vSphere Data Protection Administration Guide

vSphere Data Protection 5.5

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

EN-001198-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

EN-001091-00

About This Book

The vSphere Data Protection 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 vSphere Data Protection (VDP). The information in this book is for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

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

Document Feedback

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

Technical Support and Education Resources

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

Online Support

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

Support Offerings

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

VMware Professional Services

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

Understanding vSphere Data Protection

1

This chapter includes the following topics:

vSphere Data Protection Features

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.

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.

Introduction to VMware vSphere Data Protection

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

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

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

- A **datastore** is a virtual representation of a combination of underlying physical storage resources in the datacenter. A datastore is the storage location (for example, a physical disk, a RAID, or a SAN) for virtual machine files.
- **Changed Block Tracking (CBT)** is a VMkernel feature that keeps track of the storage blocks of virtual machines as they change over time. The VMkernel keeps track of block changes on virtual machines, which enhances the backup process for applications that have been developed to take advantage of VMware's vStorage APIs.
- **File Level Recovery (FLR)** allows local administrators of protected virtual machines to browse and mount backups for the local machine. From these mounted backups, the administrator can then restore individual files. FLR is accomplished using the vSphere Data Protection 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 vSphere data protection.

Image-level Backup and Restore

VDP 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 VADP CBT feature. CBT enables VDP to only back up disk blocks that have changed since the last backup. This greatly reduces the backup time of a given virtual machine image and provides the ability to process a large number of virtual machines within a particular backup window.

By leveraging CBT during restores, VDP offers fast and efficient recoveries when recovering virtual machines to their original location. During a restore process, VDP queries VADP to determine which blocks have changed since the last backup, and then only recovers or replaces those blocks during a recovery. This reduces data transfer within the 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.

The advantages of VMware image-level backups are:

- Provides full image backups of virtual machines, regardless of the guest operating system
- Utilizes the efficient transport method SCSI HotAdd when available and properly licensed, which avoids copying the entire vmdk file image over the network
- Provides file-level recovery from image-level backups
- Deduplicates within and across all vmdk files protected by the VDP Appliance
- Uses CBT for faster backups and restores
- Eliminates the need to manage backup agents in each virtual machine
- Supports simultaneous backup and recovery for superior throughput

Replication

Replication jobs determine which client 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 (for example: the Avamar Virtual Edition (AVE) or Avamar Server). Without restore points, there is no backup associated with the replication job.

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 vSphere Data Protection Restore Client.

See Chapter 8, "Using File Level Restore," on page 69 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. VDP 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. VDP 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.

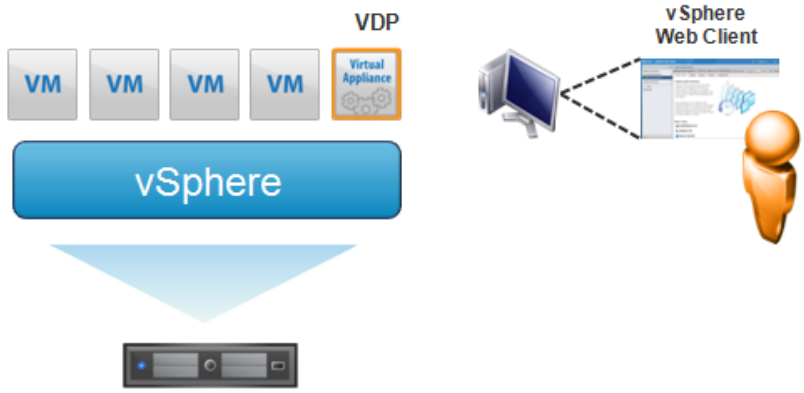
By analyzing the binary structure within the vmdk file, VDP works for all file types and sizes and intelligently deduplicates the data.

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



vSphere Data Protection Installation and Configuration

2

This chapter includes the following topics:

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

On average you can support up to 25 virtual machines per TiB of capacity.

Software Requirements

VDP 5.5 requires the following software:

- VMware vCenter Server: Version 5.1 or later
  - vCenter Server Linux or Windows

    NOTE: Backing up more than 2 TiB 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 VDP 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 VDP 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 VDP. Currently, VDP does not support the following disk types:
  - Independent
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode

System Requirements

The following section lists the system requirements for VDP.

