the SSO admin user in the format <vsphere.local\username>.

b vCenter password

c vCenter FQDN or IP

d vCenter HTTP port (default is 80)

Specify a custom value for the HTTP port if you need to connect to vCenter over the HTTP port, instead of the HTTPS port, which is used for all other communication.

e vCenter HTTPS port (default is 443)

f If disabled, select the **Use vCenter for SSO authentication** checkbox for SSO authentication.

NOTE Leave the **Use vCenter for SSO authentication** checkbox enabled if your vCenter has SSO embedded in the vCenter Server appliance. If you disable this selection by clearing the checkbox, you must enter the SSO Server FQDN or IP address and the SSO port fields.

g Click **Test Connection**.

A connection success message appears. If this message does not appear, troubleshoot your settings and repeat this step until a successful message appears.

If you receive the following message on the vCenter Registration page:

```
Specified user either is not a dedicated VDP user or does not have sufficient vCenter
privileges to administer VDP. Please update your user role and try again.
```

Refer to “User Account Configuration” on page 22 for instructions on how to update the vCenter user role.

14 Click **Next** to advance to the Create Storage page, which guides you through the storage type selection. See “Creating New Storage” on page 72 for storage configuration information and the final steps required to complete the initial configuration wizard.

VDP Appliance Upgrades 3

This chapter contains the following topics:

- "Best Practices" on page 32
- "Supported Upgrade Paths" on page 32
- "Creating a Snapshot of the VDP Appliance" on page 33
- "Mounting the Upgrade ISO Image on the Appliance" on page 34
- "Installing the Upgrade" on page 34
- "Completing the Upgrade" on page 36
- "Reverting Back to a Snapshot" on page 37
- "Upgrading Proxy Software" on page 38

Best Practices

- Before running the upgrade process, take a snapshot of the VDP Appliance from the vCenter Server. Taking a snapshot allows you to restore the VDP Appliance to a previously-known state in the event that the upgrade process does not complete successfully. For instructions, refer to "Creating a Snapshot of the VDP Appliance" on page 33.
- Run the upgrade during a time period when no backup jobs are running or scheduled to run.
- Before performing an upgrade, manually clear all VDP alarms. After the upgrade completes, manually clear the alarms again. Restart the VDP Appliance to reconfigure the alarms by using the following command:

  ```
  emwebapp.sh --start
  ```

Supported Upgrade Paths

VDP upgrades cannot occur during the maintenance window. Perform the VDP upgrade when no backup jobs are running.

IMPORTANT You cannot upgrade VDP 5.1.20 directly to VDP 6.0. You must first upgrade VDP 5.1.20 to VDP 5.1.21.x before upgrading to 6.0.

Table 3-4 lists supported upgrade paths for VDP and VDP Advanced versions.

Table 3-4. Supported Upgrade Paths

		Upgrade TO										
		VDP 5.1.0	VDP 5.1.1	VDP 5.1.10	VDP 5.1.11	VDP Advanced 5.1.20	VDP Advanced 5.1.21	VDP 5.5.1	VDP/ VDP Advanced 5.5.5	VDP/ VDP Advanced 5.5.6	VDP/ VDP Advanced/ RTI 5.8.0	VDP 6.0
Upgrade FROM	VDP 5.1.0	X	X	X	X	X	X	X	X	X	X	X
	VDP 5.1.1		X	X	X	X	X	X	X	X	X	X
	VDP 5.1.10			X		X	X	X	X	X	X	X
	VDP 5.1.11				X	X	X					
	VDP Advanced 5.1.20					X	X		X	X	X	X
	VDP Advanced 5.1.21						X		X	X	X	X
	VDP 5.5.1							X	X	X	X	X
	VDP/VDP Advanced 5.5.5								X	X	X	X
	VDP/VDP Advanced 5.5.6									X	X	X
	VDP/VDP Advanced/ Replication Target Identity (RTI) 5.8.0										X	X
	VDP 6.0											X

NOTE VDP 6.0 includes all features that in earlier versions were included in VDP Advanced.

Creating a Snapshot of the VDP Appliance

As a best practice, take a snapshot of the VDP Appliance before the upgrade. If you encounter any upgrade issues, you can roll back to the snapshot.

1 From a web browser, access the vSphere Web Client:

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

2 Log in as a user who has privileges to edit hardware settings.

3 Click **vCenter > Hosts and Clusters**.

4 In the tree on the left, click the disclosure arrows until the VDP Appliance displays.

5 Right-click the VDP Appliance and select **Shut Down Guest OS**.

NOTE Always shut down a VDP Appliance by using the **Shut Down Guest OS** action. Do not use Power Off to shut down a VDP Appliance.

6 After the appliance has shut down, right-click the VDP Appliance and choose **Edit Settings**.

7 In the Virtual Hardware table, starting with Hard disk 2, click the disclosure arrow.

8 In the Disk Mode row, click **Dependent**.

9 Continuing with Hard disk 3, repeat Step 7 until all the remaining disks have been set to Dependent mode.

10 Click **OK**.

11 Right-click the VDP Appliance and choose **Take Snapshot**.

12 Type a name for the snapshot.

13 Type an optional description.

14 Click **OK**.

15 After the snapshot completes, right-click the appliance and click **Power On**.

The VDP Appliance snapshot has been taken.

Mounting the Upgrade ISO Image on the Appliance

The VDP Appliance is upgraded with an ISO upgrade image.

To mount the upgrade ISO image:

1 Copy the upgrade ISO image to a location that is accessible to the vSphere Web Client.

2 From a web browser, access the vSphere Web Client:

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

3 Log in as a user who has privileges to edit hardware settings.

4 Click **vCenter > Hosts and Clusters.**

5 In the tree on the left, click the disclosure arrows until the VDP Appliance appears.

6 Right-click the VDP Appliance and choose **Edit Settings**.

7 In the Virtual Hardware table, click the disclosure arrow next to CD/DVD.

8 From the drop-down menu, choose **Datastore ISO File**.

The Select File screen should appear. If not, select the CD/DVD Media row and click **Browse**.

9 From the Select File screen, navigate to the datastore and the folder that contains the ISO upgrade image and select the ISO image. Click **OK**.

10 Click the **Connected** checkbox on the CD/DVD Media row, and then click **OK**.

The ISO image begins mounting on the VDP Appliance. The average time for a VDP Upgrade ISO image to mount is about five minutes.

Installing the Upgrade

The upgrade process checks for available disk space on the datastore where the VDP Appliance is installed. You need approximately 2 GB of free space, plus the size of the upgrade ISO file.

NOTE To find upgrade-related logs that you can use to troubleshoot upgrade problems, refer to the `avinstaller.log.0` file in the Log Bundler.

CAUTION If a specific dedicated role is assigned for the VDP Appliance, update the minimum required vCenter permissions before you install the upgrade. Refer to "Minimum Required vCenter User Account Permissions" on page 189 for more information.

Procedure

1 Access the VDP Configure utility:

https://<*IP_address_VDP_Appliance*>:8543/vdp-configure/

2 Log in with the VDP username and password.

3 On the **Configuration** tab, ensure that all the services are running. If all of the services are not running, the upgrade will not succeed.

4 Click the **Upgrade** tab. Upgrades that are contained on the upgrade ISO image you mounted are displayed in the SW Upgrades window.

NOTE If the ISO image does not appear, close VDP-Configure by exiting the web browser. If the ISO image is being mounted from a remote file system, the process of mounting the ISO image and decompressing the files can take up to 20 minutes.

After allowing time for the ISO image to mount, if the **Upgrade** tab still does not display an available upgrade, it may be because the image is corrupt. Any ISO images that do not pass checksum are not displayed on the **Upgrade** tab.

5 Click the upgrade you want to install, and click **Upgrade VDP.**

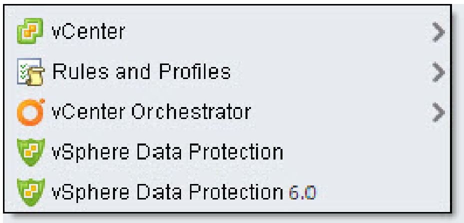
IMPORTANT The upgrade process displays the following message if you do not have enough disk space for the upgrade:

```
Please make sure you have at least 23 GB for repo. 10 GB for var, 1 GB for root partition and 2 GB for space partition.
```

Before continuing the upgrade, refer to "Freeing up space for the upgrade" on page 36 to free up disk space for the upgrade.

The upgrade begins installing. This installation portion of the upgrade can take one to four hours. A status bar updates the progress of the installation. The VDP Appliance automatically shuts down after a successful upgrade.

When VDP is upgraded, two plug-ins may be visible in the vSphere Web Client, as shown in the following figure.



To remove the old plug, first ensure that all VDP Appliances have been upgraded. Then, refer to the VMware vSphere Documentation Center web site for information about managing vSphere Web Client plug-ins.

To remove the VDP plug-in, you must upgrade all VDP Appliances to VDP version 6.0 and use the plug-in manager to disable the VDP plug-in.

Refer to VMware Knowledge Base article for information about managing vCenter plug-ins:

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=2038356

6 To complete the upgrade, perform the steps described in "Completing the Upgrade."

If the upgrade process fails, you can try to install the upgrade again. If you cannot successfully complete the upgrade, you can revert back to the snapshot you took at the start of the upgrade process. For instructions on how to revert back to this snapshot, see "Reverting Back to a Snapshot" on page 37.

Freeing up space for the upgrade

If you received the following error message after you clicked **Upgrade VDP** on the **Upgrade** tab:

```
Please make sure you have at least 23 GB for repo. 10 GB for var, 1 GB for root partition and 2 GB for space partition.
```

Perform the following procedure to free up disk space. Otherwise, you can skip this procedure.

Procedure

1 Open Putty session on the VDP Appliance.

2 Log in as root.

3 Stop the VMware VDP web services by typing the following command:

```
emwebapp.sh --stop
```

4 Stop the Apache web server by typing the following command:

```
/etc/init.d/apache2 stop
```

5 Remove log files from the `/usr/local/avamar-tomcat/logs` directory by typing the following commands:

```
cd /usr/local/avamar-tomcat/logs
rm *log*
```

6 Remove old log files from the `/root/.avamar/var/mc/cli_log` directory by typing the following commands:

```
cd /root/.avamar/var/mc/cli_log
rm *.log.*
```

7 Remove the `mod_jk.log` file by typing the following commands:

```
cd /var/log/apache2
rm mod_jk.log
```

8 Start the Apache web server by typing the following command:

```
etc/init.d/apache2 start
```

9 Start the VMware VDP web services by typing the following command:

```
emwebapp.sh --start
```

10 Perform the upgrade. Refer to "Installing the Upgrade" on page 34.

Completing the Upgrade

You must remove snapshots and unmount the upgrade image after an upgrade completes successfully.

1 From a web browser, access the vSphere Web Client:

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

2 Log in as a user who has privileges to edit hardware settings.

3 Click **vCenter > Hosts and Clusters.**

4 In the tree on the left, click the disclosure arrows until the VDP Appliance appears.

5 If your appliance has not been shut down, right-click the VDP Appliance and choose **Shut Down Guest**, and then click **Yes**.

6 After the appliance has shut down, right-click the VDP Appliance and choose **Manage Snapshots**.

7 Click the snapshot you created for the VDP Appliance.

8 Click **Delete**, and click **Yes**.

9 Click **Close**.

10 Right-click the VDP Appliance and choose **Edit Settings**.

11 Starting with Hard disk 2, click the disclosure arrow.

12 In the Virtual Hardware table, in the Disk Mode row, click **Independent - Persistent**.

13 Continuing with Hard disk 3, repeat Step 11 until all the remaining disks have been set to Independent - Persistent mode.

14 In the Virtual Hardware table, click the disclosure arrow next to CD/DVD.

15 From the drop-down menu choose **Host Device**.

16 Click **OK**.

17 After the snapshot has been removed and the appliance has been reconfigured so the upgrade ISO image is no longer mounted, right-click the VDP Appliance and choose **Power On**.

The VDP Appliance upgrade process is complete.

After the successful upgrade completes and the appliance is powered on, manually run an integrity check. See "Running an Integrity Check" on page 60 for instructions.

NOTE After upgrading the VDP Appliance, when you log in to the vSphere Web Client for the first time, the vSphere Web Client will not show VDP as an option. You must log out of the vSphere Web Client and then log in again. Subsequent logins will show VDP as an option.

Reverting Back to a Snapshot

If you need to revert back to the snapshot you took before the upgrade process, perform the following steps:

1 Log in to the vCenter Server by using the vSphere Web Client as a user who has privileges to edit hardware settings and remove a snapshot.

2 Click **Hosts and Clusters.**

3 In the tree on the left, click the disclosure arrows until the VDP Appliance appears.

4 Right-click the VDP Appliance and choose **Shut Down Guest**, and then click **Yes**.

5 After the appliance shuts down, right-click the VDP Appliance and choose **Revert to Current Snapshot.**

If you have more than one snapshot, you must choose **Manage Snapshots** to choose the snapshot you want to revert back to.

6 After reverting to the snapshot, right-click the VDP Appliance and choose **Edit Settings**.

7 Starting with Hard disk 2, click the disclosure arrow.

8 In the Virtual Hardware table, in the Disk Mode row, click **Independent - Persistent**.

9 Continuing with Hard disk 3, repeat Step 7 until all the remaining disks have been set to Independent - Persistent mode.

10 Click **OK**.

11 Right-click the VDP Appliance and choose **Power On**.

The VDP Appliance is reset back to its earlier state.

Upgrading Proxy Software

Perform this procedure when a newer version of the VMware external proxy software is available for download from the VDP Appliance.

Procedure

1 Access the vSphere Web Client:

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

where *vCenter_Server* is the network hostname or IP address for the vCenter Server.

2 In the Credentials page, enter an administrative vCenter username and password and click **Login**.

3 In the vSphere Web Client, select **VDP**.

4 In the Welcome to VDP page, select the VDP Appliance and click **Connect**.

5 From the VDP user interface, select the **Configuration** tab.

6 In the Downloads section, click the **External Proxy Upgrade ISO** link.

The VMwareVDPExternalProxy-linux-x86-version.iso dialog box displays, where *version* is the specific version Avamar software available for download.

7 Save the VMwareVDPExternalProxy-linux-x86-version.ova to a temporary folder, such as C:\Temp, or to the desktop.

8 From the vSphere Client or vSphere Web Client, log in to the vCenter Server.

9 Locate and select the ESX Server that hosts the proxy you want to update.

10 Click the **Summary** tab.

11 In the Resources pane, select a datastore in the **Datastore** list.

This datastore is where you will upload the ISO file.

If you are performing multiple upgrades, you should select a datastore that is accessible to the greatest number of proxies.

12 Right-click the datastore and select **Browse Datastore**.

The Datastore Browser window appears.

13 Select a folder in the tree.

14 Click **Upload files to this datastore**, and then select **Upload file**.

The Upload Items dialog box appears.

15 Browse to the ISO file that you downloaded.

16 Select the ISO file and click **Open**.

The Upload Items dialog box closes.

17 If an Upload/Download Operation Warning appears, click **Yes** to dismiss the warning and continue with the upload.

18 Wait for the upload to complete.

19 Switch to the VMs and Templates view by clicking **View > Inventory VMs and Templates**.

20 In the left pane, locate and select the proxy you want to upgrade.

21 Right-click **Edit Settings**.

The Virtual Machine Properties dialog box appears.

22 In the Hardware list, select **CD/DVD Drive 1**.

23 Set the following options:

   a In Device Status, select **Connected**.

   b In Device Status, select **Connect at power on**.

   c In Device Type, select **Datastore ISO File**.

24 Click **Browse**.

The Browse Datastores dialog box appears.

25 Browse to the ISO file that you downloaded.

26 Select the ISO file and click **Open**.

The Browse Datastores dialog box closes.

27 In the Virtual Machine Properties dialog box, click **OK**.

The Virtual Machine Properties dialog box closes.

The ISO file is mounted on the proxy.

The proxy automatically waits until no backups are running, then updates itself. Because the polling interval is set to 30 minutes, it make take up to 30 minutes after the last backup completes for the upgrade to begin.

NOTE When you reboot the proxy virtual machine, it updates its software. Any backups that are running during the reboot will fail. Therefore, you should only reboot when you are absolutely certain the proxy is not being used for backups.

28 Ensure that you are still in the VMs and Templates view. If not, switch to the VMs and Templates view by clicking **View > Inventory VMs and Templates**.

29 In the left pane, locate and select the proxy you just upgraded.

30 Right-click **Edit Settings**.

The Virtual Machine Properties dialog box appears.

31 In the Hardware list, select **CD/DVD Drive 1**.

32 In Device Status, clear the **Connected** checkbox.

33 Click **OK**.

The Virtual Machine Properties dialog box closes.

34 After a successful proxy client upgrade, you can check the version by running the following command on the proxy virtual machine:

```
avtar --version
```

Post-Installation Configuration of VDP Appliance

4

This chapter contains the following topics:

- "About the VDP Configure Utility" on page 42
- "Viewing Status" on page 42
- "Starting and Stopping Services" on page 43
- "Collecting Logs" on page 44
- "Modifying Configuration Settings" on page 45
- "Rolling Back an Appliance" on page 46
- "Emergency Restore" on page 46

About the VDP Configure Utility

During installation of vSphere Data Protection (VDP), the VDP Configure utility runs in "install" mode. This mode allows you to enter initial networking settings, time zone, VDP Appliance password, and vCenter credentials. Install mode also allows you to create or attach storage and optionally run the performance assessment tool. After initial installation, the VDP Configure utility runs in "maintenance" mode and displays a different user interface.

To access the VDP Configure utility, open a web browser and type:

https://<*IP_address_VDP_Appliance*>**:8543/vdp-configure/**

Use the VDP Appliance username and password. As you log into the VDP Configure utility, a system health check script runs. You must wait for the system health check to finish running before you can perform configuration tasks from any of the VDP Configure utility tabs.

NOTE After the appliance is configured, you can optionally run a performance analysis test from the VDP Configure utility. The test requires 41 GB per disk per datastore. If that amount of space is not available, the utility reports insufficient space and the performance analysis test will not run.

Use the configuration interface to perform the following configuration tasks:

- "Installing the Upgrade" on page 34 — Allows you to upgrade to a newer version of the VDP Appliance.
- "Storage Management" on page 71 — Allows you to view your storage configuration, add and edit a Data Domain system, and add or expand disk storage on the VDP Appliance.
- "Viewing Status" on page 42 — Allows you to see the services currently running (or currently stopped) on the VDP Appliance.
- "Starting and Stopping Services" on page 43 — Allows you to start and stop selected services on the VDP Appliance.
- "Collecting Logs" on page 44 — Allows you to download current logs from the VDP Appliance for troubleshooting purposes.
- "Modifying Configuration Settings" on page 45 — Allows you to view or change network settings, configure vCenter Registration, view or edit system settings (time zone information and VDP credentials), and manage proxy throughput through external proxy and internal proxy configuration options.
- "Rolling Back an Appliance" on page 46 — Allows you to restore the VDP Appliance to an earlier known and valid state.
- "Emergency Restore" on page 46 — Allows you to restore a VM directly to the host that is running the VDP Appliance. This emergency restore procedure is intended for use when the vCenter is unavailable.

Viewing Status

The **Configuration** tab lists all of the services required by VDP and the current status of each service. Table 4-5 describes the services used by VDP.

Table 4-5. Description of services running on the VDP Appliance.

Service	Description
Core services	These are the services that comprise the backup engine of the VDP 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	Management services should only be stopped under the direction of technical support.
File level restore services	These are the services that support the management of file-level restore operations.
Backup recovery services	These are the services that support backup recovery.

Table 4-5. Description of services running on the VDP Appliance. (Continued)

Service	Description
Maintenance services	These are the services that perform maintenance tasks, such as evaluating whether retention periods of backups have expired. The Maintenance services are disabled the first 24-48 hours after the VDP Appliance is deployed. This creates a larger backup window for initial backups.
Backup scheduler	The backup scheduler is the service that initiates schedule backup jobs. If the backup scheduler is stopped, no scheduled backups will run. On-demand backups can still be initiated.

NOTE If any of these services stop running, an alarm is triggered on the vCenter Server. If a stopped service is restarted, the alarm is cleared. There can be a delay of up to 10 minutes before alarms are triggered or cleared.

The status that is displayed for these services can be any of the following:

- 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

On the status screen you can restart stopped services by clicking **Start**, or you can stop running services by clicking **Stop**. In general, however, you should only stop running services under the direction of technical support.

If you see that a service is stopped, you can attempt to restart it by clicking **Start.** In some cases, however, additional troubleshooting steps are necessary for the service to work properly.

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

1. Core services
2. Management services
3. Backup scheduler
4. Maintenance services
5. File level restore services
6. Backup recovery services

Collecting Logs

The **Log Collector** tab enables you to download log files individually or collectively. The **Log Collector** tab groups log files into three sections. Table 4-6 describes the log files in each group.

Table 4-6. Log files available from the Log Collector tab

Group	Log files
All VDP Appliance Logs	All log files from the All VDP Appliance Logs group.
Core VDP Service	■ Migration Utility ■ System ■ AVI ■ GSAN ■ DPN and Workflow ■ VDP
Management Service	■ MC
File System Service	■ HFSCheck
File Level Restore Service	■ FLR Proxy
Replication	■ Replication ■ Replication Recovery
Image Backup and Restore	■ Image Proxy
Client Logs	■ Microsoft application (MSApp) The aggregated client log includes replication, backup, restore, or automatic backup verification (ABV) jobs that passed with exceptions or that failed.
Configurations	VDP configuration files from proxies, config checker, agents, and so forth. These configuration files are located in `/space/vdp/config`.

When you select a checkbox next to a group heading or next to an individual log, the VDP Configure UI, by default, creates a log bundle named `LogBundle.zip`. The log bundle is intended primarily for sending VDP Appliance logs to support personnel.

NOTE All logs are centrally located in `/space/vdp/logs`.

Procedure

1 Open a web browser and type:

https://*<IP_address_VDP_Appliance>***:8543/vdp-configure/**

2 Log in with the VDP username and password.

3 Click the **Log Collector** tab.

4 Select one or more checkboxes to download log files:

- To download all log files to a zip file, select **All VDP Appliance Logs** and click **Download** to save all log files from VDP services to a `.zip` file.

  The Select location for download dialog box appears.By default, the log bundle is named `LogBundle.zip`. Rename the file to a unique name.

- To download all logs under a specific heading, select a checkbox next to a heading, and then click **Download**:

  - Core VDP Service
  - Management Service
  - File System Service
  - File Level Restore Service

  - Replication
  - Image Backup and Restore
- To download log files listed under multiple headings, select the checkbox next to one of more log files, and then click **Download**.
- In the **Client Logs** group box, click **Download** to download an aggregated text file which contains all client failure logs.
- In the **Configurations** group box, click **Download** to download only VDP configuration file information.

Modifying Configuration Settings

When you access the VDP Configure utility after installation, it runs in maintenance mode. While in maintenance mode, by clicking the **Configuration** tab, you can set or modify any settings that were entered during installation. You can configure network settings and system settings, and you can register the vCenter.

Network Settings

You can configure the following network settings on the **Configuration** tab.

NOTE If you change any network settings, manually run an integrity check immediately after the change is made. Failure to run an integrity check could result in a VDP connection failure while rolling back to a previous checkpoint. See "Running an Integrity Check" on page 60 for instructions.

- IPv4 static address — The Internet Protocol v4 setting of the interface.
- Netmask — The network mask of the IPv4 static address.
- Gateway — The gateway address of the IPv4 static address.
- Primary DNS — The primary domain name system used for DNS resolution.
- Secondary DNS — The secondary domain name system used for DNS resolution.
- Hostname — The unique name by which a computer is known on a network (for example: vdp-primary).
- Domain — A unique name that identifies a website (for example: emc.com). *Domain* is sometimes referred to as the *domain name*.

vCenter Server Registration

CAUTION Changing the vCenter Server hostname, vCenter Server password, vCenter Server FQDN or IP address, or vCenter Server port number results in the loss of all backup jobs, replication jobs, and backup verification jobs associated with the VDP Appliance. Existing restore points remain intact, but you will be required to re-create backup jobs and replication jobs.

Before the process that reconfigures the vCenter Server registration runs, all of the following conditions must be true:

- No other reconfiguration process is running (for example, password or network reconfiguration).
- No backup, replication, or restore jobs are running.
- No integrity check is running.
- All services are running on the VDP Appliance.

If you change any vCenter registration credentials, manually run an integrity check immediately after the change is made. Failure to run an integrity check could result in a VDP connection failure while rolling back to a previous checkpoint. See "Running an Integrity Check" on page 60 for instructions.

Rolling Back an Appliance

The VDP Appliance could become inconsistent or unstable. In some cases, the VDP Configure utility can detect an inconsistent or unstable state and will provide a message similar to the following message immediately after you log in:

> It appears that your VDP Appliance has suffered an unclean shutdown and will likely require a checkpoint rollback to restore data protection functionality. This process may be initiated from the 'Rollback' tab.

CAUTION By default, VDP keeps two system checkpoints. If you roll back to a checkpoint, all backups and configuration changes taken since the checkpoint was taken will be lost when the rollback is completed.

The first checkpoint is created when VDP is installed. Subsequent checkpoints are created by the Maintenance service. This service is disabled for the first 24 to 48 hours of VDP operation. In the event that you roll back during this time frame, then the VDP Appliance is set to the default configuration and any backup configurations or backups are lost.

NOTE If any VMware VDP for Exchange Server Clients or VMware VDP for SQL Server Clients were installed between a checkpoint and a rollback, the clients must be reinstalled.

Follow the procedure below to roll back a VDP Appliance.

CAUTION Only roll back to the most recent validated checkpoint.

Prerequisite

The VDP Appliance must be installed and the VDP Appliance password is required.

Procedure

1 Open a web browser and type:

https://*<IP_address_VDP_Appliance>***:8543/vdp-configure/**

2 Log in with the VDP username and password.

3 Click the **Rollback** tab.

4 Click the lock icon to enable VDP rollback.

5 Enter the VDP Appliance password and click **OK**.

The lock icon changes to unlocked.

6 Click the checkpoint that you want to roll back to.

7 Click **Perform VDP rollback to selected checkpoint**.

A warning message appears explaining the consequences of rolling back the VDP Appliance.

8 Click **Yes**.

An information message appears telling you a rollback has been initiated.

9 Click **OK**.

The VDP Appliance attempts to roll back and displays status information. It also displays an information message indicating whether the roll back succeeded or failed.

10 Click **OK**.

If the VDP Appliance did not roll back successfully, contact Customer Support.

Emergency Restore

VDP is dependent on the vCenter Server for many of its core operations. The direct-to-host emergency restore operation provides a method for restoring the vCenter Server when the vCenter Server is unavailable or the user is unable to access the VDP user interface with the vSphere Web Client.

An emergency restore operation restores a VM directly to the host that is running the VDP Appliance. The **Emergency Restore** tab displays a list of VMs that have been backed up by the VDP Appliance. These virtual machines can be restored as new virtual machines on to the host where the VDP Appliance is running.

Best Practices and Recommendations

Ensure the following requirements are met before you perform an emergency restore operation:

- The virtual machine being restored has a virtual hardware version that is supported by the host on which the VDP Appliance is running.
- There is adequate free space in the target datastore to accommodate the entire virtual machine.
- The target VMFS datastore to which the virtual machine is being restored supports the VMDK file size.
- Network connectivity is available for the restored virtual machines from the host where the VDP Appliance is running.
- There is at least one local account with administrator privileges on the host where the VDP Appliance is running.

Limitations and Unsupported Features

- The vSphere host on which the emergency restore operation is being performed cannot be part of the vCenter inventory. A vSphere host that is currently managed by the vCenter Server must be temporarily disassociated from the vCenter Server to perform the emergency restore. To disassociate the vCenter Server, use the vSphere Client (not the vSphere Web Client) connected directly to the vSphere host.
- Emergency restore allows you to restore only to the root of the host level in the inventory.
- Emergency restore requires that the DNS server used by VDP is available and can fully resolve the target vSphere host name.
- Emergency restore restores the virtual machine in the Powered Off state. You must manually log in to the host and power on the restored virtual machine.
- Emergency restore restores the virtual machine as a new virtual machine. You must ensure that the name provided for the virtual machine is not a duplicate of a virtual machine that already exists.
- Emergency restore does not list MSapp clients.
- An internal proxy is automatically activated when an emergency restore operation is performed. If both the internal and external proxies are activated, you must disable the internal proxy on the VDP Configure utility for the emergency restore to complete successfully.

Procedure

1. If you have not already done so, log in to the vSphere client of the host and, from the **Summary** tab under Host Management, perform the following steps:

   a. Click **Disassociate Host from vCenter**.

   b. Click **Yes** when prompted to remove the host from the vCenter.

2. Log in to the VDP Configure utility:

   https://<*IP_address_VDP_Appliance*>**:8543/vdp-configure/**

3. Click the **Emergency Restore** tab.

   Virtual machines protected by VDP are listed in the Emergency Restore dialog box. Here, you can find the following details about the virtual machines:

   - Name — The name of the virtual machines protected by the VDP Appliance. By clicking the disclosure arrows, you can determine the date and time of the last restore for the selected virtual machine.

- Last Known Path — The last known location of the virtual machine in the vCenter inventory list. This location is updated if the virtual machine is moved.
- Running restore details:
  - Client Name — The name of the client on which the virtual machine is restored.
  - Status — The pass or fail status of the restore.
  - Start Time — The time the restore started.
  - Completed Time — The time the restore completed.
  - Bytes Transferred — The number of bytes that were transferred during restore.

4. Select the virtual machine that will serve as the restore point and click **Restore**.

   The Host Credentials dialog box appears.

5. In the Host Credentials dialog box, enter valid host credentials:
   - ESXi Host name or IP — Enter the vSphere hostname or vSphere host IP address.
   - Port - 443, which is the default, is prepopulated.
   - Username — Enter the vSphere host username. The recommended host username is “root.” For any other host username, the user account must have the create VM privilege.
   - Password — Enter the vSphere host password. If you enter invalid host credentials, an error message displays and you will be unable to connect to the host.

NOTE If you did not successfully disassociate the selected virtual machine from its vCenter, an error message appears and you cannot proceed.

6. Click **OK**.

   The Restore a Backup screen initiates the restore with the new name and destination.

7. The Restore a Backup dialog box displays the following information:
   - Client name — The name of the client on which the virtual machine is restored.
   - Backup — The date and timestamp of the backups.
   - New Name — The field where a new name must be entered, which cannot be a duplicate of a VM that already exists.
   - Destination — The vSphere hostname.
   - Datastore — A drop-down list of datastores available as the destination targets.

8. Enter a new name in the **New Name** field. The name must be unique and can be up to 255 characters long. The following characters cannot be used in the name: ~ ! @ $ ^ % { } [ ] | , ` ; # \ / : * ? < > ' " & . In addition, diacritical characters cannot be used (for example: â, é, ì, ü, and ñ).

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

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

10. Click **Restore**.

11. Verify that the restore submitted successfully by checking the progress in the Recent Tasks dialog box.

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

Automatic Host Detection

For vSphere Data Protection versions 5.5 and earlier, users are required to identify, disassociate, and populate vSphere host values before they perform an emergency restore. With vSphere Data Protection version 5.8 and later, the appliance automatically detects the host that it is currently registered to and pre-populates the hostname or IP value in the Host Credentials dialog box. This eases the burden for a user, who might have numerous hosts in a cluster and needs to identify the current, resident host to disassociate from the vCenter.

The following are rare cases when the appliance fails to detect the most updated host to which the appliance is registered and displays an older value:

- The vCenter is unavailable and, after the VDP Appliance migrates to a different host under HA-enabled clustering, the appliance displays the older host to which it was registered.
- The vCenter becomes unavailable immediately after the appliance is migrated to another host. In this case, the new host cannot be detected, because it takes the appliance a period of time to process and update events from the vCenter.

In both of these cases, the user must manually determine to which host the appliance is registered.

Refreshing Restore Points

1. Log in to the VDP-Configure URL:

   https://<*IP_address_VDP_Appliance*>**:8580/vdp-configure/**

2. Click the **Emergency Restore** tab.
3. Click **Refresh**.

   The loading bar refreshes the restore points.

Reconnecting the Host to the vCenter

1. Restore the vCenter. Refer to "Restore Operations" on page 128 for instructions.

NOTE The restored vCenter is powered off by default.

2. Once the vCenter restore completes, power on the vCenter.
3. Log in to the vCenter URL to verify all the services are running:

   https://<*IP_address_vCenter*>**:5480**

4. Log in to the restored vCenter through the vSphere client:

   https://<*IP_address_vCenter*>**:9443/vsphere-client/**

5. From the vSphere client, add the vSphere host to the newly-restored vCenter.

NOTE Once the vCenter has been restored, there may be a delay of approximately 20 minutes while the vCenter services start up. During this delay, you will be unable to perform a successful backup or restore operation. If you experience delays, try the backup or restore later.

Securing Communication between vCenter and VDP

5

This chapter contains the following topics:

- "Secure VDP Services Communication to vCenter" on page 52
- "Secure External Proxy Communication with vCenter" on page 53

Secure VDP Services Communication to vCenter

The VDP Appliance does not verify SSL certificates presented by vCenter during the registration process to vCenter Server Appliance (VCSA). The failure to verify the SSL certificate makes the vCenter Server and VDP prone to man-in-the-middle attacks. To prevent man-in-the-middle attacks, you must secure VDP server and management services communication to vCenter by downloading and configuring the `vcenter-hostname.crt` certificate.

By default, the VDP server management service and proxies do not validate SSL certificates when connecting to the vCenter Server. This can leave the vCenter Server vulnerable to a man-in-the-middle exploitation, which might result in unauthorized access to the vCenter Server. Configuring each proxy to use SSL certificate authentication when connecting to the vCenter Server corrects this vulnerability.

Before you begin

Ensure that a Certificate Authority (CA) signed SSL certificate is installed on the vCenter Server. Detailed instructions for generating and installing a CA signed SSL certificate and installing it on the vCenter Server are found in the following VMware Knowledge Base article: Implementing CA signed SSL certificates with vSphere 5.x (2034833) describes how to implement CS signed certificates in a vSphere 5.1 or 5.5 environment.

Procedure

1 Download `vcenter-hostname.crt` from the vCenter Server or web browser to the VDP Appliance:

a To download the certification from a browser, type the following URL in the browser:

https://*vcenter-ip-address*

where *vcenter-ip-address* is the IP address of the vCenter Server.

b Save the `vcenter-hostname.crt` certificate.

2 SSH into a VDP Appliance as the root user.

3 Create a directory in the VDP Appliance under the `root` directory or in any preferred location.

mkdir /root/*directory*

4 Copy/sftp the `vcenter-hostname.crt` certificate that you downloaded to the new directory, `/root/directory`, you created on the VDP Appliance.

5 Import the certificate into `rmi_ssl_keystore`:

a Type the following command:

/usr/java/latest/bin/keytool -import -file /root/vcentercertificate/vcenter-hostname.crt -alias *vcenter-hostname* **-keystore /usr/local/avamar/lib/rmi_ssl_keystore**

where *vcenter-hostname* is the vCenter Server hostname.

b When prompted for the keystore password, type **`changeme`**.

c Type **`yes`** to accept the certificate, and then press **Enter**.

6 Update management service preference file:

a Open `mcserver.xml` in the **`vi`** editor:

vi /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml

b Search for `ignore_vc_cert`, and then change its value to **`false`**.

c Save and close the file.

7 Update vCenter Server configuration file:

a Open `vcenterinfo.cfg` in the **`vi`** editor:

b Add **`vcenter-ignore-cert=false`** to the file.

c Save and close the file.

8 Restart MCS by typing the following commands:

```
su admin
mcserver.sh --restart
exit
```

9 Restart the Tomcat web application server by typing the following command:

```
emwebpp.sh -restart
```

Secure External Proxy Communication with vCenter

By default, the VDP server management service and proxies do not validate SSL certificates when connecting to the vCenter Server. This can leave the vCenter Server vulnerable to a man-in-the-middle exploitation, which might result in unauthorized access to the vCenter Server. Configuring each proxy to use SSL certificate authentication when connecting to the vCenter Server corrects this vulnerability.

Before you begin

Ensure that a Certificate Authority (CA) signed SSL certificate is installed on the vCenter Server. Detailed instructions for generating and installing a CA signed SSL certificate and installing it on the vCenter Server are found in the following VMware Knowledge Base article: Implementing CA signed SSL certificates with vSphere 5.x (2034833) describes how to implement CS signed certificates in a vSphere 5.1 or 5.5 environment.

Procedure

1 Open a command shell and log in to the proxy as root.

2 Copy the vCenter Server certificate to `/usr/local/avamarclient/bin` on the proxy.

NOTE If a chained SSL certificate is used for the vCenter, copy the `chain.pem` file, which contains all certificates in the chain, to `/usr/local/avamarclient/bin` on the proxy.

3 Set the proper operating system permissions on the certificate by typing the following command:

```
chmod 600 /usr/local/avamarclient/bin/vcenter-1.crt
```

where *vcenter-1.crt* is the actual certificate name.

NOTE Use `chain.pem` for chained vCenter SSL certificates.

4 Open `/usr/local/avamarclient/var/avvcbimageAll.cmd` in a UNIX text editor.

5 Append the following entry to the end of the file:

```
--ssl_server_authentication_file=/usr/local/avamarclient/bin/vcenter-1.crt
```

where *vcenter-1.crt* is the actual certificate name.

6 Close `/usr/local/avamarclient/var/avvcbimageAll.cmd` and save your changes.

7 Open `/usr/local/avamarclient/var/avvmwfileAll.cmd` in a UNIX text editor.

NOTE Use `chain.pem` for chained vCenter SSL certificates.

8 Append the following entry to the end of the file:

```
--ssl_server_authentication_file=/usr/local/avamarclient/bin/vcenter-1.crt
```

where *vcenter-1.crt* is the actual certificate name.

9 Close `/usr/local/avamarclient/var/avvmwfileAll.cmd` and save your changes.

10 Open `/usr/local/avamarclient/var/vddkconfig.ini` in a UNIX text editor.

11 Find the `vixDiskLib.linuxSSL.verifyCertificates=0` entry.

12 Change the `vixDiskLib.linuxSSL.verifyCertificates=0` entry to 1.

```
vixDiskLib.linuxSSL.verifyCertificates=1" />
```

13 Close `/usr/local/avamarclient/var/vddkconfig.ini` and save your changes.

14 Ensure that there are no running backup or restore jobs on this proxy.

15 Restart the avagent and vmwareflr services by typing the following commands:

```
service avagent-vmware restart
service vmwareflr restart
```

Results

This proxy will now use and validate SSL certificates when connecting to the vCenter Server.

Repeat this procedure for each proxy you deploy in the vCenter environment.

Configuring VDP 6

This chapter includes the following topics:

- "Login Security" on page 56
- "Configuring the Customer Experience Improvement Program" on page 56
- "Configuration and Monitoring" on page 57
- "Monitoring VDP Activity" on page 60
- "VDP Shutdown and Startup Procedures" on page 62

Login Security

To increase security of the VDP Configure UI, after 5 unsuccessful login attempts from any user, the VDP Configure UI is locked for 5 minutes. This prevents any login attempts during that time. Any existing sessions that are already logged in are unaffected.

If a lockout occurs:

- The VDP Configure UI informs the user during a login attempt.
- A vCenter event about the lockout is generated.
- The `vdp-configure.log` captures the time, the user, the source address, and request headers of the failed login attempts that led up to the lockout.

Configuring the Customer Experience Improvement Program

The Customer Experience Improvement Program is an option that enables you to send encrypted configuration and usage information about the VDP environment to VMware servers for analysis. VDP sends the following types of data to VMware:

- Version information for VDP
- VDP time zone and uptime
- Number of VMs protected and the number of VMs unprotected
- Amount of configured capacity.
- Data Domain in use (true/false)
- Capacity utilization
- Number of internal and external proxies configured and registered
- Number of work orders per proxy configured by the user
- Management services status
- Latest valid checkpoint date
- Agents in use (SQL Server, Exchange, and SharePoint)

During the installation of VDP, you can enable the Customer Experience Improvement Program from the Product Improvement page in the VDP Configuration Utility. The Product Improvement page provides the **Enable Customer Experience Improvement Program** checkbox. By default, the checkbox is not selected.

Anytime after the installation you can enable or disable the Customer Experience Improvement Program by accessing the VDP Configure Utility from the a web browse.

