# Contents

## 1 Understanding VDP 11
- Introduction to VMware vSphere Data Protection 12
- Benefits of vSphere Data Protection 12
- VDP and VDP Advanced Functionality 13
  - Image-level Backup and Restore 13
  - Single VMDK Backup and Restore 14
  - Guest-level Backup and Restore 14
- Replication 14
- File Level Recovery 14
- Deduplication Store Benefits 14
  - Variable vs. Fixed-Length Data Segments 15
  - Logical Segment Determination 15
- vSphere Data Protection Architecture 15

## 2 VDP Installation and Configuration 17
- vSphere Data Protection Sizing 18
- Software Requirements 18
  - Hardware Versions and Migration 18
  - ESXi Hosts and vFlash Compatibility 18
  - Supported Disk Types 18
- System Requirements 19
  - VDP Advanced System Requirements 19
- Preinstallation Configuration 20
  - DNS Configuration 20
  - NTP Configuration 20
  - vCenter Configuration Views 20
  - User Account Configuration 21
- VDP Best Practices 22
  - General Best Practices 22
  - HotAdd Best Practices 22
  - Storage capacity for initial VDP deployment 23
  - Monitoring VDP capacity 23
  - Integrity checks 24
- VDP Installation 24
  - Deploying the OVF Template 24
- Licensing 25
  - Adding a License Key 25
  - Upgrading from VDP to VDP Advanced 26
  - Viewing VDP Advanced License Information 26
  - Unassigning the License 26
  - Removing a License Key 27
- System Setting Configuration 27
  - Switching the VDP Appliance to a New vCenter 28

## 3 VDP Appliance Upgrades 31
- Best Practices 32
3 Allowed Upgrade Paths 32
  Selecting a Time for Upgrading the VDP Appliance 32
  Creating a Snapshot of the VDP Appliance 32
  Mounting the Upgrade ISO Image on the Appliance 33
  Installing the Upgrade 33
  Removing the Snapshot and Unmounting the Upgrade Image 34
  Reverting Back to a Snapshot 35

4 Storage Management 37
  Creating New Storage 38
  Attaching Existing Storage 39
  Detaching and Reattaching Storage 41
  Viewing the Storage Configuration 42
  Data Domain Configuration 42
    Adding a Data Domain System 43
    Editing Data Domain 44
    Deleting Data Domain 44

5 vSphere Data Protection Disk Expansion 45
  Pre-Expansion Requirements 46
  VMFS Heap Size Recommendations 46
  Performing Disk Expansion 47
    Viewing the storage configuration 48
  Performance Analysis 49
    Running the Performance Analysis Test 49
  Disk Expansion with Essentials Plus 49

6 Post-Installation Configuration of VDP Appliance 51
  About the VDP Configure Utility 52
  Viewing Status 52
  Starting and Stopping Services 53
  Collecting Logs 54
  Changing VDP Configuration 54
    Network Settings 54
    vCenter Registration 55
    System Settings 55
  Rolling Back an Appliance 55
  Emergency Restore 56
    Refreshing Restore Points 58
    Reconnecting the Host to the vCenter 58

7 Using vSphere Data Protection 59
  Accessing vSphere Data Protection 60
  Understanding the VDP User Interface 60
  Switching VDP Appliances 61
  VDP Advanced User Interface 61
  Viewing Information from the Reports Tab 62
    Filtering report information 62

8 Managing Backups 65
  Managing Backup Jobs 66
    Choosing the Virtual Machines 66
    Specifying the Backup Schedule 67
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the Retention Policy</td>
<td>67</td>
</tr>
<tr>
<td>Creating a Full Image Backup Job</td>
<td>68</td>
</tr>
<tr>
<td>Creating a Backup Job on Individual Disks</td>
<td>69</td>
</tr>
<tr>
<td>Viewing Status and Backup Job Details</td>
<td>71</td>
</tr>
<tr>
<td>Editing a Backup Job</td>
<td>71</td>
</tr>
<tr>
<td>Cloning a Backup Job</td>
<td>71</td>
</tr>
<tr>
<td>Deleting a Backup Job</td>
<td>72</td>
</tr>
<tr>
<td>Enabling or Disabling a Backup Job</td>
<td>72</td>
</tr>
<tr>
<td>Running Existing Backup Jobs Immediately</td>
<td>72</td>
</tr>
<tr>
<td>Locking and Unlocking a Backup</td>
<td>73</td>
</tr>
<tr>
<td>9 Automatic Backup Verification</td>
<td>75</td>
</tr>
<tr>
<td>Automatic Backup Verification</td>
<td>76</td>
</tr>
<tr>
<td>Limitations</td>
<td>76</td>
</tr>
<tr>
<td>Best Practices</td>
<td>76</td>
</tr>
<tr>
<td>Creating a New Backup Verification Job</td>
<td>77</td>
</tr>
<tr>
<td>Editing a Backup Verification Job</td>
<td>79</td>
</tr>
<tr>
<td>Cloning a Backup Verification Job</td>
<td>79</td>
</tr>
<tr>
<td>Executing and Running a Backup Verification Job</td>
<td>79</td>
</tr>
<tr>
<td>Monitoring Backup Verification</td>
<td>80</td>
</tr>
<tr>
<td>Enabling and Disabling a Backup Verification Job</td>
<td>80</td>
</tr>
<tr>
<td>Deleting a Backup Verification Job</td>
<td>80</td>
</tr>
<tr>
<td>10 Managing Restores</td>
<td>81</td>
</tr>
<tr>
<td>Managing Restores</td>
<td>82</td>
</tr>
<tr>
<td>Limitations</td>
<td>82</td>
</tr>
<tr>
<td>Selecting Backups to Restore</td>
<td>82</td>
</tr>
<tr>
<td>Filtering for List of Backups</td>
<td>82</td>
</tr>
<tr>
<td>Restores when Snapshots are Present</td>
<td>82</td>
</tr>
<tr>
<td>Restoring Image Backups to Original Location</td>
<td>83</td>
</tr>
<tr>
<td>Restoring Image Backups to New Location</td>
<td>84</td>
</tr>
<tr>
<td>Restoring Backups to Individual SCSI Disks</td>
<td>85</td>
</tr>
<tr>
<td>Deleting a backup from the Restore tab</td>
<td>86</td>
</tr>
<tr>
<td>Clearing all selected backups from the Restore tab</td>
<td>86</td>
</tr>
<tr>
<td>11 Replication</td>
<td>87</td>
</tr>
<tr>
<td>Managing Replication Jobs</td>
<td>88</td>
</tr>
<tr>
<td>Replication Compatibility</td>
<td>88</td>
</tr>
<tr>
<td>Replication and Data Domain</td>
<td>88</td>
</tr>
<tr>
<td>Best Practices when Replicating</td>
<td>88</td>
</tr>
<tr>
<td>Limitation</td>
<td>88</td>
</tr>
<tr>
<td>Defining Backup Types for a Replication Job</td>
<td>88</td>
</tr>
<tr>
<td>Creating a Replication Job</td>
<td>89</td>
</tr>
<tr>
<td>Editing a Replication Job</td>
<td>92</td>
</tr>
<tr>
<td>Cloning a Replication Job</td>
<td>92</td>
</tr>
<tr>
<td>Deleting a Replication Job</td>
<td>92</td>
</tr>
<tr>
<td>Enabling or Disabling a Replication Job</td>
<td>92</td>
</tr>
<tr>
<td>Viewing Status and Replication Job Details</td>
<td>92</td>
</tr>
<tr>
<td>Running Existing Replication Jobs Immediately</td>
<td>92</td>
</tr>
<tr>
<td>12 Configuring VDP Details</td>
<td>93</td>
</tr>
<tr>
<td>Configuration and Monitoring</td>
<td>94</td>
</tr>
<tr>
<td>Viewing Backup Appliance Configuration</td>
<td>94</td>
</tr>
<tr>
<td>Editing the Backup Window</td>
<td>95</td>
</tr>
<tr>
<td>Configuring Email</td>
<td>95</td>
</tr>
</tbody>
</table>
13 VDP Application Support 101
VDP Advanced Application Support 102
  Checking the User Account Control setting on Microsoft Windows 102
  Installing VDP Clients when UAC is Enabled 102
Back Up and Restoring Microsoft SQL Servers 102
  Microsoft SQL Server Options 103
  Hardware Requirements 103
  Microsoft SQL Server Support 103
  Installing the VMware VDP for SQL Server Client 104
  Creating Backup Jobs for Microsoft SQL Servers 105
  Restoring Backups of Microsoft SQL Servers 107
  Monitoring Client Activity 108
  Uninstalling the VDP Advanced Plug-in for SQL Server 108
Back Up and Restoring Microsoft Exchange Servers 108
  Microsoft Exchange Server Options 109
  Microsoft Exchange Server Support 109
  Microsoft .NET Framework 4 requirement 109
  Hardware Requirements 109
  Unsupported Microsoft Exchange Servers 109
  Installing VDP for Exchange Server Client 110
  Using the VDP Exchange Backup User Configuration Tool 110
  Manually Configuring the VDP Backup Service 112
  Creating Backup Jobs for Microsoft Exchange Servers 112
  Restoring Backups of Microsoft Exchange Servers 113
  Monitoring Client Activity 115
  Uninstalling the Exchange plug-in 115
  Granular Level Recovery on Microsoft Exchange Servers 115
Back Up and Restoring Microsoft SharePoint Servers 118
  Hardware Requirements 118
  Supported Microsoft SharePoint Servers 118
  Installing VDP plug-in for SharePoint Server Client 118
  Creating Backup Jobs for Microsoft SharePoint Servers 119
  Restoring Backups of Microsoft SharePoint Servers 120
  Monitoring Client Activity 121
  Uninstalling the VDP Advanced Plug-in for SharePoint 121

14 Using File Level Restore 123
Introduction to the VDP Restore Client 124
  File Level Restore Limitations 124
  LVM Limitations 124
  Unsupported VMDK Configurations 124
  Unsupported Windows configurations 125
Logging In to the Restore Client 125
  Basic Login 125
  Advanced Login 125
Mounting Backups 126
Filtering Backups 126
Navigating Mounted Backups 126
Performing File Level Restores 126
Using the Restore Client in Basic Login Mode 126
Using the Restore Client in Advanced Login Mode 127
Monitoring Restores 128

15 VDP Disaster Recovery 129

A vsphere Data Protection Port Usage 131

B Minimum Required vCenter User Account Permissions 133

C vsphere Data Protection Troubleshooting 137
Troubleshooting VDP Appliance Installation 138
Troubleshooting Accessing the VDP Web Client 138
Troubleshooting VDP Advanced Licensing 138
License keys entered into vsphere Licensing interface but not visible in VDP 138
License violation events are generated even though Host is licensed 138
License Keys and/or Host assignments are lost 138
Unable to successfully decode license keys 139
Unable to obtain licenses in License Assignment portlet 139
Evaluation license expires and system is degraded (unusable) 139
Troubleshooting VDP Backups 140
Troubleshooting VDP Restores 141
Troubleshooting VDP Replication Jobs 142
Troubleshooting VDP Integrity Check 142
Troubleshooting Automatic Backup Verification 142
Troubleshooting the Restore Client (File Level Recovery) 142
Troubleshooting VDP Advanced 143
Troubleshooting VDP Advanced Exchange Backups 143
Troubleshooting VDP Advanced Exchange Restores 144
Troubleshooting VDP Advanced SQL Backups 145
Troubleshooting VDP Advanced SQL Restores 145
Accessing VDP Knowledge Base Articles 145

Index 147
About This Book

The VDP Administration Guide contains information 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 using VDP (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:

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>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)</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Use for full titles of publications referenced in text</td>
</tr>
<tr>
<td><em>Monospace</em></td>
<td>Use for:</td>
</tr>
<tr>
<td></td>
<td>▪ System output, such as an error message or script</td>
</tr>
<tr>
<td></td>
<td>▪ System code</td>
</tr>
<tr>
<td></td>
<td>▪ Pathnames, filenames, prompts, and syntax</td>
</tr>
<tr>
<td></td>
<td>▪ Commands and options</td>
</tr>
<tr>
<td><em>Monospace italic</em></td>
<td>Use for variables</td>
</tr>
<tr>
<td><em>Monospace bold</em></td>
<td>Use for user input</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclosure optional values</td>
</tr>
<tr>
<td></td>
<td>Vertical bar indicates alternate selections — the bar means “or”</td>
</tr>
<tr>
<td>{ }</td>
<td>Braces enclose content that the user must specify, such as x or y or z</td>
</tr>
<tr>
<td>...</td>
<td>Ellipses indicate nonessential information omitted from the example</td>
</tr>
</tbody>
</table>

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.
This chapter includes the following topics:

- “Introduction to VMware vSphere Data Protection” on page 12
- “Benefits of vSphere Data Protection” on page 12
- “Guest-level Backup and Restore” on page 14
- “Replication” on page 14
- “File Level Recovery” on page 14
- “Deduplication Store Benefits” on page 14
- “vSphere Data Protection Architecture” on page 15
Introduction to VMware vSphere Data Protection

vSphere Data Protection (VDP) is a robust, simple to deploy, disk-based backup and recovery solution. 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.

- **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.

- **The VDP Appliance** is a purpose-built virtual appliance for VDP.

Benefits of vSphere Data Protection

The benefits of vSphere Data Protection (VDP) are explained in the following points:

- Provides fast and efficient data protection for all of your virtual machines, even those powered off or migrated between ESX 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 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.
VDP and VDP Advanced Functionality

vSphere Data Protection has two tiers: Basic VDP and VDP Advanced. Table 1-1 defines the differences between VDP and VDP Advanced.

**NOTE** Basic VDP functionality does not require a license key. For VDP Advanced users, after the host is licensed and the system is in VDP Advanced mode, the extended features become available. Once licensed, users are restricted from creating backup jobs containing virtual machines on unlicensed hosts.

<table>
<thead>
<tr>
<th>Feature</th>
<th>VDP</th>
<th>VDP Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machines supported per VDP Appliance</td>
<td>up to 100</td>
<td>up to 400</td>
</tr>
<tr>
<td>Available storage size</td>
<td>2 TB</td>
<td>8 TB</td>
</tr>
<tr>
<td>Support for image-level backups</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for individual disk backups</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for image-level restore jobs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for image-level replication jobs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for direct to host recovery</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for detachable/remountable data partitions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for file level recovery (FLR)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for guest-level backups and restores of Microsoft SQL Servers, Exchange Servers, and SharePoint Servers</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for application-level replication</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Ability to expand current datastore</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for backing up to a Data Domain system</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Ability to restore to a granular level on Microsoft Servers</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for automatic backup verification (ABV)</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Image-level Backup and Restore

vSphere Data Protection creates image-level backups, which are integrated with 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 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 eight virtual machines.