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

Vsphere Data Protection is available in three configurations:

- 0.5 TiB
- 1 TiB
- 2 TiB

IMPORTANT Once VDP is deployed the size cannot be changed.

VDP requires the following minimum system requirements:

Table 2-1. Minimum system requirements for VDP

	0.5 TiB	1 TiB	2 TiB
Processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors
Memory	4 GB	4 GB	4 GB
Disk space	873 GB	1,600 GB	3,100 GB

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

Preinstallation Configuration

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

- "DNS Configuration" on page 15
- "NTP Configuration" on page 16
- "User Account Configuration" on page 17
- "vSphere Data Protection Best Practices" on page 18

DNS Configuration

Before you deploy VDP, you must add an entry to the DNS Server for the VDP Appliance's IP address and Fully Qualified Domain Names (FQDN). 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

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 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
- 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 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 79.

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.

vSphere Data Protection 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.

HotAdd Best Practices

- If you are using ESXi 4.1 or 5.0, make sure the ESXi hosts are licensed for HotAdd. ESXi 5.1 includes this feature by default.
- To support HotAdd capability, the VDP Appliance must be deployed on an ESXi host that has a path to the storage holding the virtual disks being backed up.
- HotAdd transport is recommended for faster backups and restores and less exposure to network routing, firewall and SSL certificate issues.
- HotAdd is not used on IDE configured virtual disks; I/O over the network negatively impacts performance.

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 each day as it frees during the maintenance windows. This is referred to as achieving steady state capacity utilization. Ideal steady state capacity should be 80%.

Monitoring vSphere Data Protection 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 58 for more information.

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

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

Once you exceed 80% capacity, 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 64 for instructions.

vSphere Data Protection Installation

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

- "Deploy the OVF Template" on page 19
- "Configuring the VDP Appliance System Settings" on page 20

Deploy 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 77, 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 (this must match the entry configured on the DNS Server) and click on the folder or datacenter in which you want it deployed. The VDP Appliance Name should not be changed after installation. Click **Next.**

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

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

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

15 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.

16 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 is complete.

Configuring the VDP Appliance System Settings

Prerequisites

The VDP .ovf template (see "Deploy the OVF Template" on page 19) 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**.

In the console, the URL and the steps required to configure the VDP display.

5 Enter the required information in the console.

6 Open a web browser and type:

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

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:

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** check box for SSO authentication.

NOTE Leave the **Use vCenter for SSO authentication** check box 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 17 for instructions on how to update the vCenter user role.

15 Click **Next**.

The Create Storage screen displays. See "Creating New Storage" on page 24 to create new storage or attach existing VDP storage.

vSphere Data Protection Storage Management

3

This chapter contains the following topics:

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.

NOTE Migrating the appliance to a new host or to a new datastore is not supported during storage configuration.

Prerequisites

- The VDP Appliance is installed and configured.
- 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**.

Type of storage	Capacity in TiB
Local VDP storage	■ 0.5 ■ 1 ■ 2

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 is the default.

- 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. However, the thin disk starts small and uses only as much datastore space as the disk needs for its initial operations.
- 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 provisioning on a datastore that had previous data, the previous data is erased and cannot be recovered. It might take much longer to create disks in this format than to create other types of disks.
- Thick Lazy-Zeroed —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.

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** check box. 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.

In order to pass the performance analysis, the expected write speed is 30 MB per second, the expected read speed is 60 MB per second, and the expected seek speed is 400 seeks per second.

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** check box 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** check box 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

When you elect to attach existing VDP storage, you must locate previously-used VDP disks and add them to the new VDP Appliance. If you attach an incomplete or invalid storage configuration, an error message appears during the validation phase.

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

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

Prerequisites

- Before you can attach existing storage, you must install and configure the VDP Appliance described in "vSphere Data Protection Installation and Configuration" on page 13.
- 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.

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 for the VDP Appliance where the VMDKs originally resided.

9 Enter the VDP Appliance root password into the **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 should be 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.

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

   e Click Hard disk 2 from the list.

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

   g Click 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 Deploy a new VDP Appliance. Refer to "vSphere Data Protection Installation" on page 19 for instructions.

4 Delete the old VDP Appliance:

   a Navigate to **vCenter > Hosts and Clusters** and locate the VDP Appliance.

   b Right-click the VDP Appliance and select **Delete from Disk**.

5 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 25.

Viewing the Storage Configuration

Prerequisite

- Using the Initial Configuration wizard, you have successfully distributed the VDP storage disks across the available datastore locations.

