vSphere Data Protection Administration Guide

vSphere Data Protection 5.1

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-000846-00

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About This Book

The vSphere Data Protection Administration Guide contains information to install and manage backups for small and medium businesses.

Intended Audience

This book is for anyone who wants to provide backup solutions using vSphere Data Protection. 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

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

The benefits of vSphere Data Protection are:

- Provides fast and efficient data protection for all of your virtual machines, even those powered off or moved between physical hosts.
- Significantly reduces disk space consumed by backup data using smart deduplication across all backups.
- Reduces the cost of backing up virtual machines and minimizes the backup window using change block tracking 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, that can be managed by a web portal.
- Direct access to vSphere Data Protection configuration integrated into the standard 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.

This chapter includes the following topics:

Introduction to 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 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.
- **VMware vStorage APIs for Data Protection (VADP)** enables backup software to perform centralized VM 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 vSphere Data Protection appliance** is a purpose built virtual appliance for vSphere data protection.

Image-level Backup and Restore

vSphere Data Protection creates image-level backups, which are integrated with vStorage API for Data Protection, a feature set within vSphere to offload the backup processing overhead from the VM to the vSphere Data Protection appliance. The appliance communicates with the vCenter Server to make a snapshot of a VM's VMDK. 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 vSphere Data Protection appliance can simultaneously backup to eight virtual machines to enhance the data protection workload capacity.

To increase the efficiency of image-level backups, vSphere Data Protection utilizes VADPs Changed Block Tracking (CBT) feature. CBT is a VMware feature that enables vSphere Data Protection to only backup disk blocks that have changed since the last backup. This greatly reduces the backup time of a given VM image and provides the ability to process a large number of VMs within a particular backup window.

By leveraging CBT during restores, vSphere Data Protection offers fast and efficient recoveries when recovering VMs to their original location. During a restore process, vSphere Data Protection 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 objective (RTO).

Additionally, vSphere Data Protection 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 times. This is useful in scenarios where the change rate since the last backup in a VM being restored is very high and the overhead of a CBT analysis operation would be more costly than a direct full image recovery. vSphere Data Protection will intelligently decide which deployment method will result in the fastest VM image recovery times for your particular scenario or environment.

The advantages of VMware image backups are:

- Provides full image backups of VMs, regardless of the guest operating system
- Utilizes the efficient transport method SCSI hotadd when available and properly licensed, which avoids copying the entire VMDK image over the network

- Provides file-level recovery from image-level backups
- Deduplicates within and across all .vmdk files protected by the vSphere Data Protection appliance
- Uses changed block tracking for faster backups and restores
- Minimizes network traffic by deduplicating and compressing data
- Eliminates the need to manage backup agents in each VM
- Supports simultaneous backup and recovery for superior throughput

IMPORTANT The best practice for VM image backups is to install VMware Tools on each virtual machine. VMware Tools adds additional backup capability that quiesces certain processes on the guest OS prior to backup.

File Level Recovery

File Level Recovery (FLR) allows local administrators of protected VMs to browse and mount backups for the local machine. From these mounted backups the administrator can then restore individual files. File level recovery is accomplished using the vSphere Data Protection restore client.

Deduplication Store Benefits

Enterprise data is highly redundant, with identical files or data stored within and across systems (for example, OS files or documents sent to multiple recipients). Edited files also have tremendous redundancy with previous versions. Traditional backup methods magnify this by storing all of the redundant data over and over again. vSphere Data Protection uses patented deduplication technology to eliminate redundancy at both the file and the subfile data segment level.

Variable vs. Fixed-Length Data Segments

A key factor in eliminating redundant data at a segment (or subfile) level is the method for determining segment size. Fixed-block or fixed-length segments are commonly employed by snapshot and some deduplication technologies. Unfortunately, even small changes to a dataset (for example, inserting data at the beginning of a file) can change all fixed-length segments in a dataset, despite the fact that very little of the dataset has been changed. vSphere Data Protection uses an intelligent variable-length method for determining segment size that examines the data to determine logical boundary points, eliminating the inefficiency.

Logical Segment Determination

vSphere Data Protection uses a patented method for segment size determination designed to yield optimal efficiency across all systems. vSphere Data Protection'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 compressed to an average of 12 KB.

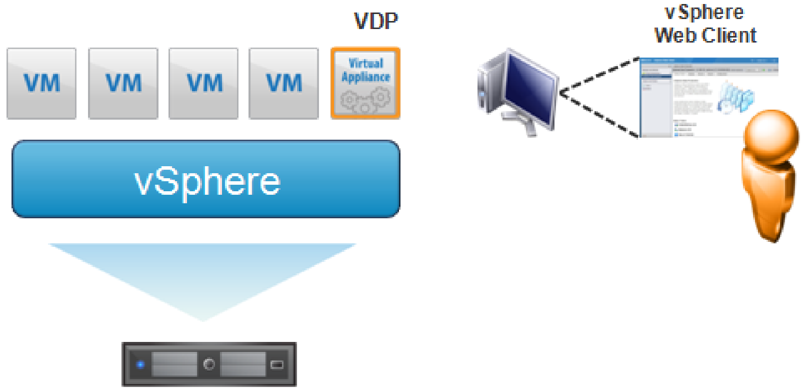
By analyzing the binary structure within the VMDK files, vSphere Data Protection works for all file types and sizes and intelligently deduplicates the data.

vSphere Data Protection Architecture

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

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

- vSphere 5.1
- vSphere Data Protection appliance (installed on ESX/ESXi 4.x or 5.x)
- vSphere Web Client.



Installing and Configuring vSphere Data Protection

2

This chapter includes the following topics:

vSphere Data Protection Sizing

vSphere Data Protection sizing helps determine the vSphere Data Protection appliance size and number of appliances required based on:

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

The following table shows examples for vSphere Data Protection sizing recommendations:

Table 2-1. Sample recommendations for vSphere Data Protection sizing

# of VMs	Data storage per client	Retention: daily	Retention: weekly	Retention: monthly	Retention: yearly	Recommendation
25	20 GB	30	0	0	0	1- 0.5 TB
25	20 GB	30	4	12	7	1- 2 TB
25	40 GB	30	4	12	7	2- 2 TB
50	20 GB	30	0	0	0	1- 1 TB
50	20 GB	30	4	12	7	2- 2 TB
50	40 GB	30	4	12	7	3- 2 TB
100	20 GB	30	0	0	0	1- 2 TB
100	20 GB	30	4	12	7	3- 2 TB
100	40 GB	30	4	12	7	6- 2 TB

The recommendations above (note these are only guidelines) are based on the following assumptions:

- The VMs primarily contain file system data. If the VMs primarily contain database data, the deduplication rates will be lower.
- 70% initial deduplication rate for file system data.
- 99.7% daily deduplication rate for file system data.
- The annual growth rate is 5%.

IMPORTANT If you are unsure of the size of the appliance to deploy, it is better to use a larger vSphere Data Protection datastore. Once a appliance has been deployed, the size of the datastore cannot change.

Software Requirements

vSphere Data Protection 5.1 requires the following software:

- VMware vCenter Server
  - vCenter Server Linux or Windows: Version 5.1
  - vSphere Web Client is supported on Microsoft Internet Explorer 7 and 8 (there are currently known issues with running the vSphere Web Client on IE 8) or Mozilla Firefox 3.6 or higher.
  - Web browsers need to be enabled with Adobe Flash Player 11.3 or higher to access the vSphere Web Client or vSphere Data Protection functionality

- VMware ESX/ESXi (the following versions are supported)
  - ESX/ESXi 4.0, ESX/ESXi 4.1,ESXi 5.0, ESXi 5.1
- Appliance version:
  - vSphere Data Protection: 5.1

System Requirements

The vSphere Data Protection appliance is available in three options:

- 0.5 TB
- 1 TB
- 2 TB

IMPORTANT Once vSphere Data Protection is deployed the size cannot be changed.

The system requirements for each option of vSphere Data Protection are specified in the following table.

	0.5 TB	**1 TB**	**2 TB**
Processors dedicated to vSphere Data Protection	Minimum four 2 GHz processors available to vSphere Data Protection at all times	Minimum four 2 GHz processors available to vSphere Data Protection at all times	Minimum four 2 GHz processors available to vSphere Data Protection at all times
Physical memory dedicated to vSphere Data Protection	4 GB	4 GB	4 GB
Disk space	850 GB	1,600 GB	3,100 GB
Network connection	1 GbE connection	1 GbE connection	1 GbE connection

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

vSphere Data Protection Specifications

vSphere Data Protection supports the following specifications:

- Each vSphere Data Protection appliance supports backup for up to 100 VMs
- Each vCenter Server can support up to 10 vSphere Data Protection appliances
- Support for 0.5 TB, 1 TB, or 2 TB of deduplication storage

Preinstallation Configuration

Prior to vSphere Data Protection installation, DNS and NTP need to be configured.

DNS Configuration

Before you deploy vSphere Data Protection, an entry needs to be added to the DNS Server for the appliance IP address and FQDN. This DNS Server must support forward and reverse lookup.

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

To confirm that DNS is configured properly:

1 Open a command prompt and type the following command:

nslookup <*VDP_IP_address*> <*DNS_IP_address*>

The nslookup command will return the FQDN of the vSphere Data Protection appliance.

2. Type the following command:

   nslookup *<FQDN_of_VDP> <DNS_IP_address>*

   The nslookup command will return the IP address of the vSphere Data Protection appliance.

3. If the nslookup commands returned the proper information, close the command prompt, if not resolve the DNS configuration prior to vSphere Data Protection installation.

NTP Configuration

vSphere Data Protection uses Network Time Protocol (NTP). Before you install vSphere Data Protection, NTP needs to be configured on the vCenter Server and the ESXi host that vSphere Data Protection will be installed on.

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

User Account Configuration

Before the vCenter user account can be used with vSphere Data Protection, or before the SSO admin user can be used with vSphere Data Protection, these users should be specifically added as administrator on the vCenter root node. The following steps are used to configure the vSphere Data Protection user or SSO admin user using the vSphere Client.

1. Login to the vSphere Web Client and select **vCenter** > **Hosts and Clusters**.
2. On the left pane, click on the vCenter Server.
3. Click the **Manage** tab and then the **Permissions** sub-tab.
4. Click the **Add permission** icon.
5. Click **Add**.
6. From the Domain drop-down select domain, server, or SYSTEM-DOMAIN.
7. Select the user that will administer vSphere Data Protection or be the SSO admin user and then click **Add**.
8. Click **OK**
9. From the Assigned Role drop down select Administrator.
10. Confirm that the Propagate to child objects box is checked.
11. 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 vSphere Data Protection backup user using the VDP-configure UI 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 then tasks related to backup job may not show up on the Recent Running tasks.

Deploy the OVF Template

Prerequisites

- The vSphere Data Protection appliance is installed on an ESXi 4.0, 4.1, 5.0, or 5.1 host.
- vCenter 5.1 is required. Login to vCenter from a vSphere Web Client to deploy the OVF template.
- The vSphere Data Protection appliance connects to ESXi using port 902. If there is a firewall between the appliance and ESXi, port 902 must be open.
- The VMware Client Integration Plug-in 5.1.0 needs to be installed in your browser.

Procedure

1 Log in to the vSphere Web Client and select **vCenter > Datacenters.**

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

3 Select the source where the vSphere Data Protection appliance is located.

4 By default the select source dialog is set to OVF Packages. Change it to **OVA Packages**.

5 Select the appliance and click **Open**.

6 After the appliance .ova file is selected, click **Next**.

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

NOTE The OVA certificate will be "Untrusted" unless the Thawte intermediary certificates are installed.