Prerequisites

In networks that are protected by a firewall, you may need to modify the network to help prevent connectivity issues when the Customer Experience Improvement Program attempts to upload data to the VMware server. To ensure that the firewall does not prevent Customer Experience Improvement Program from uploading data to the VMware server, open the network to the following VMware servers:

- https://vcsa.vmware.com:443
- https://phtransfer.vmware.com:443

Procedure

1. Open a web browser and type:

   https://<IP_address_VDP_Appliance>**:8543/vdp-configure**/

2. Log in with the VDP username and password.

3 From the **Configuration** tab, click the ⚙ icon and select **Product Improvement**.

The Product Improvement page appears.

4 Enable or disable the Customer Experience Program by selecting or clearing the **Enable Customer Experience Improvement Program** checkbox.

Configuration and Monitoring

From the vSphere Web Client, you can view and modify backup window configuration details, in addition to information about the appliance and storage. You can also configure the VDP Appliance to send email reports on a scheduled basis.

Viewing Backup Appliance Configuration

Backup Appliance information provides information for Backup Appliance Details, Storage Summary, and Backup Windows Configuration. Backup Appliance Details include:

- Display name
- IP Address
- Major Version (VDP version number)
- Minor Version (used by Technical Support)
- Status
- vCenter Server
- Host IP
- VDP backup user
- Local time
- Time zone

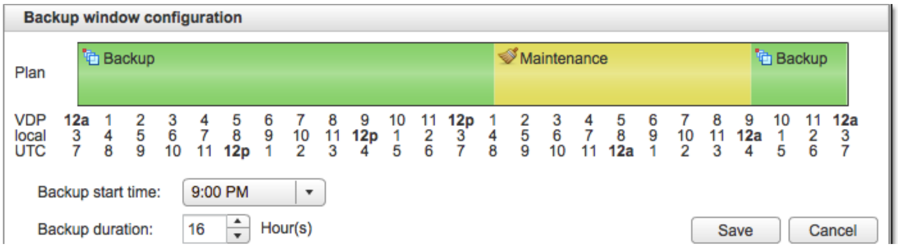
These options are configured during the VDP Appliance installation. They can be edited through the VDP Configure utility. See “Post-Installation Configuration of VDP Appliance” on page 41 for additional details.

VDP Appliance Storage Summary Details include:

- Capacity — The total capacity of the VDP Appliance.
- Space free — How much space is currently available for backups.
- Deduplicated size — The amount of disk space the backups are taking up in deduplicated format.
- Non-deduplicated size — The amount of disk space the backups would take up if they were converted to a native, non-deduplicated format.

NOTE If a Data Domain system is configured as the backup target, the Data Domain Storage Summary details appear.

Figure 6-2 is a graphical representation of the backup window configuration.



Backup window configuration

Plan: Backup | Maintenance | Backup

VDP	**12a**	1	2	3	4	5	6	7	8	9	10	11	**12p**	1	2	3	4	5	6	7	8	9	10	11	**12a**
local	3	4	5	6	7	8	9	10	11	**12p**	1	2	3	4	5	6	7	8	9	10	11	**12a**	1	2	3
UTC	7	8	9	10	11	**12p**	1	2	3	4	5	6	7	8	9	10	11	**12a**	1	2	3	4	5	6	7

Backup start time: 9:00 PM

Backup duration: 16 Hour(s)

Figure 6-2. Backup window configuration

Each 24-hour day is divided into two operational windows:

- **Backup window** — The portion of each day reserved for performing normal scheduled backups.
- **Maintenance window** — The portion of each day reserved for performing routine VDP maintenance activities, such as integrity checks. Do not schedule backups or perform a "Backup Now" operation while VDP is in maintenance mode. The backup jobs will run but they will consume resources VDP needs for maintenance tasks.

  Jobs that are running when the maintenance window begins or that run during the maintenance window will continue to run.

NOTE Since the blackout window has been eliminated, activities such as integrity checks and garbage collection will now run non-stop during the maintenance window.

Editing the Backup Window

You can change the amount of time available for processing backup requests.

Prerequisites

- Verify that VDP is installed and configured.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.

Procedure

1. From a web browser, access VDP. Refer to "Accessing vSphere Data Protection" on page 106 for instructions.
2. From the VDP user interface, select the **Configuration** tab (by default you are on the Backup Appliance view).
3. At the bottom right corner of the Backup Appliance view, click the **Edit** button.

   The backup start time and duration time options appear.
4. Use the drop down arrow to choose the start time for the backup window.
5. Enter the duration of the backup window. The minimum backup window is 4 hours and the maximum backup window is 16 hours.
6. Click **Save**.

   A dialog appears telling you that the settings were saved successfully.
7. Click **OK**.

VDP changes the backup window configuration.

Configuring Email

You can configure VDP to send SMTP email reports to specified recipients. If email notification is enabled, email messages are sent that include the following information:

- VDP Appliance status
- Backup jobs summary
- Virtual machines summary
- Replication summary

NOTE VDP email notification does not support carbon copies (CCs) or blind carbon copies (BCCs), nor does it support SSL certificates.

Prerequisites

- Verify that VDP is installed and configured.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.
- The email account for email reports must exist.

Procedure

1. From a web browser, access VDP. Refer to "Accessing vSphere Data Protection" on page 106 for instructions.
2. From the VDP user interface, select the **Configuration** tab.
3. Select **Email**.
4. Click the **Edit** button (in the bottom right corner of the page).
5. Specify the following:
   - **Enable email reports** — Check this box to enable email reports.
   - **Outgoing mail server** — Enter the name of the SMTP server that want to use to send email. This name can be entered as either an IP address, a host name, or a fully qualified domain name. The VDP 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 colon (:) and the port number to the server name. For example, to specify the use of port 8025 on server "emailserver" enter emailserver:8025.
   - (optional) **My server requires me to log in** — Check this box if your SMTP server requires authentication.
   - **User name** — Enter the username you want to authenticate with.
   - **Password** — Enter the password associated with the username. (VDP does not validate the password. The password that you enter is passed directly to the email server.)
   - **From address** — Enter the email address from where you would like the email report. This can only be a single address.
   - **To address(es)** — Enter a comma-separated list of up to 10 email addresses.
   - **Send time** — From the drop-down list, choose the time you want VDP to email reports.
   - **Send day(s)** — Check the days you want the reports sent.
   - **Report Locale** — From the drop-down list, choose the country for the email reports.
6. Click the **Save** button.
7. To test your email configuration, click **Send test email**.

Viewing the User Interface Log

Clicking **Log** on the **Configuration** tab displays the user interface log for VDP. This is a high-level log that details the activities that have been initiated with the user interface and that identifies some key status items.

Click **Export View** to save the details that are displayed on the screen to file on the machine where your browser is running.

More detailed logs can be downloaded using the VDP Configure UI. Refer to "Collecting Logs" on page 44 for instructions.

Running an Integrity Check

Integrity checks verify and maintain data integrity on the deduplication store. The output of an integrity check is a checkpoint. By default, VDP runs an integrity check every day during the maintenance window. In addition, you can start the integrity check manually.

CAUTION If the VDP Appliance displays an alarm that the last valid integrity check failed or is out of date, run a manual integrity check. If you allow for the VDP Appliance to continue to make backups while the integrity check is out of date, you are risking losing potential backup data if a rollback to the last validated checkpoint is ever required.

You can see a list of all of the VDP checkpoints through the VDP Configure utility, **Rollback** tab. See "Rolling Back an Appliance" on page 46 for additional information.

Prerequisites

- Verify that VDP is installed and configured.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.

Procedure

1. From a web browser, access VDP. Refer to "Accessing vSphere Data Protection" on page 106 for instructions.
2. From the **Configuration** tab in the VDP user interface, click the ⚙▾ icon and select **Run integrity check**.

   A confirmation screen appears, asking if you want to perform a manual integrity check.
3. Click **Yes**.

   A message appears informing you that the integrity check has been initiated.
4. Click **OK**.

   VDP starts the integrity check.
5. Monitor the Integrity Check progress through Recent Tasks.

NOTE When the VDP Integrity Check is running, the Maintenance service is stopped. This may cause a temporary VDP error. Wait until the Integrity Check is complete and the Maintenance service automatically restarts and the VDP error message is resolved.

Monitoring VDP Activity

You can monitor the activities of the VDP application by:

- "Viewing Recent Tasks" on page 61.
- "Viewing Alarms" on page 61
- "Viewing the Event Console" on page 62

Tasks, events, and alarms that are generated by VDP are prefaced by "VDP:" Note, however, that some of the tasks and events that occur as part of VDP processes are performed by the vCenter Server and do not have this prefix.

For example, if VDP runs a scheduled backup job against a running virtual machine, the following task entries are created:

1. Create virtual machine snapshot (vCenter acting on the virtual machine to be backed up)
2. VDP: Scheduled Backup Job (VDP starting the backup job)
3. Reconfigure virtual machine (the VDP Appliance requesting services from virtual center)
4. Remove snapshot (virtual center acting on the virtual machine that has completed backing up)

To see only VDP-generated tasks or events in the Tasks or Events console, enter "VDP**:**" in the **Filter** field.

Viewing Recent Tasks

VDP generates task entries in the Recent Tasks windows when it performs the following operations:

- Backups
- Automatic Backup Verification
- Restores
- Replications
- Replication Recovery
- VDP-Configuration
- 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 virtual machine icon in the **Running** tab under **Recent Tasks.**

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

Viewing Alarms

Table 6-7 lists the alarms that the vSphere Data Protection (VDP) Appliance can trigger:

Table 6-7. vSphere Data Protection alarms

Alarm Name	Alarm Description
VDP: [001] The most recent checkpoint for the VDP Appliance is outdated.	From the **Configuration** tab of the VDP user interface, click the All Actions icon and select “Run integrity check.”
VDP: [002] The VDP Appliance is nearly full.	The VDP 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.
VDP: [003] The VDP Appliance is full.	The VDP 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.
VDP: [004] The VDP Appliance datastore is approaching maximum capacity.	The datastore where the VDP Appliance provisioned its disks is approaching maximum capacity. When the maximum capacity of the datastore is reached, the VDP Appliance will be suspended. The appliance cannot be resumed until additional space is made available on the datastore.
VDP: [005] Core services are not running.	Start Core services using the VDP Configure utility.
VDP: [006] Management services are not running.	Start Management services using the VDP Configure utility.
VDP: [007] File system services are not running (supported in VDP versions 5.5 and lower)	Start File system services using the VDP Configure utility. NOTE: This alarm is not supported in VDP version 5.8 or later.
VDP: [008] File level restore services are not running.	Start File level restore services by using the VDP Configure utility.
VDP: [009] Maintenance services are not running.	Start Maintenance services by using the VDP Configure utility.
VDP: [010] Backup scheduler is not running.	Start Backup scheduler by using the VDP Configure utility.

Table 6-7. vSphere Data Protection alarms (Continued)

Alarm Name	Alarm Description
VDP: [013] Protected Virtual Machine limit exceeded.	The supported number of protected Virtual Machines has been exceeded.
VDP: [014] Backup Recovery services are not running.	Start Backup Recovery services by using the vSphere Data Protection Configuration Utility.

Viewing the Event Console

VDP can generate events of the following types: info, error, and warning. Examples of the following types of events are:

- **Info** —"VDP: Critical VMs Backup Job created."
- **Warning** —"VDP: Unable to add Host123 client to backup job Critical VMs because . . ."
- **Error** —"VDP: Appliance has changed from Full Access to Read Only."

VDP 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, VDP 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, VDP generates an event that is labeled informational because the appliance changes from read-only to full access.

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

VDP Shutdown and Startup Procedures

If you need to shut down the VDP Appliance, use the **Shut Down Guest OS** action. This action automatically performs a clean shutdown of the appliance. If the appliance is powered off without the **Shut Down Guest OS** action, corruption might occur. It can take up to 30 minutes to shut down and restart the VDP Appliance. You can monitor the status through the virtual machine console. After an appliance is shut down, it can be restarted through the **Power On** action.

If the appliance does not shut down properly, when it restarts it rolls back to the last validated checkpoint. This means any changes to backup jobs or backups that occur between the checkpoint and the unexpected shutdown are lost. This is expected behavior and is used to ensure system corruption does not occur from unexpected shutdowns. See "Rolling Back an Appliance" on page 46 for additional information.

The VDP Appliance is designed to be run 24x7 to support maintenance operations and to be available for restore operations. Do not shut down the VDP Appliance unless there is a specific reason for shutdown.

NOTE Before vCenter Server patches or upgrades, use the VDP shutdown procedure.

Proxies

7

This chapter includes the following topics:

- "Proxy Overview" on page 64
- "Managing Internal and External Proxies" on page 66
- "External Proxy Support" on page 66
- "(Optional) Configuring Proxy Certificate Authentication" on page 69
- "Monitoring External Proxy Health Status" on page 69

Proxy Overview

This chapter describes the use of internal and external proxies in VDP Appliances.

After initial deployment, a VDP Appliance has only internal proxies configured. After the VDP Appliance is fully deployed, you can deploy up to eight external proxies through the VDP Configuration UI. If you configures an external proxy for the VDP Appliance, the internal proxies are automatically disabled during the process.

Considerations Before Deploying an External Proxy

Consider the following when deploying one or more proxies for use with the VDP Appliance:

- The VDP Appliance does not have access to a datastore, preventing the HotAdd transport method from being used. Refer to the following VMware knowledgebase article to define the VMware HotAdd best practices from a backup point of view:

  http://kb.vmware.com/kb/1008072

- The need to perform more backups concurrently while not constrained by resources on the vSphere host nor by datastore performance. A maximum of 24 concurrent backup jobs are supported.
- To perform File Level Recovery (FLR) on Logical Volume Manager (LVM) or EXT4 based file systems, requires an external proxy.

Deployment of External Proxies

To take advantage of HotAdd during the backup process, the proxy appliance must have direct access to the datastore where the target VM is located. The backup agent appliance leverages the datastore access from the vSphere host to which it is associated. When deploying the external backup agent, verify that the appliance has access to the desired datastores by way of the vSphere host.

If the proxy appliance does not have access to the datastore where the target VM is located, the NBDtransport method will be invoked instead of HotAdd, which may greatly reduce the speed of the backup.

Number of Proxies to Deploy and Proxy Throughputs per Proxy

When considering the number of proxies to deploy and the configuration of the number of proxy throughputs per proxy, consider the following as best practices:

When using a single proxy

- For an external proxy, if deployed with the default configuration for memory and CPUs, the optimal number of proxy throughputs is six when running backups. Increasing the proxy throughputs per proxy beyond six leads to performance degradation.
- Increasing the CPU on the external proxy results in better performance than increasing the memory on the single external proxy.
- When the external proxy configuration is modified to eight CPUs, running eight proxy throughputs per proxy is optimal. This is true for Level 0 and Level 1 backups. With this configuration, network bandwidth becomes the limiting factor.

When using multiple external proxies for Level 0 backups

- Maximizing the number of proxies deployed may not produce the best performance results.
- As you increase the number of proxies, the optimal number of proxy throughputs per proxy may decrease. With two external proxies running, for example, you may see the best results while running six proxy throughputs per proxy. With four external proxies running, you may see the best results while running four proxy throughputs per proxy. This may be constrained by the number of proxies per vSphere host.

- It is better to increase the number of proxy throughputs per proxy instead of the number of proxies when performing a set number of backups.

When using multiple external proxies for Level 1 backups

When running incremental (Level 1) backups for a virtual machine, consider increasing the number of proxies. Running four proxy throughputs per proxy provides better performance than fewer proxies running eight proxy throughputs per proxy.

Increasing the volume of backups that run on the VDP Appliance

After backups have been running, you may need to increase the volume of the backups performed during a specific timeframe by the VDP Appliance. When increasing the quantity of backups performed in a given timeframe, consider the following best practices:

- If the vSphere server resources are a constraint, run more proxy throughputs per proxy and reduce the number of proxies.
- If the vSphere server resources are not constrained, increase the number of proxies and maintain four proxy throughputs per proxy.
- If six to eight external proxies are necessary to process the desired backups, increase the number of proxy throughputs per proxy and limit the number of external proxies deployed.

Reducing concurrent backups run on the VDP Appliance

After backups have been running on the VDP Appliance, you may need to reduce the number of concurrent backups being run by the VDP Appliance to limit the load on the datastores and associated storage. When reducing the quantity of concurrent backups being run by the VDP Appliance, consider the following best practices:

- Place the VDP Appliance on a datastore with faster write performance, preferring iSCSI to NFS for the datastore.
- If there is high load on the datastore where the protected virtual machines reside during backups, reduce the number of proxies and the number of proxy throughputs to proxy to four or less. This will reduce the quantity of seek and read operations when performing backups.

Best Practices when Deploying a VDP Appliance

The following should always be considered a best practice when deploying a VDP Appliance:

- Create a DNS record for the VDP Appliance before deploying the appliance. Ensure both forward and reverse lookup are enabled in DNS.
- One of the last steps when deploying VDP is the option to run a storage performance analysis. Run this analysis to verify the storage on which VDP is running meets or exceeds performance requirements. The analysis could take from 30 minutes to a few hours to complete.
- Place the VDP Appliance on a separate datastore than where the protected VMs will reside.
- When scheduling backup jobs, consider staggering the start times.
- When applications with high change rates (such as a database or an Exchange Server) are backed up, interleave them with the image level backups.
- Consider other processes that may be running. Try not to schedule replication or automatic backup verification when backup jobs are running. If possible, schedule these jobs to run after the backup jobs have completed, before the maintenance window opens.
- An internal proxy must be activated, and is automatically activated, when an emergency restore operation is performed.

Managing Internal and External Proxies

The Manage Proxy Throughput wizard allows you to configure the number of simultaneous backups and restores, based on your infrastructure. You can use the Manage Proxy Throughput wizard to set values for both internal and external proxies. The VDP Appliance supports up to 8 external proxies, and the maximum number of concurrent backup jobs is 24.

For more information, refer to "Number of Proxies to Deploy and Proxy Throughputs per Proxy" on page 64.

Before you run simultaneous backup and restore requests, optimize your environment by updating your configuration settings. Refer to "Modifying Configuration Settings" on page 45 for more information.

CAUTION The number you select to simultaneously back up and restore clients is a global setting. This setting applies to all internal and external proxy settings.

Procedure

1 Open a web browser and type:

https://*<IP_address_VDP_Appliance>***:8543/vdp-configure/**

2 Log in with the VDP username and password.

3 Click the **Configuration** tab.

4 From the **Action** list, select **Manage Proxy Throughput**.

The Manage Proxy page appears.

5 Select the number, from 1 to 8, of backup and restore clients that you want to run simultaneously.

6 Click **Next**.

The Ready to Complete page appears.

7 Click **Finish** to apply the changes.

External Proxy Support

VDP Advanced Appliance versions 5.5.6 and earlier are configured with internal proxies only, where the proxy services run inside the VDP Appliance and are registered to manage job requests from the appliance. External proxies can be configured for VDP 6.0 Appliances.

NOTE The VDP Appliance with external proxies supports File Level Recovery (FLR) on virtual machines with EXT4 file systems.

Best Practice for External Proxy Deployment

NOTE If configuring the appliance to use external proxies, the internal proxies are automatically disabled.

Using HotAdd transport is usually faster than over-the-network backup and restore using NBD (network block device) transport.

External Proxy Best Practices

- **Clean up orphan proxies**

  External proxies that are registered to the VDP Appliance but no longer exist in the vCenter inventory are considered orphan proxies. If the proxy virtual machine remains in the vCenter inventory and you see the "Either the VM is deleted or is currently not managed by vCenter" warning for the proxy, you can restart the proxy virtual machine through the VDP Configure UI. If the problem persists, the issue might be the hostname is not resolvable due to incorrect network configuration. To work around this issue, delete the orphan proxy and re-deploy a new proxy.

- **Remove the proxy's ESXi host from the vCenter**

  When an external proxy's ESXi host is removed from the vCenter, the VDP Appliance considers the proxy as an orphan and displays the "Either the VM is deleted or is currently managed by vCenter" warning when it is selected in the VDP Configure UI. Unless the ESXi host will be added back to the vCenter, delete the orphan proxy entry from the VDP Configure UI.

- **vCenter switch**

  If a proxy's ESXi host is not moved to the new vCenter along with the VDP's ESXi host, that proxy appears as an orphan in the VDP Configure UI. Unless you are planning to move the proxy's host to the new vCenter or move the VDP's host back to the original vCenter, delete the orphan proxy from VDP Configure UI.

- **VDP rollback**

  After the VDP Appliance rolls back to a previous checkpoint, any external proxies added or deleted after the checkpoint was taken appear as orphan proxies in the VDP Configure UI. For added external proxies, you can restart them through the VDP Configure UI to re-register or redeploy them. For the deleted proxies, delete the orphan proxy entries from the VDP Configure UI.

- **Rebuild VDP from scratch and rollback**

  If the VDP Appliance experienced issues that required a rebuild from scratch, and the appliance rolled back to a checkpoint from Data Domain, use the VDP Configure UI to change the appliance's password immediately. Any external proxies that were deployed before the checkpoint was taken are displayed as orphans. Delete these orphans from the VDP Configure UI. Any external proxies that were deployed on the rebuilt VDP Appliance before the checkpoint rollback appear with a "Failed to authenticate with the proxy" warning. Update the proxy's password after you change the VDP Appliance's password.

- **VDP disaster recovery from tape**

  If the VDP Appliance is recovered from tape after a disaster, delete the orphan external proxies from the VDP Configure UI and deploy new ones.

- **Update password**

  When the VDP Appliance's password is changed through the VDP Configure UI, the VDP Appliance updates the password on all registered external proxies. If a proxy's password is not updated, you will see a "Failed to authenticate with the proxy" warning when the proxy is selected. You can update the proxy's password manually through the VDP Configure UI.

- **Restart proxy**

  If any previously-registered external proxies appear as not registered in the VDP Configure UI, restart the proxies, which will power cycle the proxies and reregister them to the VDP Appliance.

- **Emergency restore**

  When an emergency restore operation is performed with external proxies, the internal proxy is automatically enabled. When the emergency restore operation completes and all the ESXi hosts are reconnected to the vCenter, you can either delete the internal proxy or delete all the external proxies. Do not enable both the internal and external proxies for non-emergency restore activities.

Limitations

- External VDP proxies are supported only on vSphere 5.1 and later.
- The limit of external proxies per VDP Appliance is 8.
- The maximum number of concurrent backup jobs is 24.
- File Level Recovery (FLR) in virtual machines that use the EXT4 file system requires the use of an external proxy.

Adding an External Proxy

The Add Proxy wizard allows you to add and deploy up to 8 external proxies and register them with the VDP Appliance from the VDP Configure UI.

Procedure

1 Open a web browser and type:

https://<*IP_address_VDP_Appliance*>**:8543/vdp-configure/**

2 Log in with the VDP username and password.

3 Click the **Configuration** tab.

4 From the **Action** list, select **Add Proxy**.

The Add Proxy page appears.

5 On the Host and Storage page, specify the following credentials, and then click **Next**.

- Host — Select a destination host from the list.
- Storage — Select a destination storage device from the list.
- Network Connection — Select a network connection for the virtual machine from the list.

6 On the Network page, enter the following network settings, and then click **Next**.

- IPv4 static address — The Internet Protocol v4 setting of the interface.
- Netmask — The network mask of the IPv4 static address.
- Gateway — The gateway address of the IPv4 static address.
- Primary DNS — The primary domain name system used for DNS resolution.
- Secondary DNS — The secondary domain name system used for DNS resolution.

7 On the Ready to Complete page, review the deployment settings.

NOTE You can change the name of the external proxy virtual machine on the Ready to Complete page.

8 Click **Finish** to deploy the proxy.

Make sure the proxy deploys to the datastore that was selected in Step 5. If, after successful deployment, the proxy deploys to a VMware vSphere Distributed Resource Scheduler™ (DRS) cluster, the cluster can move the proxy by using storage vMotion. Any jobs running on the proxy while it is migrating to different storage are at risk. HotAdd does not work for proxies located in a DRS cluster.You, therefore, must manually disable DRS for the proxy.

To disable DRS manually for the proxy, select the **DRS** tab on the vSphere server hosting the proxy and select **Disable**.

Disabling the Internal Proxy

When a user performs a rollback operation as a checkpoint performed during an external proxy backup, after the rollback completes, the VDP Configure UI displays the internal proxy, along with a warning message prompting the user to disable the internal proxy.

Procedure

1 In the VDP Configure UI, select the internal proxy from the **Proxies** list.

2 Select **Manage proxy** from the Proxies Actions icon.

The Manage internal proxy wizard displays.

3. Enable the **Disable internal proxy** checkbox, and click **Next**.
4. On the Ready to Complete page of the wizard, click **Finish** to apply the changes.

(Optional) Configuring Proxy Certificate Authentication

By default, proxies do not validate SSL certificates when connecting to the vCenter Server. This can leave the vCenter Server vulnerable to a man-in-the-middle exploitation, which might result in unauthorized access to the vCenter Server. Configuring each proxy to use SSL certificate authentication when connecting to the vCenter Server corrects this vulnerability. Chapter 5, "Securing Communication between vCenter and VDP," on page 51 provides more information.

Monitoring External Proxy Health Status

Health Status Criteria

The health status reported for the external proxy is based on the following criteria:

- Disk Usage
  - Warning — Any file system that is greater than 70% capacity.
  - Critical Warning — Any file system that is greater than 90% capacity.
- CPU Load
  - Warning — 15 minute load average is greater than 1.5.
  - Critical Warning — 15 minute load average is greater than 5.0.
- Memory Usage
  - Warning — Usage is greater than 85%.
  - Critical Warning — Usage is greater than 95%.

External Proxy Logs

External proxy logs are visible only if at least one external proxy is configured. Downloading this log bundle streams a `.zip` file to the browser. The `.zip` file contains all the external proxy logs. The internal proxies are excluded from this log bundle.

For information about downloading logs, refer to "Collecting Logs" on page 44.

Storage Management

8

This chapter contains the following topics:

- "Creating New Storage" on page 72
- "Attaching Existing VDP Disks" on page 73
- "Detaching and Reattaching Storage" on page 75
- "Viewing the Storage Configuration" on page 76

Creating New Storage

The Initial Configuration wizard guides you through the storage type selection, device allocation on VDP storage disks, and the option to run the performance assessment tool.

Limitations

You cannot migrate the appliance to a new host or to a new datastore while you are creating new storage.

Prerequisites

- The VDP Appliance is deployed and you are logged into the Create Storage page of the Initial Configuration wizard.
- Disable vSphere HA on the VDP Appliance immediately after OVA deployment. When performing initial configuration on the VDP Appliance, including creating new storage, you can enable vSphere HA for the appliance.

Procedure

1. On the Create Storage page of the Initial Configuration wizard, select **Create new storage**. When you create new storage, the process creates a new storage node on selected datastores.
2. Select one of the following capacity options and click **Next**.
   - 0.5
   - 1
   - 2
   - 0.5
   - 1
   - 2
   - 4
   - 6
   - 8

   The Device Allocation page appears. When you create new storage, the number of required disks is known.
3. Select the provision type from the **Provision** drop-down list.
   - Thick Lazy-Zeroed (the default and recommended provision type) — Thick lazy zeroed provisioning creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
   - Thick Eager-Zeroed — Thick eager zeroed provisioning creates a type of thick virtual disk that is used when data security is a concern. Space required for the virtual disk is allocated when the virtual disk is created. When you create a virtual disk using thick eager zeroed provisioning on a datastore that had previous data, the previous data is erased and cannot be recovered. It might take much longer to create disks in this format than to create other types of disks.
   - Thin — For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. The thin disk starts small and uses only as much datastore space as the disk needs for its initial operations.
4. After all of the disks have been allocated to datastores, click **Next**.

   The Ready to Complete page appears.

On the Ready to Complete page, you can run a performance analysis on the storage configuration and click **Next** to apply the changes. Though you can bypass the performance analysis test, you are strongly encouraged to run it.

5 When you click **Next**, you are prompted with a warning that the storage configuration will start and cannot be undone. Click **Yes** to continue.

Possible results are Passed, Failed, and Conditionally Passed. If all tests succeed, the result is Passed. If the write or read tests are unsuccessful, the result is Failed. If the write and read tests are successful but the seek test fails, the result is Conditionally Passed.

a To run the test, click the **Run performance analysis on storage configuration** checkbox to make sure the storage configuration meets minimum performance expectations. The minimum performance expectations are listed in Table 8-8.

This test performs write, read, and seek performance tests on the disks. There is a chance that data could be lost based on the write tests. It is best practice to only run this tool on newly-created disks with no data. Depending on your storage configuration, performance analysis can take from 30 minutes to several hours to complete.

b Click the **Restart the appliance if successful** checkbox to automatically restart the appliance after the test runs successfully. The test begins when you click **Next**.

The performance analysis test is server-initiated and you can close the browser while the test runs.

- If the test is successful, a message that the configuration is complete appears and the server automatically reboots the appliance.
- If the test conditionally passes or fails, the results of the performance analysis appear, but the server does not automatically reboot the appliance. To view the test results, you must log into VDP-Configure again and manually initiate a client reboot.

NOTE If you do not click **Restart** within 59 seconds, the appliance automatically reboots and starts the services. After the VDP Appliance reboots, it performs a series of automated configuration steps. These steps can take 30-45 minutes or more to complete.

Minimum Storage Performance

When configuring the VDP Appliance, the performance test produces varying results depending on the size of the appliance being deployed.

Table 8-8 lists the minimum expectations for Read, Write, and Seek performance by VDP Appliance size.

Table 8-8. Minimum expectations for storage performance

VDP Appliance Size (in TB)	Disk Size	Read Minimum	Write Minimum	Seek Minimum
0.5	256 GB	60 MB/s	30 MB/s	400 Seeks/s
1.0	512 GB	60 MB/s	30 MB/s	400 Seeks/s
2.0	1024 GB	60 MB/s	30 MB/s	400 Seeks/s
4.0	1024 GB	80 MB/s	40 MB/s	400 Seeks/s
6.0	1024 GB	80 MB/s	40 MB/s	400 Seeks/s
8.0	1024 GB	150 MB/s	120 MB/s	400 Seeks/s

Attaching Existing VDP Disks

The Create Storage page in the Initial Configuration wizard provides the **Attach existing VDP disks** option. This option enables you to browse the datastores and select the previously-used VDP disks, and then proceeds to automatically attach the selected disks to the new VDP Appliance. These disks are automatically added to the new VDP Appliance.

CAUTION Do not attempt to manually attach previously-used VDP disks to the new VDP Appliance without following the steps in this procedure. If VDP detects an incomplete or invalid storage configuration, the operation fails.

When you attach existing storage, you do not need to select a capacity option, as you are required to do when creating new storage.

The following changes occur when previously-used VDP disks are attached to the new VDP Appliance:

- All backup jobs associated with the previously-used VDP are deleted and must be re-created.
- All replication jobs associated with the previously-used VDP are deleted and must be re-created.
- Restore points that are associated with the previously-used VDP are kept intact. The restore points appear with the original VM name appended with a string of random letters.
- On the Set Restore Options page of the Restore a backup wizard, the **Restore to Original Location** option is disabled for the restore points associated with the previously-used VDP disks.
- Email reporting must be reconfigured.

Prerequisites

- Before you can attach existing storage, you must install and configure the VDP Appliance described in "VDP Installation and Configuration" on page 19.
- Ensure that you back up all the VDP storage which you intend on attaching to the VDP Appliance.

Procedure

1 On the Create Storage page of the Initial Configuration wizard, select **Attach existing VDP disks** and click **Next**.

The Device Allocation dialog box appears.

2 Click the first ellipsis button:

a Browse to the first vmdk file you want to attach.

b Highlight the vmdk file and click **Select**.

NOTE You can select to attach only the data disks of the previously-used VDP Appliance. You cannot select the OS boot partition. If you select the primary disk partition of 100 GB (the OS boot partition), an error message appears.

You can attach vmdk files in any order. After you have selected the first vmdk file, the system analyzes the disk and defines how many additional disks should be selected.

NOTE At any time during the attach process, you can click **Reset** to reset the Device Allocation dialog box to its original state.

3 Click the ellipsis button that corresponds to the next disk to be defined:

a Browse to the next vmdk file you want to attach.

b Highlight the vmdk file and click **Select**.

Each disk is validated as a matching disk before it is added. If the validation fails, an error message appears. Hover over the red highlighted disk to see the error message.

4 Repeat Step 3 for all remaining disks.

5 After all disks have been allocated, click **Next** to validate the complete set of disks.

The Ready to Complete page appears.

6 Click **Next**.

The system displays the message:

```
The following process will start the storage configuration. This cannot be undone. Do you wish to continue?
```

7 Click **Yes**.

The system prompts you to provide the root password associated with the previously-used VDP Appliance.

8 Type the root password of the previously-used VDP Appliance into the **Password** and **Verify Password** text boxes, and then click **OK**.

9 Click **Finish** to apply the changes and reboot.

NOTE After a successful storage configuration, the system automatically reboots and starts the services. After the VDP Appliance reboots, it performs a series of automated configuration steps. These steps can take 30-45 minutes or more to complete.

After the configuration is complete, an integrity check begins.

Detaching and Reattaching Storage

The following procedure explains the steps you must perform if the primary disk partition (the OS boot partition) on the VDP Appliance becomes corrupt or lost, resulting in an unrecoverable VDP Appliance.

Prerequisites

- At least one validated checkpoint is present on the VDP Appliance where the vmdk files are being detached and reattached.
- A new VDP Appliance is deployed which is compatible with the older VMDK disk data (the VDP Appliance must be the same version as the disk data or a newer version).
- The vmdk files from the previous VDP Appliance must be on a datastore that is accessible by the newly-deployed VDP Appliance.

NOTE During the reattach process, you will be prompted to enter the root password for the old VDP Appliance.

Best Practices

- Make a backup copy of all vmdk files before reattaching them to a VDP Appliance.
- If possible, detach the vmdk files from the VDP Appliance after shutting down the VDP Appliance by using the **Shut Down Guest OS** action. Otherwise, as a last resort, power off the VM.
- Before detaching a vmdk file from the VDP Appliance, note the full path and name of the vmdk file. You will need this information when reattaching the disk to the newly-deployed VDP Appliance.

Procedure

1 In the vSphere Client, navigate to the VDP Appliance and perform a **Shut Down Guest OS** action on the virtual machine.

NOTE If the **Shut Down Guest OS** action is grayed out, navigate to **vCenter > Hosts and Clusters**, right-click the VDP Appliance, and select **Power off VM**.

2 Detach the vmdk files from the VDP Appliance:

a From the vSphere Web client, log in as a user who has privileges to edit hardware settings.

b Navigate to **vCenter > Hosts and Clusters.**

c In the tree on the left, click the disclosure arrows until the VDP Appliance appears.

d Right-click the VDP Appliance and select **Edit Settings**.

The virtual machine properties appear. The **Hardware** tab is selected by default.

Hard disk 1 is always the primary, 100 GB OS boot partition. Do not remove Hard disk 1 from the VDP Appliance.

e Click Hard disk 2 from the list.

f From the **Disk File** field, note the full path and name of the vmdk file. You will need this information when reattaching the disk.

g Click **Remove**.

h Under Removal Options, select **Remove from virtual machine**.

i Repeat the removal option for each hard disk (2 through *x*) in the list.

j After removing hard disks 2 through *x*, click **OK**.

3 On the Create Storage page of the Initial Configuration wizard, select **Attach existing VDP disks**, and follow the steps in "Attaching Existing VDP Disks" on page 73.

Viewing the Storage Configuration

The **Storage** tab provides a storage summary, capacity utilization information, and performance analysis details.

The **Capacity Utilization** button displays a page that provides status information for the datastore:

- A horizontal bar graph next to the datastore icon shows how full the datastore is as a percentage.
- A pie chart shows a breakdown of the space in the datastore. Orange represents the amount of space used by the datastore. Green represents the amount free space on the datastore. Blue represents the space on the datastore that is used by other applications that run on virtual machines deployed on the datastore.
- A table next to the pie chart lists each data partition name, size, provision type, and vmdk file name. The following example shows information for a data partition named data 01:

data 01	256GiB	Thin	sample-vdp-241168_6..0.0.117_1.vmdk

In the example, 256 GiB indicates the maximum size that can be utilized.

The **Performance Analysis** button displays a table that contains statistics from a performance analysis test.

Column	Description
Datastore	Name of the datastore.
Completed On	Date that the test completed.
Result	A test can display one of the following results: ■ Never Run ■ Passed ■ Failed If the write or read tests are unsuccessful, the result is "Failed." ■ Conditionally Passed If the write and read tests are successful, but the seek test failed, the result is "Conditionally passed."
Read (MiB/s)	Megabytes per second for the read test.
Write (MiB/s)	Megabytes per second for the write test.
Seek (Seeks/s)	Megabytes per second for the seek test.

Prerequisites

The VDP storage disks are distributed across the available datastore locations, the disks are validated, the system is rebooted, and the system services are up and running.

Procedure

1 Log in to the VDP-Configure URL:

   https://<*IP_address_VDP_Appliance*>**:8580/vdp-configure/**

2 Click the **Storage** tab.

   The Storage Summary appears, displaying the available datastores and the amount of total usable storage and storage capacity that is available for each datastore.

3 To view status information about the datastore, click **Capacity Utilization**. This page is the default.

4 To run a performance test, click **Performance Analysis**, select a datastore in the table, and then click **Run**.

   The performance analysis test creates a 41 GB vmdk on the datastore, and then runs read, write and seek tests to check the datastore performance.

Data Domain Integration 9

This chapter contains the following topics:

- "VDP and Data Domain System Integration" on page 80
- "Architecture Overview" on page 80
- "VDP Client Support" on page 81
- "Best Practices" on page 81
- "Pre-integration Requirements" on page 82
- "Preparing the Data Domain system for VDP Integration" on page 85
- "Adding a Data Domain System" on page 86
- "Editing the Data Domain System" on page 87
- "Deleting the Data Domain System from the VDP Appliance" on page 88
- "Backups with VDP and Data Domain" on page 90
- "Replication Control" on page 91
- "Server Maintenance Activity Monitoring" on page 92
- "Restoring Avamar Checkpoint backups from Data Domain systems" on page 92
- "Monitoring Data Domain from the VDP Appliance" on page 94
- "Reclaiming Storage on a Full Data Domain System" on page 95
- "Common Problems and Solutions" on page 96

VDP and Data Domain System Integration

vSphere Data Protection and Data Domain system integration enables the following:

- The use of Data Domain systems as a backup target for VDP backups
- The target destination of backup data, which is set during the creation of a backup job
- Transparent user interaction to the backup destination (VDP or Data Domain)

Architecture Overview

A Data Domain system performs deduplication through DD OS software. VDP source based deduplication to a Data Domain system is facilitated through the use of the DD Boost library.

VDP uses the DD Boost library through API-based integration to access and manipulate directories, files, and so forth, contained on the Data Domain file system. The DD Boost API gives VDP visibility into some of the properties and capabilities of the Data Domain system. This enables VDP to control backup images stored on Data Domain systems. It also enables VDP to manage maintenance activities and to control replication to remote Data Domain systems.

DD Boost is automatically installed on the VDP Appliance during the addition of a Data Domain system.

Figure 9-3 depicts a high-level architecture of the combined VDP and Data Domain solution. With VDP and Data Domain integration, you can specify whether a specific backup policy targets a VDP Appliance or a Data Domain system.

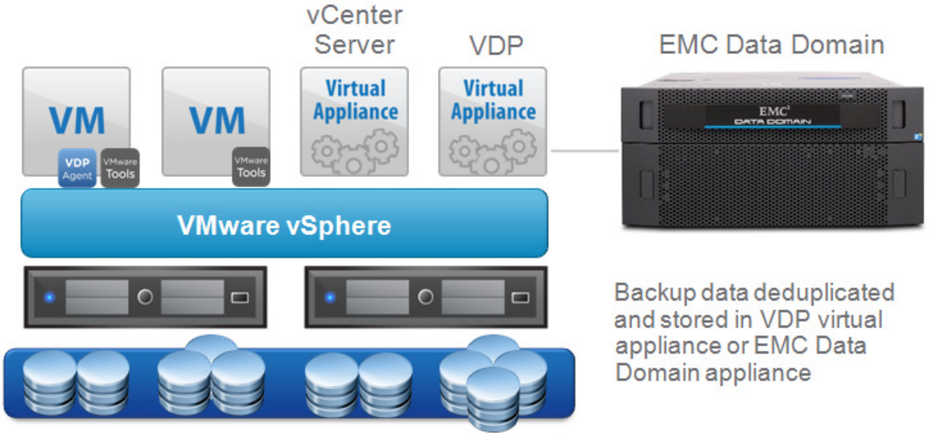


Figure 9-3. VDP and Data Domain solution

When you select the VDP Appliance as the target for backup storage, the VDP Appliance performs deduplication segment processing.