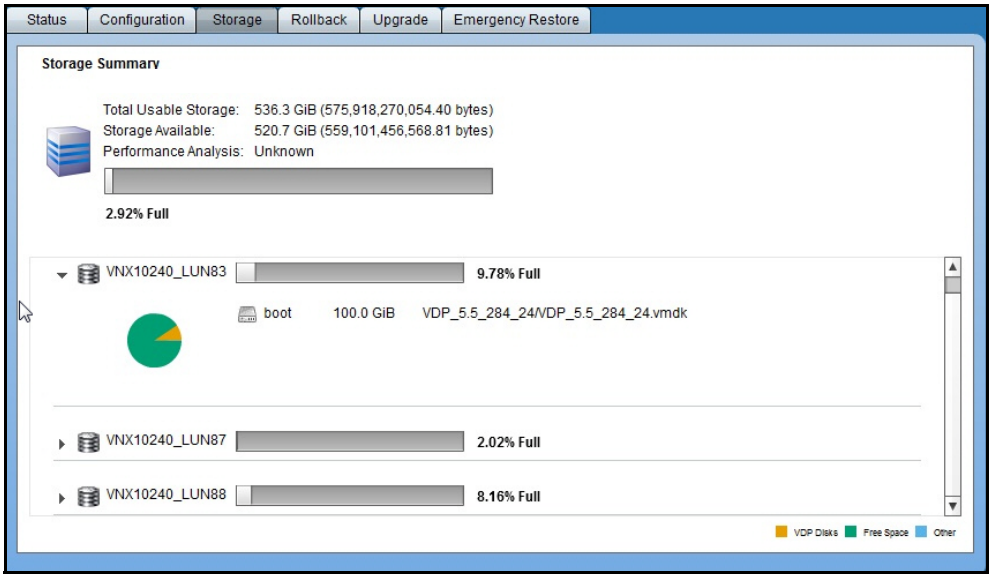
Procedure

1 Log in to the VDP-Configure URL:

   http:<*VDP appliance IP*>:8580/vdp-configure

2 Click the **Storage** tab.

The available datastores display, along with 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.



3 If the performance analysis test was run when creating storage for this VDP Appliance, click the hyperlink that corresponds to **Performance Analysis** under Storage Summary.

The Performance Analysis dialog box appears, displaying read, write, and seek measurements.

4 Click **OK** to close the Performance Analysis dialog box.

Post-Installation Configuration of vSphere Data Protection Appliance

4

This chapter contains the following topics:

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 for the following procedures:

- "Viewing Status" on page 30—Allows you to see the services currently running (or currently stopped) on the VDP Appliance.
- "Starting and Stopping Services" on page 31—Allows you to start and stop selected services on the VDP Appliance.
- "Collecting Logs" on page 32—Allows you to download current logs from the VDP Appliance for troubleshooting purposes.
- "Changing vSphere Data Protection Configuration" on page 32—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 33—Allows you to restore the VDP Appliance to an earlier known and valid state.
- "Emergency Restore" on page 34 —Allows you to restore a VM directly to the ESX host that is running the VDP Appliance. This emergency restore procedure is intended for use when the vCenter is unavailable.
- "Installing the Upgrade" on page 39 — Allows you to restore the VDP Appliance to a previously-known state in the event that the upgrade process does not complete successfully.

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 4-2. Description of services running on the VDP Appliance.

Service	Description
Core services	These are the services that comprise the backup engine of the VDP Appliance. If these services are disabled no backup jobs (either scheduled or "on demand") will run, and no restore activities can be initiated.
Management services	Management services should only be stopped under the direction of technical support.
File system services	These are the services that allow backups to be mounted for file-level restore operations.
File level restore services	These are the services that support the management of file-level restore operations.

Table 4-2. Description of services running on the VDP Appliance.

Service	Description
Maintenance services	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.
Backup scheduler	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.

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

Collecting Logs

The log bundled is intended primarily to facilitate sending logs of the VDP Appliance to support personnel. You can download all the logs from VDP services as a zip file by clicking **Collect logs**. 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.

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

Changing vSphere Data Protection 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, vCenter Registration, and System Settings.