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

9 On the Select name and folder screen, enter the name for the appliance and click on folder or datacenter you want it deployed in. Click **Next.**

10 Select the host for the appliance and click **Next**.

11 Select the virtual disk format ("Impact of Selecting Thin or Thick Provisioned Disks" on page 47 provides additional information) and the location of the storage for the appliance. Click **Next**.

12 Select the Destination Network for the appliance and click **Next**.

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

NOTE The vSphere Data Protection appliance does not support DHCP. The appliance requires a static IP address.

14 On the Ready to complete screen, confirm that all of the deployment options are correct and click **Finish**.

vCenter deploys the vSphere Data Protection appliance. Monitor **Recent Tasks** to determine when the deployment is complete.

vSphere Data Protection Installation and Configuration

Prerequisites

The vSphere Data Protection .ovf template (see "Deploy the OVF Template" on page 14) must have deployed successfully, and you must be logged into the vCenter Server from the vSphere Web Client.

Procedure

1 Select **vCenter Home > vCenter > VMs and Templates**. Expand the vCenter tree and select the vSphere Data Protection appliance. Right-click the appliance and select **Power On**.

2 Right-click the appliance and select **Open Console**.

3 After the installation files load, the Welcome screen for the vSphere Data Protection menu appears. Open a web browser and type:

https://<*ip address of VDP appliance*>:8543/vdp-configure/

4 From the VMware Login screen, enter the following:

a User: **root**

b Password: **changeme**

c Click **Login**

5 The Welcome screen appears. Click **Next**.

6 The Network settings dialog box appears. Specify (or confirm) the following:

   a IPv4 Static address

   b Netmask

   c Gateway

   d Primary DNS

   e Secondary DNS

   f Host name

   g Domain

7 Click **Next**.

8 The Time Zone dialog box appears. Select the appropriate time zone and click **Next**.

9 The vSphere Data Protection credentials dialog box appears. For vSphere Data Protection credentials type in the appliance password. This will be the universal configuration password. Specify a password that contains the following:

   - Nine characters
   - At least one uppercase letter
   - At least one lowercase letter
   - At least one number
   - No special characters

10 Click **Next**.

11 The vCenter registration dialog box appears. Specify the following:

   a vCenter user name (If the user belongs to a domain account then it should be entered in the format "SYSTEM-DOMAIN\admin".)

   b vCenter password

   c vCenter host name (IP address or FQDN)

   d vCenter port

   e SSO host name (IP address or FQDN)

   f SSO port

12 Click **Test connection**.

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

   If 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 14 for instructions on how to update the user role.

13 Click **OK**.

14 Click **Next**.

15 The Ready to Complete page appears. Click **Finish**.

16 A message appears that configuration is complete. Click **OK**.

Configuration of the vSphere Data Protection appliance is now complete, but you will need to return to the vSphere Web Client and reboot the appliance. Using the vSphere Web Client, right click on the appliance and select **Restart Guest OS**. In the Confirm Restart message, click **Yes**. The reboot can take up to 30 minutes.

Post-Installation Configuration

During installation of vSphere Data Protection, when you first run the configuration utility, it runs in “install” mode. This mode allows you to enter initial networking settings, time zone, appliance password, and vCenter credentials. After initial installation, the VDP-configure utility runs in “maintenance” mode and displays a different user interface.

To access VDP-configure, open a web browser and type:

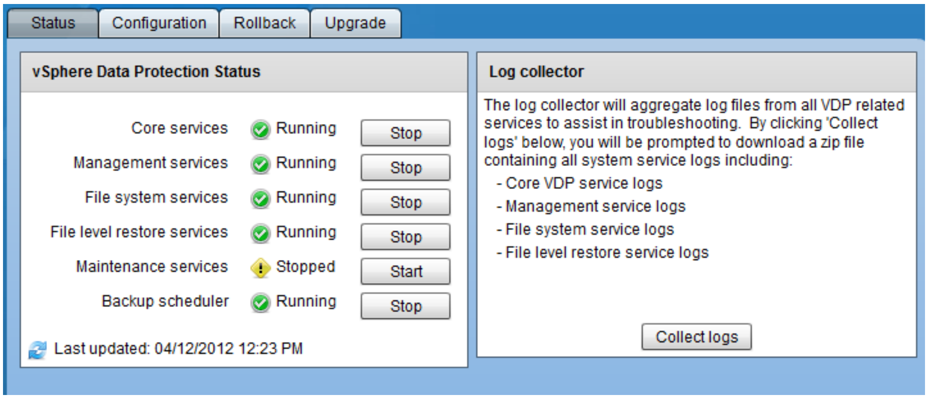
https://<*ip address of VDP appliance*>:8543/vdp-configure/

The maintenance interface is used for:

- Viewing Status—Allows you to see the services currently running (or currently stopped) on the appliance.
- Starting and Stopping Services—Allows you to start and stop selected services on the appliance.
- Collecting Logs—Allows you to download current logs from the appliance.
- View or change vSphere Data Protection configuration—Allows you to view or change network settings, configure vCenter Registration, or to view or edit system settings (timezone information and vSphere Data Protection credentials).
- Rolling Back an Appliance—Allows you to restore your appliance to an earlier known and valid state. (see “Using Checkpoints and Rollback” on page 42)
- Upgrade—Allows you to upgrade ISO images on your vSphere Data Protection appliance.

Status Tab

The Status tab is used to view (and stop or start) vSphere Data Protection services.



vSphere Data Protection Status

Core services	✓ Running	Stop
Management services	✓ Running	Stop
File system services	✓ Running	Stop
File level restore services	✓ Running	Stop
Maintenance services	! Stopped	Start
Backup scheduler	✓ Running	Stop

Last updated: 04/12/2012 12:23 PM

Log collector

The log collector will aggregate log files from all VDP related services to assist in troubleshooting. By clicking 'Collect logs' below, you will be prompted to download a zip file containing all system service logs including:

- Core VDP service logs
- Management service logs
- File system service logs
- File level restore service logs

Managing Status Options

The left-hand screen of the Status tab shows the status of key services in the vSphere Data Protection appliance. The status of the following services is displayed:

Table 2-2. Description of services running on the vSphere Data Protection appliance

Service	Description
Core services	These are the services that comprise the backup engine of the appliance. If these services are disabled no backup jobs--either scheduled or “on demand”--will run, and no restore activities can be initiated.
Management services	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 recovery operations.
File level restore services	These are the services that support the management of file level recovery operations.

Table 2-2. Description of services running on the vSphere Data Protection appliance

Service	Description
Maintenance services	These are the services that perform maintenance tasks such as evaluating whether retention periods of backups have expired. Maintenance services are disabled the first 24-48 hours the vSphere Data Protection appliance is in operation. This gives initial backups additional time to complete.
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.

The status that is displayed for these services can be:

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

Starting and Stopping Services

On the status screen you can start services that are stopped 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**, but in some cases, additional troubleshooting steps are necessary for the service to work properly.

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

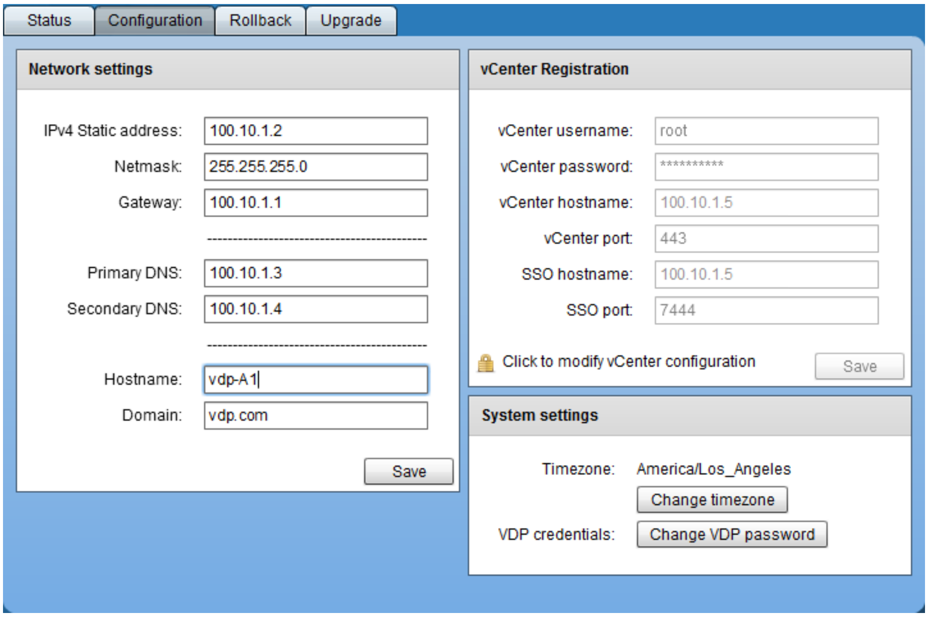
1. Core services
2. Management services
3. Backup scheduler
4. Maintenance services
5. File system services
6. File level restore services

Collecting Log Files

The log file bundle is intended to facilitate sending logs of your vSphere Data Protection appliance to support personnel. You can download all the logs from vSphere Data Protection services as a "log bundled" by clicking **Collect logs**. A "save as" dialog displays that will allow you to download the log bundle to the file system of the machine where your web browser is running. The log bundle is named LogBundle.zip.

Configuration Tab

The Configuration tab is used to view and edit vSphere Data Protection configuration.



Network settings

IPv4 Static address: 100.10.1.2
Netmask: 255.255.255.0
Gateway: 100.10.1.1
Primary DNS: 100.10.1.3
Secondary DNS: 100.10.1.4
Hostname: vdp-A1
Domain: vdp.com

vCenter Registration

vCenter username: root
vCenter password: **********
vCenter hostname: 100.10.1.5
vCenter port: 443
SSO hostname: 100.10.1.5
SSO port: 7444

System settings

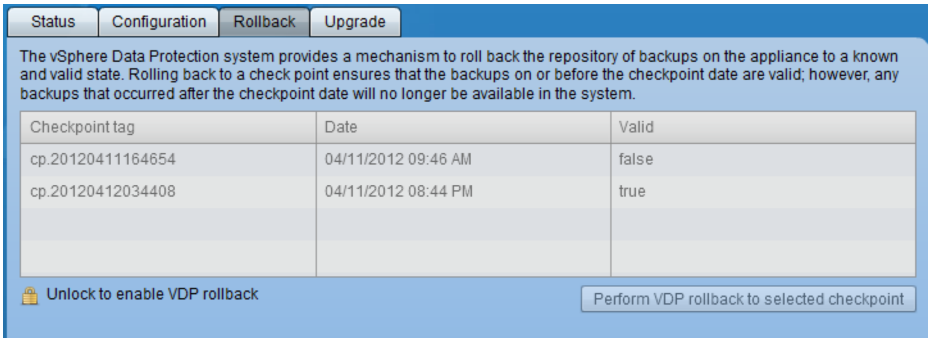
Timezone: America/Los_Angeles
VDP credentials:

vSphere Data Protection configuration that can be viewed of edited includes:

- Network settings
  - IP address
  - Netmask
  - Gateway
  - Primary DNS
  - Secondary DNS
  - Host name
  - Domain
- vCenter registration
  - vCenter user name
  - vCenter password
  - vCenter host name
  - vCenter port
  - SSO host name
  - SSO port
- System settings
  - Time zone
  - VDP credentials (change VDP password)

Rollback Tab

The Rollback tab is used to rollback to a known checkpoint in the event that the vSphere Data Protection data becomes corrupt.



The vSphere Data Protection system provides a mechanism to roll back the repository of backups on the appliance to a known and valid state. Rolling back to a check point ensures that the backups on or before the checkpoint date are valid; however, any backups that occurred after the checkpoint date will no longer be available in the system.