When you select a Data Domain system as the backup target, backup data is transferred to the Data Domain system. The related metadata that is generated is simultaneously sent to the VDP Appliance for storage. The metadata enables the VDP Appliance to perform restore operations from the Data Domain system.

VDP Client Support

VDP and Data Domain system integration supports the following plug-ins:

- VDP Plug-in for Exchange Server VSS
- VDP Plug-in for SharePoint Server VSS
- VDP Plug-in for SQL Server

Best Practices

What are the VDP limitations with a Data Domain system attached?

VMware suggests protecting up to 25 virtual machines per TB of capacity on a VDP Appliance. This variable is dependent upon the size of the virtual machines, the typical change rate, and the amount of data on each virtual machine. With these considerations, you can protect up to 200 virtual machines per VDP Appliance backing up to a Data Domain system.

Because the backup data is stored on the Data Domain system, and only the backup job metadata is stored on the VDP Appliance, deploy a 0.5 TB VDP Appliance for a standard Data Domain system and a 1 TB VDP Appliance for a 64 TB Data Domain system.

The following list provides the suggested number of VDP Appliances deployed per Data Domain system:

- 1 VDP per DD160 and DD620
- 1 VDP per DD2200
- 2 VDP per DD2500 and DD4xxx
- 3 VDP per DD7200 and DD990

What size VDP Appliance do I need if I want all my backups to go to Data Domain?

With a Data Domain system attached to a VDP Appliance as the storage device, the VDP Appliance only stores the metadata for backups using the Data Domain system as the destination. It has been determined that a 16 TB Data Domain system only requires a 0.5 TB VDP Appliance if all of the backup data is sent to the Data Domain system. If backups are going to be sent to the VDP Appliance as well, the size of the VDP Appliance should be increased accordingly based on the data to be stored on the VDP Appliance. With a 64 TB or larger Data Domain system, you can deploy a 1 TB VDP Appliance per 64 TB of Data Domain system storage you expect to consume with the backup data.

I have many images, pictures, and PDF files in my VMs. Should I set the VDP Appliance or the Data Domain system as the destination for these backups?

The Data Domain system provides better deduplication on images, pictures, and PDF files than the standard VDP Appliance deduplication algorithms.

Data Domain Limitations

The following are current limitations defined for the use of a Data Domain system with a VDP Appliance:

- If a VDP Appliance has a Data Domain system attached to it, the "Import Existing storage" functionality of the VDP Appliance cannot be used for the VMDKs of the VDP Appliance with the Data Domain system attached.
- Only one Data Domain system can be attached to a VDP Appliance at a time.
- The Data Domain system cannot be deleted from the VDP Configuration UI. Use the manual steps defined in "Deleting the Data Domain System from the VDP Appliance" on page 88 to delete a Data Domain system.
- If the Data Domain and VDP connection is broken, the VDP Appliance does not monitor the Data Domain system. Behaviors that might indicate the connection between the appliances are broken include, but are not limited to, the integrity check, `hfscheck` or backups failing.
- The Data Domain system or VDP Appliance cannot be upgraded if the connection between them is broken.

Backup

During a backup, the VDP Appliance generates a backup request for the backup destination. If the backup request includes the option to use a Data Domain system as the destination, backup data is stored on the Data Domain system. Metadata is stored on the VDP Appliance.

Restore

The process of data recovery is transparent to the backup administrator. The backup administrator uses the same VDP recovery processes that are native to current VDP implementations.

Security — Encryption

When using a VDP Appliance with a Data Domain system attached, there are two potential backup data streams. If the backup data is being written to the VDP Appliance, the backup data is always compressed and encrypted during flight. If the backup data is being routed to the Data Domain system, the `ddboost` utility encrypts the backup data as it is transmitted over the network to the Data Domain system.

Data Migration

You cannot migrate backup data directly from the VDP Appliance to the Data Domain system.

To use the Data Domain system as the backup target for backing up a VM or appliance instead of the VDP Appliance, edit the backup job and define the destination as the Data Domain system, and then start performing backups to the Data Domain system. When you change the backup target to the Data Domain system, the next backup runs as full backup.

After you successfully perform a backup to the Data Domain system, you can delete the earlier backups from the VDP Appliance. Refer to "Deleting a Backup Job" on page 118 for information on how to manually delete backups. If you do not manually delete backups, they expire without intervention.

Pre-integration Requirements

Before you integrate a Data Domain system with a VDP Appliance, review the following topics:

- "Network Throughput" on page 83
- "Network Configuration" on page 83
- "NTP Configuration" on page 83
- "Licensing" on page 84

- "Port Usage and Firewall Requirements" on page 84
- "Capacity" on page 84
- "Data Domain System Streams" on page 84
- "Existing Backup Products in Use with Data Domain" on page 85

NOTE This section assumes the VDP Appliance and the Data Domain system are installed and configured.

Network Throughput

With VDP , the VDP Appliance and Data Domain systems can connect over a Wide Area Network (WAN). Before using this configuration, validate the firewall port requirements of the Data Domain system. You can find this information in the *EMC Avamar 7.1 Product Security Guide.*

You can use VDP Appliance replication over a WAN to replicate data from source VDP Appliance and Data Domain systems to target VDP Appliances, provided they also have a Data Domain system attached.

Before integrating a Data Domain system with an VDP Appliance, ensure that enough network bandwidth is available. To obtain the maximum throughput available on a Data Domain system (for restores, level zero backups, and subsequent incremental backups after a level-zero backup), verify that the network infrastructure provides more bandwidth than the bandwidth required by the maximum throughput of the Data Domain system. To see the network throughput, use the `system show performance` command on your Data Domain system:

```
system show performance [ {hr | min | sec} [ {hr | min | sec} ]]
```

For example:

```
system show performance 24 hr 10 min
```

This command shows the system performance for the last 24 hours at 10 minute intervals. 1 minute is the minimum interval.

Network Configuration

Configure (or verify) the following network configuration:

- Assign a Fully Qualified Domain Name (FQDN) to the Data Domain system.
- Use a FQDN (not an IP address) when registering a Data Domain system. This can limit the ability to route optimized duplication traffic exclusively through a registered interface.
- Ensure that DNS on the Data Domain system is properly configured.
- Ensure forward and reverse DNS lookups work between the following systems:
  - VDP Appliance
  - Data Domain system
  - Backup and restore clients
  - vCenter Server
  - vSphere hosts
- Use Hosts files to resolve hostnames to non-routable IP addresses.
- Do not create secondary hostnames to associate with alternate or local IP interfaces.

NTP Configuration

Configure the VDP Appliance, vCenter Server, vSphere hosts, and Data Domain systems to use the same Network Time Protocol (NTP) Server.

Licensing

Ensure that the environment meets the licensing requirements in Table 9-9.

Table 9-9. Licensing requirements

Product	Licensing requirement
VDP Appliance	The VDP Appliance requires a valid vSphere host license (minimum of Essentials Plus).
Data Domain system	The DD Boost license must be installed on the Data Domain system.

Port Usage and Firewall Requirements

To enable communication between the VDP Appliance and the Data Domain systems, review and implement the port usage and firewall requirements in the following documents:

- "vSphere Data Protection Port Usage" on page 187 of this document.
- "Port Requirements for Allowing Access to Data Domain System Through a Firewall," available on the Data Domain Support Portal at:

  https://my.datadomain.com

Capacity

Carefully assess your backup storage needs when evaluating how much data to store on the Data Domain system and the VDP Appliance. Include estimates from data that is sent to the Data Domain system from any other servers.

When the Data Domain system reaches its maximum storage capacity, no further backups to the Data Domain system occur until additional capacity is added or old backups are deleted or expired.

"Data Domain Capacity Monitoring" on page 95 provides details on how to monitor capacity.

Data Domain System Streams

Each Data Domain system has a soft limit to the maximum number of connection and data streams that can be sustained simultaneously while maintaining performance. The number of streams varies depending on the Data Domain system model. For example, the DD990 can support 540 backup streams, while the DD620 can support 20 backup streams.

As a default, the VDP Appliance is configured to use a maximum of 16 streams. To override the maximum number of streams, on the VDP Appliance, change the `/usr/local/vdr/etc/vdp-options.properties` file. Add the property `com.vmware.vdp.option.datadomain.maxstreamsoverride=`*`num`* (where *num* is the new maximum number of streams) and save the file. Consult the DD OS Administration Guide for your Data Domain system to review current recommended stream settings. Setting this value forcibly overrides the maximum streams value for every add or edit operation of a Data Domain performed from the given VDP Appliance.

These changes will not take effect until the Data Domain is edited, or a new Data Domain is added to the VDP Appliance. These changes will be reflected in the `/usr/local/avamar/var/ddr_info` file or can be seen by running the `ddrmaint read-ddr-info` command.

Setting this value forcibly overrides the maximum streams value for every add or edit of a Data Domain for the given VDP Appliance.

These changes will not take effect until the existing Data Domain system is edited, or a new Data Domain system is added to the VDP Appliance. The changes will be reflected in the `ddrmaint read-ddr-info` file.

Existing Backup Products in Use with Data Domain

Data Domain systems can use other third-party backup and archiving software. The VDP Appliance does not assume it has sole ownership of the Data Domain system. Ensure that proper sizing is evaluated if the system is shared with other software products. The VDP Appliance does not use the native Data Domain system snapshot and replication features.

Replication occurs through the DD Boost SDK library by using copying and cloning. However, other third party products may make use of the native Data Domain system snapshot and replication features. In this case, a snapshot of an entire Data Domain system or a replication of an entire Data Domain system includes the VDP Appliance data.

Preparing the Data Domain system for VDP Integration

To support VDP and Data Domain system integration, ensure the environment meets the Data Domain system requirements listed in Table 9-10.

Table 9-10. Data Domain system requirements

Data Domain feature or specification	Requirement for use with the VDP Appliance
Data Domain Operating System (DD OS)	VDP integration requires DD OS 5.4.0.8 or DD OS 5.5.x or later.
DD Boost	VDP integration requires DD Boost 2.6.x DD Boost software enables backup servers to communicate with storage systems without the need for Data Domain systems to emulate tape. There are two components to DD Boost: one component that runs on the backup server and another that runs on the Data Domain system. The component that runs on the backup server (DD Boost libraries) is integrated into the VDP Appliance. DD Boost software is an optional product that requires a license to operate on the Data Domain system.
Data Domain device type	The VDP Appliance supports any Data Domain system that is running the supported DD OS version.
DD Boost user account	The DD Boost library uses a unique login account name created on the Data Domain system. This account name is known as the DD Boost account. Only one DD Boost account exists per Data Domain system. If the account is renamed and/or the password is changed, these changes must be immediately updated on the VDP Appliance by editing the Data Domain configuration options. Failure to update the DD Boost account information could potentially yield integrity check errors and/or backup/restore problems. The DD Boost account must have administrator privileges.

Before you can add a Data Domain system to the VDP configuration, prepare the Data Domain system by enabling DD Boost and creating a DD Boost user account for the VDP Appliance to use to access the Data Domain system for backups and restores (and replication, if applicable).

To prepare the Data Domain system:

1 Disable DD Boost on the Data Domain system by logging into the CLI as an administrative user and typing the following command:

```
ddboost disable
```

2 Create a DD Boost account and password:

a Create the user account with admin privileges by typing the following command:

```
user add USER role admin
```

where USER is the username for the new account.

b Set the new account as the DD Boost user by typing the following command:

```
ddboost set user-name USER
```

where USER is the username for the account.

3 Enable DD Boost to allow the changes to take effect by typing the following command:

```
ddboost enable
```

IMPORTANT If you change the DD Boost account name or password, make sure to edit the Data Domain system configuration in the VDP Configure UI. Otherwise all backups, restores, and maintenance activities fail.

Adding a Data Domain System

A Data Domain system performs deduplication through DD OS software. When you select a Data Domain system as the backup target, backup data is transferred to the Data Domain system. Only one Data Domain system can be configured.

Prerequisites

The VDP storage disks are distributed across the available datastore locations and the disks are validated.

The minimum version for Data Domain is version 5.3.

Procedure

1 To access the VDP-Configure utility, open a web browser and type:

https:<*IP_address_VDP_Appliance*>**:8543/vdp-configure/**

2 Click the **Storage** tab.

The storage summary displays statistics about the total usable storage and available capacity for the Data Domain system and for each datastore.

3 From the **Action** list, select **Add Data Domain**.

The Host Configuration dialog box appears.

4 Specify Data Domain system information:

a In the **Data Domain FQDN or IP** box, enter the FQDN or IP address of the Data Domain system to add.

NOTE Do not use an IP address or a secondary hostname that associates with alternative or local IP interfaces. It may limit the ability of the VDP Appliance to route optimized deduplication traffic.

b In the **DDBoost User Name** box, type the name of the DD Boost account for VDP to use to access the Data Domain system for backups, restores, and replication.

c In the **Password** box, type the password for the account that VDP should use to access the Data Domain system for backups, restores, and replication.

d In the **Confirm Password** box, type the password again to verify it.

e Click the **Enable Checkpoint Copy** checkbox to enable checkpoint backup support, which allows VDP checkpoints to be stored on a Data Domain system (using DD OS 5.3 or later). These checkpoints are then used if disaster recovery is required.

5 To configure SNMP, click **Next**.

The SNMP dialog box appears. The SNMP options to configure for VDP and Data Domain system integration include the following:

- The **Getter/Setter Port Number** text box lists the port on the Data Domain system from which to receive and on which to set SNMP objects. The default value is 161.

- The **SNMP Community String** text box lists the community string VDP uses for read-only access to the Data Domain system.
- The **Trap Port Number** text box lists the trap port. The default value is 163.

6 Click **Next**.

The Ready to Complete dialog box appears.

7 Click **Add** to save your Data Domain configuration.

A successful Add Data Domain operation causes the following UI changes to occur:

- The system creates a new checkpoint which takes approximately ten minutes.
- Data Domain information appears on the VDP Appliance in the following locations:
  - **Backup** tab — The Data Domain system is available as the storage target in the Create a new backup job wizard.
  - **Restore** tab — Displays the Data Domain in the Name column of the Restore backup wizard.
  - **Reports** tab — Provides backup status reports for the Data Domain system.
  - Storage summary — Displays statistics about the total usable storage and available capacity for the Data Domain. Refer to “Viewing the Storage Configuration” on page 76 for details.
  - Email reporting — Displays a summary of the Data Domain configuration.

NOTE When you add a Data Domain system to the VDP configuration, the VDP Appliance creates an MTree on the Data Domain system for the VDP Appliance. The MTree refers to the directory created within the DD Boost path. Data Domain systems support a maximum of 100 MTrees. If you reach the limit, then you cannot add the Data Domain system to the VDP configuration.

Changing the Max Streams Value

As a default, the VDP Appliance is configured to use a max streams value of 16.

If you need to modify the number of streams associated to a Data Domain system from the VDP Appliance, perform the following steps. The changes applied using these steps will only take effect during subsequent edits of or the addition of a Data Domain system to the VDP Appliance.

1 Go to the command line of the VDP Appliance (either with SSH / Putty or Terminal of the appliance) and type the following command:

```
cd /usr/local/vdr/etc/
```

2 Use a text editor to edit the `vdp-options.properties` file.

3 Insert the field `com.vmware.vdp.option.datadomain.maxstreamsoverride=`*num* where *num* is the max number of streams for the Data Domain system.

4 Save the modified file.

5 Add or edit a Data Domain system. Allow five minutes for the appropriate process to run.

The `ddrmaint read-ddr-info` file should now contain a “max-streams” attribute with the value you configured.

Editing the Data Domain System

1 To access the VDP-Configure utility, open a web browser and type:

https:<*IP_address_VDP_Appliance*>**:8543/vdp-configure/**

2 Click the **Storage** tab.

The storage summary displays statistics about the total usable storage and available capacity for the Data Domain and for each datastore.

3 From the **Action** list, select **Edit Data Domain**.

The **Host Configuration** dialog box appears.

4 Edit the settings for the Data Domain system as necessary. "Adding a Data Domain System" on page 86 provides details on each setting in the dialog box.

5 Click **Next**.

6 After the edits are complete, click **Finish**.

NOTE If you edit the Data Domain system hostname, the DD Boost username, or the DD Boost password, the system automatically creates a new checkpoint, which takes approximately ten minutes. For instructions, refer to "Rolling Back an Appliance" on page 46.

NOTE If you perform a rollback to a checkpoint with the outdated Data Domain system name or DD Boost information, then the rollback fails.

Deleting the Data Domain System from the VDP Appliance

Before you delete the Data Domain system from the VDP Appliance, note the following:

- You must delete all restore points stored on the Data Domain by using the vSphere Web Client.
- No backup jobs can exist with the Data Domain system. If any backup jobs exist where the Data Domain system is configured as the destination, you must either edit the backup jobs to set a new destination or you must delete the backup jobs.
- After the restore points are checked and the backup jobs are verified, it is best practice to run an integrity check from the **Configuration** tab of the VDP Appliance.
- Remove the Data Domain system from VDP using the command line interface. See detailed instructions below.
- After the Data Domain system is deleted, run another integrity check from the VDP user interface to verify the Data Domain system is invalid.

NOTE VMware Knowledge Base Article 2063806 provides information about deleting a Data Domain system. This is an internal article. Contact Technical Support for assistance.

Procedure

1 Before you delete the Data Domain system, delete all restore points stored on the Data Domain system. Use the vSphere Web Client to delete restore points:

a Navigate to the **Restore** tab of the VDP-A plug-in.

b Select the **Manual restore** tab on the navigation bar.

c For clients that have been backed up to the Data Domain system, remove all restore points where the location shows that they are stored on the Data Domain server.

2 Ensure that no backup jobs use the Data Domain system as the destination. If any backup jobs exist with the Data Domain system as a destination, you must edit the backup job to set a new destination or the delete the backup job.

3 After the restore points have been checked and the backup jobs have been verified, as a best practice run an integrity check from the configuration tab of the VDP plug-in.

4 Once the integrity check and validation of the integrity check complete, remove the Data Domain system from the VDP Appliance. Use the command line.

a SSH or Putty into the VDP Appliance.

b Run the `status.dpn` command and verify that the `Last checkpoint` and `Last hfscheck` have completed. If they have not, repeat this step until they show they have completed.

c Run the `mccli server show-prop` command. This command displays results similar to following output:

```
Attribute                 Value
----------------          ---------------------------------------
State                                              Full Access
Active sessions                                              0
Total capacity                                        575.9 GB
Capacity used                                          0 bytes
Server utilization                                        0.0%
Bytes protected                                        0 bytes
Bytes protected quota                           Not configured
License expiration                                       Never
Time since Server initialization             1 days 20h:58m
Last checkpoint                        2014-10-10 09:03:48 MDT
Last validated checkpoint              2014-10-09 09:02:16 MDT
System Name                              gs-pod187.test.domain
System ID                    1381255529@00:50:56:86:46:10
HFSAddr                                  gs-pod187.test.domain
HFSPort                                                  27000
```

The System ID contains a number, then an @ sign, and then the MAC address of the VDP Appliance. Note the number before the @ sign. The Data Domain system refers to this number as the DPN ID.

5 Run the following command:

```
ddrmaint has-backups –dpnid=num –ddr-server=DDRSERVER | grep ‘ hasbackups’
```

where *`num`* is the DPN ID you noted in Step c and *`DDRSERVER`* is either the hostname or the IP address of the DDR server. Note that there is a space in the `grep` command between the single quote and the word hasbackups.

This command displays either of the following results:

```
hasbackups=”true”
```

or

```
hasbackups=”false”
```

6 If the information returned is `hasbackups='true'`, then check if Step 1 and Step 2 need to be repeated. After you repeat Step 1 and Step 2 (or verify that the steps have been completed), repeat Step 5.

7 If Step 5 still shows `‘hasbackups=true’` continue to Step a. Otherwise, you need to run Step 11.

If you have attempted to remove backups from the Data Domain system by using the VDP UI and the Data Domain system still indicates that the backup data is present, then you must mount the Data Domain data partition to a Linux VM to clear out the data directory. If a Linux VM is unavailable, you can use the VDP Appliance for the next steps.

By default, all of the data for backups on a Data Domain system is stored under a single logical storage unit (LSU). The LSU for the VDP is named `Avamar-<DPNID>` and is located under `/data/col1`.

If you are unable to access the file system from the Data Domain operating system interface, you must grant remote access to the LSU. To do so, you must access the Data Domain system remotely by using the following steps:

a Putty or SSH to the Data Domain system.

b Run the `nfs add /data/col1 <`*`IP of Linux VM`*`>` command.

This command should return the results of `NFS export for “/data/col1” added`.

If the command does not return the expected results, type `nfs help` for a man page on the command. If the command returns the expected results, exit the SSH or Putty session.

c Putty or SSH to the Linux VM used in Step b as the root user.

d Run the `mkdir /mnt/DataDomain01` command.

e Run the `mount <IP of DD>:/data/col1 /mnt/DataDomain01` command.

f Run the `ls -ltr /mnt/DataDomain01/avamar-<DPNID>` command, where `DPNID` is the value noted in Step c. The output should display subdirectories where the VDP backups are stored.

g Run the `rm -rf /mnt/DataDomain01/avamar-<DPNID>/*` command where `DPNID` is the value noted in Step c. This will remove all data from the VDP backups.

8 Repeat Step f to verify that all data was removed.

9 Exit the Linux virtual machine.

10 Putty or SSH to the VDP Appliance

11 Run the `mccli dd delete --name=<DD IP or hostname> --force=true` command.

12 After you delete the Data Domain system, run an integrity check again from the VDP UI. The old checkpoints with the Data Domain information is now invalid.

Backups with VDP and Data Domain

The following topics describe VDP and Data Domain system backups:

- How backups work with VDP and Data Domain system
- Selecting a Data Domain target for backups

How Backups Work with VDP and Data Domain

During a backup, the VDP Appliance sends a backup request to the vCenter Server. If the backup request includes the option to use a Data Domain system as the target, backup data is stored on the Data Domain system and metadata is stored on the VDP Appliance.

The following topics provide additional details on how backups work with VDP and Data Domain.

Where Backup Data is Stored

All data for a backup is stored under a single dedicated MTree on a single Data Domain system.

How VDP Appliance Manages Backup Data

During a backup, the VDP Appliance sends the metadata for the backup from the client to the VDP data partitions. This process enables the VDP Appliance to manage the backup even though the data is stored on a Data Domain system.

The VDP Appliance does not store the original path and file name for a file on the Data Domain system. Instead, the VDP Appliance uses unique file names on the Data Domain system.

Supported Backup Types

Store all backup types (full, differential, incremental) for a client in the same destination (VDP Appliance or Data Domain system). Backup types should not be distributed across destinations. For example, do not store the initial full backup of a client in the VDP Appliance and subsequent differential backups on the Data Domain system.

Canceling and Deleting Backups

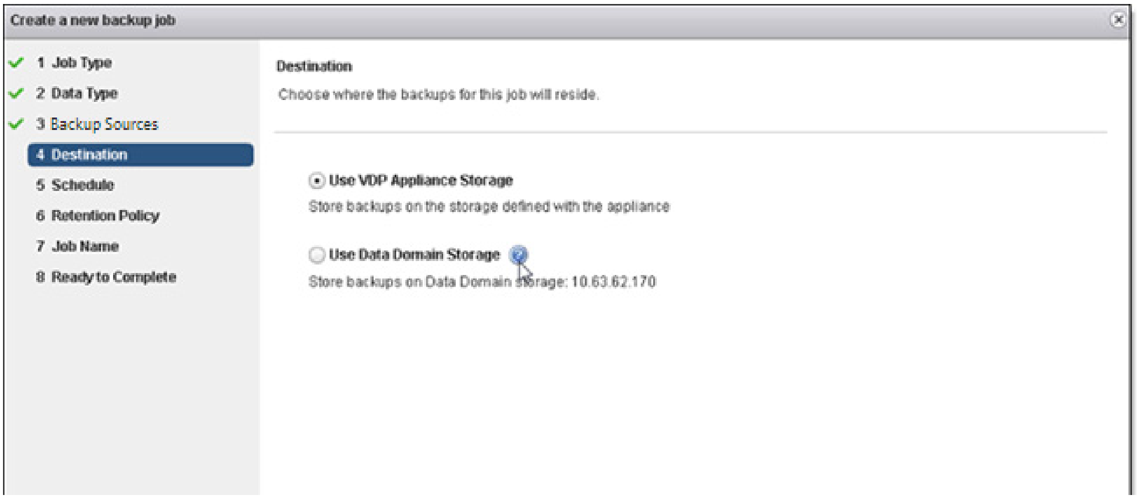
If you cancel a backup while it is in progress, then the VDP Appliance deletes the backup data that was written to the Data Domain system during the next cycle of the VDP Appliance garbage collection process.

If you delete a backup in VDP, then the backup is deleted from the Data Domain system during the next cycle of the VDP garbage collection process.

"Deleting a Backup Job" on page 118 provides instructions on how to cancel or delete a backup.

Selecting a Data Domain Target for Backups

After the VDP Appliance and the Data Domain system are integrated, any backup target for the VDP Appliance has the option to use the Data Domain storage as the “Destination” in the Create a new backup job work flow, as shown in Figure 9-4.



Create a new backup job

✓ 1 Job Type
✓ 2 Data Type
✓ 3 Backup Sources
4 Destination
5 Schedule
6 Retention Policy
7 Job Name
8 Ready to Complete

Destination

Choose where the backups for this job will reside.

● Use VDP Appliance Storage
Store backups on the storage defined with the appliance

○ Use Data Domain Storage
Store backups on Data Domain storage: 10.63.62.170

Figure 9-4. Create a new backup job wizard—Destination page

You can use the Edit a backup job wizard to change the destination for a backup job. See “Editing a Backup Job” on page 117 for more information on how to edit the backup job.

NOTE If the destination of a backup job is modified, then the next backup performed will be a full backup. The new destination will not have the previous full backup data stored with it.

Replication Control

When a VDP Appliance with a Data Domain system attached replicates backup data, replication occurs between the Data Domain systems. However, replication jobs are configured by using the VDP user interface.

You configure and monitor replication on the VDP Appliance. The replication activity can also be monitored through the Data Domain system by checking the DD Boost activity. Refer to the *Data Domain Operating Systems Administration Guide* for instructions on how to monitor this activity.

Do not use Data Domain replication functionality to initiate replication of data that was backed up from a VDP Appliance. When you use Data Domain replication, the replicated data will not refer to the associated VDP Appliance, because the metadata stored on the VDP Appliance was not replicated.

Replication Data Flow

VDP replicates the data directly from one Data Domain system to another. The replication process examines each backup to be replicated, and if it determines that the backup data is stored on a Data Domain system, the process issues a request to replicate the data from the source Data Domain system to the target Data Domain system by using DD Boost. In this instance, the Data Domain systems are responsible for the replication of the data. This is analyzed for each backup being replicated.

Replication Schedule

The replication of VDP data on a Data Domain system occurs on the VDP replication schedule. You should not schedule replication of data on the Data Domain system separately from the replication of data on the VDP Appliance.

Replication Configuration

To configure replication when you use a Data Domain system as a backup target for VDP , use the vSphere Web Client.

Refer to "Replication" on page 133 for more information on configuring VDP replication.

NOTE When replicating, if the source is a VDP Appliance with a Data Domain system attached to it, the target (whether it be an Avamar server or the VDP Appliance) must also have a Data Domain system attached to it.

Replication Monitoring with VDP

To monitor replication activity with the VDP Appliance, including replication activities associated with a Data Domain system, perform the following steps:

1. In the vSphere Web Client, log in to the vSphere Data Protection plug-in.
2. Click the **Replication** tab.
   - The **Replication** tab displays all replication jobs, and the last run time as well as the next scheduled run time.
   - Selecting a replication job displays the Destination server and the clients included in the replication job details frame.
   - If you check the Replication column, the **Reports** tab displays the replication job and the last replication run time for each protected client.

Server Maintenance Activity Monitoring

The VDP Appliance performs the system maintenance operations for backup data on the Data Domain system, including VDP integrity checks, checkpoints, rollbacks, garbage collection, and secure backup deletion.

The `ddrmaint` utility implements all required operations on the Data Domain system for the VDP Appliance. The `ddrmaint` utility logs all maintenance activities on the VDP Appliance in the `ddrmaint.log` file. This log file can be located in the `/usr/local/avamar/var/ddrmaintlogs` directory.

When the `ddrmaint.log` file reaches 25 MB in size, the existing log version will roll. The existing `ddrmaint.log` file will be renamed `ddrmaint.log.1` and a new `ddrmaint.log` file will be created. Any previous copies of `ddrmaint.log.X` will have their log counter increased by one as well (`ddrmaint.log.1` will migrate to `ddrmaint.log.2` and so forth).

Restoring Avamar Checkpoint backups from Data Domain systems

If you have created VDP checkpoint backups on a Data Domain system, you can restore a checkpoint to a new VDP Appliance in the event the original VDP Appliance fails.

Assumptions for the Restore Operation

The procedure in "Performing the Checkpoint Restore" on page 93 explains how to perform a checkpoint restore when the following assumptions are true:

- You have a valid checkpoint for a VDP Appliance on a Data Domain system target.
- The VDP Appliance that failed has been replaced.
- The replacement VDP Appliance is a new appliance with no backup data or metadata.
- The replacement VDP Appliance is the same size as or larger than the original VDP Appliance.
- The replacement VDP Appliance must have the same data partition count as the original VDP Appliance.

Performing the Checkpoint Restore

To restore a checkpoint from a Data Domain system to a new VDP Appliance:

1 Log in to the VDP Appliance as root and from a CLI prompt query the available checkpoints to recover by typing the following command:

```
ddrmaint cp-backup-list --full --ddr-server=Data_Domain_system --ddr-user=DD_Boost_user_name
--ddr-password=DD_Boost_user_password
```

where

- *Data_Domain_system* is the Data Domain system with the VDP Appliance checkpoint backup.
- *DD_Boost_user_name* is the DD Boost user account used for VDP and Data Domain system integration.
- *DD_Boost_user_password* is the DD Boost user account password used for VDP and Data Domain system integration.

The output will be similar to the following example:

```
================== Checkpoint ==================
VDP Advanced Name : a4dpe223d
VDP Advanced MTree/LSU : avamar-1346892530
Data Domain System Name : griffin-dd10.asl.lab.emc.com
VDP Advanced Client Path : /MC_SYSTEM/avamar-1346892530
VDP Advanced Client ID : 8b75468f70dc8ff0fa2e5118cec8ecdddf7fccee
Checkpoint Name : cp.20140919184604
Checkpoint Backup Date : 2014-09-19 11:51:12
Data Partitions : 6
Attached Data Domain systems : griffin-dd10.asl.lab.emc.com
```

2 Restore the backups stored on the VDP Appliance from the checkpoint stored on the Data Domain system (requires the Data Domain server name and credentials of the default backup's target Data Domain system) by using the `cprestore` command.

The `cprestore` command is used for the restore operation. The `cprestore` command completes the following tasks:

- Creates NFS export on Data Domain system.
- Mounts Data Domain NFS export on the VDP Appliance.
- Copies the backup files needed on the VDP Appliance from the backup checkpoint on the Data Domain system to the corresponding VDP Appliance checkpoint directory in each data partition.
- Undoes NFS mount and export.

To restore the backups on the Data Domain system, type the following command on the VDP Appliance:

```
/usr/local/avamar/bin/cprestore --hfscreatetime=VDP_ID --ddr-server=Data_Domain_system
--ddr-user=DD_Boost_user_name --cptag=Checkpoint_name
```

where:

- *VDP_ID* is determined from the output of Step 1. From the VDP Appliance `MTree/LSU:avamar-1346892530` field, the `VDP_ID` is `1346892530`.
- *Data_Domain_system* is the Data Domain system with the VDP Appliance checkpoint backup. In the previous checkpoint output example, the value is `griffin-dd10.asl.lab.emc.com.`
- *DD_Boost_user_name* is the DD Boost user account used for VDP and Data Domain system integration. In the previous checkpoint output example, the value is `VDP`.
- *Checkpoint_name* is the checkpoint name. In the previous checkpoint output example, the value is `cp.20140919184604`.

3 Stop the VDP Appliance by typing the following command:

```
dpnctl stop
```

A confirmation message, “Do you wish to shut down the local instance of EMS?” appears. Type **Y**.

4 To initiate a rollback, type the following command:

```
dpnctl start --foreseeability
```

A message appears that the appliance was shut down. A list of choices also appears.

5 Select option **3, “Select a specific checkpoint to which to roll back”**.

Wait for the rollback to complete. The rollback might take up to one hour, depending on the amount of data present in the VDP Appliance. When the rollback is complete, the command prompt returns.

6 Open the user-defined temporary file created during the rollback and verify that the rollback successfully completed without errors. The VDP Appliance automatically restarts after a successful rollback.

7 Create a new checkpoint on the VDP Appliance:

a On the VDP **Configuration** tab, select **Create integrity check** to create a new checkpoint.

b When the checkpoint has been initiated, click OK.

Monitoring Data Domain from the VDP Appliance

To review high-level information about the Data Domain system attached to a VDP Appliance, use either the vSphere Web Client or the VDP Configuration UI.

Monitoring Using the vSphere Web Client

1 In the vSphere Web Client, open the vSphere Data Protection plug-in.

2 Navigate to the **Configuration** tab.

In the Data Domain storage summary, the following information is displayed:

- Data Domain system FQDN or IP address
- Capacity of the Data Domain system
- Free Space on the Data Domain system
- Used Capacity on the Data Domain system

Monitoring Using the VDP Configure UI

1 In the VDP Configure UI, navigate to the **Storage** tab.

2 In the Storage Summary section, the following information is displayed:

- DD Hostname or IP address
- Total Usable Storage
- Storage Available
- Capacity consumed (in percentage)

Data Domain Capacity Monitoring

You can monitor the capacity of the Data Domain system by monitoring the vSphere Web Client or the VDP Configuration UI.

1 In the vSphere Web Client, open the vSphere Data Protection plug-in and navigate to the **Configuration** tab to view a capacity summary for the Data Domain system.

2 In the VDP Configuration UI, open the **Storage** tab to view a storage summary for the Data Domain system.

   When the Data Domain system reaches its capacity limit, you can reclaim space on the device by using the instructions in "Reclaiming Storage on a Full Data Domain System" on page 95.

NOTE When the Data Domain system reaches 99% capacity, maintenance operations fail. The best practice recommendation is to limit Data Domain capacity usage to 80%.

Reclaiming Storage on a Full Data Domain System

If you use all of the storage space on a Data Domain system, the following issues may occur:

- Backups do not succeed and may not start.
- Operations that change information on the Data Domain system fail, including the deletion of checkpoints, active backups, and expired backups during garbage collection. These operations may fail because they involve directory renames, which are not allowed on a full Data Domain system.

To reclaim the used storage on a full Data Domain system, perform the following steps:

1 Determine the source of the data that is using the storage. The data may be from a specific client, a group of clients associated with a specific VDP Appliance, or a different backup product that stores data on the Data Domain system.

2 Cancel any backups that are in progress. You must do this from the command line of the VDP Appliance.

   a Open an SSH or Putty session to the VDP Appliance and type the following commands:

   ```
   su - admin
   ssh-agent bash
   ssh-add .ssh/dpnid
   ```

   b Type the `mccli activity show` command.

   This command returns results similar to the following sample output:

```
admin@gs-pod192:~/>: mccli activity show
0,23000,CLI command completed successfully.
ID             Status    Error Code Start Time          Elapsed     End Time             Type            Progress Bytes New Bytes Client
                         Domain
---------------- --------- ---------- -------------------- ---------- -------------------- ---------------- ------------- --------- ---------
9138660744236309 Running   0 2013-12-09 09:44 MST 00h:27m:25s 2013-12-10 09:44 MST On-Demand Backup 54.3 GB
                         4.2%      Win2008R2-GSClone /10.7.242.175/VirtualMachines
9138660744234709 Completed 0 2013-12-09 09:44 MST 00h:02m:51s 2013-12-09 09:47 MST On-Demand Backup 40.0 GB
                         <0.05%    GermanExchange    /10.7.242.175/VirtualMachines
9138660718256909 Completed 0 2013-12-09 09:39 MST 00h:01m:06s 2013-12-09 09:40 MST On-Demand Backup 40.0 GB
                         <0.05%    GermanExchange    /10.7.242.175/VirtualMachines
9138660744235609 Completed 02013-12-09 09:44 MST 00h:20m:37s 2013-12-09 10:04 MST On-Demand Backup 40.0 GB
                         2.6%      ActiveDirectory   /10.7.242.175/VirtualMachines \
```

   To run the command that cancels the running backup jobs, you need to know the appliance password (entered as the 'AppliancePassword' value below). You also need to note the ID of any Running jobs.

c Type the `mccli activity cancel --mcsuserid=MCUser --mcpasswd=AppliancePassword --id=XXXXX` command, where *`AppliancePassword`* is the appliance password and `XXXX` is the ID of the Running job you wish to cancel. This command returns results similar to the following output:

```
admin@gs-pod192:~/>: mccli activity cancel --mcsuserid=MCUser --mcspasswd=Test12345 --id=9138660744236309
0,22205,Backup cancelled via console
AttributValue
--------------------------
activity-id9138660744236309
```

3 Repeat Step c for all jobs in the Running state.

4 Suspend backups and restores. On the VDP Appliance, this can be done by disabling the proxies from the command line. Verify with end users that there are no critical backups or restores that must be performed before you run these commands.

a Open an SSH or Putty session to the VDP Appliance.

b Enter the `service avagent-vmware stop` command.

5 Suspend server maintenance operations on the VDP Appliance.

a Open the VDP Configuration UI by opening a web browser and navigating to `https://<VDP_IP_Address>:8543/vdp-configure`.

b If the Maintenance services show as “Running”, click the **Stop** button.

6 On the Data Domain system, manually delete the existing STAGING, DELETED, or cur/DELETED directories for the VDP Appliance.

7 Use the Data Domain Enterprise Manager to initiate the Data Domain file system cleaning operation.

This process should free enough space to enable VDP Appliance service maintenance operations to complete successfully.

8 Restart server maintenance operations on the VDP Appliance.

a Open the VDP Configuration UI by opening a web browser and navigating to `https://<VDP_IP_Address>:8543/vdp-configure`.

b If the Maintenance services show as “Stopped”, click the **Start** button.

9 Restart the proxies on the VDP Appliance so that backups and restores can run.

a Open an SSH or Putty session to the VDP Appliance.

b Enter the `service avagent-vmware start` command.

Common Problems and Solutions

This section lists common problems and solutions when you store VDP Appliance backups on a Data Domain system.

Backup Fails if the Data Domain System is Offline

If the Data Domain system is offline when a backup starts, then the backup may take five minutes or more before it fails. The failure occurs because there is a minimum timeout period of five minutes for almost all DD Boost operations.

To resolve the failed backup, set the Data Domain system online, and then retry the backup.

Rolling Back after Deleting a Data Domain System

If you roll back to a checkpoint after following the procedure for "Deleting the Data Domain System from the VDP Appliance" on page 88, the rollback should bring you to a state where the Data Domain system is removed from the VDP Appliance.

To add the Data Domain system back to the VDP Appliance, use the VDP Configuration UI. Refer to "Adding a Data Domain System" on page 86 for more information.

If you rolled back to a checkpoint before the deletion of the Data Domain system, then the Data Domain system should be still attached and properly configured. To remove the Data Domain system, follow the procedure for "Deleting the Data Domain System from the VDP Appliance" on page 88.

If a rollback of the appliance leaves you in a different state than these, it is best to contact support to define the proper resolution.

VDP Disk Expansion 10

This chapter contains the following topics:

- "Pre-Expansion Requirements" on page 100
- "VMFS Heap Size Recommendations" on page 100
- "Performing Disk Expansion" on page 101
- "Performance Analysis" on page 103
- "Disk Expansion with Essentials Plus" on page 103

Pre-Expansion Requirements

Ensure that your configuration meets the following requirements before disk expansion. Failure to meet these requirements can corrupt vSphere Data Protection (VDP) and require a restoration from a clone or VDP backup.

- Confirm that the minimum CPU and memory requirements are met for the new configuration:
  - The minimum number of virtual CPUs is 4 for VDP capacity options of 2 TB, 4 TB, 6 TB, and 8 TB.
  - The minimum amount of memory per VM depends on the capacity:

Capacity size	Required memory
2 TB	6 GB
4 TB	8 GB
6 TB	10 GB
8 TB	12 GB

- Confirm that both CPU and Memory Hot-Add are enabled. The CPU and Memory Hot-Add options are disabled by default in the case of an upgraded appliance.