Network Settings

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

- IPv4 static address
- Netmask
- Gateway
- Primary DNS
- Secondary DNS
- Hostname
- Domain

vCenter Registration

You can configure the vCenter Registration options on the vCenter Registration tab:

- vCenter User Name (see Chapter 2, "User Account Configuration," on page 17 for additional information)
- vCenter password
- vCenter FQDN or IP (associated with the VDP Appliance)
- vCenter Port

CAUTION If you edit the vCenter host name, IP address, or port, the backup jobs associated with VDP will be deleted.

System Settings

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

- Changing time zone
- Changing VDP Appliance password

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.

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

A direct to host emergency restore operation restores a VM directly to the ESX host that is running the VDP Appliance. This emergency restore procedure is intended for use when the vCenter is unavailable.

NOTE Before you attempt to perform a direct to host operation from the VDP Appliance, ensure that the DNS server from the VDP Appliance can fully resolve the ESX host name. If the host name cannot be resolved, the host restore will fail.

Prerequisite

- The ESX 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 vSphere Data Protection 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 host credentials:

   - ESX host name or IP—enter the ESX host name or ESX host IP address.
   - Port - 443, which is the default, is prepopulated.
   - Username—enter the ESX 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 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 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 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 51 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 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.

vSphere Data Protection Appliance Upgrades

5

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.

The upgrade process consists of the following general steps:

1 "Selecting a Time for Upgrading the VDP Appliance" on page 38

2 "Creating a Snapshot of the VDP Appliance" on page 38

3 "Mounting the Upgrade ISO Image on the Appliance" on page 39

4 "Installing the Upgrade" on page 39

5 "Removing the Snapshot and Unmounting the Upgrade Image" on page 40

Allowed Upgrade Paths

Table 5-3 lists the allowed upgrade paths for VDP and VDP Advanced versions.

Table 5-3. Allowed Upgrade Paths from VDP to VDP Advanced

		Upgrade TO					
		VDP 5.1.0.0	VDP 5.1.10.32	VDP Advanced 5.1.20.24	VDP Advanced 5.1.21	VDP 5.5.1	VDP and VDP Advanced 5.5.*x*
Upgrade FROM	VDP 5.1.0.0	X	X	X	X	X	X
	VDP 5.1.10.32		X	X	X	X	X
	VDP Advanced 5.1.20.24			X	X		
	VDP Advanced 5.1.21				X		X
	VDP 5.5.1					X	X
	VDP and VDP Advanced 5.5.*x*						X

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

In the event that the upgrade does not work as expected, it is recommended to take a snapshot of the VDP Appliance prior to the upgrade. In the event of an upgrade issue, you may roll back to the snapshot.

NOTE At the time of installation, the virtual disks used by the VDP Appliance are set to be "Independent - Persistent." However, in order to take a snapshot, the disks must be temporarily changed to "Dependent."

To create a snapshot of the VDP Appliance:

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 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** check box 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.

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 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 and 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 vSphere Data Protection plug-in. VDP version 5.5 is managed using the vSphere Data Protection 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 vSphere Data Protection 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:

http://pubs.vmware.com/vsphere-51/index.jsp.

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 41.

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**.

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

7 Click the Snapshot you created for the VDP Appliance.

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

9 Click **Close**.

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

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

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

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

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

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

16 Click **OK**.

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

The VDP Appliance upgrade process is complete.

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.

Using vSphere Data Protection

6

This chapter includes the following topics:

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 "vSphere Data Protection Installation and Configuration" on page 13.

Procedure

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

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

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

VDP uses this information to connect to vCenter to perform backups, so the specified user account must have administrative privileges.