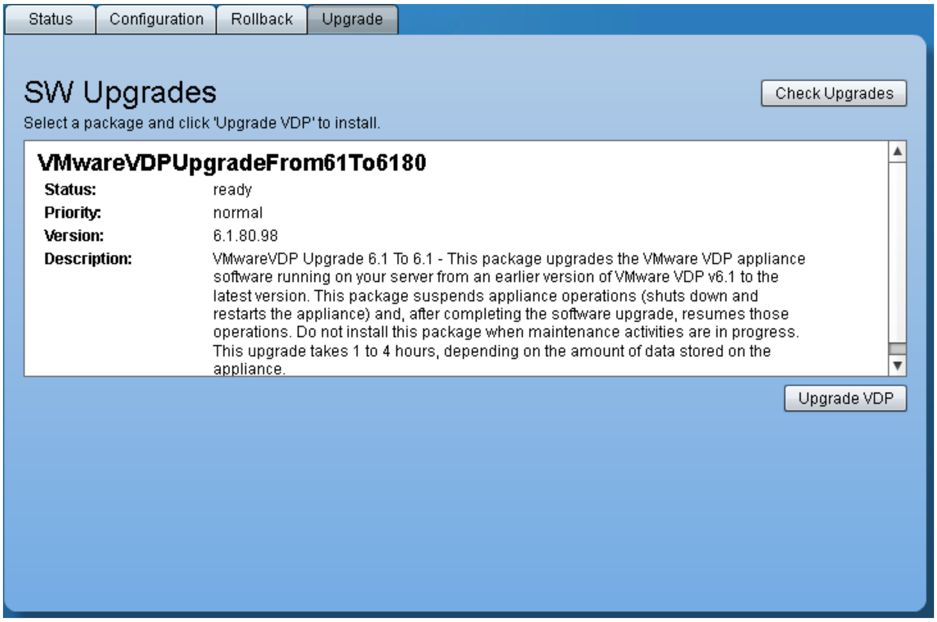
Checkpoint tag	Date	Valid
cp.20120411164654	04/11/2012 09:46 AM	false
cp.20120412034408	04/11/2012 08:44 PM	true

Unlock to enable VDP rollback
Perform VDP rollback to selected checkpoint

NOTE Using Rollback is covered in "Using Checkpoints and Rollback" on page 42.

Upgrade Tab

The Upgrade tab is used to update ISO images on the vSphere Data Protection appliance.



Select a package and click 'Upgrade VDP' to install.

VMwareVDPUpgradeFrom61To6180

Status: ready
Priority: normal
Version: 6.1.80.98
Description: VMwareVDP Upgrade 6.1 To 6.1 - This package upgrades the VMware VDP appliance software running on your server from an earlier version of VMware VDP v6.1 to the latest version. This package suspends appliance operations (shuts down and restarts the appliance) and, after completing the software upgrade, resumes those operations. Do not install this package when maintenance activities are in progress. This upgrade takes 1 to 4 hours, depending on the amount of data stored on the appliance.

NOTE Performing upgrades is covered in "Using VDP-Configure."

Using VDP-Configure

VDP-configure is used for post-installation configuration.

Prerequisites

The vSphere Data Protection appliance must be installed and configured and you must login with the vSphere Data Protection administrative account.

Procedure

1 Open a web browser and type:

https://<*ip address of VDP appliance*>:8543/vdp-configure/

2 From the VMware Login screen, enter the following:

   a User: **root**

   b Password: ***VDP password***

   c Click **Login**

3 (optional) To view vSphere Data Protection services, click the **Status** tab. To stop or start vSphere Data Protection services, click the associated Stop or Start button.

4 (optional if requested by VMware support) To create support log files, click the **Status** tab and then click the **Collect Logs** button. Save the log bundle file and follow the instructions from VMware support to submit the file.

5 (optional) To view or edit vSphere Data Protection configuration, click the **Status** tab.

   - For Network settings, view or edit the configuration. If you make configuration changes, click the **Save** button.

   - For vCenter registration, you can edit the settings. To edit the settings, click the lock icon. If you make changes to vCenter registration settings, the current backup job settings will be lost and you must reconfigure the backup jobs. If changes are made, click the **Save** button.

   - For System settings, you can view or edit the timezone. If you change the time zone, click the **Save** button. You can change the vSphere Data Protection password by clicking the **Change VDP password** button.

Upgrading the vSphere Data Protection Appliance

The upgrade process consists of the following general steps:

1 Creating a Snapshot of the vSphere Data Protection Appliance

2 Installing the Upgrade

3 Removing the Snapshot

CAUTION Do not upgrade the vSphere Data Protection appliance during the backup window or while any backup jobs are running. Also do not initiate any ad hoc backup jobs or restore requests during the upgrade process.

Prerequisites

- In order to perform a software upgrade of vSphere Data Protection, an ISO upgrade image must be downloaded to a location where your vSphere web client can navigate to it.

- All of the vSphere Data Protection services must be running.

Creating a Snapshot of the vSphere Data Protection Appliance

At installation time, the virtual disks used by the vSphere Data Protection appliance are set to be "Independent - Persistent." However, in order to take a snapshot, the disks will have to be temporarily changed to "Dependent."

To create a snapshot of the vSphere Data Protection appliance:

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

2 Click **Hosts and Clusters**

3 In the tree on the left, click the disclosure arrows until the vSphere Data Protection appliance is displayed.

4 Right-click the vSphere Data Protection appliance and select **Shut Down Guest** OS.

5 Click **Yes**. Wait for the vSphere Data Protection appliance to shut down. This can take several minutes.

6 Right-click the vSphere Data Protection appliance and select **Edit Settings**.

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

8 In the Virtual Hardware table, in the Disk Mode row, click **Dependent**.

9 Continuing with Hard disk 3, repeat step 8 until all the remaining disks have been set to Dependent mode.

10 Click **OK**.

11 Right-click the vSphere Data Protection appliance and select **All vCenter Actions > Snapshot> Take Snapshot**.

12 Type a name for the snapshot. Type an optional description. Click **OK**.

13 Right-click the vSphere Data Protection appliance and select **Power On**.

Installing the Upgrade

1 Log in to the vCenter Server using the vSphere Web Client as an administrator.

2 Click **Hosts and Clusters**

3 In the tree on the left, click the disclosure arrows until the vSphere Data Protection appliance is displayed.

4 Right-click the vSphere Data Protection appliance and select **Edit Settings**.

5 From the Virtual Hardware tab, expand the CD/DVD drive. From the drop-down menu, select **Datastore ISO File**.

6 From Select File navigate to and select the ISO image. Click **OK**.

7 To the right of Datastore ISO select the **Connected** box. Click **OK**. Depending on the size of the ISO file, it can take can take up to five minutes to mount.

8 Open a web browser and type:

https://<*ip address of VDP appliance*>:8543/vdp-configure/

9 From the VMware Login screen, enter the following:

a User: **root**

b Password: ***VDP password***

c Click **Login**

10 Click the **Upgrade** tab. Confirm that ISO image is available and status is ready. If not, the ISO image might still be loading.

NOTE If the ISO image does not appear, logout of VDP-configure and log back in. If the ISO image still does not appear it may be because the image has been corrupted. Any ISO images that do not pass checksum do not display on the Upgrade tab.

11 Click **Upgrade VDP**. The upgrade begins installing. This installation portion of the upgrade can take a long time, but a status bar will update the progress of the installation.

12 After the upgrade installs successfully, click **OK**. Right-click the vSphere Data Protection appliance and select **Shut Down Guest OS**.

Removing the Snapshot

It is strongly recommended that you remove snapshots after an upgrade completes successfully.

To remove the snapshot:

1 Log in to the vCenter Server using the vSphere Web Client as a user who has rights 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 vSphere Data Protection appliance is displayed.

4 Right-click the vSphere Data Protection appliance and select **All vCenter Actions > Snapshot > Snapshot Manager**.

5 Click the Snapshot you created for the vSphere Data Protection Appliance.

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

7 Click **Close**.

8 Right-click the vSphere Data Protection appliance and select **Edit Settings**.

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

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

11 Continuing with Hard disk 3, repeat step 10 until all the remaining disks have been set to Independent - Persistent mode.

12 Unmount the ISO image. From the Virtual Hardware tab, expand the CD/DVD drive. From the drop-down menu, select Client Device. Click **OK**.

13 Click **OK**.

14 Right-click the vSphere Data Protection appliance and select **Power On**.

15 After the reboot is complete right-click the vSphere Data Protection appliance and select **Edit Settings**.

The vSphere Data Protection appliance upgrade process is complete.

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

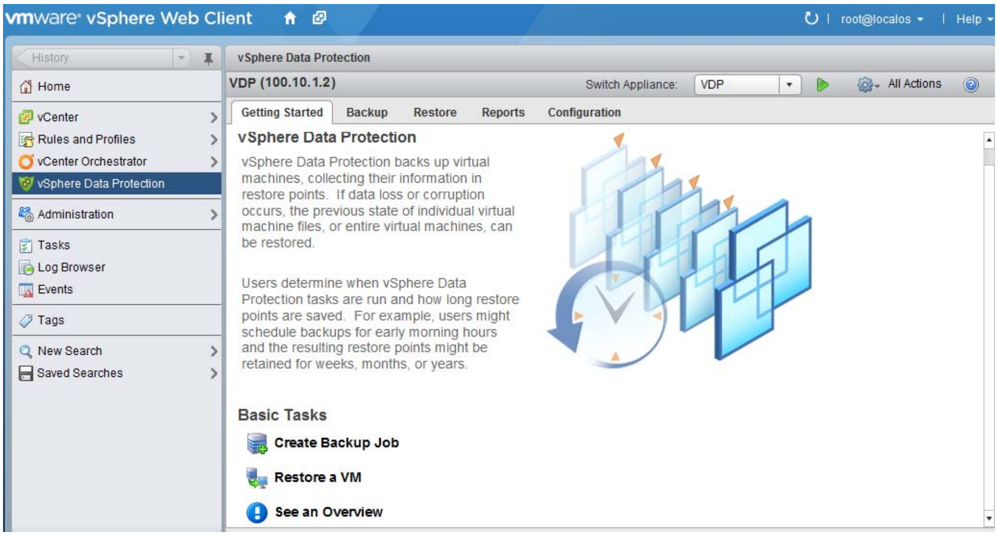
Using vSphere Data Protection 3

After vSphere Data Protection (VDP) is installed and configured, it can be managed through the vSphere Web Client for vSphere Data Protection.

This chapter includes the following topics:

Understanding the vSphere Data Protection User Interface

The vSphere Web Client for vSphere Data Protection provides a number of new user interface elements that can be used to configure and manage vSphere Data Protection.



vSphere Data Protection

vSphere Data Protection backs up virtual machines, collecting their information in restore points. If data loss or corruption occurs, the previous state of individual virtual machine files, or entire virtual machines, can be restored.

Users determine when vSphere Data Protection tasks are run and how long restore points are saved. For example, users might schedule backups for early morning hours and the resulting restore points might be retained for weeks, months, or years.

Basic Tasks

The vSphere Data Protection user interface consists of five tabs:

- **Getting Started**—provides an overview of vSphere Data Protection functionality and quick links to the Create Backup Job wizard and the Restore wizard.
- **Backup**—provides 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.
- **Restore**—provides a list of successful backups that can be restored.
- **Reports**—provides backup status reports on the virtual machines in the vCenter.
- **Configuration**—displays information about how vSphere Data Protection is configured and allows you edit some of these settings.

Each of these tabs are described in the following sections.