NOTE

- If you have an Essentials Plus license, you cannot hot-plug the required memory. You must manually increase the memory assigned to VDP. See "Disk Expansion with Essentials Plus" on page 103 for additional details.
- Confirm that you have available disk space for the expansion. You can check your disk space from the **Storage** tab. See "Viewing the Storage Configuration" on page 76.
- Perform disk expansion during the backup window when no backup jobs or any other VDP tasks are running, such as restores or integrity checks. Ensure that all the VDP services are in a running state before attempting disk expansion. See "Starting and Stopping Services" on page 43 for additional details.
- Confirm that you have administrative privileges in the vCenter. See "User Account Configuration" on page 22 to determine if you have if you have administrative privileges for the vCenter.
- Confirm that VMFS heap size is set to the correct value for the amount of virtual disk space associated with the vSphere host. See "VMFS Heap Size Recommendations" on page 100 for additional details.
- Make a note of the MAC address for the appliance before cloning. The MAC address will be used later in cases where storage has failed.
- Create a clone or backup of the VDP Appliance and verify that it is valid before disk expansion.

VMFS Heap Size Recommendations

VMFS heap size determines the amount of virtual disk space that each vSphere host supports. If you exceed the amount of virtual disk space beyond what is configured for VMFS heap size, the following can occur:

- Virtual machines behave erratically
- Cannot allocate memory error messages appear
- Virtual machines may crash or fail to start

Before disk expansion, confirm that VMFS heap size is configured properly for the new virtual disk capacity. Increasing VMFS heap size increases the amount of memory allocated to the vSphere host kernel and requires a system reboot for the changes to take effect.

VMFS3 and VMFS5 use the same settings and are defined in Table 10-1.

Table 10-1. VMFS heap size settings

Version/build	Default heap amount	Default allowed open VMDK storage per host	Minimum heap amount	Maximum heap amount	Maximum heap value	Maximum open VMDK storage per host
vSphere Host 5.0 Update 2 (914586) and earlier	80 MB	8 TB	N/A	256 MB	255	25 TB
vSphere Host 5.0 Patch 5 (1024429) and later	256 MB	60 TB	256 MB	640 MB	255	60 TB
vSphere Host 5.1 Patch 1 (914609) and earlier	80 MB	8 TB	N/A	256 MB	255	25 TB
vSphere Host 5.1 Update 1 (1065491) and later	256 MB	60 TB	256 MB	640 MB	255	60 TB

NOTE vSphere 5.5 and later include a much improved heap eviction process, so that there is no need for the larger heap size that consumes memory. vSphere 5.5 and later support a maximum heap size of 256 MB and enables hosts to access all address space of a 64 TB VMFS.

VMware Knowledge Base Article 1004424 specifies the steps to change the VMFS heap size settings.

Performing Disk Expansion

VDP enables you to expand datastore capacity by using the Expand Storage wizard. Disk expansion allows you to expand VDP storage to 2 TB, 4 TB, 6 TB, or 8 TB.

NOTE You cannot change the provision type from thin provisioning to thick provisioning. The disks inherit the provision type that was assigned to them during initial configuration.

When extending a VMDK which is thick eager-zeroed, the extended part is only thick lazy-zeroed. If you need to grow your VMDK and you require your VMDK to be thick eager-zeroed, then use the parameters outlined in the following VMware blog:

http://blogs.vmware.com/vsphere/2012/06/extending-an-eagerzeroedthick-disk.html

Prerequisite

During initial configuration, the VDP storage disks are distributed across the available datastore locations and the disks are validated.

Procedure

1 Log in to the VDP-Configure URL:

https://*<IP_address_VDP_Appliance>***:8580/vdp-configure/**

2 Click the **Storage** tab.

The available datastores appear in the Storage Summary, along with the amount of total usable storage and storage capacity that is available for each datastore.

3 From the **Action** list, select **Expand Storage**.

The Expand Storage wizard appears, displaying the current capacity.

4 Determine if you are expanding the size of the disks or increasing the number of disks.

NOTE During expansion to up to 2 TB, the number of disks remains at 3, but the size of the existing disks grows. When disks are expanded, the controls to select the number of disks on each datastore are disabled.

a To expand the size of the disks, select a new capacity from the list. You can expand VDP storage to 1 TB, 2 TB, 4 TB, 6 TB, or 8 TB.

b To add disks, increase the number of disks in the Disks column until the total number of available storage disks are allocated. You can allocate all disks to a single datastore or you can distribute the disks across multiple datastores.

5 Click **Next**.

The Device Allocation dialog box displays the datastores that are known to be available for allocation and the number of disks to be allocated.

A warning message appears if the system detects that a performance analysis has failed, has never been run, or is out of date on one or more of the selected datastores. Based on whether or not you want to run the performance analysis on the selected datastore, do one of the following:

- Click **Yes** to abort the wizard and run the performance analysis on the selected datastore. To run the performance analysis tool, refer to "Performance Analysis" on page 103.
- Click **No** to continue with the disk expansion.

6 Click **Next** to go to the next page of the Expand Storage wizard.

The CPU and Memory dialog box displays the minimum CPU and Memory requirements for the current configuration.

7 Select the number of virtual CPUs for each virtual machine.

The maximum number of virtual CPUs allowed for a VDP virtual machine is 8.

8 Select the amount of memory to be allocated to the VDP virtual machine.

- The minimum amount of memory per VM depends on the capacity:
  - 2 TB capacity — 6 GB memory
  - 4 TB capacity — 8 GB memory
  - 6 TB capacity — 10 GB memory
  - 8 TB capacity — 12 GB memory
- The maximum amount of memory allowed for a VDP virtual machine is 64 GB.

9 On the Ready to Complete dialog box, click **Finish** to apply the changes.

NOTE After a successful storage configuration, the system automatically creates a checkpoint and runs an integrity check.

Viewing the Storage Configuration

After the storage expansion completes, you can use the Storage Summary dialog box to verify the amount of total usable storage and storage capacity that is available for each datastore.

Known Limitation

Immediately following disk expansion, load balancing occurs and the result is used capacity displays incorrect values. The values appear correctly, however, after the next maintenance window has completed.

Procedure

1. Log in to the VDP-Configure URL:

   https://<*IP_address_VDP_Appliance*>**:8580/vdp-configure**

2. Click the **Storage** tab.

The Storage Summary displays total usable storage and storage capacity for each datastore.

Performance Analysis

The performance analysis test performs write, read, and seek performance tests. During initial configuration, the performance analysis test evaluates the read, write, and seek capabilities of configured VDP disks. Post initial configuration, the tests measure the performance of the datastores as seen by the VDP Appliance by creating a temporary disk of 250 GB on that datastore.

Possible test results are as follows:

- Unknown
- Failed
- Passed

Running the Performance Analysis Test

1. Log in to the VDP-Configure URL:

   https://<*IP_address_VDP_Appliance*>**:8580/vdp-configure**

2. Click the **Storage** tab.

   The Storage Summary dialog box appears.

3. Click the **Performance Analysis** tab.

   The performance analysis test creates a temporary disk on the selected datastore and runs the test on that disk. The temporary disk is automatically removed once the performance analysis completes.

4. Select the datastores on which the performance analysis test will run.

5. Click **Run** to start the performance analysis.

NOTE You can click **Cancel** at any time to stop a performance analysis test.

Disk Expansion with Essentials Plus

If you have an Essentials Plus license, you cannot enable Memory Hot-Add. You must manually adjust the memory assigned to VDP , as required for the target capacity.

NOTE This limitation is true with vSphere 5.x hosts. You must manually set the minimum required memory for a vSphere host using the memory requirements listed in Table 10-2.

VDP requires the following memory based on capacity size.

Table 10-2. Memory requirements for virtual hardware

Capacity size	Required memory
2 TB	6 GB
4 TB	8 GB
6 TB	10 GB
8 TB	12 GB

Procedure

To perform disk expansion with an Essentials Plus license complete the following steps.

1 From a web browser, access the vSphere Web Client:

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

2 Before the expansion, shut down the VDP Appliance by using the **Shut Down Guest OS** action on the virtual machine.

This action automatically performs a clean shutdown of the VDP Appliance. If the appliance is powered off without the **Shut Down Guest OS** action, corruption might occur. It can take up to 30 minutes to shut down and restart the VDP Appliance. You can monitor the status through the virtual machine console.

3 Increase the memory assigned to the VDP Appliance by using the requirements listed in Table 10-2.

a From a web browser, access the vSphere Web Client:

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

b In the vSphere Web Client, log in as a user who has privileges to edit hardware settings.

c Click **vCenter > Hosts and Clusters**.

d In the tree on the left, click the disclosure arrows until the VDP Appliance appears.

e Right-click the VDP Appliance and select **Edit Settings**.

f Click the **Virtual Hardware** tab.

g Increase the amount of memory by entering the value in the **Memory** field.

h Click **OK**.

4 To restart the VDP Appliance, right-click the VDP Appliance and select **Power On**.

Using vSphere Data Protection 11

This chapter includes the following topics:

- "Accessing vSphere Data Protection" on page 106
- "Accessing the VDP Appliance Command Line" on page 106
- "Understanding the VDP User Interface" on page 107
- "Switching VDP Appliances" on page 107
- "VDP User Interface" on page 108
- "Viewing Information from the Reports Tab" on page 108

Accessing vSphere Data Protection

vSphere Data Protection (VDP) is accessed through a vSphere Web Client and is managed only through the vSphere Web Client.

NOTE VDP cannot be used without a vCenter Server. In linked mode, the VDP Appliance works only with the vCenter Server with which it is associated. If the VDP Appliance fails to appear in the vSphere Web Client, remove your vCenter from linked mode.

Prerequisites

Before using VDP, you must install and configure the VDP Appliance described in "VDP Installation and Configuration" on page 19.

Procedure

1 From a web browser, access the vSphere Web Client:

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

2 In the Credentials page, enter an administrative vCenter username and password, and click **Login**. The specified user account must have administrative privileges.

3 In the vSphere Web Client, select **VDP**.

4 In the Welcome to VDP page, select the VDP Appliance and click **Connect**.

The VMware vSphere Web Client dialog box appears.

Accessing the VDP Appliance Command Line

Currently, users can access the VDP Appliance command line using the vSphere Client console, SSH, or Putty sessions. With the VDP 5.8 release, the ability to use SSH or Putty to log on to the VDP Appliance with the root user has been removed.

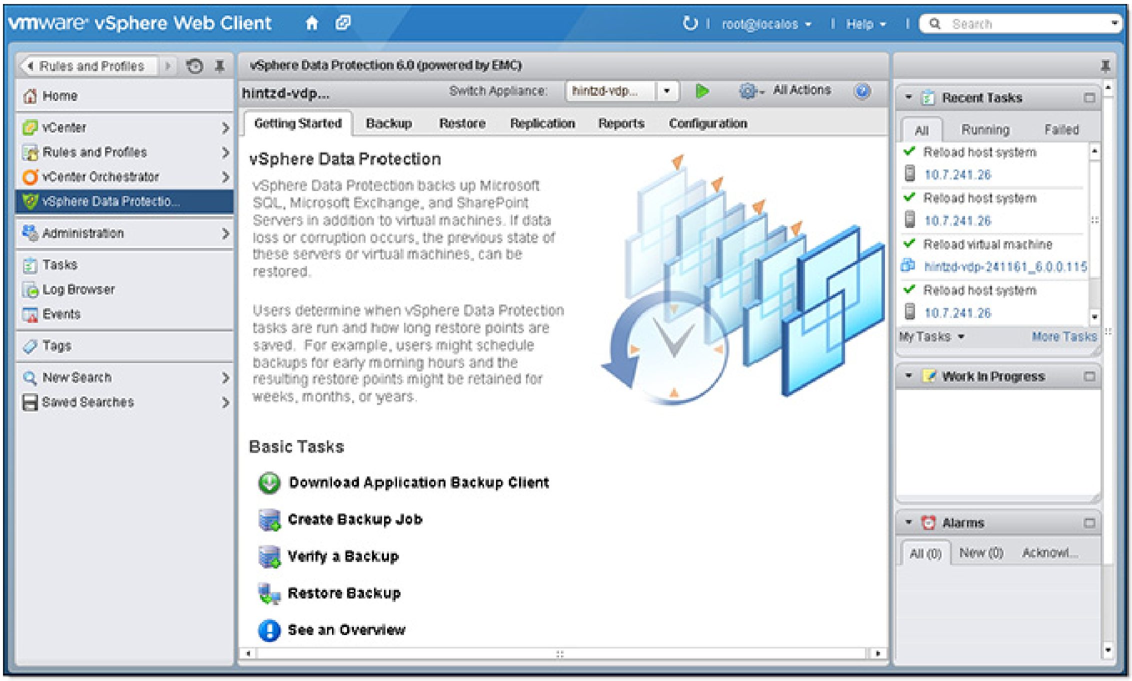
To use SSH or Putty to access the appliance, you must log in as the admin user.

With the VDP 5.8 release, the default password for the admin user has also changed. This password only applies when the user logs in to the VDP Appliance before completing the configuration of the appliance from the VDP Configuration UI. In this scenario, the admin password is `88RttoTriz!!`

After the configuration of the appliance is complete, the newly-configured appliance password can be used to access the command line as the admin user.

Understanding the VDP User Interface

The vSphere Web Client for vSphere Data Protection is used to configure and manage VDP.



vSphere Data Protection backs up Microsoft SQL, Microsoft Exchange, and SharePoint Servers in addition to virtual machines. If data loss or corruption occurs, the previous state of these servers or virtual machines, can be restored.

Users determine when vSphere Data Protection tasks are run and how long restore points are saved. For example, users might schedule backups for early morning hours and the resulting restore points might be retained for weeks, months, or years.

Figure 11-1. vSphere Data Protection user interface

The vSphere Data Protection user interface consists of six tabs:

- **Getting Started** — Provides an overview of VDP functionality and quick links to the Create a new backup job wizard, the Restore a backup job wizard, and the **Reports** tab.
- **Backup** — Provides a list of scheduled backup jobs as well as details about each backup job. You can also create and edit backup jobs from this page. This page also provides the ability to run a backup job immediately. See"Viewing Information from the Reports Tab" on page 108 for additional information.
- **Restore** — Provides a list of successful backups that you can restore. See "Restore Operations" on page 128 for additional information.
- **Replication** — Provides a list of successful backups that you can replicate. See "Replication Jobs" on page 134 for additional information.
- **Reports** — Provides backup status reports on the virtual machines on the vCenter Server. See"Viewing Information from the Reports Tab" on page 108 for additional information.
- **Configuration** — Displays information about how VDP is configured and allows you to edit some of these settings or add a VDP license. See "Configuring VDP" on page 55 for additional information.

Switching VDP Appliances

Each vCenter Server supports up to 10 VDP Appliances. You can switch appliances by choosing an appliance from the drop-down list to the right of the **Switch Appliance** option.

NOTE The VDP Appliances in the drop-down list are sorted alphabetically, and the first item in the list that is displayed on the screen may not match the current appliance. On the VDP screen, the appliance name on the left is the current appliance, and the appliance name in the drop-down list is the first in the list of available appliances.

VDP User Interface

The VDP user interface includes the following features:

- Guest-level backups of Microsoft Exchange Servers, SQL Servers, and SharePoint Servers.
- Growing and adding disks (disk expansion)
- Backing up to a Data Domain system
- Granular level recovery (GLR)
- Verifying automatic backups

These options are described in "VDP Application Support" on page 154, which also specifies how to perform application-level backups and restores.

Viewing Information from the Reports Tab

The **Reports** tab displays the following information:

Appliance Status Information

- **Appliance status** — The status of the VDP Appliance.
- **Integrity check status** — Click the green right arrow to initiate the integrity check. The status value is either Normal or Out of Date.
  - Normal indicates that a successful integrity check has been completed in the past two days.
  - Out of Date indicates that an integrity check has not run or has not completed successfully in the past two days.
- **Used capacity** — A percentage of the total VDP capacity that is occupied by backups.
- **Used DDR capacity** — A percentage of the total capacity that is occupied by the Data Domain system (if applicable.
- **Recent failed backups** — The number of virtual machines that failed to back up in the most recently completed backup job.
- **Recent failed backup verifications** — The number of backup verification jobs that have recently failed.
- **Recent failed replications** — The number of replication jobs that have recently failed.
- **Total VMs protected** —The total number of virtual machines that are protected on the VDP Appliance.

NOTE The VDP Appliance supports 400 virtual machines. If the maximum numbers of virtual machines are exceeded, an alarm is generated and the **Log** tab displays the error message.

Refresh

Click the **Refresh** button at any time to update the data in the **Reports** tab.

Task Failures Tab

The **Task Failures** tab displays details about jobs that have failed within the last 72 hours.

Failure Time — The date and time the job failed.

Reason — The reason the job failed.

Client Name — The client associated with the vCenter.

Job Name — The name of the job that failed.

Job Type — The type of job that failed; for example, Scheduled Backup or On Demand Backup.

Next Run Time — The date and time the job is next scheduled to run.

View Log link — Click to launch the Job Failure Client Log dialog box, where you can view the client log details. If log files are not available in the Client Log dialog box, one of three error messages may appear:

- Failed to retrieve log file. This message appears in the following circumstances:
    - Management services were recently restarted.
    - Regular log maintenance has removed old log files.
    - Logs may be empty or non-existent.
    - An error may have occurred.
- Failed to retrieve log. Logs are regularly removed 72 hours after the job finished.
- Log file retrieved is empty.

NOTE Not all replication source and replication destination logging is available through the **Job Failures** tab. However, you can retrieve replication logs from the VDP Configure UI using the regular log bundle. See "Collecting Logs" on page 44 for more information.

Actions icon ⚙

You can perform the following tasks from the Actions icon list, located on the right side of the **Task failures** tab:

- Rerun Job — Highlight the failed job and click to rerun the failed job. The Rerun job feature is not enabled for Restore failures.

NOTE To run a backup only for the failed client, select **Backup only out of date source** under **Backup Now** on the **Backup** tab.

- Export to CSV — Click to export the current table to a comma-separated values (.CSV) file.
- Show All Columns — Hide one or more columns by clicking **X** on the column name, and then click **Show All Columns** to show the hidden columns on the UI.

Filter

You can filter and customize the job failure details by selecting one of the following criteria. The information appears for job failures that occurred within the last 72 hours.

- **Show All** — Shows all job failure information for the virtual machines. **Show All** is the default.
- **Error** — Filters job failure information by errors messages.
- **Job** — Filters job failure information for a selected job.
- **Client** — Filters job failure information for a given client.

Job Details Tab

The **Job Details** tab allows you to select the type of job (Backups, Replication, or Backup verification) and display the details for the selected job. Backups is the default job type.

Job details are grouped into three sections:

- **Client Information**
    - **Client Name** — The client associated with the vCenter. Regular VM clients and retired VM clients from the Replicate domain displays the hashed mask value appended to the replicated, recovered, and imported names.
    - **Type** — Displays the type as Image, MS SQL Server, MS SharePoint Server, or MS Exchange Server. Applications (MS SQL Servers, MS SharePoint Servers, or MS Exchange Servers) are supported only on the VDP Appliance.
    - **Jobs** — The job name. Multiple job names appear if a virtual machine resides in two different jobs.

- **Last Execution**
  - **Job Name** — The name of the job.
  - **Completion** — The date and time the job completed.
  - **Result** — Whether the job succeeded, failed, or was canceled.
- **Next Execution**
  - Job Name — The next scheduled job name appears. If a virtual machine resides in two different jobs with different schedules, then the next scheduled job name appears.
  - **Scheduled** — The date and time the job is next scheduled to run.

Actions icon ⚙

You can perform the following tasks from the Actions icon list, located on the right side of the **Job Details** tab:

- **Export to CSV** — Click to export the current table to a comma-separated values (.CSV) file.
- **Show All Columns** — Hide one or more columns by clicking **X** on the column name, and then click **Show All Columns** to show the hidden columns on the UI.

Filter

You can filter and customize the job details by selecting one of the following criteria. The information appears for job failures that occurred within the last 72 hours.

- **Show All** — Shows all job details for the virtual machines. **Show All** is the default.
- **Client** — Filters job failure information by client.
- **Last Execution** — Filters job details for the last executed job.
- **Next Execution** — Filters job details for the next scheduled job.

Unprotected Clients Tab

- **Client Name** — The name of the unprotected client.
- **IP Address** — The IP address or hostname of the unprotected client.
- **VM Path** — The path where the virtual machine resides.

Actions icon ⚙

You can perform the following task from the Actions icon list, located on the right side of the **Unprotected Clients** tab:

- **Export to CSV** — Click to export the current table to a comma-separated values (.CSV) file.

Managing Backups

12

This chapter includes the following topics:

- "Backup Jobs" on page 112
- "Choosing the Virtual Machines" on page 112
- "Specifying the Backup Schedule" on page 113
- "Setting the Retention Policy" on page 113
- "Creating a Full Image Backup Job" on page 114
- "Creating a Backup Job on Individual Disks" on page 115
- "Viewing Status and Backup Job Details" on page 117
- "Editing a Backup Job" on page 117
- "Cloning a Backup Job" on page 117
- "Locking and Unlocking a Backup" on page 119

Backup Jobs

Backup jobs consist of a set of one or more virtual machines that are associated with a backup schedule and specific retention policies. Backup jobs are created and edited on the **Backup** tab using the Create a new backup job wizard.

Limitations

- Backing up virtual machines greater than 2 TB on Windows operating systems is not supported. This limitation does not exist on Linux operating systems.
- VDP will not back up the following specialized virtual machines:
  - VDP Appliances
  - vSphere Storage Appliances (VSA)
  - VMware Data Recovery (VDR) Appliances
  - Templates
  - Secondary fault tolerant nodes
  - Proxies
  - Avamar Virtual Edition (AVE) servers

  The wizard allows you to select these VMs. When when you click **Finish** to complete the wizard, you receive a warning that these specialized virtual machines were not added to the job.
- Virtual machines that contain special characters in their names cannot be added to any backup job. The following characters cannot be used: ~!@$^%(){}[]|,`;#\/:*?<>'"&. In addition, diacritical characters cannot be used (for example: â, é, ì, ü, and ñ).
- Using snapshots to perform a backup on VMs configured with bus sharing is not supported. If you require SCSI bus sharing, refer to the following Knowledge Base article: http://kb.vmware.com/kb/1006392.

Prerequisites

- VDP is installed and configured on your vCenter Server.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.

Choosing the Virtual Machines

You can specify collections of virtual machines, such as all virtual machines in a datacenter or select individual virtual machines. If an entire resource pool, host, datacenter, or folder is selected, any new virtual machines added to that container are included in subsequent backups. If a single virtual machine is selected, any disk subsequently added to the virtual machine is included in the backup. If a virtual machine is moved from the selected container to another container that was not originally selected, it is no longer part of the backup.

You can manually select a virtual machine to be backed up, which ensures that virtual machine is backed up, even if it is moved.

Identifying retired virtual machines

The following conditions cause a VM client to be retired and unavailable as candidates for backups, restores, or replication jobs:

- Host — Removed from inventory (this also occurs when any parent container of a host is removed, such as a cluster, a host folder, a datacenter, or a datacenter folder)
- Virtual machine — Deleted from disk
- Virtual machine — Removed from inventory

The following conditions exist when the VM client is not retired and the child VM remains in the inventory:

- Resource pool — Removed from inventory
- vApp — Removed from inventory
- Host — Disconnected
- Host — Enters maintenance mode
- Host — Shuts down

Specifying the Backup Schedule

On the Schedule page of the Create new backup job wizard (Step 7) of the procedure below), you can specify the time intervals to back up the virtual machines in your backup job. Backups occur as near to the startup of the backup window as possible. The available time intervals are daily, weekly, or monthly.

Setting the Retention Policy

Retention policies for the VDP Appliance are set individually per backup job. As each restore point is created from a backup job, it retains the retention policy at the time it was created. If a backup job's retention policy is modified, the new policy only affects newly-created restore points. Previously-created restore points retain the previous retention policy.

On the Retention Policy page of the Create Backup Job wizard (Step 8), you specify the retention period for backups.

The first three options, **Forever**, **for**, and **until**, apply to all the backups of all the virtual machines in the group equally. The fourth option, **this Schedule** or **Custom Retention Schedule**, applies only to backups that are internally assigned special Daily, Weekly, Monthly, or Yearly tags.

NOTE The **this Schedule** default is 60 days. The **Custom Retention** default is Never.

The first backup of the day receives a Daily tag. If this backup is also the first backup of the week, the month, and the year, the backup also receives the Weekly, Monthly, and Yearly tags.The time intervals specified by the **this Schedule** or **Custom Retention Schedule** options only apply to backups with the internal tags. Table 12-3 describes Retention Policy options.

Table 12-3. Retention Policy Options

Option	Description
Forever	Sets backup job to never expire. All backups for the virtual machines in this backup job are never deleted. Backup jobs that you run after the expiration date fail.
for	Sets a specific number of days, weeks, months, or years for the backup job. All backups for the virtual machines in this backup job are stored until the specified time interval has elapsed from their creation date. For example, if you set a retention policy to 30 days for a backup job, each job that runs has an expiration date of 30 days in the future.
until	Sets a specific expiration date. All backups for the virtual machines in this backup job are deleted on the date specified in the **until** field.
this Schedule or **Custom Retention Schedule**	Sets the retention time intervals for backups that are assigned internal tags of Daily, Weekly, Monthly, or Yearly. Backups can have more than one of these internal tags. The tag with the longest time interval has precedence. For example, if you set backups with a Weekly tag to be retained for 8 weeks, and backups with the Monthly tag to be retained for 1 month, then backups with both the Weekly and Monthly tags would be retained for 8 weeks.

Creating a Full Image Backup Job

Prerequisites

- VDP is installed and configured on your vCenter Server.
- The disks are supported by VDP. VDP does not support the following virtual hardware disk types:
  - Independent
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode

Procedure

1. From a web browser, access VDP.
2. Click the **Backup** tab.

   The **Backup** tab displays a list of the backup jobs that have been created. The columns in the list are described in the following table:

   Table 12-4. Column descriptions on **Backup** tab

Column	Description
Name	The name of the backup job.
State	Whether the backup job is enabled or disabled. Disabled backup jobs will not run.
Type	The type of backup, such as Application or Image.
Last Start Time	The last time the backup job was started.
Duration	How long it took to complete this job the last time it ran.
Next Run Time	When the backup job is scheduled to run again
Success Count	The number of virtual machines that were backed up successfully the last time the backup job ran. This number is updated after each backup job
Failure Count	The number of virtual machines that did not back up successfully the last time the backup job ran. This number is updated after each backup job.

3. From the **Backup Job Actions** menu, select **New** to run the Create new backup job wizard.

   You can also run the Create a new backup job wizard from the **Getting Started** tab. To do this, click **Create Backup Job** under Basic Tasks.
4. On the Job Type page, select **Guest Images**, and then click **Next**.

   The **Applications** option enables you to create backup jobs on Microsoft Exchange Servers, Microsoft SQL Servers, and Microsoft SharePoint Servers. "VDP Application Support" on page 153 provides details.
5. On the Data Type page, select **Full Image**, and then click **Next**.

   The Backup Sources page appears. This page contains all the objects and virtual machines in the vCenter Server.
6. On the Backup Sources page, click the disclosure arrows to progressively disclose the VMs. Select the checkboxes next to the items to add to the backup job, and then click **Next**.

NOTE If a Data Domain system is configured as the backup target, there is an additional step to configure the target destination. Select either **local storage** or **Data Domain storage**.

7. On the Schedule page, select the schedule for the backup job and click **Next**.

8 On the Retention Policy page, select a retention period and click **Next**. The retention periods from which you can choose are described as follows.

   - **Forever** — All backups for the virtual machines in this backup job will never expire.
   - **for** — All backups for the virtual machines in this backup job will expire after the specified time interval has elapsed from their creation date. The time interval can be specified in days, weeks, months, or years.
   - **until** — All backups for the virtual machines in this backup job will expire on the date specified.
   - **this Schedule** — Specifies the retention time intervals for backups that are assigned internal tags. When you perform scheduled daily backups on a regular basis, some of the backups are automatically assigned one of the following retention types:
     - Daily — The first successful scheduled backup each day.
     - Weekly — The first successful scheduled backup each week.
     - Monthly — The first successful scheduled backup each month.
     - Yearly — The first successful scheduled backup each year.

   The **this Schedule** default for on-demand backup jobs is 60 days.

   For the purpose of assigning retention types, each day begins at 00:00:01 GMT, each week begins on Sunday, each month begins on the first calendar day of that month, and each year begins on January 1.

   As backups may have more than one of these internal tags, the tag with the longest time interval has precedence. For example, if you were to set backups with a Weekly tag to be retained for 8 weeks, and backups with the Monthly tag to be retained for 1 month, then backups that were assigned both the Weekly and Monthly tags would be retained for 8 weeks.

CAUTION Upon entering a new maintenance period following the expiration of a backup, the VDP Appliance removes its reference to the backup data and thereafter you cannot restore the expired backup. The VDP Appliance determines if the backup data is being used by any other restore point and, if the system determines that the data is not being used, the data is removed and the disk capacity frees up.

9 On the Name page, enter a backup job name and click **Next**.

   The backup job name must be unique and can be up to 255 characters long. The following characters cannot be used in the backup job name: ~!@$^%(){}[]|,`;#\/:*?<>'"&. In addition, diacritical characters cannot be used (for example: â, é, ì, ü, and ñ).

10 On the Ready to Complete page, review the summary information for the backup job, and then click **Finish**.

   An information dialog box will confirm the backup job was created successfully. The backup operation can take several minutes.

11 Click **OK**.

The newly created backup job is now listed on the **Backup** tab.

Creating a Backup Job on Individual Disks

A full image backup job aggregates all disks in the entire virtual machine into a single image backup. Individual disk backup jobs allow you to select only the disks you need. This capability allows you to filter based on certain configuration criteria, such as by operating system or by retention policy.

Unsupported disk types

When planning for individual disk backups, make sure the disks are supported by VDP. Currently, VDP does not support the following virtual hardware disk types:

- Independent
- RDM Independent - Virtual Compatibility Mode
- RDM Physical Compatibility Mode
- Virtual disks attached to the SCSI controller with bus-sharing enabled

NOTE If a virtual machine contains a VMDK that is not supported, the VMDK is grayed out and the checkbox is unavailable.

For more information about backing up unsupported disk types, refer to "Single VMDK Backup and Restore" on page 16.

Limitation

To perform a backup of a single VMDK on the virtual machine that includes multiple VMDKs, the datastore must have enough space for snapshots of all of the VMDKs on the virtual machine. Even though the backup job is meant to back up a single VMDK, the backup process performs a snapshot of all of the VMDKs on the virtual machine. This behavior is a limitation in VMware.

Prerequisites

The VDP Appliance is installed and configured on your vCenter Server.

Procedure

1. From a web browser, access VDP.
2. Click the **Backup** tab and, from **Backup Job Actions**, click **New** to launch the Create a new backup job wizard.

NOTE You can also launch the Create a new backup job wizard from the **Getting Started** tab. To do this, click **Create Backup Job** under Basic Tasks.

3. To back up individual virtual machine disks, select **Individual Disks** as the data type, and then click **Next**.

   The Virtual Machines page displays an inventory tree. This tree contains all the objects and virtual machines in the vCenter Server.

   Click on the disclosure arrow to progressively disclose the contents of the tree. Select the checkboxes next to the items to add to the backup job, and then click **Next**.

4. On the Schedule page, select the schedule for the job and click **Next**.
5. On the Retention Policy page, accept the default retention policy or specify an alternate retention policy and click **Next**.
6. On the Name page, enter a backup job name and click **Next**.

   The backup job name must be unique and can be up to 255 characters long. The following characters cannot be used in the backup job name: ~!@$^%(){}[]|,`;#\/:*?<>'"&. In addition, diacritical characters cannot be used (for example: â, é, ì, ü, and ñ).

7. On the Ready to Complete page, review the summary information for the backup job, and then click **Finish**.

   An information dialog box will confirm the backup job was created successfully. The backup operation can take several minutes.

8. Click **OK**.

The newly-created backup job is now listed on the **Backup** tab.

Migration on Individual Disks

VMware Storage VMotion (SVMotion™) is a component of VMware vSphere that provides an intuitive interface for live migration of vmdk files with no downtime or disruption in service. You can find complete information about migrating with vMotion and SVMotion at the VMware vSphere Documentation Center web site:

http://pubs.vmware.com/vsphere-51/index.jsp.

Users have two options when migrating a virtual machine from one datastore to another:

- Migrate the full virtual machine all at once to another datastore.
- Migrate individual disks to another datastore, where disks for a single virtual machine may reside on a different datastore.

When a full virtual machine is migrated, the VDP Appliance updates the backup jobs with the new locations of the protected VMDKs.

When individual disks (vmdk files) are migrated from one datastore to another, any associated vmdk backup jobs will no longer protect the vmdk files that were migrated (because those disks cannot be found). An alert will be issued in the vCenter as an event entry, and the following user log entry will appear in the VDP user log.

```
VDP: One or more disks protected by backup job may have been migrated to new datastores. Please edit the backup job and ensure
that the required disks are included in the backup targets of the job.
```

If a backup job no longer protects the disk it originally protected, the Edit backup job wizard does not show the disk as protected. In this case, you must manually re-add the disks to the backup job.

Viewing Status and Backup Job Details

The **Backup** tab displays a list of backup jobs that have been created with VDP. By clicking on a backup job, you can see the details of the job on the Backup Job Details pane:

- **Name** — The name of the backup job.
- **Status** — Whether the backup job is enabled or disabled.
- **Sources** — A list of the virtual machines in the backup job.
- **Out of Date** — A list of all the virtual machines that failed to back up the last time the job ran.

Editing a Backup Job

After you create a backup job, you can edit the job by highlighting the backup job and selecting **Backup Job Actions** > **Edit**.

Cloning a Backup Job

After you create a backup job, you can use the job as a template for creating a different job by highlighting the backup job and selecting **Backup Job Actions** > **Clone**.

Performing the clone action launches the Cloning backup job wizard and uses information from the original job to automatically fill in the first three pages of the wizard (Virtual Machines, Schedule, and Retention Policy). The cloned job requires a unique name. Except for the data type (because an image backup cannot be changed to an individual disk backup and vice versa), any of the settings that were copied from the original job can be modified.

NOTE You can clone full image backups and individual disk backups.

Deleting a Backup Job

You can delete the job by highlighting the backup job and selecting **Backup Job Actions** > **Delete**.

NOTE When using **Delete** on the **Backup** tab you are only deleting the job. Any backups previously made by the job are still retained by VDP in accordance with the retention policy of the job. To delete backups, use **Delete** on the **Restore** tab.

You cannot delete backups that were run on individual disks. You can only delete full image backups.

Enabling or Disabling a Backup Job

If you want to temporarily stop a backup job from running in the future, you can disable it. You can edit and delete disabled backup jobs. VDP will not run a disabled job until it has been enabled.

You can enable or disable backup jobs by highlighting the backup job and selecting **Backup Job Actions** > **Enable/Disable**.

Running Existing Backup Jobs Immediately

You can run backup jobs immediately by using one of the following methods:

- Choosing to backup up a protected virtual machine
- Choosing to run an existing backup job

Immediately Backing Up a Protected Virtual Machine

1. Select the protected virtual machine you want to immediately back up by using one of the following options:
   - Right-click the virtual machine in an inventory tree and select **All VDP Actions** > **Backup Now**. The virtual machine must belong to a backup job for this selection to appear.
   - Click the virtual machine in an inventory tree, and then click the **Actions** button. Select **All VDP Actions** > **Backup Now**. The virtual machine must belong to a backup job for this selection to appear.
   - Click the virtual machine (on the **Reports** tab), click the Actions icon, and then select **Backup Now**.

   The Backup Now dialog appears.
2. Select the VDP Appliance and the backup job, and then click **OK**.

   An information dialog appears telling you the backup job has been initiated.
3. Click **OK**.

   VDP starts the backup job.

Immediately Running a Backup Job

1. From the **Backup** tab in the VDP user interface, click the job you want to run immediately.

   Multiple selections are allowed on the **Backup** tab by using Ctrl- or Shift-click. Hold down the Ctrl key and click multiple, specific backup jobs. Hold down the Shift key and click a range of backup jobs.
2. Click **Backup Now**.

   A drop-down selection appears with the following options:
   - **Backup all Sources** — Backs up all the virtual machines in the backup job.
   - **Backup only out of date sources** — Backs up only the virtual machines that did not back up successfully the last time the backup job ran.
3. Click the sources you want to back up immediately.

4 Click **OK** when you see the message that the backup has been requested.

VDP starts the backup job.

The **Backup Now** option immediately initiates backup jobs if VDP is in the backup window or the maintenance window.

Locking and Unlocking a Backup

During maintenance periods, VDP examines the backups in the appliance and evaluates whether the backup retention period has expired. If it has expired, VDP removes the expired backup from the appliance. However, if you want to prevent VDP from deleting a backup, you can lock it. VDP will not evaluate the retention period on that backup again, until it is unlocked.

NOTE Data in the VDP database drives the locked status. The VDP database is cleared when disks are imported (see “Attaching Existing VDP Disks” on page 73). When disks are imported, the original expiration date for locked backups is reassigned to “never,” and therefore, those disks cannot be unlocked.

NOTE You cannot lock individual disk backups. You can only lock full image backups.

Prerequisites

- VDP is installed and configured on your vCenter Server.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.

Procedure

1 From a web browser, access VDP.

2 From the **Restore** tab in the VDP user interface, click the disclosure arrow associated with the backups shown in the table to locate the backup you want to lock.

3 Select the checkbox next to the backup you want to lock.

4 Click the **Lock/Unlock** icon.

Locking a backup overlays a lock icon on the backup icon (🔒). The backup is now locked.

5 To unlock a backup, select the **Lock/Unlock** icon again.

The lock overlay is cleared and VDP evaluates the retention date of the backup during the next maintenance period.

Automatic Backup Verification 13

This chapter includes the following topics:

- "About Automatic Backup Verification" on page 122
- "Creating a New Backup Verification Job" on page 123
- "Editing a Backup Verification Job" on page 124
- "Cloning a Backup Verification Job" on page 125
- "Executing and Running a Backup Verification Job" on page 125
- "Monitoring Backup Verification" on page 126
- "Enabling and Disabling a Backup Verification Job" on page 126
- "Deleting a Backup Verification Job" on page 126

About Automatic Backup Verification

Automatic Backup Verification (ABV) is a scheduled or on-demand mechanism for verification of backups that ensures the integrity of restore points. ABV has the following characteristics:

- Backups are restored to a temporary virtual machine with the following naming convention:

  VDP_VERIFICATION_<*vm-name***> -<***unique number***>**

- Backups are restored with no network conflicts, because the NIC is always disabled during the ABV operation. Because the NIC is disabled, you cannot perform a ping test.
- After the backup verification job completes, temporary virtual machines, also referred to as validating VMs, are removed and deleted from the inventory.
- Only the last successful full image backup for any VM is verified. The Recent Tasks pane and Event log report which backup has been verified.

Limitations

- Backup verification is not supported for the following configurations:
  - Single VMDK backups.
  - Image backups of RDM disks (physical mode). RDM virtual dependent disks are supported.
  - Application database backups of Microsoft applications (Exchange Servers, SharePoint Servers, and SQL Servers) are not supported.
  - Replicated backups.
  - Backups from imported disks.
- The verification fails if the path to the destination host is changed. If the host is moved to a new location, you must edit the verification job and select the destination host again.
- Similarly, if the datastore name is changed, you must edit the verification job to reselect the same or different datastore before you can successfully run the job again.
- In some cases, VDP fails to automatically delete the validating VM from the vCenter inventory. In this scenario, you must manually delete the validating VM.
- vSphere hosts before version 4.0 are not supported as destination hosts to where temporary VMs will be restored.

Best Practices

Timing and Resource Conflicts

You can take steps to avoid timing and resource conflicts when using the backup verification feature.

1. When you first install VDP, run initial full backups.
2. After the initial backups run, let the first incremental backups run.
3. Determine how long it takes for the backups to run, and schedule backup verification jobs to run after the incremental backups have completed.

Selecting the Destination

Consider the following recommendations while selecting the destination:

- Load balance if multiple verification jobs are to be run at the same time. Limit the number of jobs to five if they are run simultaneously.
- Make sure there are sufficient resources available on the host and the datastore where the temporary VM will be restored.

General

- Verify VMware Tools are installed on the VM at the time the VM is backed up.
- Set the heartbeat timeout interval to its optimal value, depending on the environment. Note that some VMs may take longer to send and receive the VMware Tools heartbeat than others.
- Periodically verify the availability of the destination host and a datastore. Edit the job and reconfigure the destination if needed. If the destination host or datastore is unavailable, edit the job and choose a new destination.
- Before you select Verification Script as the advanced verification option, manually run the script on the guest OS to verify it executes successfully.