3 In the vSphere Web Client, select **vSphere Data Protection**.

4 In the Welcome to vSphere Data Protection page, select the vSphere Data Protection Appliance and click **Connect**.

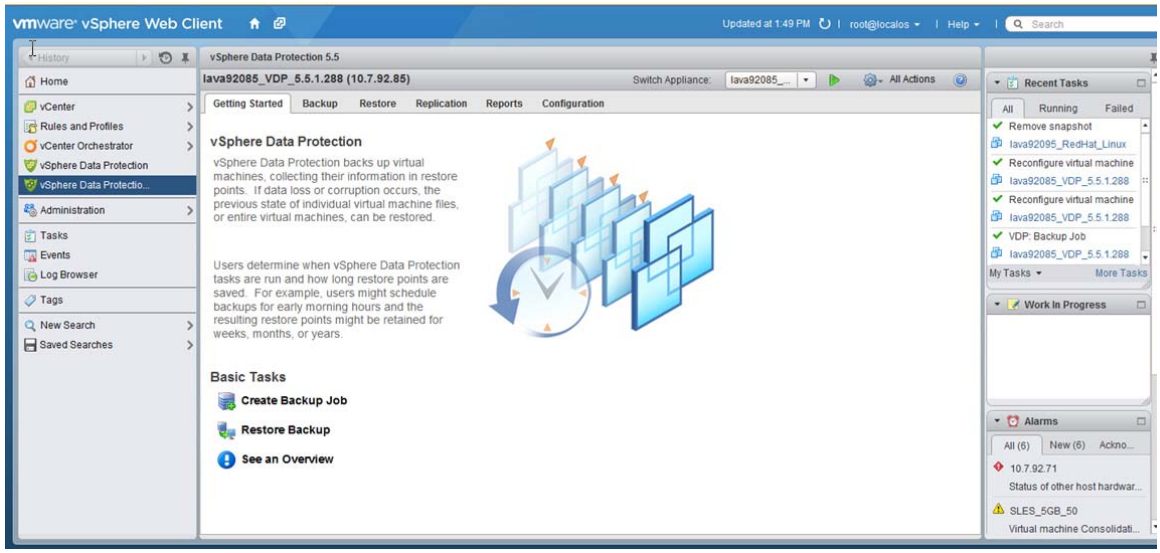
Switching vSphere Data Protection Appliances

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 vSphere Data Protection 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.

Understanding the vSphere Data Protection 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 (See an Overview).
- **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"Managing Backup Jobs" on page 45 for additional information.
- **Restore** – provides a list of successful backups that can be restored. See "Managing Restores" on page 51 for additional information.
- **Replication** – provides a list of successful backups that can be replicated. See "Managing Replication Jobs" on page 54 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 58 for additional information.
- **Configuration** – displays information about how VDP is configured and allows you to edit some of these settings. See "Configuring vSphere Data Protection Appliance" on page 61 for additional information.

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.

Managing backup jobs involves the following tasks:

Limitations

- Backing up greater than 2 TiB 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:
  - vSphere Data Protection (VDP) Appliances
  - VMware Data Recovery (VDR) Appliances
  - Templates
  - Secondary fault tolerant nodes
  - Proxies
  - Avamar Virtual Edition (AVE) Servers

NOTE The Create a new backup job wizard enables you to select these virtual machines; however, when you click Finish to complete the wizard, you receive a warning that these special virtual machines were not added to the job.

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.

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

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 disk types:
  - Independent
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode

Procedure

1 From a web browser, access vSphere Data Protection. Refer to "Accessing vSphere Data Protection" on page 44 for instructions.

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.

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**.

5 On the Data Type page, select **Full Image** or **Individual Disks**, depending on what you want to back up, 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 check boxes next to the items to add to the backup job, and click **Next**.

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

8 On the Retention Policy page, select a retention period and click **Next**. The retention periods that you can choose from are describe 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.

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 points and, if the system determines that the data is not being used, the data is removed and the disk capacity frees up.

9 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, ì, ü, and ñ).

10 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.

11 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.

Supported disk types

- When planning for individual disk backups, make sure the disks are supported by VDP. Currently, VDP does not support the following 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 check box is unavailable.

Prerequisites

The VDP Appliance is installed and configured on your vCenter Server.

Procedure

1 From a web browser, access vSphere Data Protection. Refer to "Accessing vSphere Data Protection" on page 44 for instructions.

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 check boxes 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: â, é, ì, 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:

http://pubs.vmware.com/vsphere-51/index.jsp.

Users have two options when migrating a virtual machine from one datastore to another:

- Migrate the full virtual machine all at once to another datastore. When a full virtual machine is migrated, the VDP Appliance updates the backup jobs with the new locations of the protected VMDKs.
- Migrate individual disks to another datastore, where disks for a single virtual machine may reside on a different datastore.

In the case where a user migrates individual disks (vmdk files) 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. If more than six virtual machines are in the backup job, a **Show Items** link appears.
- **Out of Date** – a list of all the virtual machines that failed to back up the last time the job ran. If more than six virtual machines are out of date, a **more** link appears. Clicking the **more** link displays the Protect Item List dialog, which displays a list of all the virtual machines in the backup job.

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 vSphere Data Protection 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."