Getting Started Tab

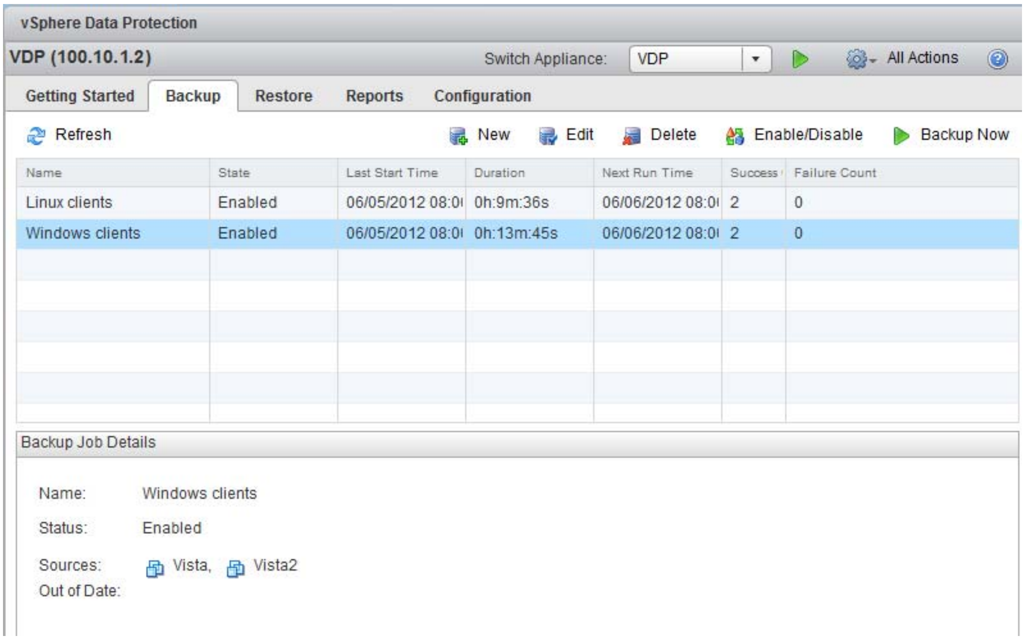
The Getting Started tab provides introductory information about vSphere Data Protection and provides a way to start common configuration tasks.

Table 3-1. Getting Started tab

Icon	Name	Description
	Create Backup Job	Launches the Backup Job wizard. For more information, see "Use the Backup Job Wizard" on page 32.
	Restore a VM	Launches the Restore a Virtual Machine wizard. For more information, see "Restore Virtual Machines from Backup" on page 34.
	See an Overview	Switches the current view to the Reports tab, which provides a way to review the status of existing jobs. For more information, see "Viewing Reports" on page 35.

Backup Tab

The Backup tab displays information about existing backup jobs and their status. It also provides a way to create, edit, delete, enable/disable, and run ad-hoc backup jobs.



vSphere Data Protection

VDP (100.10.1.2) Switch Appliance: VDP All Actions

Getting Started | Backup | Restore | Reports | Configuration

Refresh New Edit Delete Enable/Disable Backup Now

Name	State	Last Start Time	Duration	Next Run Time	Success	Failure Count
Linux clients	Enabled	06/05/2012 08:0	0h:9m:36s	06/06/2012 08:0	2	0
Windows clients	Enabled	06/05/2012 08:0	0h:13m:45s	06/06/2012 08:0	2	0

Backup Job Details

Name: Windows clients

Status: Enabled

Sources: Vista, Vista2

Out of Date:

Table 3-2. Backup tab icons

Icon	Name	Description
	New	Launches the Backup Job wizard. For more information, see "Use the Backup Job Wizard" on page 32.
	Edit	Launches the Backup Job wizard for editing an existing job.
	Delete	Deletes the selected backup job.
	Enable/Disable	Configures the backup job as enabled or disabled.
▶	Backup Now	Launches an ad-hoc backup.

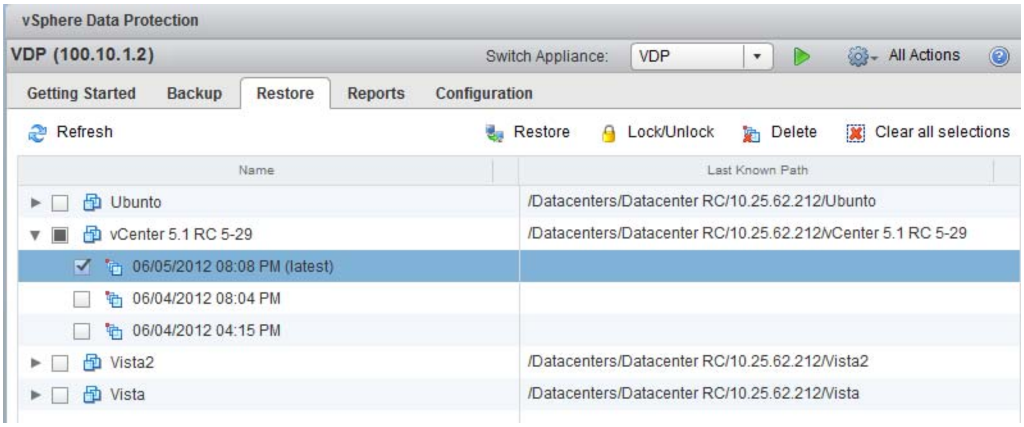
The Backup tab displays a list of the backup jobs that have been created. The backup jobs are listed in a table that contains the following information:

Table 3-3. Backup tab column descriptions

Column	Description
Name	Name of the backup job.
State	Enabled or disabled. Disabled backup jobs are not run.
Last Start Time	The last time the job was started.
Duration	How long the job took the last time it ran.
Next Run Time	When the job is scheduled to run again.
Success Count	The number of VMs backed up successfully the last time the backup job ran. This number is updated after each backup job. Changes to a job between backups will not be reflected in this number until after the job runs again. For example, if a job reports 10 VMs successfully backed up, and then the job is edited so that only one VM remains, this number will continue to be 10 until the job runs again and, if successful, the number changes to one.
Failure Count	The number of VMs that were not backed up successfully the last time the backup job ran. This number is updated after each backup job. Changes to a job between backups will not be reflected in this number until after the job runs again. For example, if a job reports 10 VMs failed to backed up, and then the job is edited so that only one VM remains, this number will continue to be 10 until the job runs again and, if the job fails, the number changes to one.

Restore Tab

The Restore tab displays a list of VMs that have been backed up to the vSphere Data Protection 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**.



Name	Last Known Path
▶ □ Ubunto	/Datacenters/Datacenter RC/10.25.62.212/Ubunto
▼ ■ vCenter 5.1 RC 5-29	/Datacenters/Datacenter RC/10.25.62.212/vCenter 5.1 RC 5-29
☑ 06/05/2012 08:08 PM (latest)	
□ 06/04/2012 08:04 PM	
□ 06/04/2012 04:15 PM	
▶ □ Vista2	/Datacenters/Datacenter RC/10.25.62.212/Vista2
▶ □ Vista	/Datacenters/Datacenter RC/10.25.62.212/Vista

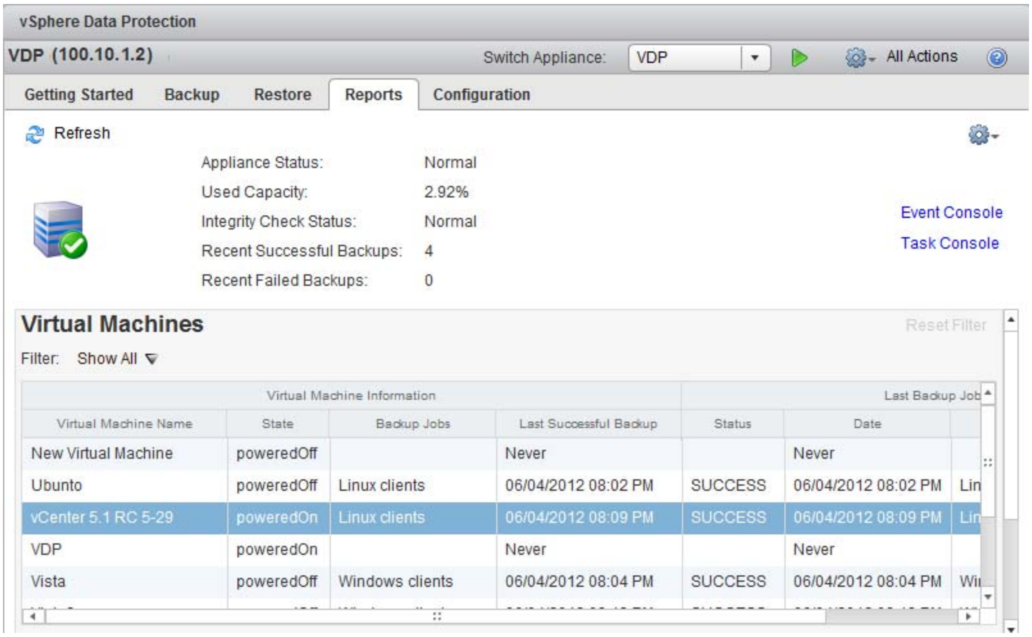
The following icons are used in the Restore tab.

Table 3-4. Restore tab icons

Icon	Name	Description
	Restore	Launches the Restore Virtual Machines from Backup, which provides a way to configure how virtual machines are restored to the state saved in the selected restore points. For more information, see "Restore Virtual Machines from Backup" on page 34. By default, vSphere Data Protection manages the storage and eventual deletion of older restore points according to the Retention Policy specified in the backup job.
🔒	Lock/Unlock	Lock changes the expiration point of a backup job to "no end date".
	Delete	Specifies that selected restore points are deleted.
☒	Clear all selections	Clears all selections in the Restore tab.

Reports Tab

The Reports tab provides overview information about the vSphere Data Protection appliance and about the VMs in the Virtual Center.



vSphere Data Protection

VDP (100.10.1.2)

Switch Appliance: VDP

All Actions

Getting Started | Backup | Restore | Reports | Configuration

Refresh

Appliance Status:	Normal
Used Capacity:	2.92%
Integrity Check Status:	Normal
Recent Successful Backups:	4
Recent Failed Backups:	0

Event Console

Task Console

Virtual Machines

Reset Filter

Filter: Show All

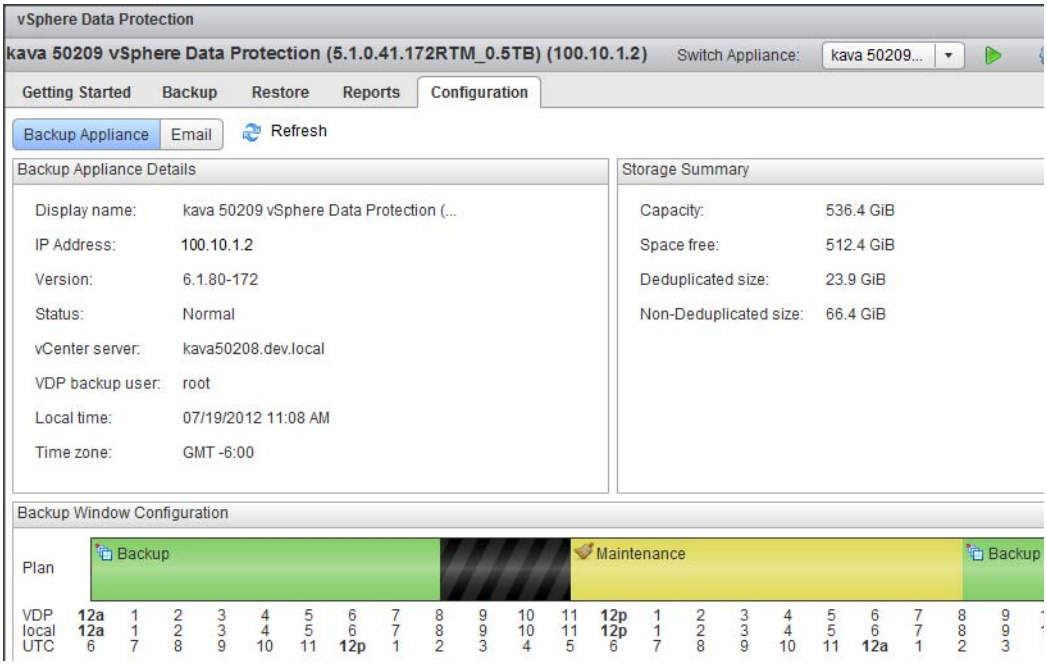
Virtual Machine Information				Last Backup Job		
Virtual Machine Name	State	Backup Jobs	Last Successful Backup	Status	Date	
New Virtual Machine	poweredOff		Never		Never	
Ubunto	poweredOff	Linux clients	06/04/2012 08:02 PM	SUCCESS	06/04/2012 08:02 PM	Lin
vCenter 5.1 RC 5-29	poweredOn	Linux clients	06/04/2012 08:09 PM	SUCCESS	06/04/2012 08:09 PM	Lin
VDP	poweredOn		Never		Never	
Vista	poweredOff	Windows clients	06/04/2012 08:04 PM	SUCCESS	06/04/2012 08:04 PM	Wi

Configuration Tab

The Configuration tab allows you to manage the maintenance tasks for the vSphere Data Protection appliance.