To increase the efficiency of image-level backups, VDP utilizes Avamar’s 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 when recovering virtual machines to their original location. During a restore process, VDP uses Avamar’s deduplication technology to determine which blocks have changed since the last backup, and then only recovers or replaces those blocks during a recovery. This reduces data transfer within the 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 will intelligently decide which method will result in the fastest virtual machine image recovery times for your particular scenario or environment.
Single VMDK Backup and Restore

Whereas 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; for example: by operating system or by retention policy.

See “Creating a Backup Job on Individual Disks” on page 69 for instructions on backing up individual disks.

Guest-level Backup and Restore

vSphere Data Protection Advanced supports guest-level backups for Microsoft SQL, Exchange, and SharePoint 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, Exchange, or SharePoint Servers in the same manner that backup agents are typically installed on physical servers.

The advantages of VMware guest-level backups are:

- Provides a higher level of deduplication than image-level backups
- Provides additional application support for Microsoft SQL, Microsoft Exchange, or SharePoint Servers inside the virtual machines
- Support for backing up and restoring entire Microsoft SQL, Microsoft Exchange, or SharePoint Servers or selected databases
- Ability to support application consistent backups
- Identical backup methods for physical and virtual machines

See “VDP Application Support” on page 101 for additional information on guest-level backup and restore.

Replication

Replication is a feature that enables efficient, encrypted, and asynchronous replication of data stored in an Avamar server to another Avamar server deployed in remote locations (Avamar Virtual Editions). Replication is a scheduled process between two independent Avamar servers, providing a higher level of reliability for stored backups.

Replication jobs can be scheduled to run at off-peak hours to minimize bandwidth impact.

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 using the VDP Restore Client.

See Chapter 14, “Using File Level Restore,” on page 123 for additional information on FLR.

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

vSphere Data Protection (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 data set (all the 0s and 1s that make up a dataset) in order 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 intelligently deduplicates the data.

vSphere Data Protection Architecture

vSphere Data Protection (VDP) uses a vSphere Web Client and a VDP Appliance to store backups to deduplicated storage.

VDP is composed of a set of components that run on different machines (shown in the following diagram).

- vCenter Server
- VDP Appliance (installed on ESX/ESXi 4.0, 4.1, ESXi 5.0, ESXi 5.1)
- vSphere Web Client
VDP Installation and Configuration

This chapter includes the following topics:

- “vSphere Data Protection Sizing” on page 18
- “Software Requirements” on page 18
- “System Requirements” on page 19
- “Preinstallation Configuration” on page 20
- “VDP Best Practices” on page 22
- “VDP Installation” on page 24
- “System Setting Configuration” on page 27
vSphere Data Protection Sizing

vSphere Data Protection (VDP) sizing helps determine the VDP Appliance size and number of appliances required based on:

- Number of and type of virtual machines (do the virtual machines contain file system or database data?)
- Amount of data
- Retention periods (daily, weekly, monthly, yearly)
- Typical change rate

**NOTE** On average you can support up to 25 virtual machines per TB of capacity.

Software Requirements

vSphere Data Protection (VDP) 5.5 requires the following software:

- VMware vCenter Server: Version 5.1 or later

**NOTE** VDP 5.1 is not compatible with vCenter 5.5.

- vCenter Server Linux or Windows
  
  **NOTE**: Backing up more than 2 TB VMs on Windows operating systems is not supported. This limitation does not exist on Linux operating systems.

- vSphere Web Client (see the VMware web site for current vSphere 5.5 web browser support)

- Web browsers must be enabled with Adobe Flash Player 11.3 or higher to access the vSphere Web Client and VDP functionality

- VMware ESX/ESXi (the following versions are supported)

  - ESX/ESXi 4.0, 4.1, ESXi 5.0, ESXi 5.1, ESXi 5.5

Hardware Versions and Migration

The virtual machine's hardware version limits virtual machines that are configured on newer versions of ESX hosts from migrating to older versions, because they are not backward compatible.

If the vSphere Data Protection Appliance were migrated to an ESXi host that was ESXi 5.1 or lower, it would not be functional.

ESXi Hosts and vFlash Compatibility

By default, the vSphere Data Protection appliance is deployed as a virtual machine with hardware version 7, which allows for backward compatibility with ESXi 4.x hosts. The vFlash-backed disks are only available on ESXi 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 vFlash-backed disk 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.

Supported Disk Types

- When planning for backups, make sure the disks are supported by vSphere Data Protection (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 and VDP Advanced.

**NOTE**  VDP can be upgraded to VDP Advanced, but VDP Advanced cannot be reconfigured to VDP.

VDP is available in three configurations:
- 0.5 TB
- 1 TB
- 2 TB

**IMPORTANT**  Once VDP is deployed the size cannot be changed.

VDP requires the following minimum system requirements:

**Table 2-2.** Minimum system requirements for VDP

<table>
<thead>
<tr>
<th></th>
<th>0.5 TB</th>
<th>1 TB</th>
<th>2 TB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Minimum four 2 GHz processors</td>
<td>Minimum four 2 GHz processors</td>
<td>Minimum four 2 GHz processors</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
<td>4 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>873 GB</td>
<td>1,600 GB</td>
<td>3,100 GB</td>
</tr>
</tbody>
</table>

**NOTE**  The additional disk space required that is above the usable capacity of the VDP Appliance is for creating and managing checkpoints.

**VDP Advanced System Requirements**

VDP Advanced is available in the following configurations:
- 0.5 TB
- 1 TB
- 2 TB
- 4 TB
- 6 TB
- 8 TB

**IMPORTANT**  Once VDP Advanced is deployed the size can be increased.

VDP Advanced requires the following minimum system requirements:

**Table 2-3.** Minimum system requirements for VDP Advanced

<table>
<thead>
<tr>
<th></th>
<th>2 TB</th>
<th>4 TB</th>
<th>6 TB</th>
<th>8 TB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Minimum four 2 GHz processors</td>
<td>Minimum four 2 GHz processors</td>
<td>Minimum four 2 GHz processors</td>
<td>Minimum four 2 GHz processors</td>
</tr>
<tr>
<td>Memory</td>
<td>6 GB</td>
<td>8 GB</td>
<td>10 GB</td>
<td>12 GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>3 TB</td>
<td>6 TB</td>
<td>9 TB</td>
<td>12 TB</td>
</tr>
</tbody>
</table>

**NOTE**  The additional disk space required that is above the usable capacity of the appliance is for creating and managing checkpoints.
Preinstallation Configuration

Prior to VDP installation, the following preinstallation steps must be completed:

- “DNS Configuration” on page 20
- “NTP Configuration” on page 20
- “User Account Configuration” on page 21
- “VDP Best Practices” on page 22

DNS Configuration

Before you deploy vSphere Data Protection (VDP), you must add an entry to the DNS Server for the VDP Appliance’s IP address and Fully Qualified Domain Names (FQDN). The DNS server must support both forward and reverse lookup.

**IMPORTANT** Failure to set up DNS properly can cause many runtime or configuration issues. In addition, communication to DNS is required by VMware proxy nodes (port 53) over both TCP and UDP protocols.

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

To verify DNS configuration, open a command prompt and type the following commands:

```
nslookup <VDP_IP_address> <DNS_IP_address>
```

The nslookup command returns the FQDN of the VDP Appliance.

```
nslookup <FQDN_of_VDP> <DNS_IP_address>
```

The nslookup command returns the IP address of the VDP Appliance.

```
nslookup <FQDN_of_vCenter> <DNS_IP_address>
```

The nslookup command returns the IP address of the vCenter Server.

If you have configured short names for the DNS entries, perform additional lookups for the short names.

If the nslookup commands returned the proper information, close the command prompt; if not, resolve the DNS configuration.

NTP Configuration

vSphere Data Protection (VDP) leverages VMware Tools to synchronize time through NTP. All ESXi hosts and the vCenter Server should have NTP configured properly. The VDP Appliance gets the correct time through vSphere and should not be configured with NTP.

**CAUTION** If you configure NTP directly on the VDP Appliance, it will cause time synchronization errors.

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

vCenter Configuration Views

The vSphere Data Protection (VDP) Appliance can work with folders and resource views that are created under the Hosts and Clusters view. Any folder or resource pool created under the VMs and Templates view are not visible to the VDP Appliance.

Hosts and Clusters

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
Chapter 2 VDP Installation and Configuration

- Remove a snapshot
- Revert back to a snapshot
- Expand disks with Essentials Plus

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. Login with administrative privileges.
3. Select vCenter > Hosts and Clusters.

VMs and Templates
The VMs and Templates view in the vSphere Web Client allow you to perform the following tasks:
- Configure the VDP Appliance system settings
- Remove the VDP Appliance from the vCenter inventory

Accessing the VMs and Templates view
1. From a web browser, access the vSphere Web Client.
   https://<IP_address_vCenter_Server>:9443/vsphere-client/
2. Login with administrative privileges.
3. Select vCenter Home > vCenter > VMs and Templates. Expand the vCenter tree and select the VDP Appliance.

User Account Configuration

Before the vCenter user account can be used with vSphere Data Protection (VDP), or before the SSO admin user can be used with VDP, these users should be explicitly added 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 133.

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.
2. Log in with administrative privileges.
3. Select vCenter > Hosts and Clusters.
4. On the left side of the page, click on the vCenter Server. It is important the vCenter be selected from the root level of the tree structure (represented under Hosts and Clusters). If you select the vCenter VM, the configuration will fail.
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 that 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 checked.
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 then it should be used in the format “SYSTEM-DOMAIN\admin” format in VDP-configure. If the user name 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 blank spaces. The VDP Appliance will initially run with this setting using a 60-day evaluation license, but if the VDP Appliance is rebooted after 60 days, the VDP Appliance will fail to restart.

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 higher to avoid block size limitations.
- Make sure that all virtual machines are running hardware version 7 or higher in order to support Change Block Tracking (CBT).
- Install VMware Tools on each virtual machine that VDP will backup. VMware Tools adds additional backup capability that quiesces certain processes on the guest OS prior to backup. VMware Tools are also required for some features used in File Level Restore and Automated Backup Verification (ABV).

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 the Network Block Device (NBD) transport mechanism is used instead of HotAdd, performance is degraded up to 60%.

It is mandatory that all of the following requirements are met for a disk to be mounted with HotAdd:

- If you are using ESXi 4.1 or 5.0, the ESXi hosts are licensed for HotAdd. ESXi 5.1 includes this feature by default.
- The VDP Appliance is deployed on an ESXi host that has a path to the storage holding 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 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.

For more information about HotAdd best practices, refer to the following Knowledge Base article:
http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=2048138&sliceld=1&docTypeID=DT_KB_1_1&dialogID=5733736&stateId=0%200%205745440

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 best leveraged 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 vSphere Data Protection (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 62 for more information.

The following table describes vSphere Data Protection (VDP) behavior for key capacity thresholds:

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

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

- Stop adding new virtual machines as backup clients
- Delete unneeded backup jobs
- Reassess retention policies to see if you can decrease retention policies
- Consider adding additional vSphere Data Protection (VDP) Appliances and balance backup jobs between multiple appliances
Integrity checks

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. Refer to “Running an Integrity Check” on page 96 for instructions.

VDP Installation

vSphere Data Protection (VDP) and VDP Advanced use the same installation process. The installation is completed through two steps:

- “Deploying the OVF Template” on page 24
- “System Setting Configuration” on page 27

Deploying the OVF Template

Prerequisites

- The VDP Appliance requires one of the following ESXi versions: 4.0, 4.1, 5.0, or 5.1.
- vCenter 5.1 or later is required. Log in to vCenter from a vSphere Web Client to deploy the OVF template. Confirm that the vSphere Web Client service is started.
- The VDP Appliance connects to ESXi using port 902. If there is a firewall between the VDP Appliance and ESXi Host, port 902 must be open. See Chapter A, “vSphere Data Protection Port Usage,” on page 131, for additional information on port usage.
- The VMware Client Integration Plug-in 5.5.0 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.
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, enter the name for the VDP Appliance. When entering the name, use the fully qualified domain name (FQDN), which the VDP configuration uses to find the Appliance in the vCenter inventory. The VDP Appliance Name should not be changed after installation.
12. Click on the folder or datacenter in which you want it deployed. 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.

**Licensing**

A VDP Advanced license is required to access additional capabilities and advanced features. For VDP Advanced users, after the host is licensed and the system is in VDP Advanced mode, the extended features become available. Once licensed, users are restricted from creating backup jobs containing virtual machines assigned to unlicensed hosts. Note the following points:

- Each host can have only one VDP Advanced license assigned to it. However, a single license can be assigned to multiple hosts, as long as the sum total CPU count of the hosts is less than or equal to the amount allowed by the license.
- Licenses are not assigned directly to clusters; they are assigned only to hosts. Therefore, ensure that all hosts in the cluster are licensed.
- If you move the VDP Advanced Appliance from the existing vCenter to a new vCenter, you must assign the appropriate VDP Advanced license in the new vCenter environment. You cannot reuse the same license key in the new vCenter. Refer to “Switching the VDP Appliance to a New vCenter” on page 28 for more information.

**NOTE** For more detailed information about VDP Advanced licensing, refer to “Troubleshooting VDP Advanced Licensing” on page 138.

**Adding a License Key**

You obtain the license key from VMware when you purchase a VDP Advanced license.

**CAUTION** You can obtain a trial evaluation license for VDP Advanced from VMware. When you decode an evaluation license during initial installation, an information message displays, notifying you of the expiration date. Once the evaluation license expires, core services shut down and you will not be able to access the VDP Appliance. Failure to install a permanent license before the trial license expires puts your data at risk; therefore, do not use a VDP Advanced trial license as the sole backup source for critical data.

**Procedure**

1 From a web browser, access VDP.

2 From the VDP user interface, select the **Configuration** tab (by default you are on the Backup Appliance Details view).

3 If any hosts are currently licensed, the Add a new license key button is enabled. If there are no licensed hosts, click **Add a new license key** in the VDP Advanced License Assignment view.

   The Add License Key dialog box displays.
4 Enter the license key in the Enter Key field and click Decode to validate the license. The Initial Configuration wizard validates the license.

5 Click OK.

6 Select an ESX host from the vCenter inventory.
   - Each host can have only one VDP Advanced license assigned to it.
   - If the virtual machines to be protected by the VDP Advanced system are in a cluster, then all hosts in the cluster must be licensed. Licenses are not assigned directly to clusters; they are assigned only to hosts.

7 Click OK.

Upgrading from VDP to VDP Advanced

Once a single license has been installed and registered, the Switch to VDPA button enables VDP Advanced mode.

1 From the VDP user interface, select the Configuration tab (by default you are on the Backup Appliance Details view).

2 In the Backup Appliance Details view, click the Switch to VDPA button.

**CAUTION** A warning displays asking you to confirm the upgrade. By upgrading to VDP Advanced, you can only back up virtual machines that are on hosts having a valid VDP Advanced license. You cannot revert to VDP Basic mode.

3 Click Yes to confirm the upgrade.

   After the upgrade is complete, you are disconnected from the VDP Appliance. On subsequent connections, the VDP Appliance is switched to VDP Advanced mode.