Creating a New Backup Verification Job

The backup verification job runs on demand or as part of a schedule. The Backup Verification section of the **Backup** tab allows you to create and manage backup verification jobs.

Prerequisites

- A backup job or a restore point must exist before you create a verification job for a virtual machine. The backup job and restore type must be full image.
- VMware Tools must be installed on virtual machines at the time of backup. If no VMware Tools are found on the validating VM, the heartbeat verification will fail.
- The selected datastore must have sufficient space available.
- If you plan to use a verification script, the verification script must not be dependent on connecting to other VMs in the network.

Procedure

1. From a web browser, access VDP.
2. Click the **Backup** tab.
3. On the **Backup** tab, click **Backup Verification**.
4. From the **Backup Verification Job Actions** menu, select **New**.

   The Create a new backup verification job wizard opens to the Virtual Machines page.
5. On the Virtual Machines page, select a virtual machine for which you want to create a verification job, and then click **Next**.
   - You can select only one virtual machine per verification. Multiple selections are not supported.
   - The virtual machine must be a part of a full image backup job or it can have restore points.
   - You can filter the virtual machines by name, if needed.
   - VMware Tools must be present on the virtual machine backups or the verification job will fail.
6. On the Verification Options page, select an option:
   - **Heartbeat Verification** — This is the default option for verification of a backup, regardless of whether you select script verification. The heartbeat verification checks whether the VMware Tools heartbeat has been received within a specific timeframe after the VM has powered on. If the VMware Tools heartbeat is received, the guest OS has booted successfully and is in a healthy state.

NOTE The **Guest OS Heartbeat** is the default option for verification.

   - **Script Verification** — This is the advanced verification option. Use script verification if you want to verify the virtual machine for the health status of applications and services that run on the guest OS. The script must be predefined and must pre-exist on the guest OS. The verification script must not be dependent on connecting to other virtual machines in the network.

If you choose to execute a script on a guest OS, supply the following information:

- **Username** — Type the user ID used to log in to the guest OS.
- **Password** — Type the password used to log in to the guest OS.
- **Confirm Password** — Retype the password.
- **Verification Script on Guest** — Type the full path to the location of the script on the guest OS.

For script configuration details, refer to "Verification Script Configuration" on page 124.

7 Click **Next**.

8 On the Destination page, select a destination:

- **Destination Path** — The destination host must be compatible with the validating virtual machine and must have sufficient resources to restore the validating virtual machine. You must select a standalone host or a host inside a cluster as a destination where backups will be temporarily restored for the purpose of verification. Resource pools and vApps are not supported as valid destinations. vSphere hosts before version 4.0 are not supported.
- **Datastore** — Depending upon the host that is selected, a list of datastores is displayed. You must select one datastore where the validating virtual machine will be restored. Make sure the selected datastore has sufficient space available.

9 Click **Next**.

10 On the Schedule page, select the schedule for the backup verification job to run. Settings made on this page determine how often and at what time of the day your verification job will run.

a **Backup verification schedule** — Specify the time intervals as daily, weekly, or monthly.

b **Start time on server** — Specify the time for the backup verification to occur on the scheduled day.

11 Click **Next**.

12 On the Job Name page, type a unique name to identify the verification job, and then click **Next**.

The verification job name can include all alphabets and numbers. The only special characters allowed are spaces, underscores, hyphens, and periods.

13 On the Ready to Complete page, review the summary of the backup verification job that you are creating. If needed, you can change the job's configuration by clicking **Back** to the appropriate page. When you are ready to save the job, click **Finish**.

NOTE You can also review the summary of the backup verification job from the Backup Verification section under the **Restore** tab.

14 Click **OK** when you see the message that the backup verification job was created successfully.

Verification Script Configuration

If you plan to use a verification script, supported script formats are .bat, .cmd, .sh, and .exe. A valid script file runs by double-clicking it in the file manager or Explorer view. If the script is an unsupported format, you must enclose the execution of the script inside a supported format.

For example, a Windows Power Shell (.ps1) script cannot be called and run directly by using VDP, because the .ps format is not supported. You can, however, call the .ps script through a supported format (such as .bat), and then specify the full path to the location of the script on the guest OS. Make sure to set the execution policy to **Unrestricted** before you run the script.

The script must return a 0 or non-0 integer. If 0 is returned, the script verification succeeded. If a non-0 value is returned, the script verification failed.

Editing a Backup Verification Job

After you create backup verification jobs, you can edit them as needed.

Procedure

1. From a web browser, access VDP.
2. Click the **Backup** tab.
3. On the **Backup** tab, click **Backup Verification**.
4. Select the backup verification job that you want to edit, and then select **Edit** from the **Backup Verification Job Actions** menu.

   The Editing backup verification job: *job_name* wizard opens to the Virtual Machines page.
5. Step through the wizard, making changes as needed.
6. When you have completed your changes, click **Finish**.
7. Click **OK** when you see the message that changes to the backup verification job were saved successfully.

Cloning a Backup Verification Job

You can use a verification job as a template for creating another job by highlighting the verification job and selecting **Backup Verification Job Actions** > **Clone**.

Performing the clone action launches the Cloning backup verification job wizard and uses information from the original job to automatically fill in the first three pages of the wizard (Virtual Machines, Schedule, and Retention Policy). The cloned job requires a unique name.

Executing and Running a Backup Verification Job

After you create a backup verification job, you can invoke verification by running on-demand verification or by waiting for the schedule to start the backup verification job. The complete backup verification cycle is as follows:

- Restore — The latest backup for the selected VM is restored into a temporary VM that is deleted after backup verification.
- Power On — After the temporary VM has been restored, it will be configured to disable the NIC before it is powered on.
- Boot OS — Wait for the guest OS to boot completely after the VM is powered on.
- Heartbeat Verification — After the guest OS has booted, the appliance waits to receive the VMware Tools heartbeat from the restored VM. In an event the heartbeat is not received for any reason, the verification job fails and the backup is not in a good state.
- Verification Script — The script is executed only when you have selected the advanced level of verification (Verification Script). This feature runs a customized script defined and specified by the user to verify the state of applications running on the guest OS.
- Power Off — After the script verification completes, the VM is powered off.
- Delete VM — In this final step, the restored VM is deleted and the results of the verification is reported by the vCenter (in the Recent Tasks pane and in the Events log).

Procedure

1. From a web browser, access VDP.
2. Click the **Backup** tab.
3. On the **Backup** tab, click **Backup Verification**.
4. Select the backup verification job that you want to run, and then click **Verify Now**.
5. Click **OK** when you see the message that the backup verification request or requests have been issued successfully.

Monitoring Backup Verification

Only the last, successful backup for any VM is verified. You can use any of the methods below to check verification job results:

- vCenter Tasks/Events
- **Reports** tab. See "Viewing Information from the Reports Tab" on page 108 for more information.
- Email reports. See "Configuring Email" on page 58 for more information.
- Client logs. You can download client logs from https://<I*P address or hostname of VDP*>:8543/vdp-configure.

Enabling and Disabling a Backup Verification Job

After you create backup verification jobs, you can enable and disable them as needed. When you disable a backup verification job, it will not run again until you enable it.

Procedure

1 From a web browser, access VDP. Refer to "Backup Jobs" on page 112 for instructions.

2 Click the **Backup** tab.

3 On the **Backup** tab, click **Backup Verification**.

4 Select the backup verification job that you want to enable or disable, and select **Enable/Disable** from the **Backup Verification Job Actions** menu.

5 Click **OK** when you see the message that the backup verification job has been successfully enabled or disabled.

Deleting a Backup Verification Job

You can delete backup verification jobs when they are no longer needed.

Procedure

1 From a web browser, access VDP. Refer to "Backup Jobs" on page 112 for instructions.

2 Click the **Backup** tab.

3 On the **Backup** tab, click **Backup Verification**.

4 Select the backup verification job that you want to delete, and select **Delete** from the **Backup Verification Job Actions** menu.

5 Click **Yes** when you are asked if you are sure you want to delete the selected job.

6 Click **OK** when you see the message that the backup verification job has been deleted successfully.

Managing Restores 14

This chapter includes the following topic:

- "Restore Operations" on page 128
- "Selecting Backups to Restore" on page 128
- "Filtering for List of Backups" on page 128
- "Restores when Snapshots Are Present" on page 128
- "Restoring Image Backups to the Original Location" on page 128
- "Restoring Image Backups to a New Location" on page 130
- "Restoring Backups to Individual SCSI Disks" on page 131
- "Deleting a Backup from the Restore Tab" on page 132
- "Clearing all Selected Backups from the Restore Tab" on page 132

Restore Operations

After you back up virtual machines, you can restore the backups to the original location or to an alternate location.

Restore operations are performed on the **Restore** tab. The **Restore** tab displays a list of virtual machines that have been backed up by the VDP Appliance. By navigating through the list of backups, you can select and restore specific backups. Before you select a backup to restore, note the expiration date of the backup.

Over time, the information displayed on the **Restore** tab may become out of date. To see the most up-to-date information on backups which are available for restore, click **Refresh**.

Limitations

- The Restore wizard does not allow you to select multiple restore points for the same MSApp client. You can select only one restore point from the same client at a time.
- If the target VM has SCSI bus sharing configured, restores to that VM are not supported.

Selecting Backups to Restore

Backups can be restored through the following options:

- Click **Restore a Backup** on the **Getting Started** tab of the VDP UI.
- From the **Restore** tab, select a restore point and click **Restore**.
- Right-click a protected virtual machine in the vCenter inventory list, and then select **All VDP Actions > Restore Rehearsal**. The Select Backup page displays a list of backups.

Filtering for List of Backups

The list of backups that can be restored can be filtered by using drop-down arrows in the following ways:

- **Backup date** — Filtered by "is before," "is after," "is on," or "is not on"
- **Client name** — Filtered by **"**contains,**" "**does not contain,**" "**is,**"** or **"**is not**"**
- **Location** — Filtered by location of backup

Clear the filter by clicking **Refresh** or by selecting **Show All** from the filter drop down menu.

The Select Backup page allows you to choose the virtual machines to restore.

Restores when Snapshots Are Present

Previous versions of VDP allowed users to perform restores to the original virtual machine even if the virtual machine contained snapshots. With VDP version 5.5 and later, snapshots are not allowed on the virtual machine.

CAUTION Before you perform restores, remove any snapshots that might exist from the virtual machine. The restore job fails if the target virtual machine contains snapshots.

Refer to the following Knowledge Base articles about how to properly use snapshots:

- http://kb.vmware.com/kb/1025279
- https://community.emc.com/thread/145249?start=0&start=0

Restoring Image Backups to the Original Location

You can restore backups manually by using the Restore backup wizard.

There are three scenarios where, if the individual disks are selected to be restored instead of the entire VM, you cannot restore to the original location:

- The original disk is marked as independent-persistent.
- The original disk has been removed from the target VM.
- The original disk has been deleted from the target VM.

NOTE A restore job of the same disk or disks from two different timestamps is not permitted. If you attempt to restore a disk that has been backed up with two different timestamps, you are presented with the option of removing the duplicated hard disk. The restore will not proceed until the duplicated hard disk is removed.

After a successful recovery action completes, VDPdisplays the recovered virtual machine under the Replicate link.

Prerequisites

- VDP is installed and configured on your vCenter Server.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.

Procedure

1 From a web browser, access VDP.

2 Click the **Restore** tab.

3 If necessary, filter the backups to narrow your search.

4 Select a virtual machine listed in the Name column. When you click on a virtual machine, it expands to list the backups that have been performed. You can select one or more backups, or you can click a backup to drill down further until you locate the disk that you want to restore.

NOTE The client (virtual machine) name that appears in the Name column is renamed to append a string of random characters if the storage has been imported from a different VDP Appliance during initial configuration.

5 Select the checkbox beside one or more items to select them for restore.

6 Click **Restore** to start the Restore backup wizard.

The Select Backup page appears.

7 On the Select Backup page, verify the list of backups to restore is correct and remove any that you want to exclude from the restore operation. Click **Next**.

The Set Restore Options page appears.

8 On the Set Restore Options page, leave the **Restore to Original Location** box checked. If the vmdk file still exists at the original location, it is overwritten.

NOTE If the virtual disk on the original VM has been removed or deleted, the restore to original location option is not allowed. The VMDK must be restored to a new location.

9 Click **Next**.

The Ready to complete page appears.

10 On the Ready to complete page, review the summary of your restore requests.

This summary identifies how many machines will be replaced (or restored to their original location) and how many will be created (or restored to a new location).

If you want to change any of the settings for your restore request, click the **Back** button to return to the appropriate screen, or click the appropriate numbered step title on the left side of the wizard screen.

11 Click **Finish** to start the restore operation.

A message appears telling you that your restore was successfully initiated.

12 Click **OK**.

13 Monitor the restore progress through the Recent Tasks pane.

NOTE If you selected **Reconnect NIC** during the restore process, confirm the network configuration for the newly-created virtual machine. It is possible that the new virtual machine NIC is using the same IP address as the original virtual machine, which will cause conflicts.

Restoring Image Backups to a New Location

You can restore backups manually by using the Restore backup wizard. On the Set Restore Options page of the Restore a backup wizard, you can specify to where you want the image backup restored.

Prerequisites

- VDP is installed and configured on your vCenter Server.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.

Procedure

1 From a web browser, access VDP.

2 Click the **Restore** tab.

3 If necessary, filter the backups to narrow your search.

4 Select a virtual machine listed in the Name column. When you click on a client (virtual machine), it expands to list the backups that have been performed. You can select one or more backups, or you can click a backup to drill down further until you locate the disk or application that you want to restore.

NOTE The client name that appears in the Name column is renamed to append a string of random characters if the storage has been imported from a different VDP Appliance during initial configuration.

5 Select the checkbox beside one or more items to select them for restore.

6 Click **Restore** to start the Restore backup wizard.

The Select Backup page appears.

7 Click the backup that you want to restore, and then click **Next**.

The Set Restore Options page appears.

8 Clear the **Restore to Original Location** box to set the restore options for each backup that you are restoring to a new location. Specify the following information:

a **New VM Name** — Type a new name for the restored VM.

b **Destination** — Click **Choose** and select the new destination.

c **Datastore** — Select the datastore in which the VM will be restored.

9 Click **Next**.

The Ready to complete page appears.

10 Review the summary of your restore requests.

This summary identifies how many machines will be replaced (or restored to their original location) and how many will be created (or restored to a new location).

If you want to change any of the settings for your restore request, click the **Back** button to return to the appropriate screen, or click the appropriate numbered step title on the left side of the wizard screen.

11 Click **Finish** to start the restore operation.

A message appears telling you that your restore was successfully initiated.

12 Click **OK**.

13 Monitor the restore progress through the Recent Tasks pane.

NOTE If you selected **Reconnect NIC** during the restore process, confirm the network configuration for the newly-created virtual machine. It is possible that the new virtual machine NIC is using the same IP address as the original virtual machine, which will cause conflicts.

Restoring Backups to Individual SCSI Disks

You can restore backups to individual SCSI disks by using the Restore backup wizard. On the Set Restore Options page of the Restore a backup wizard, you can specify to where you want the individual SCSI disks restored.

NOTE SCSI ID does not support multiple restore requests of different VMs. Although you can initiate multiple restore operations, only the first restore is successful. When restoring multiple disks as new disks on either the original or existing VM, all the disks to be restored must come from the same backup and the same VM.

Prerequisites

- VDP is installed and configured on your vCenter Server.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.

Procedure

1 From a web browser, access VDP.

2 Click the **Restore** tab.

3 If necessary, filter the backups to narrow your search.

4 Select a virtual machine listed in the Name column. When you click on a client (virtual machine), it expands to list the backups that have been performed. You can select one or more backups, or you can click a backup to drill down further until you locate the disk or application that you want to restore.

NOTE The client name that appears in the Name column is renamed to append a string of random characters if the storage has been imported from a different VDP Appliance during initial configuration.

5 Select the checkbox beside one or more items to select them for restore.

6 Click **Restore** to start the Restore backup wizard.

The Select Backup page appears.

7 Click the backup that you want to restore, and click **Next**.

The Set Restore Options page appears.

8 Clear the **Restore to Original Location** box to set the restore options for each backup that you are restoring to a new location.

9 Specify the following information:

a **Destination** — To select a new destination, click **Choose.** You can select a new location destination container (vApp, Resource pool, host, or datacenter) where the backup will be restored, or you can accept the default destination, which is the original location of the existing VM.

b **New VM Name** — The **New VM Name** field auto-populates with the existing VM name. You can modify this field to give the VM a new name if you are restoring to a container. If you are restoring to an existing VM, you cannot modify the name.

c **Datastore** — Lists the datastore in which the first disk currently resides. If you are restoring a disk to an existing VM, this field is not editable. If you are restoring a disk to a new container, select the datastore in which the VM will be restored.

d **Disk ID** — Lists the SCSI disk ID slots available as restore targets. The list shows only empty SCSI slots of the SCSI controllers that are currently attached to the virtual machine. Select a SCSI virtual disk slot as the restore target from the list.

You cannot restore to IDE-configured virtual disks. Only SCSI virtual disks are supported. A maximum of 15 disks are allowed on a SCSI controller. Slot 7 is reserved and unavailable.

NOTE The Restore backup wizard does not automatically add a new controller if there are not enough SCSI slots available. You must add a new SCSI controller before initiating the disk restore.

10 Click **Next**.

The Ready to complete page appears.

11 Review the summary of your restore requests.

This summary identifies how many machines will be replaced (or restored to their original location) and how many will be created (or restored to a new location).

If you want to change any of the settings for your restore request, click the **Back** button to return to the appropriate screen, or click the appropriate numbered step title on the left side of the wizard screen.

12 Click **Finish** to start the restore operation.

A message appears telling you that your restore was successfully initiated.

13 Click **OK**.

14 Monitor the Restore progress through the Recent Tasks pane.

Deleting a Backup from the Restore Tab

VDP deletes backups according to the retention policies that were set in the backup jobs. However, you can manually delete backups from the **Restore** tab by selecting the backup jobs for deletion and clicking the **Delete** icon.

NOTE You cannot delete individual disk backups. You can only delete full image backups.

Clearing all Selected Backups from the Restore Tab

1 From the **Manual Restore** tab, select the backups you want to clear from the list of backups, and then click **Clear All Selections**.

2 Click the **Refresh** button to update the data in the **Restore** tab.

Replication 15

This chapter includes the following topics:

- "Replication Jobs" on page 134
- "Creating a Replication Job" on page 136
- "Managing Destinations" on page 140
- "Editing a Replication Job" on page 140
- "Cloning a Replication Job" on page 141
- "Deleting a Replication Job" on page 141
- "Enabling or Disabling a Replication Job" on page 141
- "Viewing Status and Replication Job Details" on page 141
- "Running Existing Replication Jobs Immediately" on page 141
- "Replication Back to the Source" on page 141
- "Replication Recovery Compatibility" on page 142
- "Enabling or Disabling Replication Recovery" on page 143
- "Replication Recovery" on page 143
- "Multi-Tenancy" on page 144

Replication Jobs

Replication enables you to avoid data loss if the source VDP Appliance fails because copies of the backups are available on the destination target. Replication jobs determine which backups are replicated, and when and to where the backups are replicated. With scheduled or ad hoc replication jobs for clients that have no restore points, only the client gets replicated on the destination server. Backups created with the VDP Appliance can be replicated to another VDP Appliance, to an Avamar server, or to a Data Domain system.

Replication Compatibility

Table 15-5 and Table 15-6 indicate which backups can and cannot be replicated, depending on which VDP product was used to create them.

The following abbreviations are used in these tables:

- VDP-A — VDP Advanced Appliance
- RTI — Replication Target Identity

IMPORTANT VDP Advanced applies to VDP 5.8 and earlier. RTI applies only to VDP 5.8.

- DD — Data Domain System
- N — No, the target is not supported
- Y — Yes, the target is supported
- (R) — Recommended
- (NR) — Not Recommended
- (HP) — Hashed Password

Table 15-5. Replication Source Matrix - Part 1

Backups created with this product...	Can be replicated to these targets...										
	VDP 5.1.x	VDP 5.5.1.x	VDP 5.5.5.x	VDP-A 5.5.5.x	VDP-A 5.5.5.x + DD	VDP 5.5.6.x	VDP-A 5.5.6.x	VDP-A 5.5.6.x + DD	VDP 5.8.x	VDP-A 5.8.x	VDP-A 5.8.x + DD
VDP 5.1.x	N	N	N	N	N	N	N	N	N	N	N
VDP 5.5.1.x	N	N	N	N	N	N	N	N	N	N	N
VDP 5.5.5.x	N	N	N	N	N	N	N	N	N	N	N
VDP-A 5.5.5.x	N	N	N	Y (R)	Y (R)	N	Y	Y	N	Y (HP)	Y (HP)
VDP-A 5.5.5.x + DD	N	N	N	N	Y (R)	N	N	Y	N	N	Y (HP)
VDP 5.5.6.x	N	N	N	N	N	N	N	N	N	N	N
VDP-A 5.5.6.x	N	N	N	Y	Y	N	Y	Y	N	Y (HP)	Y (HP)
VDP-A 5.5.6.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y (HP)
VDP 5.8.x	N	N	N	N	N	N	N	N	N	N	N
VDP-A 5.8.x	N	N	N	Y	Y	N	Y	Y	N	Y (R)	Y
VDP-A 5.8.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y (R)
RTI 5.8.x	N	N	N	Y	Y	N	Y	Y	N	Y (R)	Y

Table 15-5. Replication Source Matrix - Part 1 (Continued)

Backups created with this product...	Can be replicated to these targets...										
	VDP 5.1.x	**VDP 5.5.1.x**	**VDP 5.5.5.x**	**VDP-A 5.5.5.x**	**VDP-A 5.5.5.x + DD**	**VDP 5.5.6.x**	**VDP-A 5.5.6.x**	**VDP-A 5.5.6.x + DD**	**VDP 5.8.x**	**VDP-A 5.8.x**	**VDP-A 5.8.x + DD**
RTI 5.8.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y (R)
VDP 6.0.x	N	N	N	Y	Y (R)	N	Y	Y (R)	N	Y	Y (R)
VDP 6.0.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y

Table 15-6. Replication Source Matrix - Part 2

Backups created with this product...	Can be replicated to these targets...									
	RTI 5.8.x	**RTI 5.8.x + DD**	**VDP 6.0.x**	**VDP 6.0.x + DD**	**Avamar SP1 6.1.1.87**	**Avamar SP2 6.1.2.47**	**Avamar 7.0.0.427**	**Avamar 7.0.1.56**	**Avamar 7.1.x.x**	**Avamar 7.1.x.x + DD**
VDP 5.1.x	N	N	N	N	N	N	N	N	N	N
VDP 5.5.1.x	N	N	N	N	Y	Y	Y	Y	Y	Y
VDP 5.5.5.x	N	N	N	N	Y	Y	Y	Y (R)	Y	Y
VDP-A 5.5.5.x	Y (HP)	Y	Y	N	Y	Y	Y (R)	Y (R)	Y	Y
VDP-A 5.5.5.x + DD	N	Y (HP)	N	Y (HP)	Y (NR)	Y (NR)	Y (NR)	Y (NR)	Y	Y
VDP 5.5.6.x	N	N	N	N	Y	Y	Y (R)	Y	Y	Y
VDP-A 5.5.6.x	Y (HP)	Y (HP)	Y (HP)	N	Y	Y	Y (R)	Y (R)	Y	Y
VDP-A 5.5.6.x + DD	N	Y (HP)	N	Y (HP)	Y (NR)	Y (NR)	Y (NR)	Y (NR)	Y	Y
VDP 5.8.x	N	N	N	N	Y	Y	Y	Y	Y (R)	Y
VDP-A 5.8.x	Y (R)	Y	Y (HP)	N	Y	Y	Y	Y	Y (R)	Y
VDP-A 5.8.x + DD	N	Y (R)	N	Y (HP)	Y (NR)	Y (NR)	Y (NR)	Y	Y	Y
RTI 5.8.x	Y (R)	Y	Y (HP)	N	Y	Y	Y	Y	Y (R)	Y
RTI 5.8.x + DD	N	Y (R)	N	Y (HP)	Y (NR)	Y (NR)	Y (NR)	Y (NR)	Y (NR)	Y (R)
VDP 6.0.x	Y	Y (R)	Y HP)	Y (R)	Y HP)	Y HP)	Y HP)	Y HP)	Y HP)	N
VDP 6.0.x + DD	N	Y	N	Y HP)	N	N	N	N	N	Y HP)

Replication and Data Domain

If the source VDP Appliance has a Data Domain system as its backup target, the replication destination VDP Appliance must also have a Data Domain system. Similarly, if replicating from VDP to an Avamar server, the Avamar server must have a Data Domain system.

NOTE DD Boost 2.6 and Data Domain version 5.3 and 5.4 are supported.

The Replication job fails if Data Domain and Avamar backup targets are combined into a single replication job. You must either configure all Data Domain clients or all Avamar clients as the backup targets.

Best Practices when Replicating

- Because only completed client backups are replicated, make every effort to schedule replication during periods of low backup activity. This ensures that the greatest number of client backups replicate during each replication session.
- If you change the user ID or password for the root account on the replication target server, you must update the destination user ID and password on the source server with the new password.
- Using replication destination management, you can update the information for one or more replication jobs associated with the same replication destination server.
- Replication of dynamic or non-static data is not supported; therefore, it is recommended to run the replication during a period of low backup activity.
- You cannot run simultaneous replication and/or recovery of multiple clients if simultaneous, multiple backup and/or restore operations are running.

Limitations

- When a replication job starts, it can process only quiescent, static data that resides on the source server. Therefore, any operation that writes data to the source server and has not fully completed (for example, an in-process backup job) will not be part of that replication job. The data will, however, be replicated during the next replication operation.
- On the source VDP Appliance, as the number of backups for replicated clients increases, the time required to browse each client increases.

Defining Backup Types for a Replication Job

You specify the retention policy and backup schedule when you create backups. Consider these factors when defining the backup types you will use for the replication job.

- Retention policy. Refer to “Setting the Retention Policy” on page 113 for detailed information.
- On-demand or scheduled backup types:
  - If any backup job is run by using the **Backup Now** option, it is considered to be an on-demand backup and is not associated with any backup type. To replicate this backup, you must select the **User Initiated** backup type (Step 6 of the Create a new replication job wizard).
  - To schedule the backup, specify the scheduling options (Step 10 of the Create a new replication job wizard).

Creating a Replication Job

You create replication jobs by using the Create a new replication job wizard.

NOTE Clients or restore points that have already been replicated from a different source server are available in the Create a new replication job wizard.

Prerequisites

- VDP is installed and configured on your vCenter Server.
- You are logged in to the vSphere Web Client and connected to the VDP Appliance.
- You selected **VDP Replication Target** as the VDP Appliance identity in the Initial Configuration wizard. For more information, refer to "Initial Configuration" on page 26.

Procedure

1 From a web browser, access VDP. Refer to "Accessing vSphere Data Protection" on page 106 for instructions.

2 Click the **Replication** tab.

The **Replication** tab displays a list of the replication jobs that have been created. The columns are described as follows:

Table 15-7. Column descriptions for the **Replication** tab

Column	Description
Name	The name of the replication job.
State	The state of the replication job.
Destination	The location where the client backups are replicated.
Last Run Time	The last time the replication job ran.
Duration	How long the replication took to complete the last time the job ran.
Next Run Time	When the replication job is scheduled to run again.
# of Clients	The number of clients whose backups are being protected and replicated in the job. This value changes only when the user adds or removes clients from a replication job using the Edit feature.

3 From the **Replication Job Actions** menu, select **New** to start the Create a new replication job wizard.

4 On the Select Type page, choose whether to replicate guest images (local backups) or replicated backups, and then click **Next**.

The Select Type page appears. On this page, the appropriate clients appear, based on the type of replication you selected.

If the type is replicated backups:

- The VDP Appliancedisplays replicated backups and recovered backup clients as options to replicate to another target server.
- The client table shows the source path in the Source Path column, rather than the last known path.

NOTE Both guest images and application backup options are available.

5 On the Select Clients page, perform one of the following tasks:

- To replicate all client backups, click **All clients**, and then click **Next**.
- To replicate backups from specific clients only, click **Select clients individually**, and then select the type from the **Type** list. Options include Image, MS SQL Servers, MS Exchange Servers, and MS SharePoint Servers.

NOTE Both regular and retired VM backups are supported for replication. If a retired VM is re-added as a regular VM, the system lists the VM twice with an identical name. The retired VM name is appended with a suffix. When selecting clients, select the regular VM without the suffix.

If you choose **Select clients individually**, you can select one or more clients. If preferred, you can filter the clients before you make any selections. To filter clients:

a Beside **Filter**, click **Show All** and select **Client**.

To filter by client name, select **Name**. The following information appears for the vCenter Client.

- Name — "Is," "Is not," "Contains," or "Does not contain" filters used to query the client name.
- Status — Values are Powered On, Powered Off, Suspended, Activated, or Not Activated.
- Client Type — The type of client.

b Click **Next**.

The Backup Selection page appears. On this page, you can limit the number of backups that are replicated when the job runs. If you choose not to select backup options, every backup for the selected virtual machines will be replicated.

6 On the **Backup Selection** page of the Create a new replication job wizard:

a Select a **Backup Type**:

Daily — Only daily backups will be replicated.

Weekly — Only weekly backups will be replicated once.

Monthly — Only monthly backups will be replicated.

Yearly — Only yearly backups will be replicated.

User Initiated — Only those backups that were user-initiated will be replicated.

NOTE User-initiated backups do not retain advanced retention options. These backups must be flagged as a separate backup type.

b Specify the **Maximum backups to replicate per client**:

No Limit — When this option is selected, all existing backups for a client that meet the **Backup Type** criteria will be replicated. The number of backups is unlimited.

Number of Backups — When this option is selected, the backups to be replicated are based on chronological order. The most recent backup is selected, regardless of whether it is an on-demand backup or a scheduled backup. The maximum number of backups is 999.

c Specify the **Date Restrictions**:

None — All backups that meet the **Backup Type** and **Maximum backups to replicate per client** criteria will be replicated. There are no other restrictions.

Last — Select a number and a time unit. This option restricts the selection of backups by including only those backups that were created during the specified number of days, weeks, months, or years.

By Range — Select a **From** date and time, and select a **To** date and time. You can specify from a specific date forward, until a specific date, or between two dates.

d Click **Next**.

The Destination page appears. On this page, you specify connection information for the destination where the client backups will be replicated.

You can use an Avamar server as a replication destination. To do this, supply the Avamar server's IP address, port, and login credentials on the Destination page.

NOTE If you change the name of the VM client, VDP displays the renamed client in the Name column on the Create a new replication job wizard. If you perform a replication of a renamed VM client and the destination is an Avamar server or Avamar Virtual Edition (AVE), the changed name is not reflected in Avamar. The Avamar server displays the older name that was previously registered before the name was changed. This is a known issue.

7 On the Destination page of the Create a new replication job wizard, provide the following information:

NOTE All references to “Destination” refer to either the Avamar server or the VDP Appliance to which the backup data is being replicated.

- **Hostname or IP** — The hostname or IP address of the destination.
- **Port** — The port number over which VDP communicates with the destination. The default value is 29000, which is the standard port for SSL encrypted replication.
- **Username** — The username used to log in to the destination.
- **Password** — The password used to log in to the destination.
- **Path** — The unique name that identifies the domain, used for multi-tenancy configurations. Refer to “Multi-Tenancy” on page 144 for details about multi-tenancy configuration.

For replication and recover replicated backup operations, use the **repluser** username. The credentials of the **repluser** username are kept in sync with the root user.

8 Click **Verify Authentication** to test the connection between VDP and the destination.

9 Click **Next**.

The Schedule page appears. On this page, you specify how often backups will be replicated and what time of the day the replications will occur.

10 On the **Schedule** page of the Create a new replication job wizard:

a Select one of the schedule options:

- **Daily** — Select this option to replicate the backups every day.
- **Weekly performed every** — Select this option, and select a day to replicate the backups on that day every week.
- **The .... of every month** — Select this option, and select a number and a day to replicate the backups on that day of every month.

b Select a **Start Time on Server** to specify the time that the replication will take place on the scheduled day.

Best practice: Because only completed client backups are replicated, you should make every effort to schedule replication during periods of low backup activity. This ensures that the greatest number of client backups replicate during each replication session.

c Click **Next**.

The Retention page appears. On this page, you specify when replicated backups will expire on the destination machine.

11 On the **Retention** page of the Create a new replication job wizard:

a To use each backup’s current expiration date, select **Keep the current expiration for each backup**.

b To specify expiration dates based on backup type, select **Set expiration by backup type**, and select the number of days, weeks, months, or years for each type.

c To keep the replication job forever, select **Keep forever**.

d Click **Next**.

The Name page appears. On this page, you name the replication job.

12 On the **Name** page of the Create a new replication job wizard:

a Type a name for the replication job.

The replication job name must be unique and can be up to 255 characters long. The following characters cannot be used in the job name: ~!@$^%(){}[]|,`;#\/:*?<>'"&. In addition, diacritical characters cannot be used (for example: â, é, ì, ü, and ñ).

b Click **Next**.

The Ready to complete page appears. On this page, you can review a summary of the replication job that you are creating before saving the job.

13 On the **Ready to complete** page of the Create a new replication job wizard:

a Review the information.

b Click **Finish** to create the job.

Managing Destinations

You can select existing replication jobs from the **Replication** tab and then change the destination connection information for all of them using the 3-step Manage Destination wizard.

Best Practice

All replication jobs associated with the same specific replication destination server should be updated, rather than selecting a combination of replication jobs with various destination servers.

Procedure

1 From a web browser, access VDP. Refer to "Accessing vSphere Data Protection" on page 106 for instructions.

2 Click the **Replication** tab.

The **Replication** tab displays a list of the replication jobs that have been created

3 Highlight the replication job, and select **Replication job actions > Manage Destination**.

The Manage Destination Wizard appears.

4 On the Replication Jobs page, click the replication job to update its associated destination, and then click **Next**. You can select multiple jobs.

5 On the **Destination** page of the Manage Destination wizard, provide the following information:

NOTE All references to "Destination" refer to the Avamar serveror to the VDP Applianceto which the backup data is being replicated.

- **Hostname or IP** — The hostname or IP address of the destination.
- **Port** — The port number over which VDP communicates with the destination. The only allowable port is 29000. This port is the standard port for SSL encrypted replication.
- **Username** — The username used to log in to the destination.
- **Password** — The password used to log in to the destination.
- **Path** — The unique name that identifies the domain. This field is used for multi-tenancy configurations. Refer to "Multi-Tenancy" on page 144 for details about multi-tenancy configuration.

For Replication and Recover Replicated backup operations, use the **repluser** username. The credentials of the **repluser** username are kept in sync with the root user.

6 Click **Verify Authentication** to test the connection between VDP and the destination.

7 Click **Next**.

8 On the Ready to Complete page, review the destination that will be assigned to the selected replication jobs. Click **Finish** to update the replication job, or click **Back** to make changes.

Editing a Replication Job

You can edit a replication job by highlighting it and selecting **Replication job actions** > **Edit**.

Cloning a Replication Job

You can use a replication job as a template for creating a different job. Highlight the replication job, and select **Replication job actions** > **Clone**.

Performing the clone action launches the Cloning replication job wizard and uses information from the original job to automatically fill in the information. The cloned job requires a unique name. You can modify any of the settings that were copied from the original job.

Deleting a Replication Job

You can delete a replication job by highlighting it and selecting **Replication job actions** > **Delete**.

NOTE You can select multiple replication jobs to delete. Deleting a replication job will decrement the count of replication jobs associated with a particular replication destination. If the replication jobs being deleted result in replication destinations with no associated replication jobs, then you are given an option to remove replication destinations as part of the delete request.

Enabling or Disabling a Replication Job

If you want to temporarily stop a replication job from running in the future, you can disable it. You can edit and delete disabled replication jobs. VDP will not run a disabled job until it has been enabled.

You can enable or disable a replication job by highlighting the job and selecting **Replication job actions** > **Enable/Disable**.

Viewing Status and Replication Job Details

The **Replication** tab displays a list of replication jobs that have been created with VDP. You can see the details of a replication job by clicking the job. The details are displayed in the Replication Job Details pane:

- **Name** — The name of the replication job.
- **State** — The state of the replication job.
- **Destination** — Where the backups specified in the job were replicated.
- **Clients** — Alist of the clients whose backups are replicated by the job.
- **Last Run time** — The last time the replication job ran.
- **Duration** — How long the replication took to complete the last time the job ran.
- **Next Run time** — The date and time the job is next scheduled to run.

Running Existing Replication Jobs Immediately

You can run a replication job immediately by highlighting the job and clicking **Replicate Now**.

Replication Back to the Source

A replication job can be set up to replicate backup data from one VDP Appliance to another VDP Appliance. In this case, target hosts of replication jobs do not need to be licensed if they are only serving as a replication destination. If the VDP Appliance serving as the replication destination is also running backup jobs, the hosts protected by this appliance must also be licensed.For information about acquiring and downloading static license keys for replication purposes, refer to the following VMware Knowledge Base article:

http://kb.vmware.com/kb/2063573

Node Structure for Recovered Backups

The first time a valid recovery action initiates using the source server, the recovery action creates the source server node under the /REPLICATE link. All recovered backups are displayed under that /REPLICATE link on the **Restore** tab of the source VDP Appliance.

After a successful replication from the source VDP Appliance to a replication target server, when a recovery occurs from the replication source server for replicated backups located at a target server, the fully qualified domain name (FQDN) of the source server appears under the /REPLICATE link on the **Restore** tab. Recovered backups do not display the target server FQDN from which it recovered.

Node Structure of Backups Replicated Again

When a user replicates a replicated backup, the replication source node is not displayed under the /REPLICATE link on the replication target server.

After a successful replication of replicated backups, the **Restore** tab of the subsequent target server displays the parent source server information (on the source server where the virtual machine was originally backed up) under the /REPLICATE link on the **Restore** tab.

After a successful replication of replicated backups from server B to server C (where the virtual machine was originally backed up using server A), the **Restore** tab on the VDP Appliance of server C displays the information for server A under the /REPLICATE link, rather than displaying information for the actual replication source server B.

Replication Destinations

The following are examples of where the replication destination is required:

- A backup that exists on the local VDP Appliance is replicated to a remote replication target, and then the backup is removed or deleted from the local appliance. With the **Replication Back to the Source** feature, you can browse the backups that reside on a remote destination and recover specific backups by copying them back to the local appliance. After the backup is recovered back on the local appliance, it can be restored with the usual process.
- A new VDP Appliance must be installed to replace a corrupted VDP. Specific backups that have already been replicated to a replication destination must be recovered. The **Replication Back to the Source** feature allows you to connect to a replication destination, browse the backups that reside there, and recover specific backups by copying them back to the local appliance. After the backup is recovered back on the new VDP Appliance, it can be restored with the usual process.

NOTE The Recover wizard is not available on the Avamar server. The ability to replicate back to the source is not an option on the Avamar server.

Replication Recovery Compatibility

Table 15-8 lists the supported replication recovery target and replication recovery source servers.

Table 15-8. Replication Recovery Compatibility Matrix

Replication Recovery Target (Recover From)	Replication Recovery Source (Recover To)			
	VDP 5.8	VDP Advanced 5.8	VDP Advanced 5.8 Target Identity	VDP 6.0
VDP 5.8.0.x	No	No	No	Yes
VDP Advanced 5.8.0.x	No	Yes	Yes	Yes
VDP Replication Target Identity 5.8.0.x	No	Yes	Yes	Yes
VDP 5.5.1.356	No	No	No	No
VDP 5.5.5.180	No	No	No	No

Table 15-8. Replication Recovery Compatibility Matrix

Replication Recovery Target (Recover From)	Replication Recovery Source (Recover To)			
	VDP 5.8	VDP Advanced 5.8	VDP Advanced 5.8 Target Identity	VDP 6.0
VDP Advanced 5.5.5.180	No	Yes	Yes	Yes
VDP 5.5.6.56	No	No	No	No
VDP Advanced 5.5.6.56	No	Yes	Yes	Yes
Avamar server 7.0.x	Yes	Yes	Yes	Yes
Avamar Virtual Edition (AVE) 6.0.x	Yes	Yes	Yes	Yes
Avamar server / AVE 7.1.x	Yes	Yes	Yes	Yes

IMPORTANT VDP Advanced applies to versions 5.8 and earlier. Replication Target Identity applies only to VDP 5.8.