There are three tasks that can be performed on this tab:

- View or edit the Backup Window (see "Backup Window Configuration" on page 37)
- Run an Integrity Check (see "Manually Run an Integrity Check" on page 39)
- Configure Email (see "Configuring Email Notification" on page 39)



vSphere Data Protection

kava 50209 vSphere Data Protection (5.1.0.41.172RTM_0.5TB) (100.10.1.2)

Switch Appliance: kava 50209...

Getting Started | Backup | Restore | Reports | Configuration

Backup Appliance | Email

Refresh

Backup Appliance Details

Display name:	kava 50209 vSphere Data Protection (...
IP Address:	100.10.1.2
Version:	6.1.80-172
Status:	Normal
vCenter server:	kava50208.dev.local
VDP backup user:	root
Local time:	07/19/2012 11:08 AM
Time zone:	GMT -6:00

Storage Summary

Capacity:	536.4 GiB
Space free:	512.4 GiB
Deduplicated size:	23.9 GiB
Non-Deduplicated size:	66.4 GiB

Backup Window Configuration

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

Accessing vSphere Data Protection

vSphere Data Protection is accessed through a vSphere Web Client.

NOTE vSphere Data Protection is only managed through the vSphere Web Client. The vSphere Client does not support managing vSphere Data Protection.

Prerequisites

Before using vSphere Data Protection, you must install and configure the vSphere Data Protection appliance described in "Installing and Configuring vSphere Data Protection" on page 11.

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 a the vCenter username and password and click **Login**.

   vSphere Data Protection uses this information to connect to vCenter to perform backups, so the specified user account must have administrative rights.

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 support up to 10 vSphere Data Protection appliances. You can switch appliances by choosing a appliance from the drop-down list to the right of the Switch Appliance label.

NOTE The vSphere Data Protection 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 appliance in the list of available appliances.

Creating Backup Jobs

You can create backup jobs that include which virtual machines to backup, how often backups occur, and the retention period for storing the backups. vSphere Data Protection uses the backup window to create new backups and the retention policy, or to remove specific older backups.

Virtual Machines

You can specify collections of VMs, such as all VMs in a datacenter, or select individual VMs. If an entire resource pool, host, datacenter, or folder is selected, any new VMs in that container are included in subsequent backups. If a VM is selected, any disk added to the VM is included in the backup. If a VM is moved from the selected container to another container that is not selected, it is no longer part of the backup.

You can manually select a VM to be backed up, this will ensure that VM is backed up, even if it is moved.

NOTE Using vSphere Data Protection to back up the vSphere Data Protection appliance is not supported.

Schedule

The backup schedule determines how often your selections are backed up. Backups will occur as near to the start of the backup window as possible. You can schedule your backups to be run daily, weekly, or on a specific day of the month.

Retention Policy

Backup retention policies enable you to specify how long to keep a backup in the system.

A retention policy is assigned to each backup when the backup occurs. When the retention for a backup expires, then the backup is deleted.

Table 3-5 describes the retention policies for backups.

Table 3-5. Retention Policy Settings

Retention setting	Description
Forever	Enables you to keep backups indefinitely. This setting is useful for ensuring that all backups that are assigned this retention policy are retained for the life of the system.
For (Retention Period)	Enables you to define a fixed retention period in days, weeks, months, or years after the backup is performed. For example, you could specify that backups expire after 6 months.
Until (End Date)	Enables you to assign a calendar date as the expiration date. For example, you could specify that backups expire on December 31, 2013.
For (This Schedule)	Enables you to define a fixed retention period based on daily, weekly, monthly, and yearly retention. For example, you could specify that backups are kept daily for 30 days, weekly for 52 weeks, monthly for 12 months, and yearly for 2 years.

Ready to Complete

Review the settings for the backup job. This page includes information including:

- Name of the backup job.
- Which virtual machines will be backed up by this job.
- The schedule on which virtual machines will be backed up.
- The retention policy selected for the backup.

Use the Backup Job Wizard

Use the Backup Job Wizard to specify which virtual machines are to be backed up and when this can occur.

Procedure

1. In the vSphere Web Client, select **vSphere Data Protection**.
2. In the Welcome to vSphere Data Protection page, select the vSphere Data Protection appliance and click **Connect**.
3. Click the **Backup** tab and click **New** to launch the Backup Job wizard.
4. In the Virtual Machines page, select individual virtual machines or containers that contain virtual machines to be backed up and click **Next**.
5. In the Schedule page, select the backup schedule for the job and click **Next**.
6. In the Retention Policy page, accept the default retention policy or specify an alternate retention policy and click **Next**.
7. In the Name page, enter a backup job name and click **Next**.
8. In the Ready to Complete page, reviewed the summary information for the backup job and click **Finish**.
9. An information dialog box will confirm the backup job was created successfully. Click **OK**.

Backup Now

After a backup job is created, you can manually initiate a backup job through the Backup Now icon.

Prerequisites

Before using the Backup Now option, you must have installed and configured vSphere Data Protection and you should have at least one backup job.

Procedure

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

2 In the Welcome to vSphere Data Protection page, select the vSphere Data Protection appliance and click **Connect**.

3 Click the **Backup** tab select a backup job. Click **Backup Now** and select either Backup all sources or Backup only out of date sources.

    - Backup all sources specifies all jobs should be backed up.
    - Backup only out of date sources specifies backup jobs that failed the last backup attempt.

Restoring Virtual Machines

You can specify which virtual machines to restore, how they are restored, and where they are restored to using the Virtual Machine Restore wizard.

CAUTION If the VM that you are restoring to contains a snapshot, the restore will fail. Remove any snapshots from the VM prior to beginning the restore process.

Select Backup

Select backup specifies the virtual machines to be restored. Restores are similar to creating backup jobs, you can specify a container of virtual machines or specific virtual machines. It is possible to restore virtual machines to alternate locations.

Set Restore Options

Set Restore options specifies where the backup is restored to.

You can specify:

- If the backup will be restored to the original location
- If the backup will be restored to an alternate location
    - New name
    - Destination
    - Datastore location

To clone a virtual machine, rename the virtual machine you are restoring.

Ready to Complete

Review the settings for the restore job. The summary contains: information on how many VMs will be restored and how many VMs will be created.

Restore Virtual Machines from Backup

Restore virtual machines to a previous backup state using the Virtual Machine Restore wizard.

Prerequisites

Before you can restore virtual machines, you must have configured vSphere Data Protection and have at least one backup from which to restore.

Procedure

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

2 In the Welcome to vSphere Data Protection page, select the vSphere Data Protection appliance and click **Connect**.

3 Click the **Restore** tab and click the **Restore** button.

4 The Restore Virtual Machines wizard appears.

5 In the Select Backup page, specify a source from which to restore virtual machines and click **Next**.

6 If the VM has more than one backup point, deselect all of the points that will not be restored. Only one backup point should be selected.

7 On the Set to Restore page, confirm that the client and backup restore point is correct. Select Restore to Original Location or to restore to an alternate location, uncheck the Restore to Original Location check box and specify the alternate Destination and Datastore. Click **Next**.

8 On the Ready to Complete page, review the configuration and click **Finish**.

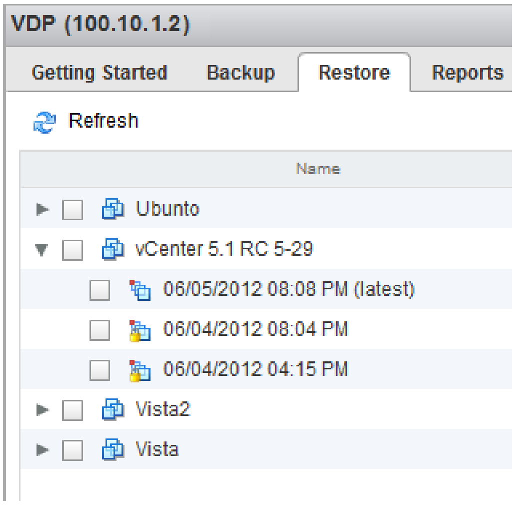
The virtual machines are restored as specified in the wizard.

Viewing Restore Job Progress

After a restore job is initiated, you can view the current restore process through the Recent Task pane.

Locking a Backup Job

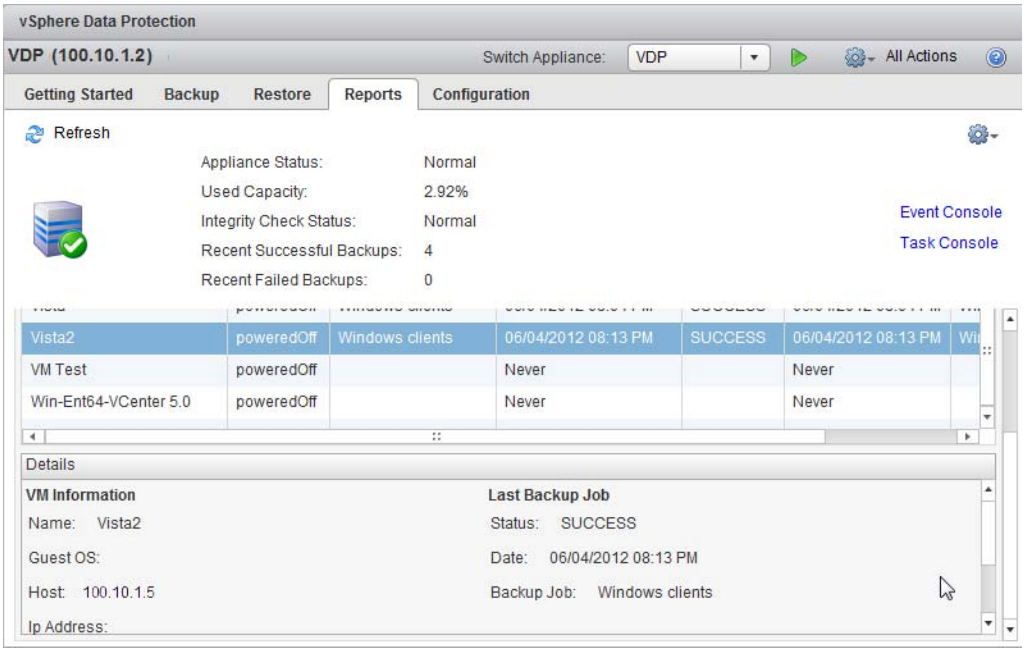
The Lock icon is used to change the expiration point of a backup job to “no end date”. This keeps a backup job from manually expiring and being automatically deleted after the expiration date passes. The lock option does not prevent a backup job from being deleted, an administrator can still manually delete a locked job. To lock a backup job, select the backup job(s) in the Restore tab and click the Lock icon. Backup jobs that are locked are displayed with a yellow lock to the left of the backup job name.