Viewing VDP Advanced License Information

You can view license statistics on the VDP user interface—Configuration tab. The VDP Advanced License Assignment table contains the following information:

- Drop-down list—a list that contains Add, Edit, or Remove options for licensed hosts.
- Key—the license key.
- CPU Count—the number of supported CPUs assigned to this license key.
- Host—the host assigned to this license key. Once the license key is expanded, the licensed hosts under the license key are displayed.

Unassigning the License

You can unassign a license when the license is assigned to a single host or to multiple hosts.

1 From the VDP user interface, select the Configuration tab (by default you are on the Backup Appliance Details view).

2 In the VDP Advanced License Assignment view, select the license you want to unassign, and then select Edit license assignment from the drop-down list.

3 Select the checkbox that corresponds to the host you are unassigning, and click OK.

   The license key is no longer assigned to the host.
Removing a License Key

When a license key is removed, the VDP Advanced Appliance continues to run backups, but the audit will generate license violation messages.

1. From the VDP user interface, select the **Configuration** tab (by default you are on the Backup Appliance Details view).
2. In the VDP Advanced License Assignment view, select the license you want to delete, and then select **Remove license key** from the drop-down list.
   
   A warning displays, asking you to confirm whether you want to remove the license key.
3. Click **Yes** to delete the license key.

System Setting Configuration

**Prerequisites**

The VDP .ovf template (see “Deploying the OVF Template” on page 24) must have deployed successfully, and you must be logged into the vCenter Server from the vSphere Web Client.

**Procedure**

1. From a web browser, access the vSphere Web 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 select **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/
   
6. From the VMware Login screen, enter the following:
   
   a. User: **root**
   
   b. Password: **changeme**
   
   c. Click **Login**.

   The VDP Welcome screen appears.

7. Click **Next**.

8. The Network settings dialog box appears by default. Specify (or confirm) the following network and server information for your VDP Appliance. If the values are not populated correctly, you will not be able to continue with the VDP configuration.
   
   a. IPv4 Static address
   
   b. Netmask
   
   c. Gateway
   
   d. Primary DNS
   
   e. Secondary DNS
   
   f. Hostname
   
   g. Domain

9. Click **Next**.
10 The Time Zone dialog box appears. Select the appropriate time zone for your VDP Appliance, and click Next.

11 The VDP credentials dialog box displays. For VDP credentials, type in the VDP Appliance password, and then verify the password by retyping it. This will be the universal configuration password. Specify a password that contains the following:

- Nine characters
- At least one upper case letter
- At least one lower case letter
- At least one number
- No special characters

12 Click Next.

13 The vCenter registration dialog box appears. Specify the following:
   a vCenter username—If the user belongs to a domain account then it should be entered in the format “SYSTEM-DOMAIN\admin”.
   
   **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 hostname (IP address or FQDN)
   d vCenter port
   e If disabled, click 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.

14 Click Test connection.

A Connection success message displays. If this message does not display, troubleshoot your settings and repeat this step until a successful message displays.

**NOTE** If on the vCenter registration page of the wizard you receive the message “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,” go to “User Account Configuration” on page 21 for instructions on how to update the vCenter user role.

### Switching the VDP Appliance to a New vCenter

If you switch the VDP Appliance to a new vCenter, you must add a new license to activate the VDP Advanced features on the new vCenter. You cannot reuse the same license key in the new vCenter.

**Procedure**

1 Remove ESXi host from vCenter-1.
2 Add ESXi host to vCenter-2.
3 Open a web browser and type:
   
   https://<IP_address_VDP_Appliance>:8543/vdp-configure/

   The VDP Welcome screen appears.
4 Click the Configuration tab, and then click the Lock icon to modify the existing credentials.
   A Warning dialog box appears.
5 Enter the VDP Appliance password on the Warning dialog box, and click OK.

6 Enter the vCenter credentials using the information in “System Setting Configuration” on page 27.

   The Configuration Status dialog box displays the status of the configuration switch.

7 Once the vCenter switch completes, add a new license using the steps in “Adding a License Key” on page 25.
This chapter contains the following topics:

- “Best Practices” on page 32
- “Allowed Upgrade Paths” on page 32
- “Allowed Upgrade Paths” on page 32
- “Selecting a Time for Upgrading the VDP Appliance” on page 32
- “Creating a Snapshot of the VDP Appliance” on page 32
- “Mounting the Upgrade ISO Image on the Appliance” on page 33
- “Installing the Upgrade” on page 33
- “Removing the Snapshot and Unmounting the Upgrade Image” on page 34
- “Reverting Back to a Snapshot” on page 35
Best Practices

- Before running the upgrade process, take a snapshot of the vSphere Data Protection (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.”

- 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 using the following command:

```bash
eemwebapp.sh --start
```

Allowed Upgrade Paths

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

<table>
<thead>
<tr>
<th>Upgrade FROM</th>
<th>Upgrade TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDP 5.1.0.0</td>
<td>VDP 5.1.10.32</td>
</tr>
<tr>
<td>VDP 5.1.0.0</td>
<td>X</td>
</tr>
<tr>
<td>VDP 5.1.10.32</td>
<td>X</td>
</tr>
<tr>
<td>VDP 5.1.11.3</td>
<td>X</td>
</tr>
<tr>
<td>VDP Advanced 5.1.20.24</td>
<td>X</td>
</tr>
<tr>
<td>VDP Advanced 5.1.21.11</td>
<td>X</td>
</tr>
<tr>
<td>VDP Advanced 5.1.21.15</td>
<td>X</td>
</tr>
<tr>
<td>VDP 5.5.1</td>
<td></td>
</tr>
</tbody>
</table>