Managing Restores

Once clients have been backed up, you can restore the backups to the original location or to an alternate location.

Restore operations are performed on the Restore tab. The Restore tab displays a list of virtual machines that have been backed up by the VDP Appliance. By navigating through the list of backups, you can select and restore specific backups.

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**.

Managing the restores of client backups involves the following tasks:

- "Restoring Backups Manually" on page 52
- "Restores when Snapshots are Present" on page 52
- "Locking and Unlocking a Backup" on page 53
- "Deleting a Backup" on page 54
- "Clearing all selected backups" on page 54

Selecting Backups to Restore

Backups can be restored through the following options:

- Click **Restore a VM** on the Getting Started tab of the vSphere Data Protection screen.
- From the Restore tab, select a restore point and click **Restore**.
- Select a protected virtual machine in the vSphere Data Protection 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.

Setting the Restore Options for Backups

On the Set Restore Options page of the Restore a backup wizard, you can specify to where you want the backup restored:

- **Restore to Original Location** – if the Restore to Original Location box is checked, the backup restores to its original location. If the vmdk file still exists at the original location it is overwritten.
- **Restore to New Location** – if you uncheck the Restore to Original Location box, then you can specify a new location where the backup will be restored.

Restores when Snapshots are Present

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.

NOTE 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.

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

http://kb.vmware.com/selfservice/microsites/search.do?language=en US&cmd=displayKC&externalId=1025279

and

https://community.emc.com/thread/145249?start=0&start=0

Restoring Backups Manually

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

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 vSphere Data Protection. Refer to "Accessing vSphere Data Protection" on page 44 for instructions.
2. Click the **Restore** tab.
3. If needed, filter the backups to narrow down your search.
4. Click a client listed in the **Name** column. When you click a client, 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 Restore points for disks that have been imported are renamed and appended by a string of random letters.

5 Click the check box 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, do one of the following:

- Leave the **Restore to Original Location** box checked if you want to the backup to restore to its original location. If the vmdk file still exists at the original location it is overwritten.

  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.

- Clear the **Restore to Original Location** box to restore the backup to a new location. Specify the following information:

  New VM Name — Type a new name for the restored VM.

  Destination — Click **Choose**, and select the new destination.

  Datastore — Select the datastore to which the VM will be restored.

  Optionally, you can set the virtual machine to **Power On** and **Reconnect NIC** after the restore process completes.

9 Click **Next**.

The Ready to complete page appears.

10 On the Ready to complete page, review the summary of your restore requests.

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.

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 25). 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 vSphere Data Protection. Refer to "Accessing vSphere Data Protection" on page 44 for instructions.

2 From the vSphere Data Protection user interface – Restore tab, click the disclosure arrows to locate the backup you want to lock.

3 Click the check box 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.

Deleting a Backup

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

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.

Managing Replication Jobs

Replication jobs determine which client 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 (for example: the Avamar Virtual Edition (AVE) or Avamar Server). Without restore points, there is no backup associated with the replication job.

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

Table 6-4. Replication compatibility matrix

Backups created with this product...	Can be replicated to this product...	
	VDP Advanced	Avamar
VDP	No	Yes
VDP Advanced	Yes	Yes

Replication operations involve the following tasks:

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.

Creating a Replication Job

You create replication jobs by using the Create a new replication job wizard, which walks you through each step.

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.

1 From a web browser, access vSphere Data Protection. Refer to "Accessing vSphere Data Protection" on page 44 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.

State — Whether the replication job is enabled or disabled. Disabled replication jobs will not run.

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**.

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:

i 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 – An unlimited number of backups the meet the **Backup Type** criteria will be replicated.

Number of Backups – Select the maximum number of backups meeting the **Backup Type** criteria that will be replicated.

c Specify the **Date Restrictions**:

None – All backups that meet the **Backup Type** criteria will be replicated.

Last – Select a number and a time unit. Backups meeting the **Backup Type** criteria that occurred during the specified number of time units will be replicated.

By Range – Select a **From** date and time, and select a **To** date and time. Backups meeting the **Backup Type** criteria that occurred during this range of time will be replicated.

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 vSphere Data Protection 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 vSphere Data Protection 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**.

Viewing Information from the Reports Tab

The portion of 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.
- **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 Successful Backups** – the number of virtual machines that successfully backed up in the most recently completed backup job.