Viewing Reports

The Reports tab shows current status for:

- Appliance Status
- Used Capacity
- Integrity Check Status
- Recent Successful Backups
- Recent Failed Backups



Appliance Status: Normal
Used Capacity: 2.92%
Integrity Check Status: Normal
Recent Successful Backups: 4
Recent Failed Backups: 0

Vista2	poweredOff	Windows clients	06/04/2012 08:13 PM	SUCCESS	06/04/2012 08:13 PM	Wi
VM Test	poweredOff		Never		Never	
Win-Ent64-VCenter 5.0	poweredOff		Never		Never	

VM Information

Name: Vista2

Guest OS:

Host: 100.10.1.5

Ip Address:

Last Backup Job

Status: SUCCESS

Date: 06/04/2012 08:13 PM

Backup Job: Windows clients

Filtering in Reports Tab

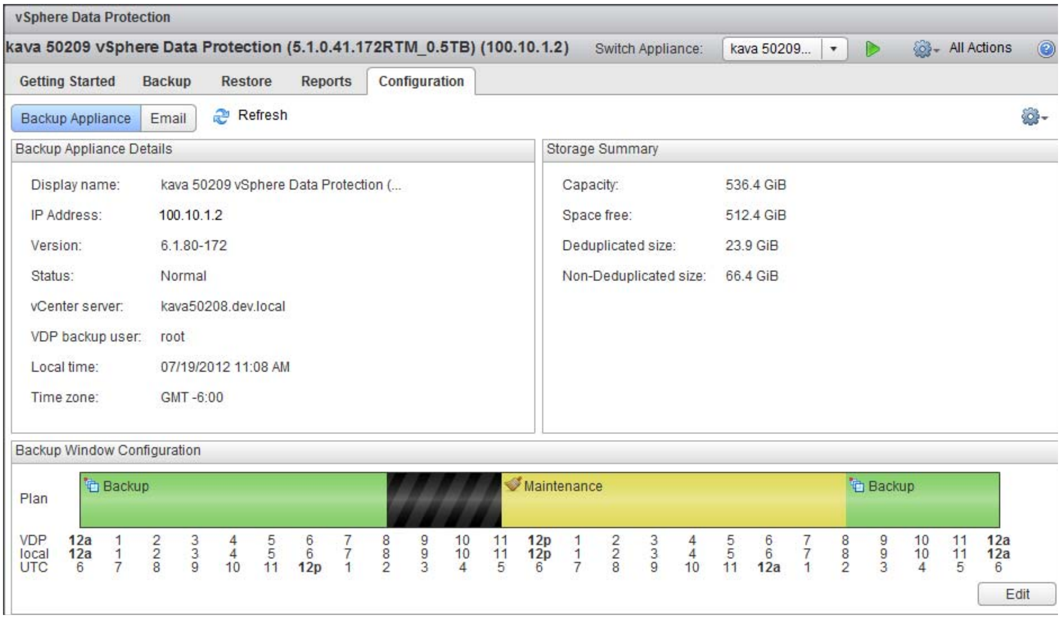
By default the Reports tab displays all Virtual Machines associated with the vCenter Server. The Filter option in the Report tab filters by:

- Show All
- Virtual Machine
  - Name
  - State
  - Last successful backup
- Last Backup Job
  - Name
  - Status
  - Date

Managing Configuration

The Configuration tab is used to view and modify configuration information. The following topics are covered in this section:

- "View and Edit Backup Appliance Details" on page 36
- "Backup Window Configuration" on page 37
- "Change Maintenance Window Settings" on page 38
- "Manually Run an Integrity Check" on page 39
- "Configuring Email Notification" on page 39



kava 50209 vSphere Data Protection (5.1.0.41.172RTM_0.5TB) (100.10.1.2)

Backup Appliance Details

Display name:	kava 50209 vSphere Data Protection (...
IP Address:	100.10.1.2
Version:	6.1.80-172
Status:	Normal
vCenter server:	kava50208.dev.local
VDP backup user:	root
Local time:	07/19/2012 11:08 AM
Time zone:	GMT -6:00

Storage Summary

Capacity:	536.4 GiB
Space free:	512.4 GiB
Deduplicated size:	23.9 GiB
Non-Deduplicated size:	66.4 GiB

Backup Window Configuration

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

You can view backup appliance details, storage overview, and backup window configuration through the Configuration tab.

View and Edit Backup Appliance Details

Backup Appliance details includes the following information:

- IP address
- VDP appliance version
- Status
- vCenter Server
- Current user
- Local time
- Time zone
- Space free
- Deduplicated size
- Non-deduplicated size

NOTE The storage capacity is displayed in GiB (as opposed to GB), which is 1024 MB.

Backup Window Configuration

Each 24-hour day is divided into three operational windows; backup, blackout, and maintenance, during which various system activities are performed.

Backup Window

The backup window is the portion of each day reserved for performing normal scheduled backups.

- Operational impact —By default, no maintenance activities are performed during the backup window.
- Default settings — The default backup window begins at 8 p.m. local server time and continues uninterrupted for 12 hours until 8 a.m. the following morning.
- Customization — You can customize the backup window start time and duration to meet specific site requirements.

vSphere Data Protection attempts to back up each virtual machine in a job once a day during its backup window. Backups start at the beginning of the backup window and up to eight backup jobs can be run at one time.

NOTE If you have multiple vSphere Data Protection appliances backing up the same virtual machines, the backup windows should be adjusted so that backup jobs on different appliances do not overlap. If backup jobs overlap, backup failures will occur.

Blackout Window

The blackout window is the portion of each day reserved for performing server maintenance activities, such as garbage collection, which require unrestricted access to the server. Garbage collection deletes the orphaned chunks of data that are no longer referenced within any backups stored on the system.

- Operational impact — No backup or administrative activities are allowed during the blackout window. You can perform restores.
- Default settings — The default blackout window begins at 8 a.m. local server time and continues uninterrupted for three hours until 11 a.m. that same morning.
- Customization — You can customize the blackout window duration to meet specific site requirements.

Any changes to blackout window duration also affect maintenance window duration. For example, changing the blackout window duration from three hours to two hours, extends the maintenance window duration one hour because it begins one hour earlier. The backup window is not affected.

NOTE Jobs that are running when the blackout window begins or that run during the blackout window may continue run. However, some maintenance processes in the blackout window may cancel the job.

Maintenance Window

The maintenance window is the portion of each day reserved for performing routine server maintenance activities such as integrity check validation.

- Operational impact — There might be brief periods when backup or administrative activities are not allowed.

  Although backups can be initiated during the maintenance window, doing so impacts both the backup and maintenance activities. For this reason, minimize any backup or administrative activities during the maintenance window. You can, however, perform restores.

  Although Integrity Check and backups can overlap, doing so might result in I/O resource contention, which can cause both activities to take longer to complete and possibly even to fail.

- Default settings — The default maintenance window begins at 11 a.m. local server time and continues uninterrupted for nine hours until 8 p.m. that evening.
- Customization — Although the maintenance window is not directly customizable, its start time and duration is derived from backup and blackout window settings.

The maintenance window starts immediately after the blackout window and continues until the backup window start time.

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

Integrity check

This operation is performed to verify and maintain data integrity on the deduplication store. vSphere Data Protection is designed to complete an incremental or full integrity checks during the maintenance window. Incremental integrity checks verify the integrity of checkpoints that have been added to the deduplication store since the most recent full or incremental integrity check. vSphere Data Protection is also designed to perform an integrity check of all checkpoints once a day. See "Using Checkpoints and Rollback" on page 42 for more information.

The maintenance window should be used to avoid the case where integrity checks may consume computing resources or otherwise interfere with any backup operations in process. As a result, the maintenance window and backup window are defined such that they do not overlap. The maintenance is stopped if it does not complete within the defined window. Even if the maintenance is stopped, the destination is not locked out from other operations such as backup and restore. The next time destination maintenance window opens, the operation continues where it was left off. For more information on configuring the maintenance window, see "Change Maintenance Window Settings" on page 38.

In addition, the integrity check can be started manually. When the integrity check is started manually, it always performs full integrity check of the entire destination, and does not use the maintenance window. Normally, the backup and restore operations are allowed from the deduplication store while the integrity check is in progress. If a restore point is manually marked for delete, backups are not allowed during integrity check but restore operations are allowed. If damaged restore points are found in the deduplication store during integrity check, a manual integrity check must be run after marking the damaged restore points for delete. During this manually run integrity check, backups and restores are not allowed. For more information on manually starting an integrity check, see "Manually Run an Integrity Check" on page 39.

vSphere Data Protection stores information about the progress of an integrity check. As a result, if the vSphere Data Protection appliance stops integrity check, the process can be restarted from where the check was stopped, thereby ensuring that work completed on an integrity check is not lost. The appliance stops integrity checks when the maintenance window passes. Tracking progress helps ensure integrity checks eventually complete. Integrity checks that are manually stopped by user intervention do not save progress information, so after such a stop, the integrity check begins again from the start.

Change Maintenance Window Settings

Change Maintenance Window Settings through the Configuration tab.

Prerequisites

Before you can change Maintenance Window Settings, you must install and configure vSphere Data Protection.

Procedure

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

2 In the Welcome to vSphere Data Protection page, select your vSphere Data Protection appliance and click **Connect**.

3 Click the **Configuration tab**.

4 In Backup Window Configuration, click **Edit**.

5 Select the Backup Start Time, Backup Duration, and Blackout Duration and click **Save**.

Manually Run an Integrity Check

Integrity Checks can be manually run from the Configuration tab.

Prerequisites

Before you can run an Integrity Check, you must have configured vSphere Data Protection.

Procedure

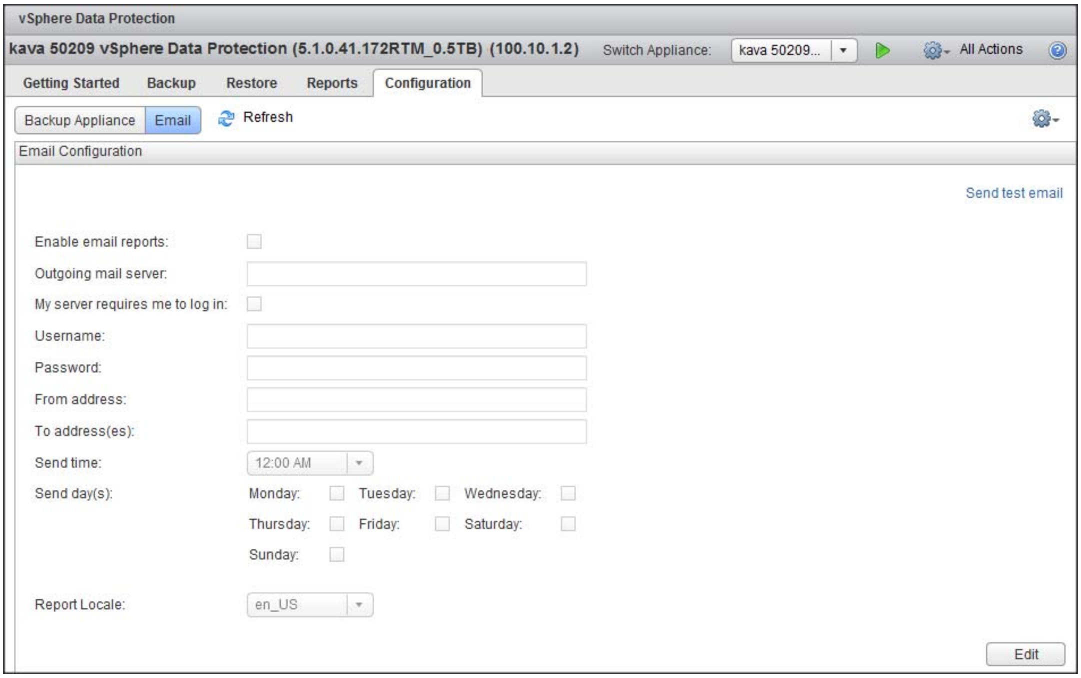
1. In the vSphere Web Client, select **vSphere Data Protection**.
2. In the Welcome to vSphere Data Protection page, select your vSphere Data Protection appliance and click **Connect**.
3. Click the **Configuration tab**.
4. In Backup Window Configuration, click the Settings icon (top right corner of the Configuration tab) and click **Run Integrity Check**.
5. A confirmation dialog box appears. Click **Yes**.