Selecting a Time for Upgrading the VDP Appliance

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

Creating a Snapshot of the VDP Appliance

As a best practice, take a snapshot of the VDP Appliance prior to 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.
   ```bash
   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 After the appliance has shut down, right-click the VDP Appliance and choose Edit Settings.
6 In the Virtual Hardware table, starting with Hard disk 2, click the disclosure arrow.
7 In the Disk Mode row, click Dependent.
8 Continuing with Hard disk 3, repeat step 7 until all the remaining disks have been set to Dependent mode.
9 Click OK.
10 Right-click the VDP Appliance and choose Take Snapshot.
11 Type a name for the snapshot.
12 Type an optional description.
13 Click OK.
14 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 displays.
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 will begin 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 will check for available disk space on the datastore where the VDP Appliance is installed. You will need approximately 2 GB of free space, plus the size of the upgrade ISO file.

CAUTION If a specific dedicated role is assigned for the VDP Appliance, please update the minimum required vCenter permissions before you install the upgrade. Refer to “Minimum Required vCenter User Account Permissions” on page 133 for more information.

1 Access the VDP Configure utility:
   \[https://<IP_address_VDP_Appliance>:8543/vdp-configure/\]
2 Login with the VDP user name and password.
3 On the Status 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. Restart the web browser and restart login to VDP-Configure. If the ISO image still does not appear, and the datastore where the ISO image is being mounted is from a remote file system, the mounting and unzipping process can take up to 20 minutes.

**NOTE** After allowing time for the ISO image to mount, if the upgrade tab still does not display an upgrade available, it may be because the image has been corrupted. 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**.

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

When the upgrade installs successfully, two plug-ins appear on the left pane of the vSphere Web Client, as shown below. VDP versions 5.1 and earlier are managed using the VDP plug-in. VDP version 5.5 is managed using the VDP 5.5 plug-in. (Two plug-ins also appear if a VDP Appliance version 5.5 is installed and versions earlier than 5.5 already exist).

To remove the VDP plug-in, you must upgrade all VDP Appliances to VDP version 5.5 and use the plug-in manager to disable the VDP plug-in.

Refer to the VMware vSphere Documentation Center web site for information about managing vCenter plug-ins:


6 To complete the upgrade, perform the steps described in “Removing the Snapshot and Unmounting the Upgrade Image.”

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 35.

### Removing the Snapshot and Unmounting the Upgrade Image

It is strongly recommended that you remove snapshots and unmount the upgrade image after an upgrade completes successfully.

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

Click the Snapshot you created for the VDP Appliance.

Click Delete, and click Yes.

Click Close.

Right-click the VDP Appliance and choose Edit Settings.

Starting with Hard disk 2, click the disclosure arrow.

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

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

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

From the drop-down menu choose Host Device.

Click OK.

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, it is highly recommended you manually run an integrity check See “Running an Integrity Check” on page 96 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 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 is displayed.
4. Right-click the VDP Appliance and choose Shut Down Guest and click Yes.
5. After the appliance has shut 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 has now been reset back to its earlier state.
This chapter contains the following topics:

- “Creating New Storage” on page 38
- “Attaching Existing Storage” on page 39
- “Detaching and Reattaching Storage” on page 41
- “Viewing the Storage Configuration” on page 42
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.

Known Limitations

- If the VDP is configured with an external Data Domain system, you cannot import the disk to a new VDP Appliance.
- When importing storage from VDP Advanced Appliance disks, you must have a VDP Advanced license installed and enabled. You can, however, import storage from VDP Appliance disks without a license.
- 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.
- Migration utilities such as vMotion, storage Distributed Resource Scheduler (sDRS), and HA are turned off.

Procedure

1. On the Create Storage page of the Initial Configuration wizard, select **Create new storage**. When you create new storage, the process creates new VMDK storage disks on selected datastores.

2. Select one of the following capacity options, and click **Next**.

<table>
<thead>
<tr>
<th>Type of storage</th>
<th>Capacity in TB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local VDP storage</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Local VDP Advanced storage</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>8</td>
</tr>
</tbody>
</table>

The Device Allocation page appears. When you create new storage, the number of required disks is known. By default, the option “Store With Appliance” is checked, which deploys the disks on the same datastore selected when deploying the VDP Appliance.

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 zero provisionning 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 If you do not wish to deploy the disks on the same datastore where the VDP Appliance is deployed, clear the **Store with Appliance** checkbox. This allows you to allocate the appropriate disks across the datastores that are visible to the VDP Appliance. Once all of the disks have been allocated to datastores, click **Next**.

The Ready to Complete page appears.

5 On the **Ready to Complete** page, you can run a performance analysis on the storage configuration, or you can bypass this test and click **Next** to apply the changes. 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 failed, 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.

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 the **Next** button.

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

- If the test is successful, a message displays that the configuration is complete and the server automatically reboots the appliance.
- If the test conditionally passes or fails, the results of the performance analysis are displayed, 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.

### Attaching Existing Storage

The Initial Configuration wizard provides the option 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 will fail.

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 recreated.
- All replication jobs associated with the previously-used VDP are deleted and must be recreated.
- Restore points that are associated with the previously-used VDP are kept intact; however, the restore points display 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 17.
- It is highly recommended 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 storage, and click Next.
   
   The Device Allocation dialog box displays.

2. Click on the first ellipsis button and browse to the first vmdk file you wish to attach.

3. Highlight the vmdk file and click the Select button. You can attach vmdk files in any order.

   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 displays.

   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 the Reset button to reset the Device Allocation dialog box to its original state.

4. Click the ellipsis button that corresponds to the next disk to be defined, and browse to the next vmdk file you wish to attach. Highlight the vmdk file and click the Select button.

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

5. Repeat Step 4 for all remaining disks.

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

   The Ready to Complete page appears.

7. Click Next.

   The system displays the message: The following process will start the storage configuration. This cannot be undone. Do you wish to continue?

8. Click Yes.

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

9. Enter the root password of the previously-used VDP Appliance into the Password and Verify Password text box, and click OK.

10. 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.
**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 as or newer version as the disk data).
- 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**

- It is highly recommended that you make a backup copy of all vmdk files prior to reattaching them to a VDP Appliance.
- If possible, it is best to detach the vmdk files from the VDP Appliance after gracefully shutting down the VDP Appliance using the **Shut Down Guest OS** option. Otherwise, as a last resort, power off the VM.
- Prior to 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** operation on the virtual machine.

   **NOTE** If the Shut Down Guest OS option 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 VMware vSphere thick client (not the 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 displays.

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

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

   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 the **Remove** button.

   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 storage, and follow the steps detailed in “Attaching Existing Storage” on page 39.

**Viewing the Storage Configuration**

**Prerequisite**

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:

   http://VDP appliance IP: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. In the following example, the primary OS boot partition and the vmdk file partitions exist on multiple datastores. All disks, including the primary OS boot partition, can, however, exist on a single datastore.

![Storage Summary Diagram](image)

**Data Domain Configuration**

A Data Domain system performs deduplication through Data Domain (DD) OS software. When you select a Data Domain system as the backup target, backup data is transferred to the Data Domain system. Backing up to a Data Domain system is supported in VDP Advanced mode only, and only one Data Domain system can be configured.

If the source VDP Advanced Appliance is configured with a Data Domain system but the destination Appliance does not have a Data Domain system, the replication will fail. Data Domain version 5.3 and 5.4 are supported.

**NOTE**

The EMC Avamar 7.0 and EMC Data Domain System Integration Guide provides complete information about Data Domain system integration.
Adding a Data Domain System

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. Log in to the VDP-Configure URL:
   http://<VDP appliance IP>:8580/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 Add Data Domain.
   The Host Configuration dialog box appears.
4. Specify Data Domain system information:
   a. In the Data Domain Host Name box, enter the FQDN or IP address of the Data Domain system to add.
   b. In the DDBost User Name box, type the name of the DD Boost account for VDP Advanced 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 Advanced should use to access the Data Domain system for backups, restores, and replication.
      NOTE: The default number of Data Domain system streams that VDP Advanced can use at any one time to perform backups and restores is 16.
5. To configure SNMP, click Next.
   The SNMP dialog box appears.
   SNMP configuration enables VDP Advanced to collect and display data for system health monitoring, system alerts, and capacity reporting.
   The SNMP options to configure for VDP Advanced 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 Advanced 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. As a best practice, it is recommended you always rollback to the most recent validated checkpoint.
   - Data Domain information appears on the VDP Appliance in the following locations:
     - Backup tab — the Data Domain 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 42 for details.
- Email reporting — displays a summary of the Data Domain configuration.

### Editing Data Domain

1. Log in to the VDP-Configure URL:
   
   http://VDP appliance IP:8580/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 43 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 hostname, the DD Boost username, or the DD Boost password, the system automatically creates a new checkpoint, which takes approximately ten minutes. As a best practice, it is recommended you always rollback to the most recent validated checkpoint.

### Deleting Data Domain

The process of deleting a Data Domain system from your configuration requires the following tasks:

- Delete all restore points stored on the Data Domain system from the vSphere Web Client.
- No backup jobs can exist with the Data Domain as the backup. If any backup jobs exist where the Data Domain 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.
- Once the Data Domain system is deleted, run another integrity check from the VDP Advanced user interface to verify the Data Domain system is invalid.

VMware Knowledge Base Article 2063806 provides the detailed information required to perform the steps to delete Data Domain. This is an internal article, so you should contact Technical Support for assistance.
vSphere Data Protection Disk Expansion

This chapter contains the following topics:

- “Pre-Expansion Requirements” on page 46
- “VMFS Heap Size Recommendations” on page 46
- “Performing Disk Expansion” on page 47
- “Performance Analysis” on page 49
- “Disk Expansion with Essentials Plus” on page 49
Pre-Expansion Requirements

It is important that you complete (or confirm) the following requirements have been met prior to disk expansion. Failure to complete these steps can corrupt vSphere Data Protection (VDP) Advanced and require a restoration from a clone or VDP Advanced backup.

- Confirm that the minimum CPU and memory requirements are met for the new configuration:
  - For all VDP Advanced capacity options (2 TB, 4 TB, 6 TB, and 8 TB), the minimum number of virtual CPUs is 4.
  - 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
- 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.
- If you have an Essentials Plus license, you cannot hot-plug the required memory; therefore, you must manually increase the memory assigned to VDP Advanced. See “Disk Expansion with Essentials Plus” on page 49 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 42.
- Disk expansion should be performed 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 running state before attempting Disk Expansion. See “Starting and Stopping Services” on page 53 for additional details.
- Confirm that you have administrative privileges in the vCenter. See “User Account Configuration” on page 21 to determine 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 ESXi host. See “VMFS Heap Size Recommendations” on page 46 for additional details.
- Create a clone or backup of the VDP Advanced Appliance and verify that it is valid prior to disk expansion.

VMFS Heap Size Recommendations

VMFS heap size determines the amount of virtual disk space supported by each ESXi host. 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 are displayed
- Virtual machines may crash or fail to start

Prior to 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 ESX/ESXi kernel and requires a system reboot for the changes to take effect.
VMFS3 and VMFS5 use the same settings and are defined in the following table.

Table 5-1. VMFS heap size settings

<table>
<thead>
<tr>
<th>Version/build</th>
<th>Default heap amount</th>
<th>Default allowed open VMDK storage per host</th>
<th>Minimum heap amount</th>
<th>Maximum heap amount</th>
<th>Maximum heap value</th>
<th>Maximum open VMDK storage per host</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi/ESX 3.5/4.0</td>
<td>16 MB</td>
<td>4 TB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ESXi/ESX 4.1</td>
<td>80 MB</td>
<td>8 TB</td>
<td>N/A</td>
<td>128 MB</td>
<td>128</td>
<td>32 TB</td>
</tr>
<tr>
<td>ESXi 5.0 Update 2 (914586) and earlier</td>
<td>80 MB</td>
<td>8 TB</td>
<td>N/A</td>
<td>256 MB</td>
<td>255</td>
<td>25 TB</td>
</tr>
<tr>
<td>ESXi 5.0 Patch 5 (1024429) and later</td>
<td>256 MB</td>
<td>60 TB</td>
<td>256 MB</td>
<td>640 MB</td>
<td>255</td>
<td>60 TB</td>
</tr>
<tr>
<td>ESXi 5.1 Patch 1 (914609) and earlier</td>
<td>80 MB</td>
<td>8 TB</td>
<td>N/A</td>
<td>256 MB</td>
<td>255</td>
<td>25 TB</td>
</tr>
<tr>
<td>ESXi 5.1 Update 1 (1065491) and later</td>
<td>256 MB</td>
<td>60 TB</td>
<td>256 MB</td>
<td>640 MB</td>
<td>255</td>
<td>60 TB</td>
</tr>
</tbody>
</table>

**Note**: ESXi 5.5 includes a much improved heap eviction process, so that there is no need for the larger heap size that consumes memory. vSphere 5.5 supports 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**

vSphere Data Protection Advanced (VDP Advanced) allows you to expand datastore capacity using the Expand Storage wizard. This feature is not available with the standard edition of vSphere Data Protection (VDP). Disk expansion allows you to expand VDP Advanced storage to 2 TB, 4 TB, 6 TB, or 8 TB.

**Prerequisite**

During initial configuration, the VDP Advanced storage disks are distributed across the available datastore locations and the disks are validated.

**Procedure**

1. Log in to the VDP-Configure URL:
   
   http://<VDP appliance IP>:8580/vdp-configure

2. Click the Storage tab.
   
   The available datastores display 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 is disabled.
To expand the size of the disks, select a new capacity from the list. You can expand VDP Advanced storage to 1 TB, 2 TB, 4 TB, 6 TB, or 8 TB.

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.

**NOTE** You cannot change the provision type (thin, thick eager-zeroed, or thick lazy-zeroed). The disks inherit the provision type that was assigned to them during initial configuration.

A warning message displays 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 wish 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 49.
- Click **No** to continue with the disk expansion.

6 To progress to the next page of the Expand Storage wizard, click **Next**.

The CPU and Memory dialog box displays the minimum CPU and Memory requirements for the current configuration.

For all VDP Advanced capacity options (2 TB, 4 TB, 6 TB, and 8 TB), the minimum number of virtual CPUs is 4.

7 Select the number of virtual CPUs for each virtual machine.

The maximum number of virtual CPUs allowed for VDP Advanced virtual machine is 8.

8 Select the amount of memory to be allocated to the VDP Advanced 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 VDP Advanced 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 will display correctly, however, after the next maintenance window has completed its run.
Procedure

1. Log in to the VDP-Configure URL:
   
   http://VDP appliance IP: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 run 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 for the initial configuration run:

- Unknown
- Failed
- Passed.

Possible test results of the post configuration run:

- Passed
- Failed
- Never Run
- Out of Date

Running the Performance Analysis Test

1. Log in to the VDP-Configure URL:

   https://VDP appliance IP:8543/vdp-configure

2. Click the Storage tab.

   The Storage Summary dialog box appears.

3. Click the Performance Analysis tab.

   Because of the potential risk of data loss, 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 datastore(s) 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 abort any running performance analysis test.

Disk Expansion with Essentials Plus

If you have an Essentials Plus license, you cannot enable Memory Hot-Add; therefore, you must manually adjust the memory assigned to vSphere Data Protection (VDP) Advanced, as required for the target capacity.

**NOTE** This limitation is true with ESX 4.x and ESX 5.x hosts. You must manually set the minimum required memory for an ESX host using the memory requirements listed in Table 5-2.
VDP Advanced requires the following memory based on capacity size.

**Table 5-2. Memory requirements for virtual hardware**

<table>
<thead>
<tr>
<th>Capacity size</th>
<th>Required memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 TB</td>
<td>6 GB</td>
</tr>
<tr>
<td>4 TB</td>
<td>8 GB</td>
</tr>
<tr>
<td>6 TB</td>
<td>10 GB</td>
</tr>
<tr>
<td>8 TB</td>
<td>12 GB</td>
</tr>
</tbody>
</table>

**Procedure**

The steps for performing disk expansion with an Essentials Plus license follows.

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

2. Before the expansion, gracefully shut down the VDP Appliance 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 shutdown and restart the VDP Appliance. You can monitor the status through the virtual machine console.

3. Increase the memory assigned to the VDP Appliance using the requirements listed in Table 5-2.
   
   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 displays.
   
   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 choose **Power On**.
This chapter contains the following topics:

- “About the VDP Configure Utility” on page 52
- “Viewing Status” on page 52
- “Starting and Stopping Services” on page 53
- “Collecting Logs” on page 54
- “Changing VDP Configuration” on page 54
- “Rolling Back an Appliance” on page 55
- “Emergency Restore” on page 56
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. It 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 user name 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.

The configuration interface is used to perform the following configuration tasks:

- “Installing the Upgrade” on page 33—Allows you to upgrade to a newer version of the VDP Appliance.
- “Storage Management” on page 37—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 52—Allows you to see the services currently running (or currently stopped) on the VDP Appliance.
- “Starting and Stopping Services” on page 53—Allows you to start and stop selected services on the VDP Appliance.
- “Collecting Logs” on page 54—Allows you to download current logs from the VDP Appliance for troubleshooting purposes.
- “Changing VDP Configuration” on page 54—Allows you to view or change network settings, configure vCenter Registration, view or edit system settings (time zone information and VDP credentials), and manage storage.
- “Rolling Back an Appliance” on page 55—Allows you to restore the VDP Appliance to an earlier known and valid state.