Enabling or Disabling Replication Recovery

For VDP versions 5.5 and later, port 29000 is used when replicating from a VDP Appliance to a replication target destination, such as an Avamar storage server or a Data Domain system.

To enable the replication recovery feature, port 29000 must be open on the replication source server. Opening port 29000 allows replicated backups to the replication target destination. If port 29000 is closed, the replication recovery becomes disabled and you are unable to verify the destination as a valid replication recovery target.

By default port 29000 is open on a VDP Appliance. Refer to standard Linux server documentation for procedures on how to open and close port 29000.

Replication Recovery

On a newly installed VDP, you can specify a destination (a machine to where backups have been replicated) by using the Create a new replication job wizard. After the destination is added, you can recover and restore any replicated backups.

NOTE With the current implementation of replication recovery, if a virtual machine client is renamed on a local VDP Appliance, then that name change will not be propagated to backups on a remote VDP Advanced Appliance that is used as a replication target. The new virtual machine name is reflected in the local restore points, but it is not reflected in the destination.

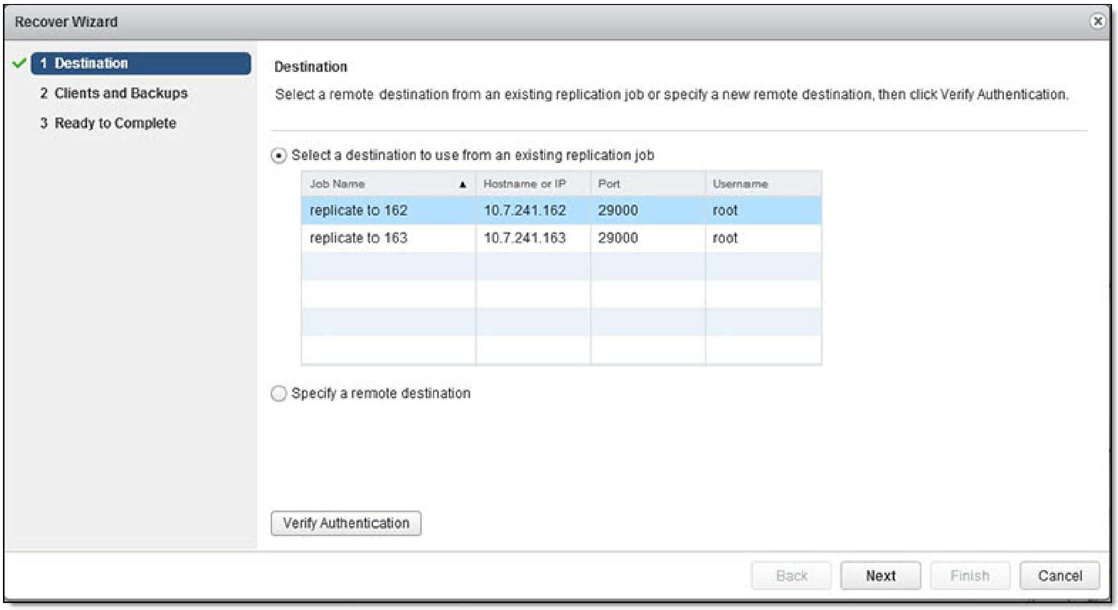
The **Select a replication target** option is disabled after a vCenter Server change and is not enabled until a new replication job is created after the vCenter Server change.

1 From a web browser, access VDP. Refer to "Accessing vSphere Data Protection" on page 106 for instructions.

2 Click the **Restore** tab.

3 From the **Restore** tab, click **Recover replicated backups**.

The Recover wizard appears.



Destination

Select a remote destination from an existing replication job or specify a new remote destination, then click Verify Authentication.

● Select a destination to use from an existing replication job

Job Name ▲	Hostname or IP	Port	Username
replicate to 162	10.7.241.162	29000	root
replicate to 163	10.7.241.163	29000	root

○ Specify a remote destination

4 On the Destination page, select one of the following options:

- **Select a destination to use from an existing replication job**
- **Specify a new remote destination**

5 Click **Verify Authentication**.

6 On the Clients and Backups page, select a remote client and backups to recover back to this appliance. You can expand a client by clicking on the arrow to view its backups.

7 On the Ready to Complete page, review the items to recover.

8 Click **Finish** to start the recover request, or click **Back** to return to the previous screen if you need to make changes.

Multi-Tenancy

VDP includes multi-tenancy support, which enables multiple customers or organizations to have separated accounts on a single VDP Appliance. Each customer or organization can replicate to the VDP Appliance as well as use the Replication Recovery feature to access their replicated data. Replicated data for a given customer or organization is only accessible using the customer or organization account credentials. Built-in credentials with full privileges such as root and repluser have access to all replicated data. These credentials should not be shared with individual customers or organizations. The replicated data for an account is isolated from the replicated data for all other accounts.

VDP, VDP Replication Target, Avamar (version 7.1 or later recommended), and Avamar Virtual Edition (version 7.1 or later recommended) are the supported targets for multi-tenancy.

You can create multi-tenancy accounts by using the `create_av_domain.rb` script, which is provided on all VDP Appliances. The `create_av_domain.rb` script defines the following parameters:

```
Usage: create_av_domain.rb
```

```
-c, --company=<Company-Name>       (Required)
-d, --department=<Department-Name> (Optional)
-u, --username=<User-Name>         (Required)
-p, --password=<User-Password>     (Required)
-h, --help
```

The company value should contain the name of the customer's company or organization. The optional department value allows for the setup of multiple accounts sharing the same company value but each having unique department values. The combined company and department values comprise an account. Each account has its own isolated bucket that can hold replicated data. The username and password parameters define the access credentials for an account. To create more than one set of access credentials for a single account, you can run the `create_av_domain.rb` script multiple times with the same values for company and department, but different values for username and password.

Follow these steps to execute the `create_av_domain.rb` script:

1 Log in (SSH) to the replication target server as the admin user.

2 Run the following command and provide the root password:

```
su – root
```

3 Change to the following directory:

```
cd /usr/local/vdr/configure/bin
```

4 Execute the following command and specify appropriate values for the account being created:

```
./create_av_domain.rb --company=<Company-Name> --department=<Department-Name> --username=<User-Name>
--password=<User-Password>
```

for example:

```
./create_av_domain.rb --company=Acme --department=Marketing --username=fred --password=topsecret
```

After you create the account, enter the account information when you define a replication destination on the VDP Appliance. The replication destination page requires a hostname or IP for the remote destination, the user credentials (username and password), and a path value. The path value is the account identifier, which is composed of the company and department values supplied when setting-up the account with the `create_av_domain.rb` script. A single forward-slash separates the company and department values. In the example above, the path value would be "Acme/Marketing".

Using File Level Restore 16

This chapter includes the following topics:

- "Introduction to the VDP Restore Client" on page 148
- "Logging in to the Restore Client" on page 149
- "Mounting Backups" on page 150
- "Filtering Backups" on page 150
- "Navigating Mounted Backups" on page 151
- "Performing File Level Restores" on page 151
- "Monitoring Restores" on page 152

Introduction to the VDP Restore Client

vSphere Data Protection (VDP) creates backups of entire virtual machines. These backups can be restored in their entirety using the VDP user interface through the vSphere Web Client. However, if you only want to restore specific files from these virtual machines, then use the VDP Restore Client (which is accessed through a web browser). This is called File Level Restore (FLR).

The Restore Client allows you to mount specific virtual machine backups as file systems, and then browse the file system to find the files you want to restore.

The Restore Client service is only available to virtual machines that have backups that are managed by VDP. This requires you to be logged in, either through the vCenter console or some other remote connection, to one of the virtual machines backed up by VDP.

NOTE FLR is not supported for the restore points which have been imported from previously-used VDP disks. This limitation does not apply to restore points that are created for any subsequent backups performed after the import.

CAUTION See "Software Requirements" on page 20 for web browsers supported by vSphere 5.5. Internet Explorer 10 is not supported and is unreliable with the Restore Client.

LVM / EXT Support

Note the following when considering logical volumes managed by the Logical Volume Manager (LVM) and extended file systems:

- One physical volume (.vmdk) must be mapped to exactly one logical volume.
- EXT2, EXT3 formatting (primary partition with master boot record (MBR) and standalone without MBR), and EXT4 are supported.

File Level Restore Limitations

FLR has the following limitations:

- VMware Tools must be installed on the target virtual machine. For best results, ensure that all virtual machines are running the latest available version of VMware Tools. Older versions are known to cause failures when browsing during the file-level restore operation.
- Symbolic links cannot be restored or browsed.
- Browsing either a given directory contained within a backup or a restore destination is limited to a total of 5,000 files or folders.
- You cannot restore more than 5,000 folders or files in the same restore operation.
- When partitions are created, the lower ordered indices must be filled first. That is, you cannot create a single partition and place it in the partition index 2, 3, or 4.
- FLR will not work if the VM is behind network address translation (NAT).

Unsupported VMDK Configurations

FLR does not support the following virtual disk configurations:

- Unformatted disks
- Dynamic disks (Windows)
- Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)
- Compressed partitions

NOTE In some cases (most notably extended partitions), it may be possible to restore the entire backup image to a temporary virtual machine, then selectively copy the folders or files you need.

- Encrypted folders or files
- SCSI disks only are supported when restoring files or folders to the original virtual machine.
- Zero-byte files

Unsupported Windows Configurations

FLR does not support the following Windows 8 and Windows Server 2012 configurations:

- Deduplicated New Technology File System (NTFS)
- Resilient File System (ReFS)
- Extensible Firmware Interface (EFI) bootloader

Logging in to the Restore Client

The Restore Client operates in either Basic or Advanced mode. You can only restore files from a Windows backup to a Windows machine, and you can only restore files from a Linux backup to a Linux machine.

NOTE If you are attempting to log in to Restore Client from a Windows 7 virtual machine, you must set the User Access Control (UAC) settings to the least restrictive settings for FLR to be able to function.

Basic Login

With basic login, you connect to the Restore Client from a virtual machine that has been backed up by VDP. You log in to the Restore Client with the local administrative credentials of the virtual machine to which you are logged in, as shown in Figure 16-2.

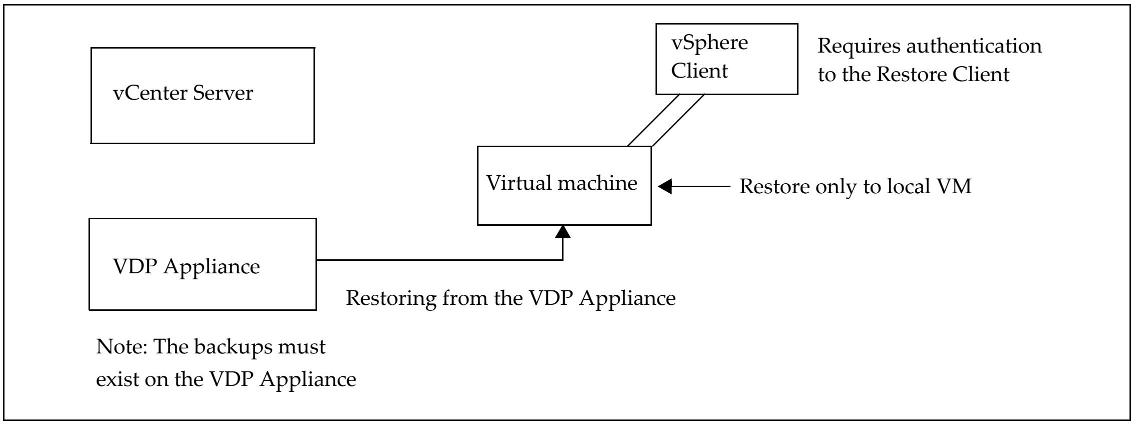

vCenter Server
vSphere Client
Requires authentication to the Restore Client
Virtual machine
Restore only to local VM
VDP Appliance
Restoring from the VDP Appliance
Note: The backups must exist on the VDP Appliance

Figure 16-2. FLR Basic Login

For login instructions, refer to "Using the Restore Client in Basic Login Mode" on page 151.

With basic login, the Restore Client only displays backups for the local virtual machine. For example, if you are logged in to the Restore Client in basic mode from a Windows host named "WS44" then you are only able to mount and browse backups of "WS44."

For login instructions, refer to "Using the Restore Client in Basic Login Mode" on page 151.

With basic login, the Restore Client only displays backups for the local virtual machine. For example, if you are logged in to the Restore Client in basic mode from a Windows host named "WS44" then you are only able to mount and browse backups of "WS44."

Advanced Login

With advanced login, you connect to the Restore Client from a virtual machine that has been backed up by VDP. You log in to the Restore Client with the local administrative credentials of the virtual machine you are logged in to, as well as with the administrative credentials used to register the VDP Appliance to the vCenter Server, as shown in Figure 16-3.

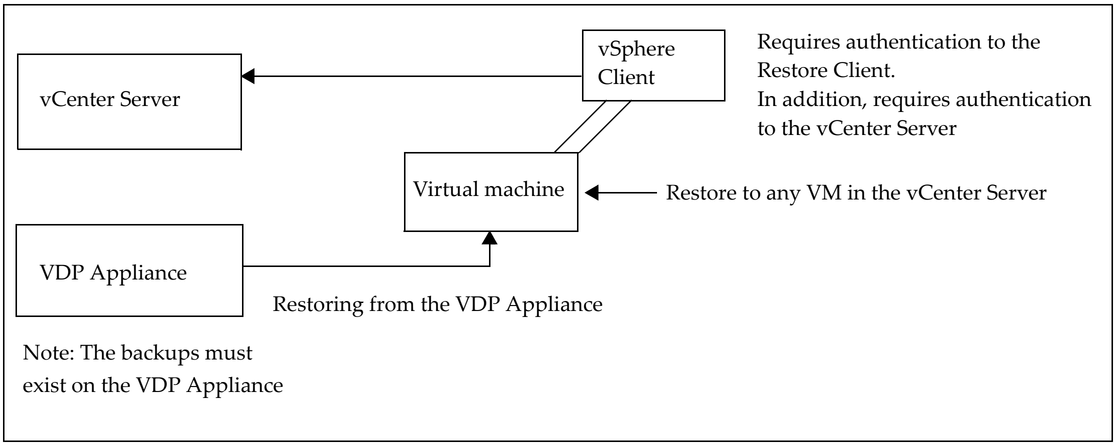

vCenter Server
vSphere Client
Requires authentication to the Restore Client.
In addition, requires authentication to the vCenter Server
Virtual machine
Restore to any VM in the vCenter Server
VDP Appliance
Restoring from the VDP Appliance
Note: The backups must exist on the VDP Appliance

Figure 16-3. FLR Advanced Login

For login instructions, refer to "Using the Restore Client in Advanced Login Mode" on page 152.

After connecting to the Restore Client, you are able to mount, browse, and restore files from any virtual machine that has been backed up by VDP. All restore files are restored to the virtual machine to which you are currently logged in.

FLR advanced login requires you to use the same vCenter user credentials specified when the VDP Appliance is installed. See "VDP Installation" on page 25 for additional information.

Mounting Backups

After you successfully log in, the Manage mounted backups dialog appears, and by default, displays all the backups that are available to be mounted. The format of this dialog varies depending on how you log in.

- If you use basic login, the dialog lists all the backups from the client you logged into that can be mounted.
- If you use advanced login, the dialog lists of all clients that have backed up to VDP. Under each client, there is a list of all available backups to be mounted.

NOTE You can mount up to 254 vmdk file images by using the **Mount**, **Unmount**, or **Unmount** all buttons on the bottom right-hand corner of the dialog.

Filtering Backups

In the Manage mounted backups dialog, you have the option of displaying all the backups or of filtering the list of backups. The list can be filtered in the following ways:

- **All restore points** display all backups.
- **Restore point date** display only backups within the specified date range.
- **VM name** displays only backups of hosts whose display name contains the text entered in the filter field. (This option is not available with basic login because only the backups belonging to the virtual machine you logged in with are displayed.)

Navigating Mounted Backups

After backups have been mounted, you can navigate the contents of the backup by using the tree display on the left side of the Restore Client user interface. The appearance of the tree will vary depending on whether you used basic or advanced login.

Performing File Level Restores

Using the main screen of the Restore Client, you can restore specific files by navigating the file system tree in the left-hand column, and then clicking directories in the tree or clicking files or directories in the right-hand column.

Using the Restore Client in Basic Login Mode

Use the Restore Client on a Windows or Linux virtual machine in basic login mode to access individual files from restore points for that machine, rather than restoring the entire virtual machine.

Prerequisites

- Verify that vSphere Data Protection (VDP) is installed and configured on your vCenter Server.
- For basic login, you can only log in to the Restore Client from a virtual machine that has been backed up by VDP.
- VMware Tools must be installed on the virtual machine in order to perform file-level restores from backups. Refer to the VMware website for list of operating systems that support VMware Tools.

Procedure

1 Use Remote Desktop or a vSphere Web Client to access the local host that has been backed up through VDP.

2 Access the VDP Restore Client:

https://*<IP_address_of _VDP_appliance>***:8543/flr**

3 In the Credentials page under Local Credentials, specify the **Username** and **Password** for the local host and click **Login**.

The Manage mounted backups dialog box appears and lists all of the restore points for the client you are accessing.

4 Select the mount point that will be restored and click **Mount**.

When the mount is complete, the drive icon will appear as a green networked drive .

5 Click **Close**.

6 In the Mounted Backups window, navigate to and select the folders and files you want to recover.

7 Click **Restore selected files.**

8 In the Select Destination dialog box, navigate to and select the drive and destination folder for recovery.

9 Click **Restore**.

An Initiate Restore confirmation dialog box appears.

10 Click **Yes**.

A successfully initiated dialog box appears.

11 Click **OK**.

12 Click the **Monitor Restores** tab to view restore status.

13 Confirm that the job status is completed.

Using the Restore Client in Advanced Login Mode

Use the restore client on a Windows or Linux virtual machine in advanced login mode to access virtual machines on a vCenter Server that contain restore points to perform file-level recovery.

Prerequisites

- Verify that VDP is installed and configured on your vCenter Server.
- FLR advanced login requires you to use the same vCenter user credentials specified when the VDP Appliance is installed. See "VDP Installation" on page 25 for additional information.
- VMware Tools must be installed on the virtual machine in order to perform file-level restores from backups. Refer to the VMware website for list of operating systems that support VMware Tools.

Procedure

1 Log in remotely using Remote Desktop, or use a vSphere Web Client to access a virtual machine.

2 Access the VDP Restore Client:

https://*<IP_address_of _VDP_appliance>***:8543/flr**

3 In the Credentials page under Local Credentials, specify the **Username** and **Password** for the local host. In the vCenter Credentials field, specify the vCenter administrator **Username** and **Password** and click **Login**.

The Manage mounted backups dialog box appears. It lists all of the restore points for the client you are accessing.

4 Select the mount point that will be restored and click **Mount**.

5 When the mount is complete, the drive icon will display as a green networked drive .

6 Click **Close**.

7 In the Mounted Backups window, navigate to and select the virtual machine, folders, and files for recovery.

8 Click **Restore selected files.**

9 In the Select Destination dialog box, navigate to and select the drive and destination folder for recovery.

10 Click **Restore**.

An Initiate Restore confirmation dialog box appears.

11 Click **Yes**.

A successfully initiated dialog box appears.

12 Click **OK**.

You can determine when the restore is complete by clicking the **Monitor Restores** tab to view restore status.

Monitoring Restores

To monitor current and past activity of the Restore Client, click the **Monitor Restores** button. The monitor restore screen displays information about current and recently-completed restore operations.

The columns in this table are sortable by clicking on the column heading. Clicking multiple times on a table heading will reverse the sort order, and an up or down arrow reflects whether the sort order is ascending or descending.

By default, Monitor Restores shows all the jobs that in are in process or that have completed during your current session. If you want to see jobs that completed or failed in a previous session, check the **Show Completed Activities** box, and all past completed and failed jobs will then be displayed along with running and pending jobs.

17 VDP Application Support

This chapter includes the following topics:

- "VDP Application Support" on page 154
- "Backing Up and Restoring Microsoft SQL Servers" on page 155
- "Backing Up and Restoring Microsoft Exchange Servers" on page 164
- "Backing Up and Restoring Microsoft SharePoint Servers" on page 177

VDP Application Support

VDP supports granular guest-level backup and recovery support for Microsoft Exchange Servers, SQL Servers, and SharePoint Servers. To support guest-level backups, a VDP client is installed on the Exchange Servers, SharePoint Servers, and SQL Servers.

Installing Application Agents

To install application agents, refer to the following application-specific instructions:

- "Installing VDP for SQL Server Client" on page 156
- "Installing VDP for Exchange Server Client" on page 165
- "Installing VDP for SharePoint Server Client" on page 178

Checking the User Account Control Setting on Microsoft Windows

The User Account Control (UAC) feature limits application software to standard user privileges. You must provide administrator privileges for certain tasks, such as installing software. UAC is enabled by default.

If you start an VDP client or plug-in installer without administrator privileges on a computer with UAC enabled, the software does not install correctly. You can disable or bypass UAC. The installation procedures in this chapter provide one method to bypass UAC. Other methods and additional information are available in the Microsoft documentation.

Installing VDP Clients when UAC is Enabled

When you attempt to install VDP clients with UAC enabled, the installation displays the following error:

The VMware VDP for <*Microsoft Application*> Server cannot be installed. Please confirm that you are logged in as an administrator and that all installation prerequisites have been met.

To resolve this issue, you must run the installer with administrative privileges by performing the following steps:

1. In Windows, right-click the Command Prompt icon and select **Run as administrator**.
2. In the Command Prompt window, change the working directory to the location of the installation package by typing the following path:

   cd *install_path*

   where *install_path* is the full path of the temporary folder that contains the installation package.
3. Type the appropriate command to start the installer:

   msiexec /i VMwareVDPExchange-windows-x86_64-<*version*>.msi
   msiexec /i VMwareVDPMoss-windows-x86_64-<*version*>.msi
   msiexec /i VMwareVDPSQL-windows-x86_64-<*version*>.msi
   msiexec /i VMwareVDPSQL-windows-x86_32-<*version*>.msi

   where *version* is the VDP client version.

Backing Up and Restoring Microsoft SQL Servers

VDP supports enhanced backup and restore options for Microsoft SQL Servers.

This section covers the following topics:

- "Microsoft SQL Server Support" on page 155
- "Installing VDP for SQL Server Client" on page 156
- "Creating Backup Jobs for Microsoft SQL Servers" on page 160
- "Restoring Backups of Microsoft SQL Servers" on page 163

Microsoft SQL Server Options

The following options are supported for Microsoft SQL Servers:

- Backup selected SQL Servers
- Select entire database instances for backup
- Select individual databases for backup
- Support for full, differential, or incremental backups
- Support to use incremental backups after full backups
- Support for multi-streaming backups (up to six streams)
- Support for simple-mode database backups (skips incremental)
- Restore to original or alternate location
- Restore a database in the original instance using specified path
- Restore a database to a different instance using specified path

Hardware Requirements

Table 17-1 lists the hardware requirements for the Microsoft SQL Server.

Table 17-1. Hardware Requirements for Microsoft SQL Server

Requirement	Minimum
Memory (RAM)	512 MB (2 GB recommended)
Hard drive space	1 GB permanent hard drive space for software installation. The Microsoft SQL Server software also requires an additional 12 MB of permanent hard drive space for each 64 MB of physical RAM. The space is necessary for local cache files.

Microsoft SQL Server Support

VDP supports the following versions of the SQL Server:

- SQL Server failover clusters for the following SQL versions:
  - SQL Server 2014
  - SQL Server 2012
  - SQL Server 2008, 2008 R2
  - SQL Server 2005

- SQL AlwaysOn clusters for the following SQL versions in VDP 5.8:
  - SQL Server 2014
  - SQL Server 2012
- SQL Server 2014
  - SQL Server 2014 x86/x64 on Windows Server 2012
  - SQL Server 2014 x86/x64 on Windows Server 2008 SP2 or later
  - SQL Server 2014 x86/x64 on Windows Server 2008 R2 SP1 or later
- SQL Server 2012 x86/x64 on Windows Server 2012
- SQL Server 2012 x86 on Windows Server 2008 SP2 or later
- SQL Server 2012 x64 on Windows Server 2008 R2 SP1 or later
- SQL Server 2008 R2 and later:
  - Windows Server 2003 SP1 or later, x86/x64
  - Windows Server 2003 R2, SP2 or later, x86/x64
  - Windows Server 2008 SP1 or later, x86/x64
  - Windows Server 2008 R2. x64
  - Windows Server 2012
- SQL Server 2008 SP1 or later on:
  - Windows Server 2003 SP1 or later, x86/x64
  - Windows Server 2003 R2, SP2 or later, x86/x64
  - Windows Server 2008 SP1 or later, x86/x64
  - Windows Server 2008 R2. x64
  - Windows Server 2012
- SQL Server 2005 SP3 x64 on:
  - Windows Server 2003 SP1 or later, x86/x64
  - Windows Server 2003 R2, SP2 or later, x86/x64
  - Windows Server 2008 SP1 or later, x86/x64
  - Windows Server 2008 R2. x64

Installing VDP for SQL Server Client

To support guest-level backups, the VDP for SQL Server Client must be installed on each SQL Server for backup and restore support.

To install the VDP for SQL Server Client in a cluster, install the VDP for SQL Server Client on each node, register each node, and then configure the VDP cluster client. To install the VDP for SQL Server Client in a cluster, perform the following steps:

1. Install the VDP for SQL Server Client in the same folder on each node in the cluster.

   The installation process installs the software, and then registers and activates each node in the cluster with the VDP Appliance.

2. Use the VMware VDP Windows Cluster Configuration Wizard to configure the VDP Appliance.

Prerequisites

- Before using VDP, you must install and configure the VDP Appliance described in "VDP Installation and Configuration" on page 19 and you must have administrative rights to the SQL Server.
- The following software must be installed on the SQL Server:
  - .NET 4.0
  - SQL Server Installation Component
  - Client Tools SDK

Procedure

1. On each SQL Server client, access the vSphere Web Client:

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

2. In the Credentials page, enter an administrative vCenter username and password and click **Login**.
3. In the vSphere Web Client, select **VDP**.
4. In the Welcome to VDP page, select the VDP Appliance and click **Connect**.
5. Click the **Configuration** tab.
6. In **Client Downloads**, click **Microsoft SQL Server 32-bit** or **Microsoft SQL Server 64-bit** (based on the version of the SQL Server client).
7. Depending on your browser, you can save `.msi` file or you can run it. When you run the `.msi` file, the VMware VDP for SQL Server Setup wizard starts. Click **Next**.
8. On the End-User License Agreement page, read the license and if acceptable, click **I accept the terms in the License Agreement**, and click **Next**.
9. On the Appliance Registration Information page, type the name of the VDP Appliance that will back up the SQL Server, and click **Next**.
10. On the Ready to install VMware VDP for SQL Server page, click **Install**.
11. On the Completed the VMware VDP for SQL Server Setup Wizard page, click **Finish**.

Repeat this procedure for additional SQL Servers.

Configuring the Cluster Client in a Failover Cluster

The VDP cluster client in a failover cluster enables you to back up and restore SQL Server data on shared storage in the cluster, regardless of which node is managing the data at the time of the backup or restore. The VMware VDP Windows Cluster Configuration Wizard provides the steps to configure the cluster client for the SQL Server plug-in in a failover cluster.

Procedure

1. Log in to the active node in the cluster as a domain administrator. The account must also be a member of the local Administrators group on each cluster node.
2. Start the VMware VDP Windows Cluster Configuration Wizard:
   - On Windows Server 2012, open the **Start** screen and select **VMware VDP Windows Cluster Configuration Wizard.**
   - On Windows Server 2008, open the **Start** menu and select **Program Files > VMware VDP > VMware VDP Windows Cluster Configuration Wizard**.

   The welcome page appears.
3. Click **Next**.

   The Plug-Ins page appears.

4 Select SQL and click **Next**.

The Cluster Nodes page appears with a list of nodes and their status.

5 Ensure that the environment meets the following requirements:

- The status for each SQL Server node is Up.
- The installation status of the Windows client software for each node is Installed.
- The installation status of the SQL Server plug-in on each node is Installed.

6 Click **Next**.

The Operations page appears.

7 Select **Configure a new cluster client for all nodes**, and then click **Next**.

The Prerequisites page appears. A check mark next to a prerequisite indicates that the environment meets the prerequisite.

8 Ensure that the environment meets all prerequisites on the Prerequisites page.

If the environment does not meet a prerequisite, then exit the wizard, resolve the issue, and restart the wizard.

9 Select the IP version that the environment uses, and then click **Next**.

The SQL Settings page appears.

10 Select the cluster group, service, or role for the cluster client from the list:

- On Windows Server 2012, select the cluster role for the cluster client from the **Cluster role for cluster client** list.
- On Windows Server 2008, select the cluster service for the cluster client from the **Cluster service for cluster client** list.

11 Select the shared volume for the cluster client from the Shared volume for the cluster client list.

12 Click **Next**.

The Server Settings page appears.

13 Specify the settings for the VDP Appliance:

a Type either the DNS name of the VDP Appliance in the **Name** box or the IP address in the **IPv4/IPv6 address** box.

b Type the data port for VDP client/server communication in the **Port number** box.

NOTE Port 28001 is the default port that the VDP client uses to communicate with the VDP Appliance.

c Type the name of the folder or volume in the **Cluster client's var directory** box, or click **Browse** to select a folder or volume.

This folder or volume stores the cluster client configuration and log files. All nodes in the cluster must have write access to this folder or volume.

NOTE Select a volume that the cluster owns instead of a remote pathname on the network.

d Click **Next**.

The Summary page appears.

14 Review the configuration settings, and then click **Configure**.

The Progress page provides the status of the configuration. When the configuration is complete, the Results page appears.

15 Click **Close**.

Configuring the Cluster Client for an AlwaysOn Availability Group

The VDP cluster client for an AlwaysOn availability group enables you to back up and restore SQL Server databases in an availability group. The VMware VDP Windows Cluster Configuration Wizard provides the steps to configure the VDP cluster client for the SQL Server plug-in in an AlwaysOn availability group.

Procedure

1 Log in to a cluster node as a domain administrator. The account must also be a member of the local Administrators group on each cluster node.

2 Start the VMware VDP Windows Cluster Configuration Wizard:

- On Windows Server 2012, open the **Start** screen and select **VMware VDP Windows Cluster Configuration Wizard**.
- On Windows Server 2008, open the **Start** menu and select **Program Files > VMware VDP > VMware VDP Windows Cluster Configuration Wizard**.

The welcome page appears.

3 Click **Next**.

The Plug-Ins page appears.

4 Select **SQL AlwaysOn** and click **Next**.

The Cluster Nodes page appears with a list of nodes and their status.

5 Ensure that the environment meets the following requirements:

- The status for each SQL Server node is Up.
- The installation status of the Windows client software for each node is Installed.
- The installation status of the SQL Server plug-in on each node is Installed.

6 Click **Next**.

The Operations page appears.

7 Select **Configure a new cluster client for all nodes**, and then click **Next**.

The Prerequisites page appears. A check mark next to a prerequisite indicates that the environment meets the prerequisite.

8 Ensure that the environment meets all prerequisites on the Prerequisites page.

If the environment does not meet a prerequisite, then exit the wizard, resolve the issue, and restart the wizard.

9 Select the IP version that the environment uses, and then click **Next**.

The SQL AlwaysOn Settings page appears.

10 Select the cluster group, service, or role for the cluster client from the list:

- On Windows Server 2012, select the cluster role for the cluster client from the Cluster role for cluster client list.
- On Windows Server 2008, select the cluster service for the cluster client from the Cluster service for cluster client list.

The name of the cluster client appears in the Cluster client name box.

NOTE You must configure an availability group listener for each availability group. Do not configure a cluster client for an availability group that does not have a listener.

11 Click **Next**.

The Server Settings page appears.

12 Specify the settings for the VDP Appliance:

   a Type either the DNS name of the VDP Appliance in the **Name** box or the IP address in the **IPv4/IPv6 address** box.

   b Type the data port for VDP client/server communication in the **Port number** box.

NOTE Port 28001 is the default port that the VDP Appliance uses to communicate.

   c Type the name of the folder or volume in the **Cluster client's var directory** box, or click **Browse** to select a folder or volume.

   This folder or volume stores the cluster client configuration and log files. All nodes in the cluster must have write access to this folder or volume.

NOTE Select a volume that the cluster owns instead of a remote pathname on the network.

   d Click **Next**.

   The Summary page appears.

13 Review the configuration settings, and then click **Configure**.

   The Progress page provides the status of the configuration. When the configuration is complete, the Results page appears.

14 Click Close.

Creating Backup Jobs for Microsoft SQL Servers

The VMware VDP for SQL Server Client must be installed on each SQL Server that will be available for backup. See "Installing VDP for SQL Server Client" on page 156 for additional information on client installation.

1 In the vSphere Web Client, select the **Backup** tab.

2 In the **Backup** tab, click **Backup Job Actions** and select **New** to start the **Create a new backup job** wizard.

   On the Job Type page of the wizard, select **Applications**. This option lets you back up the full server or selected databases.

Backing up Applications

If you select **Applications** on the Job Type page, you can choose to back up application servers or individual databases.

1 On the Job Type page of the Create a new backup job wizard, select **Applications**, and then click **Next**.

2 On the Data Type page, select one of the following options, and then click **Next**:

   - **Full Server** — This option lets you back up entire applications servers.
   - **Selected Databases** — This option lets you back up individual application server databases.

3 On the Backup Sources page, click the arrow beside one of the following backup sources to expand the list:

   - Microsoft SQL Server(s) — Select for SQL Server backup.
   - Microsoft SQL Failover Cluster(s) — Select for SQL Failover Cluster backup.
   - Microsoft SQL AlwaysOn Cluster(s) — Select for SQL AlwaysOn availability group backup.

4 Do one of the following:

   - If you chose to back up a full server, select the checkbox next to the SQL server that you want to back up, and then click **Next**.

     NOTE Best practice is to select only one SQL Server per backup job.

   - If you chose to back up selected databases, click the arrow beside an SQL Server, continue drilling down until you can select the database or storage group that you want to back up, and click **Next**.

5 On the Backup Options page, select a backup type of **Full**, **Differential**, or **Incremental**. The options that you can configure depend on which one you choose.

- **Full** — The **Full** option backs up the entire database, including all objects, system tables, and data. The options for full backup are described as follows:

    - **Force incremental backup after full backup** — Selecting or clearing this checkbox specifies whether to force an incremental backup that contains the transactions that occur between full backups. This creates a point-in-time recovery to a point between full backups.

      Do not use this option on databases that use the simple recovery model because those databases do not support transaction log backups. This includes system databases such as the master and msdb databases.

      For simple model recovery databases, use the **For simple model recovery databases** option.

    - **Enable multi-stream backup** — You can either back up multiple databases in parallel with one stream per database, or back up a single database using multiple parallel streams. If you choose to back up a single database with multiple parallel streams, you can specify the minimum size of each stream during the backup.

      After you determine the minimum stream size, you can calculate the number of streams used to back up the database using the following equation:

      Database size/minimum stream size = Number of streams

      For example, if a database is 1,280 MB and you set the minimum stream size to the default setting of 256 MB, then the number of streams that are used to perform a full backup of the database is five, as shown in the following equation:

      1,280 MB/256 = 5

      For transaction log and differential backups, the size of the data to back up, and not the total database size, is used to calculate the number of streams. If the database size is less than the minimum stream size, VDP uses a single stream to back up the database.

      If you calculate the number of streams for a database based on the minimum stream size, and the number exceeds the maximum number of streams that you configured for the backup, the backup of the database uses only the maximum number of streams.

    - **For simple recovery model databases** — This option specifies how VDP handles incremental (transaction log) backups of databases that use the simple recovery model, which does not support transaction log backups:

      Skip incremental with error (default setting) — If you select databases with different recovery models for the backup, the backup does not include the databases with the simple recovery model. The backup completes with exceptions, and an error message is written to the log. If you select only databases with the simple recovery model for the backup, the backup fails.

      Skip incremental with warning — If you select databases with different recovery models for the backup, the backup does not include databases with the simple recovery model. The backup completes successfully, and a warning is written to the log for each database that uses the simple recovery model. If you select only databases with the simple recovery model for the backup, the backup fails.

      Promote incremental to full — A full backup occurs automatically instead of a transaction log backup for databases that use the simple recovery model.

    - **Truncate database log** — This option specifies how database transaction log truncation behavior is controlled. Truncate options include the following:

      Only for incremental backup (default setting) — The database transaction log is truncated if the backup type is set to incremental (transaction log). No log truncation occurs if the backup type is full or differential.

For all backup types — The database transaction log is truncated regardless of the backup type. This setting breaks the chain of log backups and should not be used unless the backup type is set to full.

Never — The database transaction log is not truncated under any circumstances.

- **Authentication method** — The authentication method specifies whether to use NT authentication or SQL Server authentication to connect to SQL Server. If you select SQL Server authentication, specify the SQL Server login name and password.

- **Availability group replica for backup** — There are four options:

  Primary — If selected, the backup is executed on the primary replica of selected AlwaysOn availability group.

  Prefer secondary — If selected, the backup is executed on the secondary replica of selected AlwaysOn availability group. If no secondary replica is available, the backup will be performed on the primary replica.

  Secondary only — If selected, the backup is executed on the secondary replica of selected AlwaysOn availability group. If no secondary replica is available, the backup will be interrupted and an appropriate error message will be written to the log file.

  SQL Server defined — If selected, the backup is executed on the primary or secondary replica based on the SQL server configuration. If Automated_Backup_Preference is set to none the backup will be executed on primary replica.

- **Differential** or **Incremental** — The **Differential** option backs up any data that has changed since the last full backup. The **Incremental** option backs up only the transaction logs. The only configuration option that differs from a full backup is that you can force a full backup rather than an incremental backup.

  - **Force full backup** — Selecting or clearing the checkbox determines whether to perform a full backup when VDP detects a log gap or when there is no previous full backup, from which a transaction log (incremental) or differential backup can be applied. Effectively, this option automates taking a full backup when necessary.

    If you select **Differential** or **Incremental**, you should leave this option selected (the default setting). Otherwise, you might not be able to restore data in the event that no existing full backup is present on VDP.

6. Click **Next**.

7. On the Schedule page, select the backup schedule and start time for the backup job, and then click **Next**.

   See "Specifying the Backup Schedule" on page 113 for additional information on configuring the schedule.

8. On the Retention Policy page, select an option for how long to keep the backup, and then click **Next**.

   See "Setting the Retention Policy" on page 113 for additional information on configuring the retention policy.

9. On the Name page, type a name for the backup job, and then click **Next**.

10. On the Ready to Complete page, review the summary information about the backup job, and click **Finish**.

11. Click **OK** when you see the confirmation that the backup job was created successfully.

Restoring Backups of Microsoft SQL Servers

Once backups have been run on Microsoft SQL Servers, you can restore these backups to their original location or to an alternate location.

Procedure

1. In the vSphere Web Client, select the **Restore** tab.
2. Select the backup that you want to restore. While you can select multiple SQL Servers, you can only select one restore point for each SQL Server.
3. Click **Restore**.

   The Select Backup page appears.
4. Select the backup job that you want to restore, and then click **Next**.

   The Select Restore Options page appears.
5. Do one of the following.
   - Leave the **Restore to Original Location** option selected (the default setting) to restore the backup to its original location.
   - Clear the **Restore to Original Location** option to restore the backup to an alternate location, and then do the following:

     i Click **Choose** to select the destination client.

     ii In the **SQL instance** box, type the name of the SQL instance. If you use "local," it must be in parentheses.

     iii In the **Location path** box, type the existing full Windows path where the database files will be restored.

     If the Location path does not exist, it will not be created, and the restore will fail.

     iv In the **Log file path** box, type the existing full Windows path where the log files will be restored.
6. If you want to specify advanced options, click the arrow beside **Advanced options** to expand the list. The options are described as follows:
   - **Use SQL REPLACE** — This option specifies that the SQL Server should create any necessary database and related files even if another database or file already exists with the same name.

     This option overrides a SQL Server safety check that is intended to prevent you from accidentally overwriting a different database or file. This safety check is described in the Microsoft Transact-SQL Reference Manual under the RESTORE command section.
   - **Tail-log backup** — To perform a tail-log backup during the restore process, the database must be online and using either the full or bulk-logged recovery model. You cannot perform a tail-log backup on the system databases because those databases use the simple recovery model (for example, the master and msdb databases).

     Do not select tail-log backup if you are performing a redirected restore to a different SQL Server instance.
   - **Restore system databases** — You rarely need to restore only system databases. However, the restore might be required if one or more system databases are damaged.