Configuring Email Notification

If email notification is enabled, emails are sent that include the following information:

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

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



vSphere Data Protection

kava 50209 vSphere Data Protection (5.1.0.41.172RTM_0.5TB) (100.10.1.2)   Switch Appliance: kava 50209...   All Actions

Getting Started | Backup | Restore | Reports | Configuration

Backup Appliance | Email   Refresh

Email Configuration

Send test email

Enable email reports: □

Outgoing mail server:

My server requires me to log in: □

Username:

Password:

From address:

To address(es):

Send time: 12:00 AM

Send day(s): Monday: □ Tuesday: □ Wednesday: □ Thursday: □ Friday: □ Saturday: □ Sunday: □

Report Locale: en_US

Edit

Prerequisites

Before you can run configure email reports, the email account must exist.

Procedure

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

2 In the Welcome to vSphere Data Protection page, select your vSphere Data Protection appliance and click **Connect**.

3 Click the **Configuration tab**.

4 Click the **Email** button.

5 Click the **Edit** button the bottom right side of the screen.

6 Specify the following:

  a Select **Enable email reports**.

  b Specify the **Outgoing mail server**.

  The server name can be entered as either an IP address, a host name, or a fully qualified domain name. The vSphere Data Protection 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
  ```

  c (optional) Select **My server requires me to log in** if your SMTP server requires authentication. If this option is selected, specify the associated **Username** and **Password**. (vSphere Data Protection does not validate the password entered in any way; the password entered is passed directly to the email server.)

  d Specify the **From address**. This can only be a single address.

  e Specify the **To address(es)**. This can be a comma separated list of up to 10 email addresses.

  f Select **Send time**.

  g Select the **Send day(s)**.

  h Select the **Report Locale**.

7 Click the **Save** button.

vSphere Data Protection reports sent by Email will contain information similar to that shown below. Explanatory comments have been added to the report in blue.

Table 3-6. Example of vSphere Data Protection Email Reports with explanatory comments

```
lava10036AVE-6.1.80.42 - (100.10.1.1)
---------------------------------------------------------------------------------------------
Report Date:                            February 27, 2012 - 15:12
Last Report Date:                       February 27, 2012 - 14:45

Appliance Status:                       Normal
Byte Capacity:                          498.945 GiB
Bytes Free:                             498.196 GiB
Used Capacity:                          0.50%
Bytes Protected:                        8 GiB
Bytes Deduped:                          0.748 GiB
Integrity Check Status:                 Normal
Recent Successful Backups:                  1
                                                          This is the sum of VMs successfully
                                                          backed up over the past 72 hours.

Recent Failed Backups:                  1
                                                          This is the sum of VMs which either
                                                          failed to back up, or had their
                                                          backups canceled over the
                                                          past 72 hours.

Backup Jobs Summary
---------------------------------------------------------------------------------------------
Backup Job: another-one-with-vm-315
  Backup Sources:                       VM-315
  Last Start Time:                      February 27, 2012 - 15:07
  Next Run Time:                        February 27, 2012 - 20:00
  Last Successful Backups:              0
                                                          This is the sum of VMs successfully
                                                          backed up the last time this backup
                                                          job was run.

  Last Failed Backups:                  1
                                                          This is the sum of VMs which either
                                                          failed to back up or had their
                                                          backup canceled the last time this
                                                          backup job was run.

 Backup Job: VM-315
  Backup Sources:                       VM-315
  Last Start Time:                      February 27, 2012 - 15:01
  Next Run Time:                        February 27, 2012 - 20:00
  Last Successful Backups:              1
  Last Failed Backups:                  0


Virtual Machines Summary
---------------------------------------------------------------------------------------------
Virtual Machine: @#_+-&<>.
  State:                                poweredOff
  Backup Jobs:
  Last Backup Job:
  Last Successful Backup:               Never
  Last Backup Job Date:                 Never