- “Emergency Restore” on page 56—Allows you to restore a VM directly to the ESX/ESXi host that is running the VDP Appliance. This emergency restore procedure is intended for use when the vCenter is unavailable.

Viewing Status

The Status tab lists all of the services required by VDP and the current status of each service. The following table describes the services used by VDP.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core services</td>
<td>These are the services that comprise the backup engine of the VDP Appliance.</td>
</tr>
<tr>
<td></td>
<td>If these services are disabled no backup jobs (either scheduled or “on demand”) will run, and no restore activities can be initiated.</td>
</tr>
<tr>
<td>Management services</td>
<td>Management services should only be stopped under the direction of technical support.</td>
</tr>
<tr>
<td>File system services</td>
<td>These are the services that allow backups to be mounted for file-level restore operations.</td>
</tr>
<tr>
<td>File level restore services</td>
<td>These are the services that support the management of file-level restore operations.</td>
</tr>
</tbody>
</table>
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 re-start 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 system services
6. File level restore services

### Table 6-3. Description of services running on the VDP Appliance.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance services</td>
<td>These are the services that perform maintenance tasks, such as evaluating whether retention periods of backups have expired. The Maintenance service is disabled the first 24-48 hours after the VDP Appliance is deployed. This creates a larger backup window for initial backups.</td>
</tr>
<tr>
<td>Backup scheduler</td>
<td>The backup scheduler is the service that initiates schedule backup jobs. If this is stopped, no scheduled backups will run; however, “on demand” backups can still be initiated.</td>
</tr>
</tbody>
</table>
Collecting Logs

Procedure
1. Open a web browser and type:
   https://<IP_address_VDP_Appliance>:8543/vdp-configure/
2. Login with the VDP user name and password.
3. Click the Status tab.
4. Depending on which type of log information you want to collect, download one of the following files:
   - Log bundle — Click Collect all logs to download a zip file containing all the logs from VDP services. A “Save as” dialog displays that allows you to download the log bundle to the file system of the machine where your web browser is running. By default, the log bundle is named LogBundle.zip, but should be given a unique name.
   - Client logs — Click Collect client logs to download an aggregated text file which contains all client failure logs.

Log Bundle
The log bundle is intended primarily to facilitate sending logs of the VDP Appliance to support personnel. The LogBundle.zip file contains the following logs:
- Core VDP Service Log
- Management Service Log
- File System Service Log
- File Level Restore Service Log
- Image Backup and Restore Log
- Replication Log

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 that failed.

Changing VDP Configuration
When you access the vSphere Data Protection (VDP) configuration utility after installation, it runs in “maintenance mode.” In this 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, it is highly recommended you manually run an integrity check. 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 96 for instructions.
- IPv4 static address
- Netmask
- Gateway
Chapter 6 Post-Installation Configuration of VDP Appliance

- Primary DNS
- Secondary DNS
- Hostname
- Domain

**vCenter Registration**

**CAUTION** Changing the vCenter hostname, vCenter password, vCenter FQDN or IP address, or vCenter Port number results in the loss of all backup jobs, replication jobs, and backup verification jobs associated with the VDP Appliance. Existing backups remain intact, but you will be required to rebuild your VDP environment, including VDP Advanced license host assignment.

If you change any vCenter registration credentials, it is highly recommended you manually run an integrity check. 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 96 for instructions.

**System Settings**

You can edit the system settings on the System Settings tab:

- Changing time zone
- Changing VDP Appliance password

If you change any system settings, it is highly recommended you manually run an integrity check. 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 96 for instructions.

**NOTE** Before the system allows for reconfiguration to take place, it checks to see if a backup or restore job or an integrity check are running. If any of these processes are running, an error message displays stating you cannot proceed with the reconfiguration at this time.

After successful reconfiguration of the timezone, VDP Appliance password, or vCenter configuration settings, you are automatically logged out of the VDP-Configure user interface and the web server restarts. While the web server restarts, you will not have access to the VDP-Configure plug-in. In addition, any users who are logged in to the vSphere Web Client and are using the VDP Appliance will be notified that the system is being reconfigured and their session will end.

**Rolling Back an Appliance**

The vSphere Data Protection (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 this 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 rollback to a checkpoint, then any backups or configuration changes to the VDP Appliance between the checkpoint and the rollback are lost.

The first checkpoint is created when VDP is installed. Subsequent checkpoints are created by the Maintenance service. This service is disable the first 24-48 hours of VDP operation. In the event that you rollback during this time frame, then the VDP Appliance is set to 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 occur, the clients must be reinstalled.

Follow the procedure below to roll back a VDP Appliance.

**CAUTION** It is strongly recommended that you only roll back to the most recent validated checkpoint.
Prerequisites
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. Login with the VDP user name 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.
6. The lock icon changes to unlocked. 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 ("emergency restore") provides a disaster recovery mechanism to protect a vCenter Server and all its components in case the vCenter Server is unavailable due to an outage, or if the user is unable to access the VDP user interface by way of the vCenter Web Client.

An emergency restore restores a virtual machine (VM) directly to the ESX/ESXi 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 VMs can be restored as new VMs on to the ESX/ESXi server where VDP is running.

Best Practices and Recommendations
Ensure the following requirements are met before you perform an emergency restore operation:

- The VM which is being restored has a virtual hardware version that is supported by the ESX/ESXi host on which VDP is running. It is recommended you run VDP on the latest ESX/ESXi host to avoid incompatibility issues.
- There is adequate free space in the target datastore to accommodate the entire VM.
- The target VMFS datastore to which the VM is being restored should support the VMDK file size.
- Network connectivity is available for the restored VMs from the ESX/ESXi host where VDP is running.
- There is at least one local account with Administrator privileges on the ESX/ESXi host where VDP is running.

Limitations and Unsupported Features

- Emergency restore allows you to restore only to the root of the ESX/ESXi level in the inventory.
- Emergency restore requires that the DNS server used by VDP is available and can fully resolve the ESX/ESXi host name.
Emergency restore restores the VM in the Powered Off state. You must manually log in to the ESX/ESXi host and power on the restored VM.

Emergency restore restores the VM as a new VM. You must ensure that the name provided for the VM is not a duplicate of a VM that already exists.

Emergency Restore does not list MSapp clients.

**Prerequisites**

- The ESX/ESXi host is disassociated from the vCenter.
- You have backups for the vCenter through the VDP Appliance.

**Procedure**

1. If you have not already done so, log in to the vSphere client of the ESX host and, from the Summary tab under Host Management, do the following:
   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 VDP. 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 VM 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 VM which will serve as the restore point and click **Restore**.

   The Host Credentials dialog box displays.

5. In the Host Credentials dialog box, enter valid ESX/ESXi host credentials:
   - **ESX/ESXi host name or IP**—enter the ESX/ESXi host name or ESX/ESXi host IP address.
   - **Port**—443, which is the default, is prepopulated.
   - **Username**—enter the ESX/ESXi 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 ESX/ESXi 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 VM from its vCenter, an error message displays 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 VM 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 ESX/ESXi host name
- 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 will cause 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 VM is listed at the ESX/ESXi host level in the inventory. Restoring to a more specific inventory path is not supported.

**Refreshing Restore Points**

1 Log in to the VDP-Configure URL:

   http://<VDP appliance IP>: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 “Managing Restores” on page 82 for instructions.

   NOTE The restored vCenter is powered off by default.

2 Once the vCenter restore completes, power on the vCenter.

3 Log into the vCenter URL to verify all the services are running:

   https://<IP_address_vCenter>:5480

4 Log into the restored vCenter through the vSphere client:

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

5 From the vSphere client, add the ESX/ESXi 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, please try the backup or restore later.
This chapter includes the following topics:

- “Accessing vSphere Data Protection” on page 60
- “Understanding the VDP User Interface” on page 60
- “Switching VDP Appliances” on page 61
- “Viewing Information from the Reports Tab” on page 62
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 display 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 17.

**Procedure**

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

2. In the Credentials page, enter an administrative vCenter user name and password, and click Login. The specified user account must have administrative privileges.

   **NOTE** The default user name and password are `root/vmware`.

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.

**Understanding the VDP User Interface**

The vSphere Web Client for vSphere Data Protection (VDP) is used to configure and manage VDP.
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. Backup jobs can also be created and edited from this page. This page also provides the ability to run a backup job immediately. See “Viewing Information from the Reports Tab” on page 62 for additional information.

- **Restore** – provides a list of successful backups that can be restored. See “Managing Restores” on page 82 for additional information.

- **Replication** – provides a list of successful backups that can be replicated. See “Managing Replication Jobs” on page 88 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 62 for additional information.

- **Configuration** – displays information about how VDP is configured and allows you to edit some of these settings or add a VDP Advanced license. See “Configuring VDP Details” on page 93 for additional information.

**Switching VDP Appliances**

Each vCenter Server supports up to 10 vSphere Data Protection (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 Advanced User Interface**

vSphere Data Protection Advanced (VDP Advanced) offers additional functionality.

With VDP Advanced, Basic Tasks also include:

- Adding a VDP Advanced license
- Guest-level backups of Microsoft SQL, Exchange, 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 Advanced Application Support” on page 102, which also specified how to perform application-level backups and restores.
Viewing Information from the Reports Tab

The Reports tab displays the following information:

- **Appliance status** — the status of the VDP Appliance.
- **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).
- **Integrity check status** — this 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.
- **Recent failed backups** — the number of virtual machines that failed to back up in the most recently completed backup job.

The Clients section in the middle of the Reports tab lists all of the clients associated with the vCenter Server. Clients information is divided into three sub-sections:

- **Client Information** — Contains the following:
  - **Client Name**
  - **State** — The Current state for VDP Advanced (VDP uses standard VMware state information. For VDP Advanced, state is Activated, which indicates that the VMware VDP Client is installed and registered or Inactivated which indicates that the VMware VDP Client is not installed or registered on the VDP Advanced Appliance.)
  - **Type** (This option is only available in VDP Advanced and can be “Image” or “Application.”)
  - **Backup Jobs** — The names of the backup jobs with which the client is associated.
  - **Last Successful Backup** — The date and time the last backup job ran successfully. If no backup job has run, this column contains “Never.”

- **Last Backup Job** — Contains the following:
  - **Last Result** — The status of the last backup job.
  - **Last Run Time** — The date and time that the last backup job ran.
  - **Last Job Name** — The name of the last backup job that ran.

The bottom portion of the Reports tab contains details about a client that is selected in the Clients section above.

On the right side of the Reports tab, there are links to the Event Console and the Task Console. Clicking on these links displays the vCenter Server Event Console or Tasks Console.

Filtering report information

You can filter virtual machine reporting information using a combination of the following criteria:

- **Filter drop-down list**
  - **Show All** — shows all reporting information for the virtual machines. This is the default.
  - **Client** — shows reporting information for the vCenter Client.
  - **Name** — “Is,” “Is not,” “Contains,” or “Does not contain” filters used to query the client name
  - **State** — Values are Powered On, Powered Off, Suspended, Activated, or Not Activated
  - **Type** — Values are Image or Application
  - **Last Successful Backup** — Default is today’s date, or click the calendar to specify a date
  - **Last Backup Job**
- Name – “Is,” “Is not,” “Contains,” or “Does not contain” filters used to query the client name
- Status – Values are Success, Failure, Canceled, or Failure or Canceled
- Date – Default is today’s date, or click the calendar to specify a date

- Refresh button – Click to update the data in the Reports tab.
- Reset filter link – Click to reset the filter criteria to the default, which shows all reporting information.
- All Actions icon

  - Select the protected virtual machine you want to restore from the most recent backup, click the All Actions icon, and then click Restore from Last Backup. If there are no backups found for the selected virtual machine, an error message displays.

  - Select the protected virtual machine you want to backup immediately, click the All Actions icon, and then click Backup now. For complete information about backing up a client immediately, refer to “Immediately Backing up a Protected Virtual Machine” on page 72.

  - Select the protected virtual machine you want to backup immediately, click the All Actions icon, and then click Verify now.

  - Select the protected virtual machine you want to backup immediately, click the All Actions icon, and then click Replicate now. For complete information about replication, refer to “Managing Replication Jobs” on page 88.

For more information on using these consoles to monitor VDP operations see “Viewing the Event Console” on page 98 or “Viewing Recent Tasks” on page 97.
Managing Backups

This chapter includes the following topics:

- “Managing Backup Jobs” on page 66
- “Choosing the Virtual Machines” on page 66
- “Specifying the Backup Schedule” on page 67
- “Setting the Retention Policy” on page 67
- “Creating a Full Image Backup Job” on page 68
- “Creating a Backup Job on Individual Disks” on page 69
- “Viewing Status and Backup Job Details” on page 71
- “Editing a Backup Job” on page 71
- “Cloning a Backup Job” on page 71
- “Deleting a Backup Job” on page 72
- “Enabling or Disabling a Backup Job” on page 72
- “Running Existing Backup Jobs Immediately” on page 72
- “Locking and Unlocking a Backup” on page 73
Managing 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 in the Backup tab using the Create a new backup job wizard.

Limitations

- Backing up greater than 2 TB virtual machines on Windows operating systems is not supported. This limitation does not exist on Linux operating systems.
- vSphere Data Protection (VDP) will not back up the following specialized virtual machines: The wizard allows you to select these VMs; however, when you click Finish to complete the wizard, you receive a warning that these special virtual machines were not added to the job
  - vSphere Data Protection (VDP) Appliances
  - vSphere Storage Appliances (VSA)
  - VMware Data Recovery (VDR) Appliances
  - Templates
  - Secondary fault tolerant nodes
  - Proxies
  - Avamar Virtual Edition (AVE) Servers
- 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: à, é, í, 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/selfservice/microsites/search.do?language=enUS&cmd=displayKC&externalId=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 virtual machine (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 in 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

On the Retention Policy page of the Create Backup Job wizard (Step 8 in the procedure below), you specify the retention period for backups.

The first three options—Forever, for, and until—are applied 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 a given day receives a Daily tag. If it is also the first backup of the week, it will also receive a Weekly tag. If it is also the first backup of the month, it will receive the Monthly tag as well. And if it is the first backup of the year, it will receive the Yearly. The time intervals specified in the this Schedule or custom retention schedule only apply to backups with the internal tags. Retention policy options are described in Table 8-4.

Table 8-4. Retention Policy Options

<table>
<thead>
<tr>
<th>Time Interval</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forever</td>
<td>All backups for the virtual machines in this backup job will never be deleted.</td>
</tr>
<tr>
<td>For specified time interval</td>
<td>All backups for the virtual machines in this backup job will be stored until the specified time interval has elapsed from their creation date. The time interval can be specified in days, weeks, months, or years.</td>
</tr>
<tr>
<td>Until specified date</td>
<td>All backups for the virtual machines in this backup job will be deleted on the date specified in the Until field.</td>
</tr>
<tr>
<td>This Schedule or Custom Retention Schedule</td>
<td>Specifies the retention time intervals for backups that are assigned internal tags of Daily, Weekly, Monthly, or Yearly. 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.</td>
</tr>
</tbody>
</table>
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 as follows:
   - 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; for example: 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 launch the Create new backup job wizard.
   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.
4. On the Job Type page, select Guest Images, and click Next.
   The Applications option is a VDP Advanced feature, and lets you create backup jobs on Microsoft Exchange, Microsoft SQL, and Microsoft SharePoint servers. “VDP Application Support” on page 101 provides details.
5. On the Data Type page, select Full Image, and click Next.
   The Backup Targets page appears. This page contains all the objects and virtual machines in the vCenter Server.
6. On the Backup Targets page, click the disclosure arrows to progressively disclose the VM machines. Click the checkboxes next to the items to add to the backup job, and 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.
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.

In 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, í, ü, and ñ).

In the Ready to Complete page, review the summary information for the backup job, and click **Finish**.

An information dialog box will confirm the backup job was created successfully. The backup operation can take several minutes.

Click **OK**.

The newly created backup job is now listed on the Backup tab.

**Creating a Backup Job on Individual Disks**

Whereas 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; for example: 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.

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 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. Click the checkboxes next to the items to add to the backup job, and click **Next**.

4. On the Schedule page, select the schedule for the job and click **Next**.

5. In the Retention Policy page, accept the default retention policy or specify an alternate retention policy and click **Next**.

6. In 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: à, ô, í, ü, and ñ).

7. In the Ready to Complete page, review the summary information for the backup job, and 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 virtual machine disk files (vmdk files) with no downtime or disruption in service. You can find complete information about migrating with vMotion and storage vMotion (svMotion) at the VMware vSphere Documentation Center web site:


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 will simply 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 in 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

Once you have created a backup job, you can edit the job by highlighting the backup job and selecting **Backup Job Actions > Edit**.

Cloning a Backup Job

Once you have created 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

Once you have created 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, but 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 backup immediately through one of the following options:
   - Right-click on the virtual machine in an inventory tree and choose All VDP Actions > Backup Now. The virtual machine must belong to a backup job for this selection to appear.
   - Click on the virtual machine in an inventory tree, and then click the Actions button. Choose All VDP Actions > Backup Now. The virtual machine must belong to a backup job for this selection to appear.
   - Click the virtual machine (in the Reports tab), and then click the floating Actions icon and choose Backup Now.

2. The Backup Now dialog displays. Select the VDP Appliance and the Backup Job and click OK.

3. An information dialog displays telling you the backup job has been initiated. Click OK.

VDP starts the backup job.

**Immediately Running a Backup Job**

1. From the VDP user interface – Backup tab, click the job you want to run immediately. Multiple selections are allowed on the Backup tab using Ctrl- or Shift-click. Holding down the Ctrl key while clicking allows you to select multiple, specific backup jobs; holding down the Shift key while clicking allows you to select a range of backup jobs between the first click and the second click.

2. Click Backup Now.

   A drop down selection appears, giving you 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 which 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.

   “Backup Now” 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 Storage” on page 39). 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 VDP user interface – Restore tab, click the disclosure arrows to locate the backup you want to lock.
3. Click 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

This chapter includes the following topics:

- “Best Practices” on page 76
- “Creating a New Backup Verification Job” on page 77
- “Editing a Backup Verification Job” on page 79
- “Cloning a Backup Verification Job” on page 79
- “Executing and Running a Backup Verification Job” on page 79
- “Monitoring Backup Verification” on page 80
- “Enabling and Disabling a Backup Verification Job” on page 80
- “Deleting a Backup Verification Job” on page 80
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_VALIDATING_<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 reports 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 (SQL, Exchange, and Share Point) are not supported.
  - Replicated backups
  - Backups from imported disks

- The verification will fail 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 in order to reselect the same or different datastore before you can successfully run the job again.

- In some cases, VDP Advanced fails to automatically delete the validating VM from the vCenter inventory. In this scenario, you must manually delete the validating VM.

- ESX and ESXi hosts prior to 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 Advanced, 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. It is recommended you 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.
Chapter 9 Automatic Backup Verification

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 Restore tab allows you to create and manage backup verification jobs.

Prerequisites
- VDP Advanced is installed and configured on the vCenter Server.
- 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 machine(s) 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 Restore tab.
3. On the Restore tab, click Backup Verification.
   NOTE: The Backup Verification section is visible only when VDP Advanced is enabled.
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 VM for which you want to create a verification job, and click Next.
   - You may select only one VM per verification. Multiple selections are not supported.
   - The VM must be a part of a full image backup job or it may have restore points.
   - You can filter the virtual machines by name, if needed.
   - VMware Tools must be present on the VM backups or the verification job will fail.
6. On the Verification Options page:
   - Heartbeat Verification: This is the default option for verification of a backup, regardless of whether you select script verification or not. 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. You can use script verification if you would like the restored VM to be verified for the health status of applications and services running 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 VMs in the network.

If you choose to execute a script on a guest, 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 78.

7 Click Next.

8 On the Destination page, select a destination:

- **Destination Path** — The destination host must be compatible with the validating VM, and the destination host must have sufficient resources to restore the validating VM. 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. ESX and ESXi hosts prior to 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 VM 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 will determine how often and at what time of the day your verification job will run.

- **Backup verification schedule**: Specify the time intervals as daily, weekly, or monthly.
- **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 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 is a file that runs simply 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 using VDP Advanced, 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**

Once backup verification jobs have been created, you can edit them as needed.

**Procedure**

1. From a web browser, access VDP.
2. Click the *Restore* tab.
3. On the *Restore* tab click *Backup Verification*.
4. Select the backup verification job that you want to edit, and 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**

Once you have created a verification job, you can use the job as a template for creating a different 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**

Once a backup verification job has been created, you can invoke verification by running “on demand” verification or by waiting for the schedule to trigger 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 will be deleted after backup verification.
- **Power On** — Once 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 has been powered on.
- **Heartbeat Verification** — Once the Guest OS has booted, the appliance will wait 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** — Once 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 Restore tab.
3. On the Restore tab, click Backup Verification.
4. Select the backup verification job that you want to run now, and 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 62 for more information.
- Email reports — see “Configuring Email” on page 95 for more information.
- Client logs. You can download client logs from https://<IP address or hostname of VDP>:8543/vdp-configure.

Enabling and Disabling a Backup Verification Job

Once backup verification jobs have been created, 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 “Managing Backup Jobs” on page 66 for instructions.
2. Click the Restore tab.
3. On the Restore 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 “Managing Backup Jobs” on page 66 for instructions.
2. Click the Restore tab.
3. On the Restore 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

This chapter includes the following topic:

- “Selecting Backups to Restore” on page 82
- “Filtering for List of Backups” on page 82
- “Restores when Snapshots are Present” on page 82
- “Restoring Image Backups to Original Location” on page 83
- “Restoring Image Backups to New Location” on page 84
- “Restoring Backups to Individual SCSI Disks” on page 85
- “Deleting a backup from the Restore tab” on page 86
- “Clearing all selected backups from the Restore tab” on page 86
Managing Restores

Once virtual machines have been backed up, you can restore the backups to the original location or to an alternate location. If you are using VDP Advanced, you can also create backup verification jobs to ensure that the backups were successful and that they will restore as expected.

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 MS App 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 VM on the Getting Started tab of the VDP screen.
- From the Restore tab, select a restore point and click Restore.
- Select a protected virtual machine in the VDP Reports tab, and then click the All Actions icon and click Restore from Last Backup.
- 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 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”

Clear the filter by clicking Reset Filter 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 higher, snapshots are not allowed on the virtual machine.

**CAUTION** Prior to performing any restores, remove any snapshots that might exist from the virtual machine. The restore job will fail if being restored to a virtual machine that contains snapshots.

Refer to the following Knowledge Base articles about how to use snapshots wisely:


and

https://community.emc.com/thread/145249?start=0&start=0
Restoring Image Backups to Original Location

You can restore backups manually by using the Restore backup wizard, which guides you through each step. 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.

**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. Click 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 wish 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, then the restore to original location option is not allowed, and 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).

   **NOTE** If you want to change any of the settings for your restore request, either use the **Back** button to return to the appropriate screen, or click the appropriate numbered step title on the left side of the wizard screen.
11 Click **Finish** to start the restore operation.

A message displays telling you that your restore was successfully initiated. Click **OK**.

12 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 New Location

You can restore backups manually by using the Restore backup wizard, which guides you through each step. 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. Click 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, click the backup that you want to restore, and click **Next**.

The Set Restore Options page appears.

8. On the Set Restore Options page, 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. 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, either use 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 displays telling you that your restore was successfully initiated. Click OK.

12 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, which guides you through each step. 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 VM. Though user allowed to initiate multiple restore operations but only first restore will succeeds.
- 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. Click 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, click the backup that you want to restore, and click Next.
   The Set Restore Options page appears.
8. On the Set Restore Options page, 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:
   - **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.
   - **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 VM 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 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, either use 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 displays telling you that your restore was successfully initiated. Click **OK**.

13 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.
This chapter includes the following topics:

- “Replication Compatibility” on page 88
- “Replication and Data Domain” on page 88
- “Defining Backup Types for a Replication Job” on page 88
- “Creating a Replication Job” on page 89
- “Editing a Replication Job” on page 92
- “Cloning a Replication Job” on page 92
- “Deleting a Replication Job” on page 92
- “Enabling or Disabling a Replication Job” on page 92
- “Viewing Status and Replication Job Details” on page 92
- “Running Existing Replication Jobs Immediately” on page 92
Managing Replication Jobs

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 Advanced appliance can be replicated to another VDP Advanced Appliance, an Avamar Server, an Avamar Virtual Edition (AVE) Server, or a Data Domain System.

**NOTE** Imported backups (that is, backups that were created from a previous appliance, from where disks were imported to a new appliance) cannot be replicated.

Replication Compatibility

The following table indicates which backups can and cannot be replicated, depending on which VDP product was used to create them.

**Table 11-5. Replication compatibility matrix**

<table>
<thead>
<tr>
<th>Backups created with this product...</th>
<th>Can be replicated to this product...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VDP</td>
</tr>
<tr>
<td>VDP</td>
<td>No</td>
</tr>
<tr>
<td>VDP Advanced</td>
<td>No</td>
</tr>
</tbody>
</table>

Replication and Data Domain

If the source VDP Advanced Appliance has a Data Domain as its backup target, the replication destination VDP Advanced Appliance must also have a Data Domain system. Similarly, if replicating from VDP Advanced to an Avamar Server, the Avamar server must have a Data Domain system.

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.

Limitation

When a replication job initiates, 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.

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 67 for detailed information.
On-demand or scheduled backup types:

- If any backup job is run 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 5 of the Create a new replication job wizard).

- To schedule the backup, specify the scheduling options (Step 7 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, which walks you through each step.

**NOTE** Clients or restore points that have already been replicated from a different source server do not appear as available in the Create a new replication job wizard, because the wizard does not support them.

### 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. Refer to "Accessing vSphere Data Protection" on page 60 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:

   - **Name** — The name 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.

   The Select Clients page appears. On this page, you select the clients whose backups you want to include in this replication job.

4. On the **Select Clients** page of the Create a new replication job wizard:

   - If you want to replicate all client backups, click **All clients**, and then click **Next**.
   - If you want 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, MS Exchange, and MS SharePoint.

**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, so when selecting clients, select the regular VM without the suffix.

   If you choose this option, you can select one or more clients. If preferred, you can filter the clients before you make any selections. To filter clients:

   - Beside **Filter**, click **Show All**, and select **Client**.
ii If you want to filter by client name, select Name. The following information displays for the vCenter Client.

- Name – “Is,” “Is not,” “Contains,” or “Does not contain” filters used to query the client name
- State – Values are Powered On, Powered Off, Suspended, Activated, or Not Activated
- Last Successful Backup – Default is today’s date, or click the calendar to specify a date

iii Select one or more clients in the list.

iv 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.

5 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; they 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), however, 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.
6 On the **Destination** page of the Create a new replication job wizard:

a Supply the following information:

- **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, as this 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.

b Click **Verify Authentication** to test the connection between VDP and the destination.

c 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.

7 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.

8 On the **Retention** page of the Create a new replication job wizard:

a If you want to use each backup's current expiration date, select **Keep the current expiration for each backup**.

b If you want 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 Click **Next**.

The Name page appears. On this page, you name the replication job.

9 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.
10 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.

Editing a Replication Job

Once you have created a replication job, you can edit the job by highlighting it and selecting Replication Job Options > Edit.

Cloning a Replication Job

Once you have created a replication job, you can use the job as a template for creating a different job. To do this, highlight the replication job, and select Replication Job Options > 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

Once you have created a replication job, you can delete the job by highlighting it, and selecting Replication Job Options > Delete.

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, but 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 Options > 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** – a list of the clients whose backups are replicated by the job.

Running Existing Replication Jobs Immediately

You can run a replication job immediately by highlighting the job and clicking Replicate Now.
The Configuration tab is used for the following tasks.

- “Viewing Backup Appliance Configuration” on page 94
- “Editing the Backup Window” on page 95
- “Configuring Email” on page 95
- “Viewing the User Interface Log” on page 96
- “Running an Integrity Check” on page 96
- “Installing Client Downloads” on page 97
- “Viewing Recent Tasks” on page 97
- “Viewing Alarms” on page 98
- “Viewing the Event Console” on page 98
- “VDP Shutdown and Startup Procedures” on page 99
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 VDP 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/ESX 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 51 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.

The following figure is a graphical representation of the backup window configuration.

![Backup Window Configuration](image)

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 60 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.
4. The backup start time and duration time options appear. 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.
7. A dialog displays telling you that the settings were saved successfully. 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 60 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 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 user name 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.

**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 creates 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, then you will want to run a manual integrity check. If you allow 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 55 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 60 for instructions.
2. From the VDP user interface – Configuration tab, click the icon and select **Run integrity check**.
3. A confirmation screen displays, asking if you want to perform a manual integrity check. Click **Yes**.
4. A message displays informing you that the integrity check has been initiated. 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.

Installing Client Downloads

This option only appears if you are using VDP Advanced. To install client downloads see “VDP Application Support” on page 101.

Monitoring VDP Activity

You can monitor the activities of the VDP application by:

- “Viewing Recent Tasks” on page 97.
- “Viewing Alarms” on page 98
- “Viewing the Event Console” on page 98

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
- Restores
- Replications
- 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 cancelled from the **Running** tasks jobs pane by clicking the delete icon.
Viewing Alarms

The vSphere Data Protection (VDP) Appliance can trigger the following alarms:

Table 12-6. vSphere Data Protection alarms

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDP: [001] The most recent checkpoint for the VDP Appliance is outdated.</td>
<td>From the Configuration tab of the VDP user interface, click the All Actions icon and select “Run integrity check.”</td>
</tr>
<tr>
<td>VDP: [002] The VDP Appliance is nearly full.</td>
<td>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.</td>
</tr>
<tr>
<td>VDP: [003] The VDP Appliance is full.</td>
<td>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.</td>
</tr>
<tr>
<td>VDP: [004] The VDP Appliance datastore is approaching maximum capacity.</td>
<td>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.</td>
</tr>
<tr>
<td>VDP: [005] Core services are not running.</td>
<td>Start Core services using the VDP configure utility.</td>
</tr>
<tr>
<td>VDP: [006] Management services are not running.</td>
<td>Start Management services using the VDP configure utility.</td>
</tr>
<tr>
<td>VDP: [007] File system services are not running.</td>
<td>Start File system services using the VDP configure utility.</td>
</tr>
<tr>
<td>VDP: [008] File level restore services are not running.</td>
<td>Start File level restore services using the VDP configure utility.</td>
</tr>
<tr>
<td>VDP: [009] Maintenance services are not running.</td>
<td>Start Maintenance services using the VDP configure utility.</td>
</tr>
<tr>
<td>VDP: [010] Backup scheduler is not running.</td>
<td>Start Backup scheduler using the VDP configure utility.</td>
</tr>
<tr>
<td>VDP: [011] Host license does not permit VDP</td>
<td>The ESX host license does not permit usage of VDP and the 60 day evaluation period has ended.</td>
</tr>
</tbody>
</table>

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 shutdown the vSphere Data Protection (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 shutdown 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 shutdown properly, when it restarts it will roll back to the last validated checkpoint. This means any changes to backup jobs or backups that occur between the checkpoint and the unexpected shutdown will be lost. This is expected behavior and is used to ensure system corruption does not occur from unexpected shutdowns. See “**Rolling Back an Appliance**” on page 55 for additional information.

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

**NOTE** Prior to vCenter Server patches or upgrades, use the VDP shutdown procedure.
This chapter includes the following topics:

- “VDP Advanced Application Support” on page 102
- “Backing Up and Restoring Microsoft SQL Servers” on page 102
- “Backing Up and Restoring Microsoft Exchange Servers” on page 108
- “Backing Up and Restoring Microsoft SharePoint Servers” on page 118
VDP Advanced Application Support