     You will more likely need to restore system databases at the same time that you restore user databases. When you select both the system and user databases for restore, the system databases are restored first.

     When you restore system databases, the VDP Microsoft SQL Server Client automatically restores the databases in the correct order (master, msdb, then model) managing SQL Server services.

Authentication method — The authentication method specifies whether to use NT authentication or SQL Server authentication to connect to SQL Server. If you select SQL server authentication, specify the SQL Server login name and password.

- **Restore only on primary replica** checkbox — Sets the `--recover-primary-only` flag, which disables the automatic recovery of secondary replicas and performs the recovery only on the primary replica. By default, the check box is enabled, so the recovery will be performed only on the primary replica. This option is enabled only for databases that reside in an AlwaysOn availability group.

NOTE After you restore a database on only the primary replica, the corresponding database on the secondary replica is in a restoring state.

7 Click **Next**.

The Ready to complete page appears.

8 Review the restore requests, and then click **Finish**.

9 Click **OK** when you see the message telling you that your restore was successfully initiated.

10 Monitor the restore's progress in the Recent Tasks pane.

Monitoring Client Activity

You can monitor tasks and events for all the client activity by collecting and analyzing the client logs. The client logs are Microsoft application (MSApp)-related logs. The aggregated client log includes any replication, backup, restore, or automatic backup verification (ABV) job that passed with exceptions or failed. For more information, refer to "Collecting Logs" on page 44.

Uninstalling the VDP Plug-in for SQL Server

To uninstall the VDP Plug-in for SQL Server:

- On Windows Server 2012 or Windows Server 2008, use **Programs and Features**.
- On Windows Server 2003, use **Add/Remove Programs**.

Backing Up and Restoring Microsoft Exchange Servers

This section covers the following topics:

- "Microsoft Exchange Server Support" on page 165
- "Installing VDP for Exchange Server Client" on page 165
- "Using the VMware Exchange Backup User Configuration Tool" on page 168
- "Manually Configuring the VDP Backup Service" on page 170
- "Creating Backup Jobs for Microsoft Exchange Servers" on page 170
- "Restoring Backups of Microsoft Exchange Servers" on page 172
- "Granular Level Recovery on Microsoft Exchange Servers" on page 174
- "Uninstalling the Exchange Server Plug-in" on page 174

Microsoft Exchange Server Options

VDP supports the enhanced backup and restore options for Microsoft Exchange Servers:

- Backup selected Exchange Servers
- Backup selected individual Exchange databases or storage groups
- Ability to perform incremental backups
- Support for multi-streaming backups (up to ten streams)

- Support for circular logging (promote, circular, and skip)
- Ability to restore Exchange to original location or alternate location
- Option for no replay logs during restore
- Recovery Storage Groups (RSG)/Recovery database (RDB)
- Granular-level restores

Microsoft Exchange Server Support

Table 17-2 lists the Microsoft Exchange Server versions and operating systems that the VDP plug-in for Microsoft Exchange supports.

Table 17-2. Supported Microsoft Exchange Server Versions and Operating Systems

Exchange Server version	Operating systems
■ Exchange Server 2013 ■ Exchange Server 2013 database availability group (DAG) ■ Exchange Server 2013 SP1	■ Windows Server 2012 x64 ■ Windows Server 2012 R2 x64 ■ Windows Server 2008 R2 x64
■ 2010 SP3 Server ■ Exchange Server 2010 Database Availability Group (DAG)	■ Windows Server 2012 x64 ■ Windows Server 2008 R2 x64 ■ Windows Server 2008 SP2 x64
■ 2007 SP3	■ Windows Server 2008 R2 x64 ■ Windows Server 2008 SP2 x64

Microsoft .NET Framework 4 Requirement

The Exchange Server VSS plug-in requires installation of Microsoft .NET Framework 4 on each server in the Exchange Server forest. Search the Microsoft Download Center for “Microsoft .NET Framework 4” to find downloads and additional information.

Hardware Requirements

Table 17-3 lists the hardware requirements for the VDP Plug-in for Microsoft Exchange Server.

Table 17-3. Hardware Requirements for Microsoft Exchange Server

Requirement	Minimum
Memory (RAM)	64 MB
Hard drive space	Software installation requires at least 100 MB of permanent hard drive space, with 1 GB recommended. Local cache files require an additional 12 MB of permanent hard drive space for each 64 MB of physical RAM.

Unsupported Microsoft Exchange Servers

Microsoft Exchange Server 2007 clusters (SCC, CCR, SCR) are not supported with the VDP plug-in for Microsoft Exchange Server.

Installing VDP for Exchange Server Client

To support guest-level backups, the VMware vSphere Data Protection (VDP) for Exchange Server Client must be installed on each Exchange Server for backup and restore support.

Prerequisites

Before using VDP, you must install and configure the VDP Appliance described in “VDP Installation and Configuration” on page 19 and you must have administrative rights to the Exchange Server.

Procedure

1 On each Exchange Server client, access the vSphere Web Client:

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

2 In the Credentials page, enter an administrative vCenter username and password, and then click **Login**.

3 In the vSphere Web Client, select **VDP**.

4 In the Welcome to VDP page, select the VDP Appliance and click **Connect**.

5 Click the **Configuration** tab.

6 In **Client Downloads**, click **Microsoft Exchange Server 64-bit**.

7 Depending on your browser, you can save the `.msi` file or run it. When you run the `.msi` file, the VMware VDP for Exchange Server Setup wizard starts. Click **Next**.

8 On the End-User License Agreement page, read the license and if acceptable, click **I accept the terms in the License Agreement** and click **Next**.

9 On the Appliance Registration Information page, type in the IP address or fully qualified domain name of the VDP Appliance that will back up the Exchange Server.

10 (Optional) Select the option to install the **Exchange Server GLR** plug-in if you plan to use the server for granular level recovery.

NOTE You must reboot the Microsoft Exchange Server if you select the Exchange Server GLR option.

11 If this is the first Exchange Server in the Active Directory to have the VMware VDP for Exchange Server Client installed, confirm that the **Launch Exchange Backup User Configuration Utility** checkbox is selected. If the VMwareVDPBackupUser account has already been created in the Active Directory forest, clear this checkbox. Click **Next**.

12 On the Ready to install VMware VDP for Exchange Server page, click **Install**.

13 On the Completed the VMware VDP for Exchange Server Setup Wizard page, click **Finish**.

If you selected the **VDP Exchange Backup User Configuration Tool** checkbox, proceed to "Using the VMware Exchange Backup User Configuration Tool" on page 168.

If you did not select the **VDP Exchange Backup Configuration Tool** checkbox, proceed to "Manually Configuring the VDP Backup Service" on page 170.

Repeat this procedure for additional Exchange Servers.

Installing in a DAG or Cluster Environment

Procedure

1 Exchange for VDP consists of a single, standalone installer. Install the VDP for Exchange Client Plug-in on each Microsoft Exchange server with the Mailbox server role.

To use a server for granular level recovery, select the options to install both the Exchange GLR plug-in and the Exchange VSS plug-in. In a DAG environment, you should configure at least one server for GLR.

NOTE You must restart the Exchange server after you install the Exchange GLR plug-in.

2 Register each Exchange server as a client with the VDP Appliance.

3 Create and configure the VmwareVDPBackupUser account.

4 Use the VMware VDP Windows Cluster Configuration Wizard to configure the Exchange DAG client or the VDP cluster client.

Configuring an Exchange DAG Client

Configuring an Exchange DAG client allows you to perform federated backups of databases in an Exchange Server 2013 or 2010 DAG.

Prerequisites

Verify that the DAG cluster environment meets the following prerequisites before configuring the Exchange DAG client.

- The VDP Windows Client has been installed.
- The VDP Backup Plug-in for Exchange DAG has been installed.
- The DAG Group exists if the DAG client is already configured for any nodes.
- An unused static IP address is available to be assigned to the new VDP Exchange DAG Client.
- The machine accounts for all the cluster nodes must have full access to the SMB share.
- The Exchange DAG federated backup must have a network share created (to be used as the `var` directory).

Procedure

1. Log in to an Exchange server in the DAG with the VmwareVDPBackupUser account.
2. Start the VMware VDP Windows Cluster Configuration Wizard:
   - On Windows Server 2012, open the **Start** screen and select **VMware VDP Windows Cluster Configuration Wizard**.
   - On Windows Server 2008, open the **Start** menu and select **Program Files > VMware VDP > VMware VDP Windows Cluster Configuration Wizard**.

   The welcome page appears.
3. Click **Next**.

   The Plug-Ins page appears.
4. Select **Exchange DAG** and click **Next**.

   The DAG Nodes page appears with a list of DAG servers and their status.
5. Ensure that the environment meets the following requirements:
   - The status for each Exchange server is Up.
   - The installation status of the Windows client software for each server is Installed.
   - The installation status of the Exchange VSS plug-in on each server is Installed.
6. Click **Next**.

   The Operations page appears.
7. Select **Configure a new DAG client for all nodes** and click **Next**.

   The Prerequisites page appears. A check mark next to a prerequisite indicates that the environment meets the prerequisite.
8. Ensure that the environment meets all prerequisites on the Prerequisites page. You select the Internet Protocol version that the environment uses (IPv4 or IPv6) on the Prerequisites page, and then click **Next**.

   If the environment does not meet a prerequisite, then exit the wizard, resolve the issue, and restart the wizard.

   The DAG Client Settings page appears.

9 Specify the client settings for the cluster group for the DAG client:

   a Select the network in the network list.

   b Type the IP address for the DAG client cluster group in the **Exchange DAG client IPv4/IPv6 address** box. The IP address must be a unique, unused IP address. Do not use the IP address for the DAG.

   c Type the network mask for the DAG client cluster group in the **Exchange DAG client IP subnet mask** box.

10 Click **Next**.

   The User Settings page appears.

11 Select one of the following login accounts:

   - Local System account
   - This account, and specify the Account Name and Password for the VmwareVDPBackupUser account.

12 Click **Next**.

   The Server Settings page appears.

13 Specify the settings for the VDP Appliance:

   a Type either the DNS name of the VDP Appliance in the **Name** box or the IP address in the **IPv4/IPv6 address** box.

   b Type the name of the VDP domain for the Exchange DAG client in the **VDP client domain for the DAG client** box.

   c Type the data port for the VDP client/server communication in the **Port number** box.

   d Type the path to the `var` folder for the cluster client in the **Cluster client's var directory** box, or click **Browse** to select a location.

   The `var` folder stores the Exchange DAG client configuration and log files. The VmwareVDPBackupUser account and all nodes in the cluster must have write access to this location.

NOTE Select a volume that each server in the DAG can access.

14 Click **Next**.

   The Summary page appears.

15 Review the settings that you specified in the wizard, and then click **Configure**.

   The Progress page provides the status of the configuration. When the configuration is complete, the Results page appears.

16 Click **Close**.

Using the VMware Exchange Backup User Configuration Tool

If the **Launch Exchange Backup User Configuration Utility** checkbox is selected during VMware VDP for Exchange Server Client installation, the VMware Exchange Backup User Configuration Tool starts automatically after installation completes.

VMwareVDPBackupUser Account

The VDP Microsoft Exchange Server Client requires direct access to the Exchange Server. A special user account, called VMwareVDPBackupUser, is required to provide VDP with appropriate domain and administrator-level permissions. This user account is set up through the VDP Exchange Backup User Configuration Tool, which runs by default after the VDP Microsoft Exchange Server Client installation.

NOTE The VDP Backup Agent service is no longer required to be run under this account, nor is the user required to select the **Configure Backup Agent** checkbox. If the VDP Backup Agent is configured to run under the Local System account, the user is required to enter credentials when creating backup jobs or when performing backup and restore operations.

VMwareVDPBackupUser is configured with the following:

- The user account is added and activated for the appropriate Active Directory, Exchange, and group accounts. The user account is added to the following groups:
  - Backup Operators
  - Domain Users
  - Domain Admin (for Exchange Server 2007)
  - Exchange Servers
  - Exchange Organization Management (in Microsoft Exchange Security Groups) for Exchange Servers 2010 and 2013
  - Exchange Organization Administrators for Exchange Server 2007
- A mailbox is created, activated, and tested for the user account.
- A user account is set up and activated in the Exchange domain, and then on each Exchange Server running the VDP Microsoft Exchange Server Client. VDP Backup services must be configured to use the VMwareVDPBackupUser account.

Prerequisites

- Before using VDP, you must install and configure the VDP Appliance described in "VDP Installation and Configuration" on page 19.
- The **Launch Exchange Backup User Configuration Utility** checkbox must be selected during VMware VDP for Exchange Server Client installation. If the user does not select the checkbox at installation, the user can start the VMware Exchange Backup User Configuration Tool manually from the following location:

  x:\program files\avp\bin\vmbackupusercfg.exe
- .NET 4.0 must be installed on the Exchange Server:

Procedure

1. In the VMware Exchange Backup User Configuration Tool, select **New user** or **Existing user** depending on the status of the user you are configuring.
2. In the **User Name** field, type a username for the VMwareVDPBackupUser Account. You can use the default name of VMwareVDPBackupUser if needed.
3. In the **Password** field, type a password for the account.
4. In the **Confirm password** field, re-type the password.
5. In the **Exchange Server** field, select the name of the Exchange Server that the VDP Microsoft Exchange Server Client was installed on.
6. In the **Storage group** field (only active for Exchange Server 2007), select the Storage group name.
7. In the **Mailbox store** field, select the mailbox database for the VMwareVDPBackupUser account.
8. Click **Check** to test the new user settings. If the user does not exist in Active Directory, the check fails.
9. Click **Configure Services**.
10. The message log lists a set of tests that have passed or were successful. If all of the check test pass, click **Close**.

Manually Configuring the VDP Backup Service

If you have already run the VDP Exchange Backup User Configuration Tool, the VMwareVDPBackupUser account is created. The following steps are used to manually configure the VMwareVDPBackupUser account to run the VDP Backup Service.

- Before using VDP, you must install and configure the VDP Appliance described in "VDP Installation and Configuration" on page 19.
- The VMwareVDPBackupUser account has been created through the Launch Exchange Backup User Configuration Utility.

Procedure

1. Log in to the Exchange Server as VMwareVDPBackupUser or as another user with Administrative rights.
2. Start the Services application by selecting **Start** > **Programs** > **Administrative Tools** > **Services**.
3. From the Services window, right-click **Backup Agent** in the Services list, and select **Properties**.
4. From the Backup Agent Properties dialog box, click the **Logon** tab.
5. Select the **This account** button and specify the username created by the VDP Exchange Backup User Configuration Tool (VMwareVDPBackupUser by default).
6. Type the password for the VMwareVDPBackupUser account in the **Password** and **Confirm password** fields, and then click **OK**.
7. Right-click the Backup Agent service in the Services list and select **Restart**.

NOTE If GLR is installed, you must repeat this procedure on the "VMware VDP Exchange GLR Service" as well.

Creating Backup Jobs for Microsoft Exchange Servers

Microsoft Exchange Server clients must have the VMware VDP Microsoft Exchange Server Client installed in order to be available for backup. See "Installing VDP for Exchange Server Client" on page 165 for additional information on client installation.

1. In the vSphere Web Client, select the **Backup** tab.
2. In the **Backup** tab, click **Backup Job Actions**, and select **New** to start the **Create a new backup job** wizard.
3. On the Job Type page of the wizard, select **Applications**. This option lets you back up the full server or selected databases.

   The job type that you choose determines the options that you can select from here on. Based on your selection, follow the instructions in the appropriate section below.

Backing up Applications

If you select **Applications** on the Job Type page, you can choose to back up application servers or individual databases.

1. On the Job Type page of the Create a new backup job wizard, select **Applications** and click **Next**.
2. On the Data Type page, select one of the following options and click **Next**:
   - **Full Server** — This option lets you back up entire applications servers.
   - **Selected Databases** — This option lets you back up individual application server databases.

3 On the Backup Sources page, click the arrow beside **Microsoft Exchange Servers(s)** to expand the list.

4 Do one of the following:

NOTE Best practice is to select only one Exchange Server per backup job.

- If you chose to back up a full server, select the checkbox next to the Exchange Server that you want to back up, and then click **Next**.
- If you chose to back up selected databases, click the arrow beside an Exchange Server, continue drilling down until you can select the database or storage group that you want to back up, and then click **Next**. Note that if the client is running as a local system account, the user must provide Exchange Administrator credentials to drill down the Exchange server.

  NOTE If the backup target is an Exchange 2007 Server, you cannot select an individual database, and must select a storage group instead.

5 On the Backup Options page:

a Select a backup type of **Full** or **Incremental**. Incremental backups are automatically promoted to full backups if a full backup does not exist.

NOTE If the client is running as a Local System account, the user must provide Exchange Administrator credentials. If not running as a Local System account, credentials are not required.

If you select **Incremental**, you can specify circular logging options. Circular logging allows you to reduce the number of transaction logs resident on the system. For mixed environments where some, but not all, storage groups or databases have circular logging enabled, you can select one of these settings to specify how VDP handles incremental backups.

- **Promote** (default setting) — This option promotes an incremental backup to a full backup if any database in the saveset has circular logging enabled. All databases will be backed up whether they have circular logging enabled or not. If one or more databases has circular logging enabled, all databases in the saveset will have any incremental backup promoted to a full backup.
- **Circular** — This option promotes all incremental backups of all databases with circular logging enabled to a full backup and skips any databases that do not have circular logging enabled.
- **Skip** — This option performs an incremental backup of all databases that have circular logging disabled and skips any databases that have circular logging enabled.

b (Available for DAG clusters only) In the **Preferred server order** list box, specify the priority of servers to use to back up the Exchange databases. Specify the server name, not the FQDN. Separate multiple entries with commas. If you do not specify a list, the Exchange VSS plug-in adds all servers in the DAG to the list in alphabetical order.

c (Available for DAG clusters only) From the **Set the preference for what types of database to back up** list, select the type of database to back up:

- Select **Prefer passive** to back up a passive copy of each database, if a healthy passive copy is available. If a healthy passive copy is not available, the VDP Appliance backs up the active copy.
- Select **Active** only to back up only the active copy of each database.
- Select **Passive** only to back up only the passive copy of each database. If a healthy passive copy is not available, the backup does not include the database.

6 Select the **Enable multi-stream backup** option if you want to allow the parallel processing of backup jobs using multiple processors. Use the slider bar to select the number of streams to use.

You can use as many as ten streams. Each stream requires a separate processor core. By taking advantage of multi-processors, you can improve backup performance.

7 Click **Next**.

8 On the Schedule page, select the backup schedule and start time for the backup job, and then click **Next**.

See "Specifying the Backup Schedule" on page 113 for additional information on configuring the schedule.

9 On the Retention Policy page, select an option for how long to keep the backup, and then click **Next**.

See "Setting the Retention Policy" on page 113 for additional information on configuring the retention policy.

10 On the Name page, type a name for the backup job, and then click **Next**.

11 On the Ready to Complete page, review the summary information about the backup job, and then click **Finish**.

12 Click **OK** when you see the confirmation that the backup job was created successfully.

Restoring Backups of Microsoft Exchange Servers

After you run backups on Microsoft Exchange Servers, you can restore these backups to their original location or to an alternate location.

CAUTION The target Microsoft Exchange Server must have the same Microsoft Exchange Server version and service pack as the Exchange Server on which the backup occurred. Otherwise, the restore will fail.

Procedure

1 In the vSphere Web Client, select the **Restore** tab.

2 Click the client whose backup you want to restore.

3 Click the backup that you want to restore.

4 To restore the entire contents of the backup, select the **Exchange Information Store** checkbox.

5 After you select all the targets, click the **Restore** button.

NOTE If the client is running as a local system account, the user must provide Exchange Administrator credentials. If not running as a local system account, credentials are not required.

6 On the Select Restore Options page, the **Restore to Original Location** option is the default setting and cannot be modified.

7 (Optional) For GLR, on the Select Restore Options page, do the following.

- **Restore to Original Location** — Clear this box if you would like to select a different client to create the RDB on or to restore to a different mailbox.
- **Destination Client** — This is the Exchange Server where the RDB will be created and mounted from the backup. This client must be an Exchange Server with the VDP Exchange GLR plug-in installed.
- **Destination Mailbox** — Set to the email address of the mailbox where the selected mailboxes should be restored to.

8 If you want to specify advanced options, click the arrow beside **Advanced options** to expand the list.

The options are described as follows:

- **Allow database overwrite** — Forces any existing databases to be overwritten that have the same name or names included in the restore job. When this option is selected, it modifies the "Allow File Restore" flag, which is internal to the Exchange Server.

- **Restore into RSG/RDB** — Restore Storage Groups (RSG) are used in Exchange Server 2007 and Recovery Databases (RDB) are used in Exchange Server 2010 and Exchange Server 2013. RSG/RDB is used to restore to an RSG/RDB instead of to a production database. When you select **Restore into RSG/RDB**, you can configure the following options:
    - **Overwrite existing RSG/RDB** — Overwrites any existing RSG/RDB. Use this option with caution.
    - **RSG/RDB name** — The name of the RSG/RDB that is used for the restore. If a RSG/RDB with the specified name does not already exist, it will be created. If an RSG/RDB with the specified name already exists, use the **Overwrite existing RSG/RDB** option to overwrite it.
    - **RSG/RDB database path** — The path where the RSG/RDB database file will be restored (for example, `C:\myrdb`). This is an optional field. The default location is used if this field is left blank.
    - **RSG/RDB log path** — The path where the RSG/RDB log file will be restored (for example, `C:\myrdb`). This is an optional field. The default location is used if this field is left blank.
- Select whether to restore but not replay transaction logs by selecting or clearing the **Do not replay the transaction logs** checkbox. When you select this option, you can manually copy additional transaction logs before you mount the database.
- If log file conflicts occur during the restore, use the **Move logs path** box to specify a location to move the existing log files to before the restore. If you do not specify a path for the log files and there is a gap in the transaction log, the restore process automatically moves the current transaction logs to a subfolder named `logs_time_date`. The time and date values are the time and date of the restore. The subfolder is in the transaction log folder for the database or storage group. You can use these logs to analyze the restore operation, if necessary, or apply those logs up to where the failure occurred.
- For Restore Options in Exchange DAG Cluster configurations, refer to "Suspending Replication in a DAG or Cluster" on page 173.

9. On the Ready to complete page, review the restore requests, and then click **Finish**.
10. Click **OK** when you see the message telling you that your restore was successfully initiated.
11. Monitor the restore's progress in the Recent Tasks pane.

Suspending Replication in a DAG or Cluster

The VDP Appliance automatically suspends replication from active databases or storage groups to passive databases or storage groups during a restore when you select the **Automate replication suspension** checkbox during a restore.

You also can manually suspend replication to the passive databases or storage groups by using the Exchange Management Shell before you perform the restore.

Procedure

In Exchange Server 2013 or 2010, type the following command in the Exchange Management Shell on any server in the DAG to manually suspend replication to passive databases or storage groups before a restore:

```
suspend-MailboxDatabaseCopy -Identity database\I
```

where *`database`* is the name of the database and *`server`* is the name of the DAG server with the passive copy.

Monitoring Client Activity

You can monitor tasks and events for all the client activity by collecting and analyzing the client logs. The client logs are Microsoft application (MSApp)-related logs. The aggregated client log includes any replication, backup, restore, or automatic backup verification (ABV) job that passed with exceptions or failed. For more information, refer to "Collecting Logs" on page 44.

Uninstalling the Exchange Server Plug-in

To uninstall the Exchange Server plug-in, use **Programs and Features**.

The Exchange Server GLR plug-in uninstalls automatically when you uninstall the Exchange Server plug-in. You must restart the computer after you uninstall the Exchange Server plug-in.

Granular Level Recovery on Microsoft Exchange Servers

The VDP Plug-in for Exchange Granular Level Recovery (GLR) mounts a temporary virtual drive on the target server and restores an Exchange Server database or storage group from a backup to a Recovery Database (RDB) or Recovery Storage Group (RSG) on the virtual drive.

Note the following:

- GLR in VDP supports recovery at the mailbox level only. GLR is not supported at the individual item level.
- The backup must be a full backup with the VMware VDP Exchange Server plug-in.
- You can perform GLR operations on backups that contain public folder databases, but you cannot use GLR to browse or restore from the public folder database itself.

GLR System Requirements

The GLR process with the VDP Plug-in for Exchange Server GLR places additional demands on computer hardware and resources beyond the base requirements for backup and restore. Table 17-4 describes the system requirements for the VDP Plug-in for Exchange Server GLR.

Table 17-4. GLR System Requirements

Requirement	Minimum
Memory (RAM)	The VDP Plug-in for Exchange Server GLR requires additional memory (RAM). Start with 1 GB of RAM. The required amount of additional or total memory depends on current system performance with existing memory: ■ If resources are already strained and performance is slow with regular operations of the VDP Plug-in for Exchange Server VSS, add significantly more memory to support VDP Plug-in for Exchange Server GLR operations. ■ If performance is currently adequate with regular operations of the VDP Plug-in for Exchange Server VSS, additional memory may not be required to support VDP Plug-in for Exchange Server GLR operations.
Hard drive space	Additional disk space is required to provide a disk staging area to hold writes to the Exchange Server database and log files.

NOTE You also must download the latest MAPI client libraries and CDO 1.2.1 from the Microsoft website, and install the libraries and CDO on each Exchange Server with the Exchange Server GLR plug-in. Some features might not work unless you have the latest versions.

Multi-Streaming Requirements

Multi-streaming places additional demands on computer hardware and resources beyond the base requirements for the VDP Plug-in for Exchange Server VSS. In addition, there are several configuration recommendations for multi-streaming.

Table 17-5 lists hardware and software recommendations for multi-streaming.

Table 17-5. Multi-Streaming Requirements

Hardware and Software	Recommendations
CPU	At least one processor core per stream
Memory (RAM)	48 GB or more

Table 17-5. Multi-Streaming Requirements (Continued)

Hardware and Software	Recommendations
Hard disk	1 disk drive for operating system/Exchange Server installation 1 to 2 disk drives or RAID drive group for each Exchange Server database 7200 RPM or faster disk drives
Network adapter	1 GB
Operating system	Windows Server 2008 SP2 or later

Multi-Streaming Exchange Server Configuration Requirements

VDP consumes significantly more CPU during backups with multi-streaming. This additional CPU consumption on an active Exchange Server can impact performance and affect end users.

Ensure that the Exchange Server environment meets the following requirements for multi-streaming:

- Locate each database on a separate physical disk. If possible, locate the database file on one disk and the transaction logs on a separate disk for each database.
- Best results occur when each database or storage group is approximately the same size.

When you specify multi-streaming options for a backup, specify a maximum of one backup stream for each disk in the backup set. For example:

- If you are backing up two databases, with each database on its own disk, specify a maximum of two streams.
- If you are backing up two databases, with each database and its logs on two disks (for a total of four disks), specify a maximum of four streams.

VSS Requirements

The VDP Plug-in for Exchange Server VSS uses Microsoft Volume Shadow Copy Service (VSS) technology to perform backups. VSS is a framework that enables performance of volume backups while applications on a system continue to write to the volumes.

Supported VSS Providers and Writers

The Exchange Server VSS plug-in uses the Microsoft Software Shadow Copy Provider and the following VSS writers:

- Microsoft Exchange Server Store VSS Writer
- Microsoft Exchange Server Replication VSS Writer

The Exchange Server VSS plug-in does not support hardware providers.

VSS Snapshot Volume Requirements

The Microsoft VSS framework supports as many as 64 volumes in a VSS snapshot. When you create a dataset or perform an on-demand backup, do not include more than 64 volumes. If you include more than 64 volumes in a snapshot, backup fails and the event log lists the following error:

```
VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED.
```

The VSS framework also limits the number of shadow copies to 64 per volume. If the number of shadow copies in a volume exceeds 64, backup fails and the event log lists the following error:

```
VSS_E_MAXIMUM_NUMBER_OF_SNAPSHOTS_REACHED.
```

Enabling GLR Log Files before you Perform GLR

GLR log files enable you to trace and debug granular level restore. Perform the following steps to enable the GLR log files:

1. Use a text editor to create the command file in the `C:\Program Files\avp\var` folder, where `C:\Program Files\avp` is the installation folder.
2. Save and close the command file.

Table 17-6 lists the VDP log files that you can enable to trace and debug GLR.

Table 17-6. VDP Log Files

Log File	Contents	Flag to Enable Debugging	Command File for Flags

`Axionfs.log`	Trace and debugging information for AvFS file system calls.	`--debug`
		`x19=327680`
			`axionfs.cmd`

`avmapi.log`	Trace and debugging information for MAPI calls.	`--debug`	`avmapi.cmd`
`avexglr_plugin.log`	Trace and debugging information for RDB and RSG creation, mount, browse, and restore.	`--debug`	`avexchglr.cmd`
`Aveexchglrsvc.log`	Trace and debugging information for RDB and RSG creation, mount, browse, and restore.	`--debug`	`aveexchglrsvc.cmd`
`ps_exec.log`	Trace and debugging information for execution of PowerShell commands on the Exchange Server client.	`--debug`	`ps_exec.cmd`

Backing Up Exchange Server Databases

For instructions on how to back up Exchange Server databases, refer to "Backing up Applications" on page 160.

Restoring Individual Mailboxes

NOTE You must manually delete all RDBs on the target Exchange Server (2010 or 2013) before performing granular level recovery. The GLR process automatically deletes RSGs on target Exchange Server 2007 servers.

After you have backed up individual mailboxes, you can browse and extract individual mailboxes from the database to restore. The selected items restore from the VDP Appliance to a Recovered Items folder in the original mailbox. You can then browse and select the items to keep. For instructions on how to restore a backup at the granular level, refer to "Restoring Backups of Microsoft Exchange Servers" on page 172.

The virtual drive automatically dismounts and the RDB or RSG is deleted from the target server for GLR after the restore completes. Exchange Server 2007 is automatically deleted. For Exchange Servers 2010 and 2013, you must automatically delete before you perform GLR.

Procedure

1. In the vSphere Web Client, select the **Restore** tab.
2. Select the backup to restore and click the **Restore** icon to start the Restore backup wizard.

   The Select backup page appears.
3. Click the client whose backup you want to restore.
4. Click the backup that you want to restore.

5 Select to restore at any level in the hierarchy. The restore is considered GLR if the restore targets are at the mailbox level.

- For Microsoft Exchange 2007 servers, the backup hierarchy is as follows:

  Exchange server name - > Backup date - > Exchange Information Store - > Storage groups - > Databases - > Mailboxes.

- For Microsoft Exchange 2010 or 2013 servers, the backup hierarchy is as follows:

  Exchange server name - > Backup date - > Exchange Information Store - > Databases - > Mailboxes.

6 Once all the targets have been selected, click the **Restore** button.

NOTE If the client is running as a local system account, the user must provide Exchange Administrator credentials. If the client is not running as a local system account, credentials are not required.

7 On the Ready to complete page, review the restore requests, and then click **Finish**.

8 Click **OK** when you see the message telling you that your restore was successfully initiated.

9 Monitor the restore's progress in the Recent Tasks pane.

Backing Up and Restoring Microsoft SharePoint Servers

VDP supports the backup and restore of Microsoft SharePoint Servers. Only one SharePoint Server system per farm is currently supported.

NOTE Restoring only the SharePoint Server Configuration or Administrator's database can corrupt the SharePoint Server application. Therefore, if you are not restoring only content databases, you must restore the entire backup.

Hardware Requirements

Table 17-7 lists the hardware requirements for the Microsoft SharePoint Server.

Table 17-7. Hardware Requirements for Microsoft SharePoint Server

Requirement	Minimum
Memory (RAM)	2 GB
File systems	NTFS

Supported Microsoft SharePoint Servers

VDP supports the following versions of Microsoft SharePoint Server:

- SharePoint Server 2007 SP2 or later:
  - Windows Server 2008 R2
  - Windows Server 2008
- SharePoint Server 2010, 2010 SP1:
  - Windows Server 2008 SP2
  - Windows Server 2008 R2
- SharePoint Server 2013:
  - Windows Server 2012
  - Windows Server 2008 R2 SP1 or later

Installing VDP for SharePoint Server Client

Install the VDP client plug-in on each SharePoint Server in the farm. (A SharePoint farm is a collection of SharePoint Servers that work together to provide a set of basic SharePoint Server services that support a single site.)

Limitations

- The SharePoint Server VSS Writer must run with the SharePoint Server Farm Administrator account.

Prerequisites

- The VDP Appliance must be installed and configured as described in "VDP Installation and Configuration" on page 19.
- You must have local administrator privileges to each SharePoint Server.

Procedure

1 On each SharePoint Server client, access the vSphere Web Client:

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

2 On the Credentials page, enter an administrative vCenter username and password and click **Login**.

3 In the vSphere Web Client, select **VDP**.

4 On the Welcome to VDP page, select the VDP Appliance and click **Connect**.

5 Click the **Configuration** tab.

6 Under **Client Downloads**, click **Microsoft SharePoint Server 64 bit**. Depending on your browser, you can save the `.msi` file or run it.

The VMware VDP for SharePoint Server Setup wizard starts.

7 Click **Next**.

8 On the End-User License Agreement page, read the license and if acceptable, click **I accept the terms in the License Agreement** and click **Next**.

9 On the Appliance Registration Information page, type in the IP address or the name of the VDP Appliance that will back up the SharePoint Server. Click **Next**.

10 On the Ready to install VMware VDP for SharePoint Server page, click **Install**.

11 During installation, select whether the server on which you are installing will be the primary back up server (front end) or another member server of the SharePoint Server farm (back end).

NOTE The front-end server can only be installed on one farm server, and it must be a Web front end or an application server.

12 On the Completed the VMware VDP for SharePoint Server Setup Wizard page, click **Finish**.

Creating Backup Jobs for Microsoft SharePoint Servers

After you have installed the VDP for SharePoint Server client, SharePoint VM clients are available for backup.

1 In the vSphere Web Client, click the **Backup** tab.

2 In the **Backup** tab, click **Backup Job Actions**, and then select **New** to start the **Create a new backup job** wizard.

3 On the **Job Type** page of the wizard, select **Applications**. This option backs up the SharePoint Server application running on the virtual machine.

4 Click **Next** and follow the instructions below.

Backing Up Applications

You can only back up the entire SharePoint Server application server. Backing up individual databases is not supported in the current release.

1 On the Data Type page, select **Full Server** and click **Next**.

2 On the Backup Sources page:

   a Click the arrow beside **Microsoft SharePoint Servers(s)** to expand the list.

   b Select the checkbox next to the SharePoint Server that you want to back up.

   c Click **Next**.

3 On the Backup Options page, scroll down, if necessary, to locate the SharePoint Server you have installed as the front end:

   a In the **Farm Administrator Credentials** section, type the administrator **Login ID** and **Login password**.

   b Select the **Enable multi-stream backup** option to allow multiple threads of execution during the backup. Use the slider bar to select the number of streams to use, and then select **Database** or **Volume** in the **Group by** menu.

   c Click **Next**.

4 On the Schedule page, select the backup schedule and start time for the backup job, and then click **Next**.

5 On the Retention Policy page, select an options for how long to retain the backup, and then click **Next**.

6 On the Name page, type a name for the backup job, and then click **Next**.

7 On the Ready to Complete page, verify your selections.

   If the settings are correct, click **Finish**. If the settings are not correct, click **Back** to correct them as needed.

Restoring Backups of Microsoft SharePoint Servers

After you run backups on SharePoint servers, you can restore these backups to their original location or to an alternate location.

1 In the vSphere Web Client, click the **Restore** tab.

2 Select the backup to restore and click the **Restore** icon.

   The Select backup page appears.

3 Select the backup job that you want to restore. While you can select multiple SharePoint Servers, you can only select one restore point for each server. Make (or confirm) the backup jobs for restoration and click **Next**.

4 On the Select Restore Options page, do one of the following.

   - Leave the **Restore to Original Location** option selected (the default setting) to restore the backup to its original location.
   - Clear the **Restore to Original Location** option to restore the backup to an alternate location. Click **Choose** to select a destination and type the full Windows path to the location on the destination where the backup will be restored.

5 To specify advanced options, click the arrow beside **Advanced options** to expand the list. The options are described as follows:

   - **Login ID** — Type the SharePoint Server Administrator's login ID. The format is **DOMAIN\user**.
   - **Login Password** — Type the Farm Administrator's password used to log in to the destination client.
   - **Application Pool** (optional) — For SharePoint Server 2013, type the name of an existing application pool to which the Search Service Application will be restored.

- **Encryption method** — Select an encryption method from the list.
- **Advanced options** (Support Only) — Do not type anything in this box. It is for EMC Support use only.

6 Click **Next**.

7 On the Ready to complete page, verify your selections. If they are correct, click **Finish**. If the settings are not correct, click **Back** to create the correct configuration.

8 Click **OK** when you see the message telling you that your restore was successfully initiated.

9 Monitor the restore's progress in the Recent Tasks pane.

Monitoring Client Activity

You can monitor tasks and events for all the client activity by collecting and analyzing the client logs. The client logs are Microsoft application (MSApp)-related logs. The aggregated client log includes any replication, backup, restore, or automatic backup verification (ABV) job that passed with exceptions or failed. For more information, refer to "Collecting Logs" on page 44.

Uninstalling the VDP Plug-in for SharePoint Server

To uninstall the VDP Plug-in for SharePoint Server on a Windows Server 2008 or Windows Server 2012 installation, use **Programs and Features**.

VDP Disaster Recovery 18

This chapter includes the following topics:

- "Basic Disaster Recovery" on page 182
- "Extended Data Protection" on page 182
- "Best Practices for Archiving the VDP Appliance to Tape" on page 182
- "Exporting the Replication Target" on page 183
- "Configuring Backups for Tape-Out" on page 183
- "Backing Up VDP Replication Target to Tape" on page 183
- "Restoring the VDP Replication Target from Tape to the vCenter" on page 184

Basic Disaster Recovery

VDP is robust in its ability to store and manage backups. In the event of failure, the first course of action is to roll back to a known validated checkpoint (see"Rolling Back an Appliance" on page 46). To recover from a VDP Appliance failure, the following procedure creates backups of the appliance and all of the associated VDP backups for use in disaster recovery.

The following provides guidelines for VDP disaster recovery:

1. Before shutting down the VDP Appliance, verify that no backup or maintenance tasks are running. Depending on the backup method used and how long it takes, schedule your VDP backup during a time when no tasks are scheduled. For example, if your backup window is eight hours and backups only take one hour to complete, you have an additional seven hours before maintenance tasks are schedule. This is an ideal time to shut down and back up the appliance.

2. In the vSphere Client, navigate to the appliance. Perform a **Shut Down Guest OS** action on the virtual machine. 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 a clean shutdown process. See "VDP Shutdown and Startup Procedures" on page 62 for more information.

3. Once you have confirmed that the appliance has been shut down, proceed with your preferred method of protection.

4. Verify that the backup of VDP is complete and that no backup, snapshot, or copy jobs are being performed against VDP.

5. From the vSphere Client, perform a **Power On** operation for the appliance.

Extended Data Protection

To recover from a VDP Appliance failure, protect either the appliance or selective backups by storing backup data outside of the VDP Appliance. VDP supports the ability to replicate backup data to a replication target. For VDP, this replication target can be an Avamar server only. With VDP, the replication target can be an Avamar server or another VDP Appliance.

A possible strategy for long-term retention with VDP is to replicate your backups to a secondary VDP Appliance, shut down that target VDP Appliance, and send the files that make up the target appliance to tape. If there is a need to restore this archived backup data, copy the files that make up the target VDP Appliance back into a vSphere environment, re-register the appliance with the vCenter Server, and perform restores using the VDP plug-in in the vSphere Web Client.

NOTE It is best to only replicate those clients that are needed for long-term retention on tape. Limiting the backups that are replicated reduces the disk consumption on the vCenter and the consumption on tape.

Best Practices for Archiving the VDP Appliance to Tape

When installing another VDP Appliance to serve as a replication target for tape out, configure the replication target using the following guidelines:

- Use the smallest disk size needed for your replication target. The replication target disks are in dependent mode, are thin-provisioned, and are set at 50% capacity.

- Because the replication target is a target for tape out, only dependent disk storage is allowed. You can change the disk storage type to independent persistent when you restore the replication target from tape to the vCenter.

NOTE The term "replication target" refers to the secondary appliance which is the replication target set on the primary VDP Appliance. This replication target is the best target for tape out of the backups.

"Best Practices for Archiving the VDP Appliance to Tape" on page 182 provides instructions.

Exporting the Replication Target

You can export the replication target by moving the replication target to tape, or by creating and then moving an OVF file to other storage.

Moving the Replication Target to Tape

From the perspective of your backup tool, the replication target is a virtual machine.