Virtual Machine: VM-315
State:                                 poweredOff
Backup Jobs:                           VM-315, another-one-with-vm-315
Last Backup Job:                       another-one-with-vm-315
Last Successful Backup:                February 27, 2012 - 15:03
Last Backup Job Date:                  February 27, 2012 - 15:09
```

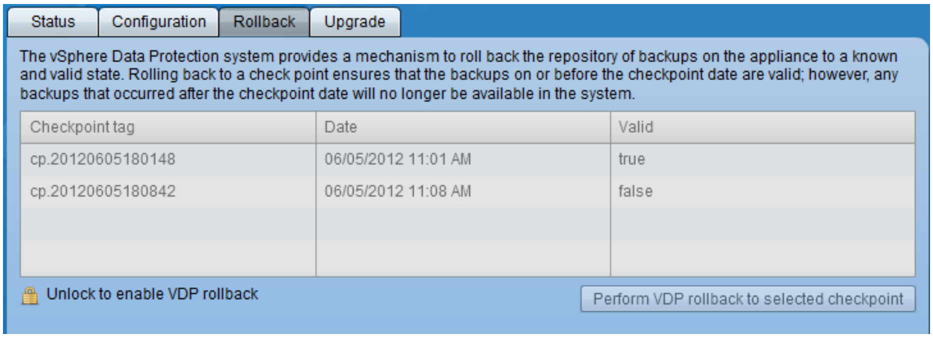
Using Checkpoints and Rollback

A checkpoint is a system-wide backup taken for the express purpose of assisting with disaster recovery. Checkpoints are scheduled and created once a day during the maintenance window, which is discussed in "Maintenance Window" on page 37. The vSphere Data Protection stores two checkpoints (one validated and one unvalidated). Rollback is the process of restoring the vSphere Data Protection appliance to a known good state using data stored in a validated checkpoint. By default maintenance services are disabled for the 24-48 hours after a appliance is deployed. This allows for a longer backup window to support the initial backups.

In the event of an unexpected shutdown, the appliance will rollback to the last validated checkpoint when it is restarted. This is expected behavior and is used to avoid appliance corruption.

When the appliance is deployed an ad-hoc checkpoint is created. This checkpoint contains the appliance settings from the installation. If an unexpected shutdown occurs during the first 24-48 hours a appliance is deployed, the appliance will rollback to the ad-hoc checkpoint. Any backup jobs or backups that were created between the creation of the ad-hoc checkpoint and the unexpected shutdown will be lost. If you want to create a checkpoint during this window, manually run an Integrity Check. See "Manually Run an Integrity Check" on page 39 for additional information.

NOTE If you use rollback, any backups that occurred after the selected checkpoint are lost.



The vSphere Data Protection system provides a mechanism to roll back the repository of backups on the appliance to a known and valid state. Rolling back to a check point ensures that the backups on or before the checkpoint date are valid; however, any backups that occurred after the checkpoint date will no longer be available in the system.

Checkpoint tag	Date	Valid
cp.20120605180148	06/05/2012 11:01 AM	true
cp.20120605180842	06/05/2012 11:08 AM	false

Unlock to enable VDP rollback
Perform VDP rollback to selected checkpoint

Prerequisites

Before you can run a rollback, you must have installed and configured vSphere Data Protection and checkpoints must have been created and validated.

CAUTION It is strongly recommended that you only roll back to the most recent validated checkpoint.

Procedure

1 Open a web browser and type:

http://<*IP_address_of _VDP_appliance*>:8543/vdp-configure/

2 From the VMware Login screen, enter the following:

a User: **root**

b Password: ***VDP password***

c Click **Login**

3 Click the **Rollback** tab.

4 Click **Unlock to enable VDP rollback**.

5 A Warning dialog box warns that any backups that occurred after the selected checkpoint will be lost. If this is acceptable, type in the vSphere Data Protection appliance password and click **OK**.

6 Select a validated checkpoint and click **Perform VDP rollback to selected checkpoint**.

Using File Level Recovery

vSphere Data Protection creates backups of entire virtual machines. These backups can be restored in their entirety using the vSphere Web Client for vSphere Data Protection. However, if you only want to restore specific files from these virtual machines, then use the vSphere Data Protection Restore Client.

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 operates in one of two modes:

- Basic—allows you to only mount backups that were made from the machine you are logging in with, and any files that you restore will be restored to this client.

  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—allows you to mount and browse any backups that are contained in vSphere Data Protection.

You can only have a maximum of eight backups mounted at a given time.

NOTE In order to restore files with file level recovery, the virtual machine you are connecting to the restore client from has to have VMware tools installed. A virtual machine with VMware tools installed can use the restore client to restore files from backups of machines that did not have VMware Tools installed, but virtual machines without VMware Tools won’t be able to successfully restore any backed up files at all with the restore client.

NOTE The restore client does not support using VMware vSphere vMotion or VMware vSphere Storage vMotion.

File Level Recovery Supported Configurations:

File Level Recovery can be performed on backups of the following file systems:

- NTFS (Primary Partition with MBR)
- Ext2 (Primary Partition with MBR)
- Ext3 (Primary Partition with MBR)
- LVM with ext2 (Primary Partition with MBR and a Standalone [without MBR] LVM w/ ext2)
- LVM with ext3 (Primary Partition with MBR and a Standalone [without MBR] LVM w/ ext3)

File Level Recovery Limitations

File Level Recovery 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)
- GUID Partition Table (GPT) disks
- ext4 filesystems
- FAT16 filesystems
- FAT32 filesystems
- Extended partitions
- Encrypted partitions
- Compressed partitions

File Level Recovery also 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

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

- One Physical Volume (.vmdk) must be mapped to exactly one logical volume
- Only ext2 and ext3 formatting is supported

Logon Options

You can log in to the vSphere Data Protection Restore Client in one of two ways:

The file level recovery service is only available to virtual machines whose backups are managed by vSphere Data Protection. This means that you will need to be logged in, either through the vCenter console or some other remote connection, to one of the virtual machines backed up by vSphere Data Protection, in order to log in to the restore client.

Basic Login

To connect with basic login, you will first need to connect to the restore client from a virtual machine that has been backed up by vSphere Data Protection. You will log in to the restore client with the local administrative credentials of the virtual machine you are logged in to. The restore client will only display backups for the virtual machine you are logged in on, and all restored files will be restored to the virtual machine you are currently logged in to.

Advanced Login

To connect with advanced login, you will need to connect to the restore client from a virtual machine that has been backed up by vSphere Data Protection. You will 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 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 vSphere Data Protection. All restore files will be restored to the virtual machine you are currently logged in to.

Use 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

Prior to a vSphere Data Protection backup, the VM must have VMware Tools installed (refer to the VMware website for list of operating systems that support VMware Tools).

The following disk types are supported by the restore client:

- Windows (basic disk, non-extended): NTFS
- Linux (basic disk, non-extended): LVM, Ext 2, Ext 3

Procedure

1. Remote Desktop or use a vSphere Web Client to access the local host that has been backed up through vSphere Data Protection.
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 appears, click **Yes**.
12. A successfully initiated dialog box appears, click **OK**.
13. Click the **Monitor Restores** tab to view restore status.
14. Confirm that the job status is completed.

Use 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

Prior to the backup, the VM must have VMware Tools installed (refer to the VMware website for list of operating systems that support VMware Tools).

The following disk types are supported by the restore client:

- Windows (basic disk, non-extended): NTFS
- Linux (basic disk, non-extended): LVM, Ext 2, Ext 3

Procedure

1. 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 vCenter Credentials, specify the vCenter administrator **Username** and **Password** 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 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 appears, 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.

vSphere Data Protection Shutdown and Startup Procedures

If you need to shutdown the vSphere Data Protection 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. After a 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 rollback 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 "Using Checkpoints and Rollback" on page 42 for additional information.

IMPORTANT The vSphere Data Protection 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.

vSphere Data Protection Capacity Management 4

This chapter focuses on vSphere Data Protection capacity management and includes the following topics:

- "Impact of Selecting Thin or Thick Provisioned Disks" on page 47
- "Impact of Storage Capacity for Initial vSphere Data Protection Deployment" on page 48
- "Monitoring vSphere Data Protection Capacity" on page 48
- "vSphere Data Protection Capacity Thresholds" on page 48
- "Capacity Management" on page 49

Impact of Selecting Thin or Thick Provisioned Disks

There are advantages and disadvantages of selecting thin or thick disk partitioning for the vSphere Data Protection datastore.

Thin provisioning uses virtualization technology to allow the appearance of more disk resources than what might be physically available. This can be used if an administrator is actively monitoring disk space and is able to allocate additional physical disk space as the thin disk grows. If this is not managed and the vSphere Data Protection datastore is on a thin provisioned disk that cannot allocate space, the vSphere Data Protection appliance will fail. If this happens, you can rollback to a validated checkpoint (see "Using Checkpoints and Rollback" on page 42 for additional information). Any backups that occurred after the checkpoint will be lost.

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

The following procedure is used to convert thin provisioning to thick provisioning. This procedure requires that the vSphere Data Protection appliance be shut down and can take several hours to complete.

Prerequisites

It is strongly recommended that the vSphere Data Protection appliance be installed with thin provisioning. However, there must be sufficient disk space available to inflate the disk to thick provisioning.

Procedure

1. In the vSphere Client, right-click the vSphere Data Protection appliance and select **Shut Down Guest OS**.
2. Highlight the appliance and select the **Summary** tab. In the **Storage** section right-click the datastore and select **Browse Datastore...**
3. From the Datastore Browser screen, select your appliance and expand the associated datastore.

4 Right click a .vmdk file and select **Inflate**.

5 Repeat this step for each .vmdk file.

- For 0.5 TB appliance, there are three .vmdk files used for backup storage.
- For 1 TB appliance, there are six .vmdk files used for backup storage.
- For 2 TB appliance, there are 12 .vmdk files used for backup storage.

Impact of Storage Capacity for Initial vSphere Data Protection Deployment

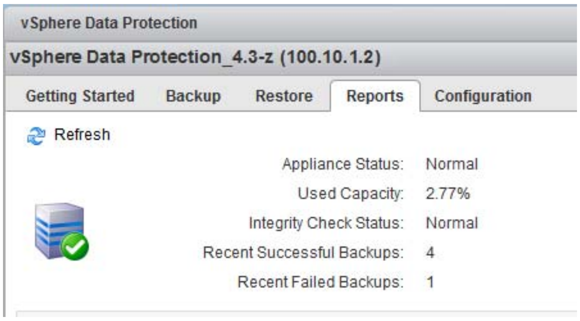
When a new vSphere Data Protection appliance is deployed, the appliance typically fills rapidly for the first few weeks. This is because nearly every client that is backed up contains unique data. vSphere Data Protection deduplication is best leveraged when other similar clients have been backed up, 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 capacity. You can view vSphere Data Protection capacity through the vSphere Data Protection Report tab, Used Capacity.



Appliance Status: Normal
Used Capacity: 2.77%
Integrity Check Status: Normal
Recent Successful Backups: 4
Recent Failed Backups: 1

vSphere Data Protection Capacity Thresholds

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

Table 4-1. vSphere Data Protection capacity thresholds

Threshold	Value	Behavior
Capacity warning	80%	vSphere Data Protection 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. vSphere Data Protection issues warning events.
Server read-only limit	100%	vSphere Data Protection transitions to read-only mode and no new data is allowed.

Capacity Management

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

- Stop adding new VMs as backup clients
- Delete uneeded backup jobs
- Reassess retention policies to see if you can decrease retention policies
- Consider adding additional vSphere Data Protection appliances and balance backup jobs between multiple appliances

vSphere Data Protection Troubleshooting

5

This chapter includes the following troubleshooting topics:

vSphere Data Protection Appliance Installation

If you have problems with the vSphere Data Protection appliance installation:

- Confirm that all of the software meets the minimum software requirements (see "Software Requirements" on page 12).
- Confirm that the hardware meets the minimum hardware requirements (see "System Requirements" on page 13).
- Confirm that DNS is properly configured for the vSphere Data Protection appliance. (see "Preinstallation Configuration" on page 13).

vSphere Data Protection Backups

The following are known issues for vSphere Data Protection 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, delete, 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, this 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.

Windows 2008 R2 VMs can fail to backup with "disk.EnableUUID" configured to "true."

Windows 2008 R2 backups can fail if the VM is configured with *disk.EnableUUID* set to *true*. To correct this problem, you can manually update the vmx configuration parameter *disk.EnableUUID* to *false*.

To configure *disk.EnableUUID* to *false* using the vSphere Web Client:

1. Shut down the VM by right clicking the VM and selecting **Shut Down Guest OS**.
2. Right dick the VM and select **Edit Settings**.
3. Click **VM Options**.
4. Expand the **Advanced** section and click **Edit Configuration**.
5. Locate the name *disk.EnableUUId* and set the value to *false*.
6. Click **OK**.
7. Click **OK**.
8. Right click the VM and click **Power On**.

After updating the configuration parameter, backups of the Windows 2008 R2 VM should succeed.

Backup fails if vSphere Data Protection there is not sufficient vSphere Data Protection datastore capacity.

Scheduled backups will fail at 92% complete if there is not sufficient vSphere Data Protection datastore capacity. If the vSphere Data Protection datastore is configured with thin provisioning and maximum capacity has not been reached, add additional storage resources. If the vSphere Data Protection datastore is configured with thick provisioning and is at capacity, see “vSphere Data Protection Capacity Management” on page 47.

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, vSphere Data Protection 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.

Anytime an unexpected shutdown occurs, the vSphere Data Protection appliance uses rollback to the last validated checkpoint. This is expected behavior. See “Using Checkpoints and Rollback” on page 42 for additional information.

vSphere Data Protection Restores

The following are known issues for vSphere Data Protection 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 fails to original location if VM has associated snapshots.

If a VM has associated snapshots, the restore to original location will fail. This is expected behavior, vSphere Data Protection does not support restoring VMs that have snapshots to the original location. Restore the VM to an alternate location or delete the snapshots before restoring to the original location.

File Level Recovery

The following are known issues for file level recovery with the vSphere Data Protection restore client.

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.

manually copy the files needed.

Symbolic links are not displayed in the restore client.

The restore client does not support browsing symbolic links.

vSphere Data Protection Reporting

The following are known issues for vSphere Data Protection reporting.

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 has taken up to four and a half minutes.

vSphere Data Protection Port Usage 6

vSphere Data Protection uses the ports listed in the following table.

Table 6-1. vSphere Data Protection port usage

Product	Port	Protocol	Source	Destination	Purpose
vSphere Data Protection	22	TCP			ssh
vSphere Data Protection	80	TCP			http
vSphere Data Protection	111	TCP			rpcbind
vSphere Data Protection	443	TCP			https
vSphere Data Protection	700	TCP			Loginmgr tool
vSphere Data Protection	5555	TCP			Postgres
vSphere Data Protection	5558	TCP			Postgres
vSphere Data Protection	7778	TCP			VDP RMI
vSphere Data Protection	7779	TCP			VDP RMI
vSphere Data Protection	8509	TCP			Tomcat AJP Connector
vSphere Data Protection	8543	TCP			Redirect for Tomcat
vSphere Data Protection	8580	TCP			VDP Downloader
vSphere Data Protection	9443	TCP			VDP Web Services
vSphere Data Protection	25000	TCP/UDP			VDP Internal Communications
vSphere Data Protection	26000	TCP/UDP			VDP Internal Communication
vSphere Data Protection	27000	TCP			VDP Client Server Communications
vSphere Data Protection	28001	TCP			VDP Internal Proxy

Table 6-1. vSphere Data Protection port usage

Product	Port	Protocol	Source	Destination	Purpose
vSphere Data Protection	28002	TCP			VDP Internal Proxy
vSphere Data Protection	28003	TCP			VDP Internal Proxy
vSphere Data Protection	28004	TCP			VDP Internal Proxy
vSphere Data Protection	28005	TCP			VDP Internal Proxy
vSphere Data Protection	28006	TCP			VDP Internal Proxy
vSphere Data Protection	28007	TCP			VDP Internal Proxy
vSphere Data Protection	28008	TCP			VDP Internal Proxy
vSphere Data Protection	28009	TCP			VDP Internal Proxy
vSphere Data Protection	29000	TCP			VDP internal client secure communications
vSphere Data Protection	34250	TCP			ssl/soap gSoap (localhost)
vSphere Data Protection	53	UDP			DNS
vSphere Data Protection	111	UDP			RPC
vSphere Data Protection	941	UDP			RPC

vSphere Data Protection Disaster Recovery

7

vSphere Data Protection 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 "Using Checkpoints and Rollback" on page 42). To recover from a vSphere Data Protection appliance failure, the following procedure is used to create backups of the appliance and all of the associated vSphere Data Protection backups for use in disaster recovery.

The following provides guidelines for vSphere Data Protection disaster recovery:

1 Before shutting down the vSphere Data Protection appliance, verify that no backup or maintenance tasks are running. Depending on the backup method used and how long it takes, schedule your vSphere Data Protection 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. See "Backup Window Configuration" on page 37 for additional information.

2 In the vSphere Client, navigate to the appliance. Perform a Shut Down Guest OS on the VM. Do not use Power Off. A power off task is equivalent to pulling the plug on a physical server and may not result in a a clean shut down process. See "vSphere Data Protection Shutdown and Startup Procedures" on page 46 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 vSphere Data Protection is complete and that no backup/snapshot/copy jobs are being performed against vSphere Data Protection.

5 From the vSphere Client, perform a Power On for the appliance.

Minimum Required vCenter User Account Permissions

8

In high-security environments, you can restrict the vCenter user account permissions required to configure and administer the Backup and Recovery appliance to all of the following:

Datastore

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

Folder

- Create Folder

Global

- Cancel task
- Log event
- Settings

Network

- Assign network
- Configure

Resource

- Assign virtual machine to resource pool

Sessions

- Validate session

Tasks

- Create task
- Update task

Virtual machine > Configuration

- Add existing disk
- Add new disk
- Add or Remove device
- Advanced
- Change CPU count
- Change Resource
- Disk change Tracking
- Disk Lease
- Host USB device
- Memory
- Modify device setting
- Raw device
- Reload from path
- Remove disk
- Rename
- Reset guest information
- Settings
- Swapfile placement
- Upgrade virtual hardware
- Extend Virtual disk

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 > State

- Create snapshot
- Remove Snapshot
- Revert to snapshot

Index