vSphere Data Protection Advanced (VDP Advanced) supports granular guest-level backup and recovery support for Microsoft SQL, Exchange, and SharePoint Servers. In order to support guest-level backups, a VDP client is installed on the SQL, Exchange, and SharePoint Servers.

NOTE Guest-level backups are only supported in VDP Advanced mode.

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 Advanced client or plug-in installer without administrator privileges on a computer with UAC enabled, then 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 following error displays:

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.

In order 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 following 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 Advanced client version.

Backing Up and Restoring Microsoft SQL Servers

vSphere Data Protection (VDP) Advanced supports enhanced backup and restore options for Microsoft SQL Servers.

This section covers the following topics:

- “Microsoft SQL Server Support” on page 103
- “Installing the VMware VDP for SQL Server Client” on page 104
- “Creating Backup Jobs for Microsoft SQL Servers” on page 105
- “Restoring Backups of Microsoft SQL Servers” on page 107
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

The following table lists the hardware requirements for the Microsoft SQL Server.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory (RAM)</td>
<td>512 MB (2 GB recommended)</td>
</tr>
<tr>
<td>Hard drive space</td>
<td>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.</td>
</tr>
</tbody>
</table>

Microsoft SQL Server Support

VDP Advanced supports the following versions of the SQL Server:

- 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 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 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 the VMware VDP for SQL Server Client

To support guest-level backups, the VMware VDP for the SQL Server Client must be installed on each SQL Server for backup and restore support.

Prerequisites

- Before using VDP, you must install and configure the VDP Advanced Appliance described in “VDP Installation and Configuration” on page 17 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 user name 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. In Client Downloads, click Microsoft SQL Server 32-bit or Microsoft SQL Server 64-bit (based on the version of the SQL Server client).
6. Depending on your browser, you can save .msi file or you can run it. Once you run the .msi file, the VMware VDP for SQL Server Setup wizard starts. Click Next.
7. 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.
8. 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 Completed the VMware VDP for SQL Server Setup Wizard page, click Finish.

Repeat this procedure for additional SQL Servers.
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 the VMware VDP for SQL Server Client” on page 104 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 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 application servers.
   - Selected Databases — This option lets you back up individual application server databases.

3. On the Backup Targets page, click the arrow beside Microsoft SQL Servers(s) to expand the list.

4. Do one of the following:
   - If you chose to back up a full server, click the checkbox next to the SQL server that you want to back up, and click Next.
     
     **NOTE**: Best practice is to select only one SQL server for 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.
       
       This option should not be used 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, there is a separate option: Use the For simple model recovery databases.

     - **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, then 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:

\[ \frac{1,280 \text{ MB}}{256 \text{ MB}} = 5 \]

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, then 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, then 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, then 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, then the backup fails.
  - **Skip incremental with warning** — If you select databases with different recovery models for the backup, then 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, then 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.

- **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 backups, 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.
Chapter 13 VDP Application Support

6 Click Next.

7 On the Schedule page, select the backup schedule and start time for the backup job, and click Next.

See “Specifying the Backup Schedule” on page 67 for additional information on configuring the schedule.

8 On the Retention Policy page, select an option for how long to keep the backup, and click Next.

See “Setting the Retention Policy” on page 67 for additional information on configuring the retention policy.

9 On the Name page, type a name for the backup job, and 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 On the Select Backup page, select the backup job that you want to restore, and click Next. The Select Restore Options page appears.

5 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, 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 option — 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.

7. Click **Next**. The Ready to complete page appears.

8. On the Ready to complete page, review the restore requests, and 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 54.

### Uninstalling the VDP Advanced Plug-in for SQL Server

To uninstall the VDP Advanced 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 109
- **“Installing VDP for Exchange Server Client”** on page 110
- **“Using the VDP Exchange Backup User Configuration Tool”** on page 110
- **“Manually Configuring the VDP Backup Service”** on page 112
- **“Creating Backup Jobs for Microsoft Exchange Servers”** on page 112
- **“Restoring Backups of Microsoft Exchange Servers”** on page 113
- **“Granular Level Recovery on Microsoft Exchange Servers”** on page 115
- **“Uninstalling the Exchange plug-in”** on page 115
Microsoft Exchange Server Options

VDP Advanced supports enhanced backup and restore options for Microsoft Exchange Servers.

The following options are supported 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
- RSG/RDB restores
- Granular-level restores

Microsoft Exchange Server Support

The following table lists the Microsoft Exchange Server versions and operating systems that the VDP Advanced plug-in for Microsoft Exchange supports.

Table 13-1. Supported Microsoft Exchange Server Versions and Operating Systems

<table>
<thead>
<tr>
<th>Exchange Server version</th>
<th>Operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Windows Server 2012 x64</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 x64</td>
</tr>
<tr>
<td>2010 SP3</td>
<td>Windows Server 2012 x64</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 x64</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 SP2 x64</td>
</tr>
<tr>
<td>2007 SP3</td>
<td>Windows Server 2008 R2 x64</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 SP2 x64</td>
</tr>
</tbody>
</table>

Microsoft .NET Framework 4 requirement

The Exchange VSS plug-in requires installation of Microsoft .NET Framework 4 on each server in the Exchange forest. Search the Microsoft Download Center for “Microsoft .NET Framework 4” to find downloads and additional information.

Hardware Requirements

The following table lists the hardware requirements for the VDP Advanced Plug-in for Microsoft Exchange.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory (RAM)</td>
<td>64 MB</td>
</tr>
<tr>
<td>Hard drive space</td>
<td>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.</td>
</tr>
</tbody>
</table>

Unsupported Microsoft Exchange Servers

The following servers are not supported with the VDP plug-in for Microsoft Exchange:

- Microsoft Exchange Server 2013 or 2010 database availability group (DAG) environments
- Microsoft Exchange 2007 clusters (SCC, CCR, SCR)
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 Advanced Appliance described in “VDP Installation and Configuration” on page 17 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 user name 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. In Client Downloads, click Microsoft Exchange Server 64-bit. Depending on your browser, you can save the .msi file or run it. Once you run the .msi file, the VMware VDP for Exchange Server Setup wizard starts. Click Next.


7. 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.

8. On the Appliance Registration Information page, type in the IP address or fully qualified domain name of the VDP Appliance that will backup the Exchange Server.

9. (Optional) Select the option to install the Exchange GLR plug-in, if you plan to use the server for granular level recovery.

   NOTE A reboot of the Microsoft Exchange server is required if you select the Exchange GLR option.

10. If this is the first Exchange Server in the Active Directory to have the VMware VDP for Exchange 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 uncheck this box. Click Next.


   If the checkbox for the VDP Exchange Backup User Configuration Tool was selected, proceed to “Using the VDP Exchange Backup User Configuration Tool” on page 110.

   If the checkbox for the VDP Exchange Backup Configuration Tool was unselected, proceed to “Manually Configuring the VDP Backup Service” on page 112.

Repeat this procedure for additional Exchange Servers.

Using the VDP 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 VDP 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.

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 2007
- A mailbox is created, activated, and tested for the user account.
- A user account is set up and activated in the Exchange domain, 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 Advanced Appliance described in “VDP Installation and Configuration” on page 17.
- The Launch Exchange Backup User Configuration Utility checkbox must be selected during VMware VDP for Exchange Server Client installation.
- .NET 4.0 must be installed on the Exchange Server:

**Procedure**

1. In the VDP 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 user name 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 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 will fail.
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, then the VMwareVDPBackupUser account is already 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 Advanced Appliance described in “VDP Installation and Configuration” on page 17.
- 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. Launch 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 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 110 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.

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 Targets 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. See “Troubleshooting VDP Advanced” on page 143 for additional information.
If you chose to back up a full server, click the checkbox next to the Exchange server that you want to back up, and 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 click Next.

**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, select a backup type of **Full** or **Incremental**. Incremental backups are automatically promoted to full backups if a full backup does not exist.

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 Advanced 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.

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 click Next.

See “Specifying the Backup Schedule” on page 67 for additional information on configuring the schedule.

9 On the Retention Policy page, select an option for how long to keep the backup, and click Next.

See “Setting the Retention Policy” on page 67 for additional information on configuring the retention policy.

10 On the Name page, type a name for the backup job, and click Next.

11 On the Ready to Complete page, review the summary information about the backup job, and click Finish.

12 Click OK when you see the confirmation that the backup job was created successfully.

**Restoring Backups of Microsoft Exchange Servers**

Once backups have been run 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 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 Select the backup to restore and click the Restore icon to start the Restore backup wizard. The Select backup page appears.
3 Click on the client whose backup you want to restore.
4 Click on the backup that you want to restore from.
5 To restore the entire contents of the backup, click the Exchange Information Store checkbox.
6 Once all the targets have been selected, click the Restore button.
7 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 the destination client, and type the full Windows path to the location on the destination where you want the backup to restore.
8 (Optional) For GLR, on the Select Restore Options page, do the following.
   - Restore to Original Location — Uncheck 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 plugin installed.
   - Destination Mailbox — Set to the email address of the mailbox where the selected mailboxes should be restored to.
9 If you want to specify advanced options, click the arrow beside Advanced options to expand the list. The options are described as follows:
   - Note: The Advanced options are not available when recovering a mailbox using the Exchange GLR plug-in.
     - Allow database overwrite — Forces any existing databases to be overwritten that have the same name(s) included in the restore job. When this option is selected, it modifies the “Allow FileRestore” flag, which is internal to Exchange.
     - 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 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.
10 On the Ready to complete page, review the restore requests, and click Finish.
11 Click OK when you see the message telling you that your restore was successfully initiated.
12 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 54.

**Uninstalling the Exchange plug-in**

To uninstall the Exchange plug-in, use Programs and Features.

The Exchange GLR plug-in uninstalls automatically when you install the Exchange plug-in. You must restart the computer after you uninstall the Exchange plug-in.

**Granular Level Recovery on Microsoft Exchange Servers**

The VDP Advanced Plug-in for Exchange Granular Level Recovery (GLR) mounts a temporary virtual drive on the target server and restores an Exchange database or storage group from a backup to a recovery database (RDB) or recovery storage group (RSG) on the virtual drive.

**Note the following:**
- The backup must be a full backup with the VMware VDP Exchange plug-in.
- The VDP client plug-in for Microsoft Exchange does not support clusters.
- The VDP client plug-in for Microsoft Exchange Servers 2010 or 2013 does not support database availability groups (DAG).
- 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 Advanced Plug-in for Exchange GLR places additional demands on computer hardware and resources beyond the base requirements for backup and restore. The following table describes the system requirements for the VDP Advanced Plug-in for Exchange GLR.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory (RAM)</td>
<td>The VDP Advanced Plug-in for Exchange 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:</td>
</tr>
<tr>
<td></td>
<td>- If resources are already strained and performance is slow with regular operations of the VDP Advanced Plug-in for Exchange VSS, then add significantly more memory to support VDP Advanced Plug-in for Exchange GLR operations.</td>
</tr>
<tr>
<td></td>
<td>- If performance is currently adequate with regular operations of the VDP Advanced Plug-in for Exchange VSS, then additional memory may not be required to support VDP Advanced Plug-in for Exchange GLR operations.</td>
</tr>
<tr>
<td>Hard drive space</td>
<td>Additional disk space is required to provide a disk staging area to hold writes to the Exchange database and log files.</td>
</tr>
</tbody>
</table>

**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 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 Advanced Plug-in for Exchange VSS. In addition, there are several configuration recommendations for multi-streaming.

The following table lists hardware and software recommendations for multi-streaming.

<table>
<thead>
<tr>
<th>Hardware and Software</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>At least one processor core per stream</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>48 GB or more</td>
</tr>
<tr>
<td>Hard disk</td>
<td>1 disk drive for operating system/Exchange installation</td>
</tr>
<tr>
<td></td>
<td>1 to 2 disk drives or RAID drive group for each Exchange database</td>
</tr>
<tr>
<td></td>
<td>7200 RPM or faster disk drives</td>
</tr>
<tr>
<td>Network adapter</td>
<td>1 GB</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows Server 2008 SP2 or later</td>
</tr>
</tbody>
</table>

**Multi-streaming Exchange configuration requirements**

VDP Advanced 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 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), then specify a maximum of four streams.

**VSS requirements**

The VDP Advanced Plug-in for Exchange 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 VSS plug-in uses the Microsoft Software Shadow Copy Provider and the following VSS writers:

- Microsoft Exchange Store VSS Writer

- Microsoft Exchange Replication VSS Writer

The Exchange 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, then 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, then 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. Open the command file in the text editor, and add the flags to enable debugging.
3. Save and close the command file.

The following table lists the VDP Advanced log files that you can enable to trace and debug GLR.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Contents</th>
<th>Flag to enable debugging</th>
<th>Command file for flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Axionfs.log</td>
<td>Trace and debugging information for AvFS file system calls.</td>
<td>--debug</td>
<td>axionfs.cmd</td>
</tr>
<tr>
<td>avmapi.log</td>
<td>Trace and debugging information for MAPI calls.</td>
<td>--debug</td>
<td>avmapi.cmd</td>
</tr>
<tr>
<td>avexgldr_plugin.log</td>
<td>Trace and debugging information for RDB and RSG creation, mount, browse, and restore.</td>
<td>--debug</td>
<td>avexgldr.cmd</td>
</tr>
<tr>
<td>Aveexgldrsvc.log</td>
<td>Trace and debugging information for RDB and RSG creation, mount, browse, and restore.</td>
<td>--debug</td>
<td>aveexgldrsvc.cmd</td>
</tr>
<tr>
<td>ps_exec.log</td>
<td>Trace and debugging information for execution of PowerShell commands on the Exchange client.</td>
<td>--debug</td>
<td>ps_exec.cmd</td>
</tr>
</tbody>
</table>

**Backing up Exchange databases**

For instructions on how to back up Exchange databases, refer to “Backing up Applications” on page 105.

**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 Advanced 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 113.

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 prior to performing 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 on the client whose backup you want to restore.
4. Click on the backup that you want to restore from.
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.

7 On the Ready to complete page, review the restore requests, and 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 Advanced supports the backup and restore of Microsoft SharePoint servers. Only one SharePoint system per farm is currently supported.

**NOTE** Restoring only the SharePoint Configuration or Administrator’s database can corrupt the SharePoint application. Therefore, if you are not restoring only content databases, you must restore the entire backup.

### Hardware Requirements

The following table lists the hardware requirements for the Microsoft SharePoint Server.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory (RAM)</td>
<td>2 GB</td>
</tr>
<tr>
<td>File systems</td>
<td>NTFS</td>
</tr>
</tbody>
</table>

### Supported Microsoft SharePoint Servers

VDP Advanced supports the following versions of Microsoft SharePoint Server:

- SharePoint 2007 SP2 or later:
  - Windows Server 2008 R2
  - Windows Server 2008

- SharePoint 2010, 2010 SP1:
  - Windows Server 2008 SP2
  - Windows Server 2008 R2

- SharePoint 2013
  - Windows Server 2012
  - Windows Server 2008 R2 SP1 or later

### Installing VDP plug-in for SharePoint Server Client

Install the VDP Advanced 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 services that support a single site.)
Limitations
- The SharePoint VSS Writer must run with the SharePoint Farm Administrator account.

Prerequisites
- The VDP Advanced Appliance must be installed and configured as described in “VDP Installation and Configuration” on page 17.
- 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 user name 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.
7. The VMware VDP for SharePoint 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 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 backup server (front end) or if it another member server of the SharePoint 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.

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 select New to start the Create a new backup job wizard.
3. On the Job Type page of the wizard, select Applications - This option will backup up the SharePoint application running on the virtual machine.
4. Click Next and follow the instructions below.
**Back up Applications**

You can only back up the entire SharePoint 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 Targets** page:
   a. Click the arrow beside **Microsoft SharePoint Servers(s)** to expand the list.
   b. Click 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 if you want to allow multiple threads of execution during the backup. Use the slider bar to select the number of streams to use, and 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 click **Next**.

5. On the **Retention Policy** page, select an options for how long to retain the backup, and click **Next**.

6. On the **Name** page, type a name for the backup job, and 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**

Once backups have been run 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. If you want 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 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 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 54.

**Uninstalling the VDP Advanced Plug-in for SharePoint**

To uninstall the VDP Advanced Plug-in for SharePoint on a Windows Server 2008 or Windows Server 2012 installation, use Programs and Features.