- **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 for VDP or 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:
  - Status – The status of the last backup job.
  - Date – The date and time that the last backup job ran.
  - Backup Job Name – The name of the last backup job that ran.
- Replication Information – Contains the following:
  - Replication Jobs – The names of the replication jobs with which the client is associated.
  - Last Replication Run Time – The date and time the most recent replication job ran successfully. If no replication job has run, this column contains "Never."

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 50.

For more information on using these consoles to monitor VDP operations see "Viewing the Event Console" on page 66 or "Viewing Recent Tasks" on page 65.

Configuring vSphere Data Protection Appliance 7

The Configuration tab is used for the following tasks.

Configuring VDP Details

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:

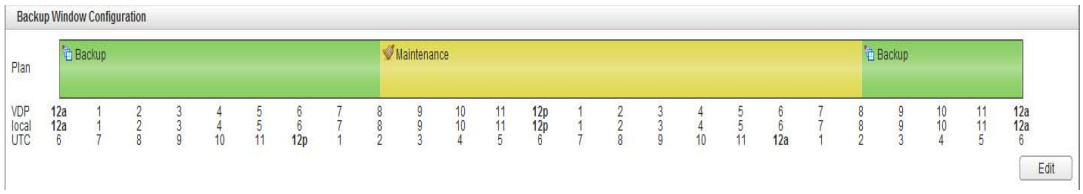
- Display name
- IP Address
- Major Version (VDP version number)
- Minor Version (used by Technical Support)
- Status
- vCenter Server
- Host/ESX IP
- VDP backup user
- Local time
- Time zone

These options are configured during the VDP Appliance installation. They can be edited through the VDP configure utility. See "Post-Installation Configuration of vSphere Data Protection Appliance" on page 29 for additional details.

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.

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



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

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

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

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

Editing the Backup Window

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

Prerequisites

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

Procedure

1. From a web browser, access vSphere Data Protection. Refer to "Accessing vSphere Data Protection" on page 44 for instructions.
2. From the vSphere Data Protection 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

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 vSphere Data Protection. Refer to "Accessing vSphere Data Protection" on page 44 for instructions.
2. From the vSphere Data Protection 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.

Refreshing the Configuration

To refresh the information and see the latest entries, click **Refresh** on any screen.

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 for the VDP Appliance to continue to make backups while the integrity check is out of date, you are risking losing potential backup data if a rollback to the last validated checkpoint is ever required.

You can see a list of all of the VDP checkpoints through the VDP configure utility, Rollback tab. See "Rolling Back an Appliance" on page 33 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 vSphere Data Protection. Refer to "Accessing vSphere Data Protection" on page 44 for instructions.

2 From the vSphere Data Protection user interface – Configuration tab, click the  icon and select **Run integrity check**.

3 A confirmation screen displays, asking if you want 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.

Monitoring vSphere Data Protection Activity

You can monitor the activities of the vSphere Data Protection application by:

- "Viewing Recent Tasks" on page 65.
- "Viewing Alarms" on page 66
- "Viewing the Event Console" on page 66

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 (vSphere Data Protection starting the backup job)

3 Reconfigure virtual machine (the vSphere Data Protection 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 7-5. VDP alarms

Alarm Name	Alarm Description
VDP: [001] The most recent checkpoint for the VDP Appliance is outdated.	From the Configuration tab of the VDP user interface, click the All Actions icon and select "Run integrity check."
VDP: [002] The VDP Appliance is nearly full.	The VDP Appliance is nearly out of space for additional backups. You can free space on the appliance by manually deleting unnecessary or older backups and by changing retention policies on backup jobs to shorten the time that backups are retained.
VDP: [003] The VDP Appliance is full.	The VDP Appliance has no more space for additional backups. The appliance will run in read-only (or restore-only) mode until additional space is made available. You can free space on the appliance by manually deleting unnecessary or older backups and by changing retention policies on backup jobs to shorten the time that backups are retained.
VDP: [004] The VDP Appliance datastore is approaching maximum capacity.	The datastore where the VDP Appliance provisioned its disks is approaching maximum capacity. When the maximum capacity of the datastore is reached, the VDP Appliance will be suspended. The appliance cannot be resumed until additional space is made available on the datastore.
VDP: [005] Core services are not running.	Start Core services using the VDP configure utility.
VDP: [006] Management services are not running.	Start Management services using the VDP configure utility.
VDP: [007] File system services are not running.	Start File system services using the VDP configure utility.
VDP: [008] File level restore services are not running.	Start File level restore services using the VDP configure utility.
VDP: [009] Maintenance services are not running.	Start Maintenance services using the VDP configure utility.
VDP: [010] Backup scheduler is not running.	Start Backup scheduler using the VDP configure utility.
VDP: [011] Host license does not permit VDP	The ESX host license does not permit usage of VDP and the 60 day evaluation period has ended.