1. Shut down your replication target by using the **Shut Down Guest OS** action on the virtual machine.
2. Take a snapshot of the replication target.
3. Move the replication target to tape by using the backup tool of your choice.

Creating an OVF File from the Replication Target

You can also use the replication target to create an OVF of the virtual machine, and then you can move that OVF file to other storage. When selecting clone to template, an OVF doubles the storage requirements of the original VM.

1. Shut down your replication target using the **Shut Down Guest OS** action on the virtual machine.
2. Select **Template** and either use the **Clone to Template** action or the **Convert To Template** action.
3. Once complete, move the template to the storage location of your choice, or use the backup tool to move the template to tape or disk.

Configuring Backups for Tape-Out

Prerequisites

- The backup tool is configured with tape libraries and devices for backup and restore operations.
- Media pool and tape volumes are configured for tape-out.
- Backups on the primary VDP Appliance are replicated to the replication target. You can find instructions for replicating backups from the primary VDP Appliance to supported replicated targets in "Creating a Replication Job" on page 136. The **Replication** tab displays a list of the replication jobs that have been created.

Backing Up VDP Replication Target to Tape

Procedure

1. Before shutting down the VDP Appliance, run an integrity check.

   a. From the VDP user interface – **Configuration** tab, click the ⚙▾ icon and select **Run integrity check**.

      A confirmation screen displays, asking if you want perform a manual integrity check.

   b. Click **Yes**.

      A message displays informing you that the integrity check has been initiated.

   c. Click **OK**.

      The VDP Appliance starts the integrity check.

   d. Monitor the Integrity Check progress through Recent Tasks.

2. In the vSphere Client, navigate to the VDP Appliance and perform a **Shut Down Guest OS** action on the virtual machine.

   NOTE If the **Shut Down Guest OS** action is grayed out, navigate to **vCenter** > **Hosts and Clusters**, right-click the VDP Appliance, and select **Power off VM**.

3 Using the vSphere Web Client, ensure that the hardware disk type is set to **Dependent**:

   a From a web browser, access the vSphere Web Client:

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

   b Log in as a user with privileges to edit hardware settings.

   c Click **vCenter > Hosts and Clusters**.

   d In the tree on the left, click the disclosure arrows until the VDP Appliance appears.

   e After the appliance has shut down, right-click the VDP Appliance and choose **Edit Settings**.

   f In the Virtual Hardware table, starting with Hard disk 2, click the disclosure arrow.

   g In the Disk Mode row, click **Dependent**.

4 Using the backup tool of your choice, back up the replication target to tape.

5 Ensure the backup to tape operation completed successfully.

Restoring the VDP Replication Target from Tape to the vCenter

Prerequisites

- The original VDP Appliance from which the backups are deleted from the vCenter.
- The user has VMware privileges to register and create virtual machines.
- Only full image backups are selected to restore from tape to the vCenter.
- Appropriate transport modes (for example, NBD, SAN, or HotAdd) are used for the restore.
- The datastores have sufficient capacity.

Procedure

Using the backup tool, restore the VDP replication target from tape to the vCenter. To perform an image-level recovery of a full virtual machine to the VMware vCenter Server:

1 If you are restoring the VDP replication target to the original VMware vCenter Server, you must first delete the original VDP Appliance from which the backups were replicated:

   a Open the vSphere web client for the vCenter where the VDP was deployed.

   b Navigate to the **Hosts and Clusters** view.

   c Expand until you view the VDP Appliance you want to delete.

   d Make sure the VDP Appliance is powered off.

   e Right-click the original VDP Appliance and select **All vCenter Actions > Delete from Disk**.

   f When prompted to confirm the deletion, click **Yes**.

   g Wait for all tasks related to the virtual machine deletion to complete before proceeding to the next step.

2 Run the backup tool you are using to restore the VDP replication target from tape to the vCenter.

3 Perform a full level restore of the virtual machine by using the instructions specific to the backup tool.

4 After the restore has successfully completed, edit the appliance to make all the data disks Independent-Persistent by using the vSphere Web Client:

   a Log in as a user who has privileges to edit hardware settings.

   b Click **vCenter > Hosts and Clusters**.

   c In the tree on the left, click the disclosure arrows until the VDP Appliance appears.

d After the appliance shuts down, right-click the VDP Appliance and select **Edit Settings**.

e In the Virtual Hardware table, starting with Hard disk 2, click the disclosure arrow.

f In the Disk Mode row, click **Independent - Persistent**.

5 Run a manual integrity check to verify the configuration.

vSphere Data Protection Port Usage

A

vSphere Data Protection (VDP) uses the ports listed in Table A-1.

Table A-1. VDP port usage

Product	Port	Protocol	Source	Destination	Purpose
VDP	22	TCP	User	VDP	Secure Shell (SSH) access for debugging
VDP	53	TCP/UDP	VDP	DNS server	Required for name resolution
VDP	80	TCP	VDP	vCenter	http (for licensing)
VDP	111	TCP/UDP	VDP	vSphere Host	Access to RPC port mapper functionality; only required when backups are stored on a Data Domain system
VDP	443	TCP	VDP	vCenter or SSO	https
VDP	700	TCP	VDP LDAP	Active Directory	Loginmgr tool
VDP	8509	TCP	vCenter	VDP	Tomcat AJP Connector
VDP	8543	TCP	vSphere Web Client	VDP	Redirect for Tomcat
VDP	8580	TCP	vCenter	VDP	VDP Downloader
VDP	9443	TCP	vCenter	VDP	VDP Web Services
VDP	27000	TCP	VDP	vCenter	Licensing communication
Note: VDP requires that port 27000 be open for licensing purposes. Port 27000 is not required for vCenter communication.					
VDP	28001	TCP	MSApp Client	VDP	Client Software
VDP 5.5 and later	29000	TCP	VDP 5.5 and later	Avamar Virtual Edition (AVE) or Avamar storage server	Replication with high SSL encryption

NOTE Refer to Knowledge Base article 2034929 for more information about required ports for VMware VDP 5.*x*.

Minimum Required vCenter User Account Permissions

B

See "User Account Configuration" on page 22 to configure the VDP user or SSO admin user by using the vSphere Web Client. In high-security environments, you can restrict the vCenter user account permissions required to configure and administer the VDP Appliance to all of the following categories:

Alarms

- Create
- Modify

Datastore

- Allocate space
- Browse datastore
- Configure datastore (for VSAN support)
- Low level file operations
- Move datastore
- Remove datastore
- Remove file
- Rename datastore

Extension

- Register extension
- Update extensions

Folder

- Create folder

Global

- Cancel task
- Disable methods
- Enable methods
- Licenses
- Log event
- Manage custom attributes
- Settings

Network

- Assign network
- Configure

Resource

- Assign virtual machine to resource pool

Sessions

- Validate session

Tasks

- Create task
- Update task

Virtual machine > Configuration

- Add existing disk
- Add new disk
- Add or remove device
- Advanced
- Change cpu count
- Change resource
- Disk change tracking
- Disk lease
- Extend virtual disk
- Host usb device
- Memory
- Modify device setting
- Raw device
- Reload from path
- Remove disk
- Rename
- Reset guest information
- Set annotation
- Settings
- Swapfile placement
- Upgrade virtual machine compatibility

Virtual machine > Guest operations

- Guest Operation Modifications
- Guest Operation Program execution
- Guest Operation Queries

Virtual machine > Interaction

- Console interaction
- Device connection
- Guest operating system management by VIX API
- Power off
- Power on
- Reset
- VMware tools install

Virtual machine > Inventory

- Create new
- Register
- Remove
- Unregister

Virtual machine > Provisioning

- Allow disk access
- Allow read-only disk access
- Allow virtual machine download
- Mark as template

Virtual machine > Snapshot management

- Create snapshot
- Remove snapshot
- Revert to snapshot

vApp

- Export
- Import
- vApp application configuration

vSphere Data Protection Troubleshooting

C

This chapter includes the following troubleshooting topics:

- "Troubleshooting VDP Appliance Installation" on page 194
- "Troubleshooting Accessing the VDP Web Client" on page 194
- "Troubleshooting VDP Advanced Licensing" on page 199
- "Troubleshooting VDP Backups" on page 194
- "Troubleshooting VDP Restores" on page 196
- "Troubleshooting VDP Replication Jobs" on page 197
- "Troubleshooting VDP Integrity Check" on page 197
- "Troubleshooting Automatic Backup Verification" on page 197
- "Troubleshooting the Restore Client (File Level Recovery)" on page 198
- "Troubleshooting the VDP Appliance" on page 201
- "Troubleshooting VDP Microsoft Exchange Server" on page 201
- "Troubleshooting VDP Microsoft SQL Server" on page 203
- "Troubleshooting VDP Microsoft SharePoint" on page 203
- "Accessing VDP Knowledge Base Articles" on page 203

Troubleshooting VDP Appliance Installation

If you have problems with the vSphere Data Protection (VDP) Appliance installation:

- Confirm that all of the software meets the minimum software requirements. See "Software Requirements" on page 20 for more information.
- Confirm that the hardware meets the minimum hardware requirements. See "System Requirements" on page 20 for more information.
- Confirm that DNS is properly configured for the VDP Appliance. See "Preinstallation Configuration" on page 21 for more information.

Troubleshooting the Installer Package

To find upgrade-related logs that you can use to troubleshoot, refer to the `avinstaller.log.0` file in the Log Bundler.

Troubleshooting Accessing the VDP Web Client

The following troubleshooting topics describe how to identify and resolve some common issues with managing VDP.

The VDP appliance is not responding. Please try your request again.

If you were previously able to connect to VDP and this message appears, check the following:

- Confirm that the username or password that is used to validate VDP to the vCenter Server has not changed. Only one user account and password are used for VDP validation. This is configured through the VDP Configure utility. See "vCenter Server Registration" on page 45 for additional information.
- Confirm that the network settings for IP and DNS configuration have not changed since the initial VDP installation. See "DNS Configuration" on page 21 for additional information.

Troubleshooting VDP Backups

The following troubleshooting items topics describe how to identify and resolve some common issues with vSphere Data Protection (VDP) backups.

Loading backup job data

This message can appear for a long time (up to five minutes) when a large number of VMs (~100 VMs) are selected for a single backup job. This message can also apply to lock/unlock, refresh, or delete actions for large jobs. This is expected behavior when very large jobs are selected. This message will resolve itself when the action is completed, which can take up to five minutes.

Unable to add client {client name} to the VDP appliance while creating backup job {backupjob name}

This error can occur if there is a duplicate client name on the vApp container or the vSphere 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 VMs cannot be located during Edit of a backup job. This is a known issue.

Backup fails if VDP does not have sufficient datastore capacity

Scheduled backups will fail at 92% complete if there is not sufficient datastore capacity. If the VDP datastore is configured with thin provisioning and maximum capacity has not been reached, add additional storage resources.

Backup fails if VM is enabled with VMware Fault Tolerance

If a VM has fault tolerance enabled, the backup will fail. This is expected behavior. VDP does not support backing up VMs that have Fault Tolerance enabled.

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

When hosts are moved into clusters with the option to retain the resource pools and vApps, the containers are recreated, not copied. As a result, it is no longer the same container even though the name is the same. Validate or re-create 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

Any time an unexpected shutdown occurs, the VDP Appliance uses rollback to the last validated checkpoint. This is expected behavior. See "Rolling Back an Appliance" on page 46 for additional information.

vMotion operations are not allowed during active backup operations

vSphere vMotion is a feature that enables the live migration of running virtual machines from one physical server to another. vMotion operations are not allowed to run on the VDP Appliance during active backup operations. This is expected behavior. Wait until all backup operations have completed before you perform a vMotion operation.

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

When special characters are used in the virtual machine name, datastore, folder, or datacenter names, the `.vmx` file is not included in the backup. The following is a list of the special characters (in the format of character/escape sequence format) that prevent the `.vmx` file from being backed up:

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

Rerun option from the Actions icon, runs backups for all clients, not just for the failed client backups

If one client backup fails in a backup job, and then you use the **Rerun Job** option from the Actions icon on the **Reports** tab to rerun the failed backup, the system runs a backup of all of the clients in the backup job.

To run a backup only for the failed client, select **Backup only out of date source** under **Backup Now** on the **Backup** tab.

Troubleshooting VDP Restores

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

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, the **Restore** tab can be slow to load or refresh. In tests with 100 VMs, this can take up to four and a half minutes.

Disk-level restore does not provide an option to specify target datastores

Disk-level restore to a new location does not provide an option to specify the target datastores for each disk of the virtual machine. Currently, VDP restores all the disks of the virtual machine, including the disks that were skipped during backup, into the specified target datastore.

The workaround is to specify a target datastore that has enough free space to accommodate all the disks of the virtual machine, including the disks that were skipped during backup.

Deleted disks are skipped when restoring to original location

If the target VM no longer has the same disk footprint as the original VM that was backed up (if the disks have been removed or deleted from the VM), performing a ”Restore to original location” operation, after selecting a restore point timestamp in the Restore pane, will silently fail to restore the missing disk of the VM.

The workaround is to restore the disk to its original location after manually adding the missing disk to the VM. Ensure the disk is the same size as it was when the VM was backed up.

If this workaround fails, restore the disk to a new location to create a new VM. When the restore task completes, detach the restored disks from the new VM and attach them to the required VM.

Name conflict when restoring a disk to an existing virtual machine

Restoring a disk to an existing VM might fail because of a name conflict. The conflict occurs when an existing .vmdk disk is present in the same datastore where the new disk is being restored.

To work around this issue, rename or remove existing disks that are causing the name conflict.

No time stamp detail displays for Emergency Restore restore points

When navigating through the restore points in the VDP Configure utility’s **Emergency Restore** tab, the user may see no timestamp detail for the restore points. This issue occurs when the time zone is defined as UTC.

Perform the following steps to change the UTC time zone:

1 Open the VDP Configure UI.

2 From the **Configuration** tab, select **Change time zone**.

3 Select a time zone other than the UTC time zone, and click **Save**.

4 Click **Apply Changes**.

5 After the web services restart, log in to the VDP Configure UI and verify the timestamp.

Troubleshooting VDP Replication Jobs

Last successful and last failed replication information not part of email report

The scheduled and ad hoc email reports that are generated after a replication job completes do not contain information about the last successful replication and the last failed replication in the Replication Jobs Summary.

You cannot obtain information about successful and failed replication jobs from VDP.

Replication job failure errors

If the destination server is in a Normal or Full Access state, the VDP Appliance correctly reports the state of the destination server. If the destination server is in an Admin, Read-Only, or Synchronous state, the VDP Appliance reports a "miscellaneous error" when a replication job fails.

With inaccurate reporting of execution errors, the user cannot determine the state of the destination server.

Replication job progress seems stuck in an incomplete status indefinitely

The VDP task panel delivers a "miscellaneous error" for the replication job and fails to initiate the session with servers for replication. One possible cause of this error is the core management service has stopped running for the target server.

Check the management services and restart the core service if it is not running, and then retry the replication job.

Multiple replication jobs for different VMs created inside a single job run in series and not in parallel

The replication activity for multiple virtual machines should process in parallel. The sequential behavior occurs only when another replication job with the same clients is already running. In this case, the client replication task waits for the already-running replication job to complete.

To work around this issue, you must add the `com.vmware.vdp.option.replicate.maxtreams` property to the `/usr/local/vdr/etc/vdp-options.properties` file. The default value is 1. After you change the default setting when you add or edit the property, the appliance sets the new value as the maximum concurrent number of processes for a replication job.

Troubleshooting VDP Integrity Check

After starting an integrity check there can be a delay of a few seconds before the "VDP: Integrity Check" task shows up in the **Running** tasks tab under Recent Tasks. Similarly, when canceling an integrity check, there can be a delay of several seconds before the task is actually canceled.

In some cases (for example, if the integrity check progress is above 90%), the integrity check may actually complete before being canceled. Even though the integrity check may have completed successfully, the Task Console may still show an error indicating the integrity check was canceled.

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 canceling the job to see if the cancel operation succeeded. If the Integrity Check Status is "Normal," the check was successful. If the status is "Out of Date," the check was canceled.

Troubleshooting Automatic Backup Verification

Automatic Backup Verification job fails after renaming the datastore

This error can occur if you rename or move the destination datastore outside of VDP.

Edit the job and select the renamed or moved destination datastore as the new destination. For instructions, refer to "Editing a Backup Verification Job" on page 124.

One or more ABV jobs fail with a “Failed to create VM” error and leave behind an orphaned VM in the vCenter inventory

ABV has triggered the validation of a restored VM on a host that has an earlier version that is incompatible with the version that was used to create the VM. The fact that this leaves behind an orphaned VM is by design because this is necessary for administrators to properly troubleshoot an issue with restores in this type of situation.

Manually delete or unregister the temporary virtual machines that remain in the vCenter or the datastore inventory.

When an ABV job is canceled, a VDP_VERIFICATION_XXXX VM is left behind on the destination host

You can work around this issue by looking for and manually removing VDP_VERIFICATION_* virtual machines left over on the destination host after an ABV job cancellation.

Insufficient space available on datastores for the requested actions

ABV jobs or scheduled jobs fail, sometimes with actual data loss, with error messages in the logs to the effect that datastore actions could not be completed because of insufficient space.

Free up space on datastores and retry the ABV job that failed. Perform ongoing routine space management on datastores to prevent running out of space, especially before scheduled jobs affecting datastore space usage.

Troubleshooting the Restore Client (File Level Recovery)

The following troubleshooting items provide some direction on how to identify and resolve some common issues with the restore client.

Login failed. Cannot locate vm at *10.100.1.10* in vCenter.

This error can occur if you are trying to connect to the Restore Client from a host that has not been backed up by VDP.

Log in to a virtual machine that has been backed up by VDP, and then connect to the Restore Client.

Login failed. Cannot locate vm in vCenter

When you log in to the source virtual machine after you perform a file level restore, the login fails with the following error:

```
Login failed. Cannot locate vm in vCenter
```

This error can occur when you restore a VM image to a new virtual machine without a NIC attached. In this case, the FLR is unable to log in to the source virtual machine for a short period of time after the restore completes. To work around this issue, wait a few minutes after the restore completes before you log in to the source virtual machine.

Restore operation fails with error code *10007*

If a restore operation fails with error code 1007, “Activity Failed - client error(s)” it may be because you selected a read-only destination (for example, a CD drive) or a removable media device that has no media loaded (for example, a diskette drive).

Try the restore again using a new destination or ensure your destination device is writable.

During a file level recovery mount, only the last partition is displayed if the VMDK file contains multiple partitions.

The restore client does not support extended volumes. This is expected behavior. Perform an image-level recovery and manually copy the files needed.

During an file level recovery mount, unsupported partitions fail to mount.

The following disk formats are not supported by the restore client, and it is expected behavior that the restore client mount will fail.

- Unformatted disk
- FAT16 or FAT32 file systems
- Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)
- Dynamic disks (Windows) / multi-drive partitions (any partition that consists of 2 or more virtual disks)
- Deduplicated NTFS
- Resilient File System (ReFS)
- EFI bootloader
- Encrypted partitions
- Compressed partitions

Perform an image-level restore and manually copy the files needed.

Symbolic links are not displayed in the restore client.

The restore client does not support browsing symbolic links.

After importing VMs, FLR login fails for VMs backed up before the import

File Level Recovery (FLR) is not supported for the restore points that have been imported from previously-used VDP disks. This limitation does not apply to restore points that are created for any subsequent backups performed after the import.

Nested container limitations

When restoring a VMware container that contains other containers (that is, a nested container structure; for example vApp-1 contains several virtual machines, and nested inside vApp-1 is a container called vApp-2, which also contains several virtual machines), the VDP Appliance only restores the top-level of the hierarchy. Two interim solutions exist for this limitation:

- Flatten the container structure.
- Add both v-Apps (vApp-1 and vApp-2) as separate container entities so that they can be backed up separately. When restoring, restore vApp-1 first, and then restore vApp-2 into vApp-1.

Troubleshooting VDP Advanced Licensing

License keys entered into vSphere Licensing interface but not visible in VDP

VDP Advanced license keys should not be entered into the standard VMware Licensing user interface. They are valid VMware keys and can be entered and decoded, but are not managed with this interface. Instead you must enter and assign these license keys by using the **Configuration** tab in the VDP interface. Entering them directly into vSphere will not cause any harm but will not provide any utility either. It is recommended that you remove them and assign them.

License violation events are generated even though Host is licensed

When licensing hosts in a cluster, all hosts in the cluster must be licensed. Otherwise, all hosts will be considered in violation of the license agreement. Due to the nature of clusters, there is no way to tell which host a VM belongs to at any given time. Therefore the entire cluster must be covered by valid licenses. It is the administrator’s responsibility to assign license keys appropriately.

License Keys and/or Host assignments are lost

The license keys, and their respective Host assignment, are stored in vCenter and are associated with the `com.vware.vdp2.config` extension. If this extension is unregistered for any reason, the VDP Advanced license keys and Host assignment will also be removed.

Alternatively, if you have redirected your VDP Appliance to another vCenter, it will then display the license keys and Host assignments for the new vCenter and not the old one. There is no cross-vCenter coordination of license keys. Any other VDP Appliances on the old vCenter will continue to show the existing license keys and Host assignments.

To recover from either scenario, simply restart the web services on one of the VDP Appliances. After they have restarted, re-enter the appropriate keys and Host assignments using the VDP interface. Ensure that you are complying with the legal requirements of the license by not reusing license keys in multiple vCenter environments.

Unable to successfully decode license keys

VDP Advanced license keys are decoded and verified prior to persisting them. If this is failing, make sure you entered the appropriate license key value and that there is no extra white space surrounding the key. This can easily happen when copying and pasting the value.

If the license key value is correct (as provided by VMware) then it is possible the license definition file was not successfully uploaded to the vCenter. Restarting the web services on the appliance will again push the license definition file to vCenter, which may resolve the problem.

Unable to obtain licenses in License Assignment portlet

If the License Assignment portlet on the **Configuration** tab in VDP Advanced continuously displays the "Loading…" message, review the following possible causes:

- If you have modified the default HTTP port (80) on the vCenter, you will need to modify the `com.vmware.vdp.option.vcenter.http_port` property in the `/usr/local/vdr/etc/vdp-options.properties` file on the VDP Appliance to specify the new port value. Restart the web services on the VDP Appliance to allow the value to take effect.
- The connection infrastructure used for managing the license keys is missing or corrupt. Restarting the web services on the appliance will attempt to reload any missing components and may correct the issue.

Evaluation license expires and system is degraded (unusable)

By design, the VDP Appliance shuts down integral services whenever license requirements are not met. This can happen when an evaluation license expires.

Do not use an evaluation appliance for any mission critical data. It is intended only as an opportunity to experiment with the VDP Advanced Appliance, and the appliance should be considered throw-away.

If, however, you have since purchased a permanent (non-evaluation) vSphere Data Protection license key, there is a mechanism for recovering the appliance. You must perform the following steps between the one hour intervals at which the system forcibly disables key services.

1 Manually restart all services by using the VDP Configuration Utility.

2 Access the VDP Appliance from the vSphere Web Client.

  a Navigate to the License Assignment portlet on the **Configuration** tab.

  b Add the new permanent license key to the system.

This process upgrades the status of the appliance to permanent and the services should remain operational.

NOTE If you have multiple evaluation appliances that need to be recovered in this manner, you must repeat the process above on each appliance. You can simply remove and then re-add the permanent license key to force the update.

Alternatively, you can install the license key once and wait 24 hours for the license audit to run. The license audit process detects the presence of the permanent license key and upgrades the appliance from its evaluation license key. You must manually restart the services by using the VDP Configuration Utility.

Troubleshooting the VDP Appliance

The following are known issues for the VDP Appliance.

The VMware VDP for Exchange Server Clients or the VMware VDP for SQL Server Clients are no longer registered with the VDP Appliance.

This problem can occur if the VDP Appliance has been renamed, or if the clients were installed and a new checkpoint was not created, and a rollback occurred. To work around this problem, reinstall all of the VDP SQL Server and Exchange Server Clients.

If a Backup Job contains more than one SQL Server or Exchange Server and the servers have identical database paths, if you select a database in one server instance, and not the other instance with the same path, the second instance with the same path will also be backed up.

To resolve this issue, either include only one Exchange Server or SQL Server per backup job or ensure that all of your database paths are unique.

One or more clients cannot be restored. The client is inactive and there are no comparable clients to which a restore can be made.

This problem can occur if a user attempts to invoke the restore wizard without selecting a restore point, or a restore point exists for an unregistered client. In either case, the restore cannot occur when there is an inactive client and no comparable target client exists in the environment.

VDP Appliance Guest OS (Linux) becomes read only

The Linux guest operating system becomes read-only if all of the following symptoms appear:

1 Fails to contact or check the status of services, as shown in the following message:

```
root@ldummyxxx:/usr/local/#: dpnctl status
/bin/chown: changing ownership of `/usr/local/avamar/var/log': Read-only file system
dpnctl: ERROR: running as user "root" - problem opening log file "/usr/local/avamar/var/log/dpnctl.log" (-rw-rw-r--) -
dpnctl: ERROR: traceback on exit:
dpnctl_util: pen_log_file (/usr/local/avamar/bin/dpnctl line YYY)
```

2 Unable to log in to the VDP-Configure UI.

3 Unable to connect to the VDP plug-in from within the vCenter Server web client.

The following VMware Knowledgebase article provides more information about file systems that may become read-only: http://kb.vmware.com/kb/51306

Before you contact Technical Support, restart the appliance. This might fix the problem.

Troubleshooting VDP Microsoft Exchange Server

Unmounted or offline databases are skipped

If a database is unmounted or offline when a backup is performed, the backup skips that database. Generally, this is not an issue because databases that are not mounted are not in production.

Backups may fail when drive letters and volumes are mixed

If you configure the Exchange Server to point to the same database files through different paths, such as volume `G:\` and `C:\MOUNTPOINT`, then backups may fail.

To avoid this backup failure, configure the Exchange Server databases to point to the database files by using the same path. For example, if you have three databases, DB1, DB2, and DB3, that are at the same location as either drive `G:\` or on `C:\`*`mountpoint`*, then use one, but not both, of the following example paths:

- `G:\DB1,G:\DB2,G:\DB3`
- `C:\`*`mountpoint`*`\DB1,C:\`*`mountpoint`*`\DB2,C:\`*`mountpoint`*`\DB3`

Restore to RDB fails or results in an unusable RDB

VDP uses wait times that Microsoft recommends for RDB stabilization in Exchange Server 2013 before the restore starts. The restore either fails or results in an unusable RDB if the stabilization exceeds the wait time. You can increase the wait time to allow more time for the RDB to stabilize.

To increase the RDB stabilization wait time:

1. Use a text editor to create an `avexchglr.cmd` file in the `C:\Program Files\avp\var` folder, where `C:\Program Files\avp` is the installation folder.
2. Type the following text in the command file:

   --rdb_stabilize_wait=*n*

   where *n* is the wait time in seconds. The default value is 60 seconds.
3. Save and close the file.

Restore requirements are not met

When you restore an Exchange Server database, the destination Exchange Server must have the same Exchange Server version and service pack as the Exchange Server where the backup was performed.

If the Exchange Server version on the destination and source servers do not match, then the restore fails.

Log files are moved if gaps are detected

During a normal restore, if a transaction log gap is detected, any existing log files are moved to a folder named logs_TIME_DATE, where TIME and DATE are the time and date of the restore. The folder is created as a subfolder in the transaction log file path of the Exchange Server 2007 storage group or Exchange Server 2010 database. You can use these logs to analyze the restore operation, if necessary, or apply those logs up to when the failure occurred.

Exchange Server 2007 databases are mounted after restore

Before starting a restore, VDP dismounts all databases in a storage group, even if the databases are not being selected for restore. When the restore completes, VDP attempts to mount all existing databases in the storage group, even if they were not previously mounted. VDP does not attempt to mount databases that do not exist on disk, even if they exist in Active Directory.

Selective restore of databases from an older backup may fail

If you attempt to restore selected databases from an older backup when newer backups exist, then the restore may fail. If this occurs, delete the `restore.env` file created in the log folder path, along with all the log files in that path, and rerun the restore. Also, check the event logs through the Event Viewer if mounting one or more databases.

Troubleshooting VDP Microsoft SQL Server

Not all databases are visible on SQL Server 2012

This problem can be fixed by adding the Windows system service account to SQL Server administrator group:

1 In SQL Server Management Studio, expand the Security node and then the login node for the instance.

2 Right-click the NT AUTHORITY\SYSTEM account and select **Properties**.

The Login Properties dialog box appears.

3 Select the **Server Roles** page from the list and select the checkbox next to the sysadmin user.

4 Click **OK**.

A database backup will fail if it is currently being restored

Microsoft SQL Server does not support backups if the database is in a restore state.

A SQL Server restore with the tail-log backup option selected fails

This problem can be caused if the last restore was performed after the last full backup. Perform a full backup on the database before restore.

The restore can also fail if the **Tail-log backup** restore option is enabled and the database does not exist or is offline. In this case disable the **Tail-log backup** option.

Troubleshooting VDP Microsoft SharePoint

SharePoint redirected restore job status shows success even when some databases fail to restore

When an IP address is used instead of a server name, backing up part of a SharePoint farm fails when running a redirected restore, even though the UI indicates success.

Use the server name, not an IP address, when creating an alias for a redirected restore of all or part of a SharePoint farm.

Accessing VDP Knowledge Base Articles

Additional troubleshooting information is available through VDP Knowledge Base Articles, which are located at.

http://www.vmware.com/selfservice/microsites/microsite.do

Select **Products** > **VMware vSphere Data Protection** Category > **Troubleshooting**

Index

A

Adobe Flash Player **20**
alarms, viewing **61**
appliance
  rolling back **46**
archiving to tape **182**
automatic backup verification
  best practices **122**
  described **122**
  troubleshooting **197**
automatic backup verification. *See also backup verification jobs*

B

backup and recovery
  using changed block tracking **14**
  using datastore **14**
  using file level recovery **14**, **148**
  using Virtual Machine Disk (VMDK) **14**
  using VMware vStorage APIs for Data Protection (VADP) **14**
backup job
  full image **114**
  individual disks **114**
  on individual disks **115**
backup schedule **136**
backup verification job
  cloning **125**
  deleting **126**
  disabling **126**
  editing **124**
  monitoring **126**
  running **125**
backup verification jobs
  creating **123**, **126**
  limitations **122**
backup window, editing **58**
backups
  filtering **150**
  increasing number that run **65**
  mounting **150**
  reducing number of concurrent backups **65**
  verifying **126**
best practices
  archiving to tape **182**
  automatic backup verification **122**
  backups **65**
  Data Domain **81**
  deploying proxies **64**
  emergency restore **46**
  general **23**
  HotAdd **24**, **64**, **66**
  proxies **66**
  replication **136**, **140**
  storage capacity for initial VDP deployment **24**
  supported disk types **20**, **116**
  upgrading **32**
  VDP Appliance deployment **65**

C

capacity
  insufficient for backups **194**
  monitoring **24**
  requirements **20**
  steady state **24**
  utilization **76**
  VDP, initial deployment **24**
Certificate Authority (CA) **52**, **53**
Changed Block Tracking (CBT) **14**, **16**, **23**
collecting logs **44**
compatibility matrix
  replication recovery **142**
  replication source **134**
concurrent backups **65**
configuring Data Domain storage **80**
CPU load **69**
customer experience improvement program **17**, **56**

D

Data Domain
  adding a system to VDP configuration **86**
  architecture overview **80**
  backups with VDP **90**
  best practices **81**
  capacity monitoring **95**
  changing the max streams value **87**
  client support with VDP integration **81**
  common problems and solutions **96**
  configuration **80**
  deleting from VDP appliance **88**
  editing system configuration settings **87**
  limitations in VDP environment **82**

- monitoring from the VDP Appliance **94**
- port usage requirements for VDP communication **84**
- pre-integration requirements **82**
- preparing the system for VDP integration **85**
- reclaiming storage on a full system **95**
- selecting a target for backups **91**
- server maintenance activity monitoring **92**

data protection
- using changed block tracking (CBT) **14**
- using datastore **14**
- using File Level Recovery (FLR) **14**, **148**
- using Virtual Machine Disk (VMDK) **14**
- using VMware vStorage APIs for Data Protection (VADP) **14**

deduplication, benefits of **15**

direct to host restore **47**

disaster recovery **182**

disk expansion
- growing and adding disks **101**
- limitation **102**
- requirements **100**
- with Essentials Plus **103**

disk usage **69**

disks, types supported by VDP **20**, **116**

Distributed Resource Scheduler (DRS) **68**

DNS configuration
- setting up **21**
- verifying **21**

E

email reports **57**, **58**

emergency restore
- automatic host detection **49**
- best practices **46**
- limitations **47**
- performing **47**
- troubleshooting restore points **196**
- unsupported features **47**

Essential Plus license **100**

ESXi compatibility with vSphere Flash Read Cache **20**

event console, viewing **62**

F

File Level Recovery (FLR)
- benefits **17**
- limitations **67**, **148**
- overview **14**, **148**
- requirement **64**
- support **66**
- unsupported VMDK configurations **148**

filtering backups **150**

fixed-length data segment **15**

G

granular level restore (GLR)
- log files **176**
- Microsoft Exchange 2007 servers **177**
- Microsoft Exchange 2010 or 2013 servers **177**
- troubleshooting **176**

H

hardware versions
- migrating **20**
- upgrading **20**

HotAdd **20**, **24**, **64**, **66**, **68**, **148**, **184**

I

image-level backups **16**

individual disk backups
- procedure **116**
- supported disk types **116**

individual disks
- creating a backup job **16**, **115**
- impact when migrating **117**

installation requirements **20**

installing vSphere Data Protection (VDP)
- software requirements **20**

integrity checks, running **60**

internal proxy, disabling **68**

J

job details tab **109**

K

knowledge base, accessing articles **203**

L

license audit **200**

license key
- permanent **200**
- requirement **15**

licensing
- Essential Plus **100**
- troubleshooting **199**
- troubleshooting evaluation license expiration **200**
- troubleshooting inability to obtain license **200**
- troubleshooting license key decoding **200**
- troubleshooting license keys **199**
- troubleshooting lost assignments **200**

log bundle, file name of **44**, **194**

log collection **44**

Logical Volume Manager (LVM) **64**, **148**

logs
- bundle **44**, **194**
- collection **44**
- proxy **69**
- viewing **59**

M

man-in-the-middle attacks **52**, **53**
master boot record **148**
media pool **183**
memory usage **69**
Microsoft Exchange
- backing up applications **170**
- creating backup jobs **170**
- increasing RDB wait time **202**
- installing clients when UAC is enabled **154**
- installing the client **165**
- manually configuring the backup service **170**
- restoring backups **172**
- server options **164**
- using the configuration tool **168**

Microsoft SharePoint
- backing up and restoring servers **177**
- creating backup jobs **178**
- restoring backups **179**

Microsoft SQL
- backing up and restoring **155**
- backing up applications **160**
- creating backup jobs **160**
- installing the client **156**
- restoring backups **163**
- server options **155**
- server support **155**

monitoring
- backup verification jobs **126**
- capacity **24**
- Data Domain capacity **95**
- Data Domain from VDP Appliance **94**
- Data Domain maintenance activity **92**
- VDP activity **60**

mount limitations **150**
mounting backups **150**
multi-tenancy, support for **144**

N

network address translation (NAT) **148**
network block device (NBD) **20**, **24**, **66**, **184**
network settings, configuring **45**
node structure, replication **142**
NTFS **149**, **177**, **199**

O

OVF template file **26**, **183**
OVF template file, deploying **25**

P

performance analysis
- running **103**
- test results **103**

platform product support **16**
port 29000 **143**
provision type **72**
proxies
- adding **68**
- best practices **66**
- deploying **64**
- external support **66**
- health status **69**
- internal, disabling **68**
- managing **66**

proxy logs **69**
proxy software, upgrading **38**

R

replication
- back to source **141**
- best practices **136**, **140**
- cloning a job **141**
- creating a job **137**
- creating OVF file **183**
- Data Domain as backup target **136**
- deleting a job **141**
- destinations **142**
- editing a job **140**
- enabling or disabling a job **141**
- exporting to tape **183**
- limitations **136**
- managing destinations **140**
- moving target to tape **183**
- node structure **142**
- recovery **143**
- restoring target from tape **184**
- running existing jobs immediately **141**
- scheduling and managing jobs **17**, **134**
- selecting backups to replicate **137**
- viewing job status and details **141**

Replication Target Identity (RTI) **134**, **143**
reports tab
- viewing Data Domain status **87**
- viewing information **108**

restore
- replication target from tape **184**
- to read-only media **198**
- to removable media **198**

restore points, refreshing **49**

restoring backups
- direct to host **47**
- manually **128**, **130**, **131**
- to new location **129**, **130**, **131**
- to original location **129**, **130**, **131**
- to SCSI disk ID **129**, **130**, **131**
- when snapshots are present **128**

retention policy **115**, **136**
reverting to a snapshot **37**
rolling back an appliance **46**

S

SAN **184**
security
- Certificate Authority (CA) **52**, **53**
- login attempts **56**
- man-in-the-middle attacks **52**, **53**
- SSL certificates **52**, **53**

services
- backup scheduler **42**
- core services **42**
- file level restore services **42**
- file system services **42**
- maintenance services **42**
- management services **42**
- starting and stopping **43**
- status of **43**

show completed activities **152**
shutting down VDP Appliance **62**
snapshot
- removing **36**
- reverting to **37**

software requirements **20**
SSL certificates **52**, **53**
SSO admin user **22**
starting VDP Appliance **62**
steady state capacity **24**
storage
- attaching existing VDP disks **73**
- creating **72**
- detaching **75**
- import existing **72**
- summary **57**
- viewing summary **76**

storage summary, viewing **102**
supported disk types **20**, **116**

T

tape libraries **183**
tape volume **183**
tape-out **183**
task failure tab **108**
tasks, viewing **61**
technical support resources **12**
time synchronization errors **22**
troubleshooting
- after an unexpected shutdown, recent backups are lost **195**
- associated backup sources may be lost **195**
- automatic backup verification (ABV) **197**
- backup fails if VM is enabled with VMware fault tolerance **195**
- backup fails if vSphere Data Protection does not have sufficient datastore capacity **194**
- backups are slow to load **196**
- backups fail if certain characters are used **195**
- decoding license keys **200**
- file level recovery **198**, **199**
- granular level restores **176**
- guest OS (Linux) becomes read-only **201**
- inability to obtain license in portlet **200**
- items could not be located **194**
- license keys **199**
- license violation events **199**
- loading backup job data **194**
- lost license keys **200**
- Microsoft Exchange RDB wait time **202**
- name conflicts when restoring a disk to an existing VM **196**
- replication job failure errors **197**
- replication jobs **197**
- restore operation fails **198**
- unable to add client **194**
- VDP Advanced **201**
- VDP Appliance is not responding **194**
- VDP Exchange backups **201**
- VDP SQL backups **203**
- VDP SQL restores **203**
- vSphere Data Protection Exchange restores **202**
- vSphere Data Protection integrity check **197**

U

upgrading
- best practices **32**
- hardware versions **20**

V

variable-length data segment **15**
vCenter
- user account permissions **189**

vCenter Server
- changing hostname, password, and so forth **45**
- supported versions **25**
- switching VDP Appliances **107**
- version requirements **20**

vCenter Server Appliance (VCSA) **16**, **52**

VDP Advanced licensing, troubleshooting **199**
VDP Configure Utility **42**
VDP disks
  attaching **73**
VDP, types of disks not supported **20**, **116**
viewing
  alarms **61**
  event console **62**
  storage summary **76**, **102**
  tasks **61**
Virtual Machine Disk (VMDK) **14**
VMFS heap size **100**
VMware Tools **22**, **123**
VMware vStorage APIs for Data Protection (VADP) **14**
vSphere Data Protection (VDP)
  accessing from command line **106**
  accessing knowledge base articles **203**
  accessing with vSphere Web Client **106**
  changing a configuration **45**
  collecting logs **44**
  disaster recovery **182**
  installation **27**
  monitoring activity **60**
  sizing **20**
  software requirements **20**
  starting and stopping services **43**
  storage capacity **24**
  supported configurations **21**
  user interface **108**
  viewing status of services **42**
vSphere Data Protection (VDP) Appliance
  best practices when deploying **65**
  corruption **75**
  description of **14**
  rolling back an appliance **46**
  shutdown **62**
  startup **62**
  switching from vCenter Server **107**
vSphere Flash Read Cache and ESXi compatibility **20**
vSphere HA **72**
vSphere host, supported versions **20**
vSphere Web Client **107**
  Adobe Flash Player requirement **20**
  supported web browser **20**