This chapter includes the following topics:

- “Introduction to the VDP Restore Client” on page 124
- “Logging In to the Restore Client” on page 125
- “Mounting Backups” on page 126
- “Filtering Backups” on page 126
- “Navigating Mounted Backups” on page 126
- “Performing File Level Restores” on page 126
- “Monitoring Restores” on page 128
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** File level recovery (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 18 for web browsers supported by vSphere 5.5. Internet Explorer 10 is not supported and is unreliable with the Restore Client.

File Level Restore Limitations

File Level Restore has the following limitations:

- 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 5000 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.

LVM Limitations

The following limitations apply to logical volumes managed by the Logical Volume Manager (LVM):

- One Physical Volume (.vmdk) must be mapped to exactly one logical volume.
- Only Ext2 and Ext3 formatting (primary partition with master boot record (MBR) and standalone without MBR) is supported.

Unsupported VMDK Configurations

File Level Restore does not support the following virtual disk configurations:

- Unformatted disks
- Dynamic disks (Windows) / Multi-Drive Partitions (that is, any partition which is composed of 2 or more virtual disks)
- EXT4 filesystems
- FAT16 and FAT32 filesystems
- GUID partition tables (GPT)
- Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)
- Two or more virtual disks mapped to single partition
- Encrypted partitions
- Compressed partitions
Unsupported Windows configurations

File Level Restore 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 one of two modes: Basic or Advanced. 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 14-1. For login instructions, refer to “Using the Restore Client in Basic Login Mode” on page 126.

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.”

![Figure 14-1. FLR Basic Login](image)

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 14-2. For login instructions, refer to “Using the Restore Client in Advanced Login Mode” on page 127.

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.

**NOTE** FLR Advanced Login requires you to use the same vCenter user credentials specified when the VDP Appliance is installed. See “VDP Installation” on page 24 for additional information.
Mounting Backups

After you successfully log in, the Manage mounted backups dialog displays. By default this displays all the backups that are available to be mounted. The format of this dialog will vary depending on how you logged in.

- If you use basic login, you will see a list of all the backups from the client you logged into that can be mounted.
- If you used advanced login, you will see a list 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 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**—all backups are displayed.
- **Restore point date**—only backups within the specified date range are displayed.
- **VM name**—display 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 Login 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. Remote Desktop or use a vSphere Web Client to access the local host that has been backed up through VDP.
2. Access the VDP Restore Client through:
   \[https://<IP_address_of_VDP_appliance>:8543/flr\]
3. In the Credentials page under Local Credentials, specify the Username and Password for the local host and click Login.
4. The Manage mounted backups dialog box appears. It lists all of the restore points for the client you are accessing. Select the mount point that will be restored and click Mount.
5. When the mount is complete, the drive icon will appear as a green networked drive.
6. Click Close.
7. In the Mounted Backups window, navigate to and select the folders and files you want to recover.
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.
11. An Initiate Restore confirmation dialog box displays. Click Yes.
12. A successfully initiated dialog box displays. Click OK.
13. Click the Monitor Restores tab to view restore status.
14. 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 24 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 through:
   \[https://<IP_address_of_VDP_appliance>:8543/flr\]
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**.

4 The Manage mounted backups dialog box displays. It lists all of the restore points for the client you are accessing. 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**.

11 An Initiate Restore confirmation dialog box displays. Click **Yes**.

12 A successfully initiated dialog box appears, 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.
vSphere Data Protection (VDP) is robust in its ability to store and manage backups. In the event of failure, the first course of action should be to rollback to a known validated checkpoint (see “Rolling Back an Appliance” on page 55). To recover from a VDP Appliance failure, the following procedure is used to create 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 where no tasks are scheduled. For example, if your backup window is eight hours and backups only take one hour to complete, you have an additional seven hours before maintenance tasks are schedule. This is an ideal time to shut down and backup the appliance.

2. In the vSphere Client, navigate to the appliance. Perform a Shut Down Guest OS operation 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 clean shut down process. See “VDP Shutdown and Startup Procedures” on page 99 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/copy jobs are being performed against VDP.

5. From the vSphere Client, perform a Power On for the appliance.
vSphere Data Protection (VDP) uses the ports listed in the following table.

**Table A-1. VDP port usage**

<table>
<thead>
<tr>
<th>Product</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDP</td>
<td>22</td>
<td>TCP</td>
<td>User</td>
<td>VDP</td>
<td>ssh (for debugging)</td>
</tr>
<tr>
<td>VDP</td>
<td>53</td>
<td>UDP</td>
<td>VDP</td>
<td>DNS server</td>
<td>DNS</td>
</tr>
<tr>
<td>VDP</td>
<td>80</td>
<td>TCP</td>
<td>VDP</td>
<td>vCenter</td>
<td>http (for licensing)</td>
</tr>
<tr>
<td>VDP</td>
<td>111</td>
<td>TCP/UDP</td>
<td>VDP</td>
<td>ESX/ESXi</td>
<td>rpcbind</td>
</tr>
<tr>
<td>VDP</td>
<td>443</td>
<td>TCP</td>
<td>VDP</td>
<td>vCenter or SSO</td>
<td>https</td>
</tr>
<tr>
<td>VDP</td>
<td>700</td>
<td>TCP</td>
<td>VDP LDAP</td>
<td>Active Directory</td>
<td>Logingmgr tool</td>
</tr>
<tr>
<td>VDP</td>
<td>7778</td>
<td>TCP</td>
<td>vCenter</td>
<td>VDP</td>
<td>VDP RMI</td>
</tr>
<tr>
<td>VDP</td>
<td>7779</td>
<td>TCP</td>
<td>vCenter</td>
<td>VDP</td>
<td>VDP RMI</td>
</tr>
<tr>
<td>VDP</td>
<td>8509</td>
<td>TCP</td>
<td>vCenter</td>
<td>VDP</td>
<td>Tomcat AJP Connector</td>
</tr>
<tr>
<td>VDP</td>
<td>8543</td>
<td>TCP</td>
<td>vSphere Web Client</td>
<td>VDP</td>
<td>Redirect for Tomcat</td>
</tr>
<tr>
<td>VDP</td>
<td>8580</td>
<td>TCP</td>
<td>vCenter</td>
<td>VDP</td>
<td>VDP Downloader</td>
</tr>
<tr>
<td>VDP</td>
<td>9443</td>
<td>TCP</td>
<td>vCenter</td>
<td>VDP</td>
<td>VDP Web Services</td>
</tr>
<tr>
<td>VDP</td>
<td>27000</td>
<td>TCP</td>
<td>VDP</td>
<td>vCenter</td>
<td>Licensing communication</td>
</tr>
<tr>
<td>VDP</td>
<td>28001</td>
<td>TCP</td>
<td>MS App Client</td>
<td>VDP</td>
<td>Client Software</td>
</tr>
<tr>
<td>VDP 5.5</td>
<td>29000</td>
<td>TCP</td>
<td>VDP 2013</td>
<td>Avamar Virtual Edition (AVE) or Avamar storage server</td>
<td>Replication with high SSL encryption</td>
</tr>
</tbody>
</table>
Minimum Required vCenter User Account Permissions

See “User Account Configuration” on page 21 to configure the VDP user or SSO admin user 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
- 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
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
- vApp application configuration
This chapter includes the following troubleshooting topics:

- “Troubleshooting VDP Appliance Installation” on page 138
- “Troubleshooting Accessing the VDP Web Client” on page 138
- “Troubleshooting VDP Advanced Licensing” on page 138
- “Troubleshooting VDP Backups” on page 140
- “Troubleshooting VDP Restores” on page 141
- “Troubleshooting VDP Replication Jobs” on page 142
- “Troubleshooting VDP Integrity Check” on page 142
- “Troubleshooting Automatic Backup Verification” on page 142
- “Troubleshooting the Restore Client (File Level Recovery)” on page 142
- “Troubleshooting VDP Advanced” on page 143
- “Troubleshooting VDP Advanced Exchange Backups” on page 143
- “Troubleshooting VDP Advanced Exchange Restores” on page 144
- “Troubleshooting VDP Advanced SQL Backups” on page 145
- “Troubleshooting VDP Advanced SQL Restores” on page 145
- “Accessing VDP Knowledge Base Articles” on page 145
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 18).
- Confirm that the hardware meets the minimum hardware requirements (see “System Requirements” on page 19).
- Confirm that DNS is properly configured for the VDP Appliance. (see “Preinstallation Configuration” on page 20).

Troubleshooting Accessing the VDP Web Client

The following troubleshooting items provide some direction on how to identify and resolve some common issues with managing vSphere Data Protection (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 user name 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 Registration” on page 55 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 20 for additional information.

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 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, as specified in “Adding a License Key” on page 25.

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. 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’ve entered the appropriate license key value and that there are no extra whitespaces 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’s 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 perpetually displays the “Loading…” message there are a couple of potential 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 will shutdown integral services whenever the required license requirements are not met. This can happen when an evaluation license expires.

It is generally not recommended that an evaluation appliance be used 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 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 will upgrade 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 will have to 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. This will detect the presence of the permanent license key and upgrade the appliance from it’s evaluation license key. You will still need to manually restart the services via the Configuration Utility.
Troubleshooting VDP Backups

The following troubleshooting items provide some direction on 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 issue 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 ESX/ESXi host. In this case only one backup job is added. Resolve any duplicate client names.

**The following items could not be located and were not selected {client name}**

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

**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 recreate any backup jobs that protect containers after moving hosts in or out of a cluster.

**After an unexpected shutdown, recent backup jobs and backups are lost**

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 55 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 prior to performing 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

Troubleshooting VDP Restores

The following troubleshooting items provide some direction on 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 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.
Troubleshooting VDP Replication Jobs

Last successful and last failed replication information not part of email report

The scheduled and ad hoc email reports that generate after a replication job completes do not contain information about the last successful replication and the last failed replication in the Replication Jobs Summary.

The user 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, however, 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.

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 cancelling an integrity check, there can be a delay of several seconds before the task is actually cancelled.

In some cases (for example, if the integrity check progress is above 90%), the integrity check may actually complete before being cancelled. Even though the integrity check may have completed successfully, the Task Console may still show an error indicating the integrity check was cancelled.

If you knew that the Integrity Check Status of the appliance (shown on the Reports tab) was “Out of Date” before you started the integrity check, then you can look at the status immediately after cancelling 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 cancelled.

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 79.

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 into a virtual machine that has been backed up by VDP, and then connect to the restore client.

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
- FAT32
- Extended partitions
- Dynamic disks
- GPT disks
- Ext4 fs
- 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.

Troubleshooting VDP Advanced

The following are known issues for vSphere Data Protection (VDP) Advanced.

The VMware VDP for Exchange Server Clients or the VMware VDP for SQL Server Clients are no longer registered with the VDP Advanced Appliance.

This can occur if the VDP Advanced Appliance has been renamed or if the clients were installed and a new checkpoint has not been created and a rollback occurred. If this happens re-install all of the VDP SQL and Exchange Clients.

If a Backup Job contains more than one SQL 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.

This issue can be resolved by either including only one Exchange or SQL Server per Backup Job or by ensuring 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 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.

Troubleshooting VDP Advanced Exchange Backups

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 Exchange to point to the same database files through different paths, such as volume G:\ and C:\MOUNTPOINT, then backup may fail.

To avoid this backup failure, configure Exchange databases to point to the database files 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

Troubleshooting VDP Advanced Exchange Restores

Restore to RDB fails or results in an unusable RDB

VDP Advanced 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:

3. 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.

4. 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.

5. Save and close the file.

Restore requirements are not met

When you restore an Exchange database, the destination Exchange server must have the same Exchange Server version and service pack as the Exchange server on which 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, respectively. 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 where the failure occurred.

Exchange Server 2007 databases are mounted after restore

Before starting a restore, VDP Advanced dismounts all databases in a storage group, even if the databases are not being selected for restore. When the restore completes, VDP Advanced attempts to mount all existing databases in the storage group, even if they were not previously mounted. VDP Advanced 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 Advanced SQL Backups

Not all databases are visible on SQL 2012

This problem can be fixed by adding the Windows system service account to SQL Sever administrator group through the following steps:

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.
3. The Login Properties dialog box appears. 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

MS SQL Server does not support backups if the database is in a restore state.

Troubleshooting VDP Advanced SQL Restores

A SQL restore with the tail-log backup option selected fails

This 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 restore option ‘Tail-log backup’ is enabled and the database doesn’t exist or is offline. In this case disable the ‘Tail-log backup’ option.

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
- appliance
  - creating a snapshot 32
  - rolling back 55
- automatic backup verification
  - troubleshooting 142

## B
- backup and recovery
  - using changed block tracking 12
  - using datastore 12
  - using file level recovery 12
  - using Virtual Machine Disk (VMDK) 12
  - using VMware vStorage APIs for Data Protection (VADP) 12
- backup job
  - full image 68
  - individual disks 68
  - on individual disks 69
- backup verification jobs
  - creating 80
- backups
  - filtering 126
  - mounting 126
  - verifying 80
- best practices
  - general 22
  - HotAdd 22
  - integrity checks 24
- storage capacity for initial VDP deployment 23
- supported disk types 18, 70

## C
- capacity
  - monitoring 23
- Changed Block Tracking (CBT) 12
- collecting logs 54

## D
- data protection
  - using changed block tracking (CBT) 12
  - using datastore 12
  - using file level recovery (FLR) 12
  - using Virtual Machine Disk (VMDK) 12
  - using VMware vStorage APIs for Data Protection (VADP) 12
- deduplication, benefits of 14
- direct to host restore
  - performing 57
- disk expansion
  - growing and adding disks 47
  - on VDP Advanced appliance 47
  - with Essentials Plus 49
- disks, types supported by VDP 18, 70
- DNS configuration
  - importance of setting up properly 20
  - verifying 20

## E
- ESXi compatibility with vFlash 18

## F
- file level recovery (FLR) 12
- filtering backups 126
- fixed-length data segment 15

## G
- GLR
  - on Microsoft Exchange 2007 servers 118
  - on Microsoft Exchange 2010 or 2013 servers 118
- granular level restore (GLR)
  - troubleshooting 117
- granular level restores (GLR)
  - log files 117

## H
- hardware versions
  - migrating 18
  - upgrading 18

## I
- Image-level backups 13
- individual disk backups
  - procedure 70
  - supported disk types 70
- individual disks
  - creating a backup job 14, 69
  - impact when migrating 71
- integrity checks 24

## K
- knowledge base, accessing articles 145
Index

L
license
  unassigning 26
license key
  deleting 26
  installing 25
  upgrading 26
  viewing information 26
licensing
  troubleshooting 138
  troubleshooting evaluation license expiration 139
  troubleshooting inability to obtain license 139
  troubleshooting license key decoding 139
  troubleshooting license keys 138
  troubleshooting lost assignments 138
log bundle, file name of 54
log collection 54

M
Microsoft Exchange
  backing up applications 112
  creating backup jobs 112
  increasing RDB wait time 144
  installing clients when UAC is enabled 102
  installing the client 110
  manually configuring the backup service 112
  restoring backups 113
  server options 109
  unsupported servers 109
  using the configuration tool 110
Microsoft SharePoint
  backing up and restoring servers 118
  creating backup jobs 119
  restoring backups 120
Microsoft SQL
  backing up and restoring 102
  backing up applications 105
  creating backup jobs 105
  installing the client 104
  restoring backups 107
  server options 103
  server support 103
mount limitations 126
mounting backups 126

N
network settings, configuring 54

O
OVF template file 24

P
performance analysis
  possible test results 49
  running 49
platform product support 13

R
replication
  cloning a job 92
  creating a job 89
  deleting a job 92
  editing a job 92
  enabling or disabling a job 92
  naming the job 91
  reviewing and completing the job 92
  running existing jobs immediately 92
  scheduling and managing jobs 88
  selecting backups for replication 90
  selecting backups to replicate 89
  setting the destination 91
  setting the retention period 91
  setting the schedule 91
  viewing job status and details 92
reports tab
  viewing information 62
restore
  to read-only media 142
  to removable media 142
restoring backups 82
  manually 83, 84, 85
  to new location 83, 84, 85
  to original location 83, 84, 85
  to SCSI disk ID 83, 84, 85
  when snapshots are present 82
retention policy 69
reverting to a snapshot 35
rolling back an appliance 55

S
services
  backup scheduler 52
  core services 52
  file level restore services 52
  file system services 52
  maintenance services 52
  management services 52
  starting and stopping 53
  status of 53
show completed activities 128
snapshot
  creating 32
  removing 34
  reverting to 35
steady state capacity 23
storage
import existing 38
supported disk types 18, 70
switching VDP Appliance to new vCenter 28
system settings, configuring 55

T
technical support resources 10
trial licenses 139
troubleshooting 139
  after an unexpected shutdown, recent backups are lost 140
  associated backup sources may be lost 140
  automatic backup verification (ABV) 142
  backup fails if VM is enabled with VMware fault tolerance 140
  backup fails if vSphere Data Protection does not have sufficient datastore capacity 140
  backups are slow to load 141
  backups fail if certain characters are used 141
  decoding license keys 139
  file level recovery 142, 143
  granular level restores 117
  inability to obtain license in portlet 139
  items could not be located 140
  license keys 138
  license violation events 138
  loading backup job data 140
  lost license keys 138
Microsoft Exchange RDB wait time 144
replication job failure errors 142
replication jobs 142
restore operation fails 142
unable to add client 140
VDP appliance is not responding 138
vSphere Data Protection Advanced 143
vSphere Data Protection Advanced Exchange backups 143
vSphere Data Protection Advanced Exchange restores 144
vSphere Data Protection Advanced SQL backups 145
vSphere Data Protection Advanced SQL restores 145
vSphere Data Protection integrity check 142

U
upgrade matrix 32
upgrading
  from VDP to VDP Advanced 26
  upgrading hardware versions 18

V
variable-length data segment 15
vCenter
  switching VDP Appliance 28
  user account permissions 133
vDP Advanced licensing
  deleting a license key 26
  viewing information 26
VDP Configure Utility 52
VDP, types of disks not supported 18, 70
vFlash and ESXi compatibility 18
Virtual Machine Disk (VMDK) 12
VMware vStorage APIs for Data Protection 12
VMware vStorage APIs for Data Protection (VADP) 12
vSphere Data Protection
  accessing knowledge base articles 145
  appliance 15
  architecture 15
  changing a configuration 54
  collecting logs 54
  disaster recovery 129
  starting and stopping services 53
  viewing status of services 52
vSphere Data Protection Appliance
description of 12
  rolling back an appliance 55
vSphere Data Protection installation 27
vSphere Data Protection sizing 18
vSphere Data Protection storage capacity 23