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 33 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.

Using File Level Restore

8

This chapter includes the following topics:

Introduction to the vSphere Data Protection Restore Client

vSphere Data Protection (VDP) creates backups of entire virtual machines. These backups can be restored in their entirety using the vSphere Data Protection user interface through the vSphere Web Client. However, if you only want to restore specific files from these virtual machines, then use the vSphere Data Protection 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 14 for web browsers supported by vSphere 5.5. Internet Explorer 10 is not supported and is unreliable with the Restore Client.

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 filesystems
- 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

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.

Logging In to the Restore Client

The Restore Client operates in one of two modes:

- **Basic**—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. The Restore Client only displays backups for the local virtual machine.

  For example, if you were logging in to the Restore Client in Basic mode from a Windows host named "WS44" then you would only be able to mount and browse backups of "WS44."

- **Advanced**—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. After connecting to the Restore Client, you will be able to mount, browse, and restore files from any virtual machine that has been backed up by VDP. All restore files will be 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 "vSphere Data Protection Installation" on page 19 for additional information.

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.

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 vSphere Data Protection 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 "vSphere Data Protection Installation" on page 19 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 vSphere Data Protection 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 Disaster Recovery

9

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 33). 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 a clean shut down process. See "VDP Shutdown and Startup Procedures" on page 67 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 Port Usage

A

vSphere Data Protection (VDP) uses the ports listed in the following table.

Table A-1. VDP port usage

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

Minimum Required vCenter User Account Permissions

B

See "User Account Configuration" on page 17 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 vSphere Data Protection Appliance to all of the following categories:

Datastore

- Allocate space
- Browse datastore
- Low level file operations
- Move datastore
- Remove datastore
- Remove file
- Rename datastore

Folder

- Create folder

Global

- Licenses
- Settings
- Manage custom attributes
- Cancel task
- Log event
- Disable methods
- Enable methods

Network

- Assign network
- Configure

Resource

- Assign virtual machine to resource pool

Alarms

- Create alarm

Sessions

- Validate session

Extension

- Register extension
- Update extensions

Tasks

- Create task
- Update task

vApp

- Configure vApp application
- Export

Virtual machine > guest operations

- Guest operation modifications
- Guest operation program execution
- Guest operations queries

Virtual machine > interaction

- Console interaction
- Guest operating system management by VIX API
- VMware tools install

Virtual machine > interaction

- Allow disk

Virtual machine > Configuration

- Add existing disk
- Add new disk
- Add or remove device
- Advanced
- Change CPU count
- Change resource
- Disk change tracking
- Disk lease
- Extend virtual disk
- Host USB device
- Memory
- Modify device setting
- Raw device

- Reload from path
- Remove disk
- Rename
- Reset guest information
- Settings
- Swapfile placement
- Upgrade virtual machine compatibility

Virtual machine > Interaction

- Power Off
- Power On
- Reset

Virtual machine > Inventory

- Create new
- Register
- Remove
- Unregister

Virtual machine > Provisioning

- Allow read-only disk access
- Allow virtual machine download
- Mark as Template

Virtual machine > Snapshot management

- Create snapshot
- Remove snapshot
- Revert to snapshot

vSphere Data Protection Troubleshooting

C

This chapter includes the following troubleshooting topics:

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 14).
- Confirm that the hardware meets the minimum hardware requirements (see "System Requirements" on page 15).
- Confirm that DNS is properly configured for the VDP Appliance. (see "Preinstallation Configuration" on page 15).

NOTE Refer to VMware KB article 2041813 for additional information.

Troubleshooting Accessing the vSphere Data Protection 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 32 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 15 for additional information.

Troubleshooting vSphere Data Protection 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 33 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 vSphere Data Protection 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 cam 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 vSphere Data Protection 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 innacurate reporting of execution errors, the user cannot determine the state of the destination server.

Troubleshooting vSphere Data Protection 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 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.

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

R

S

T

U

V