

VMware Data Protection and Recovery

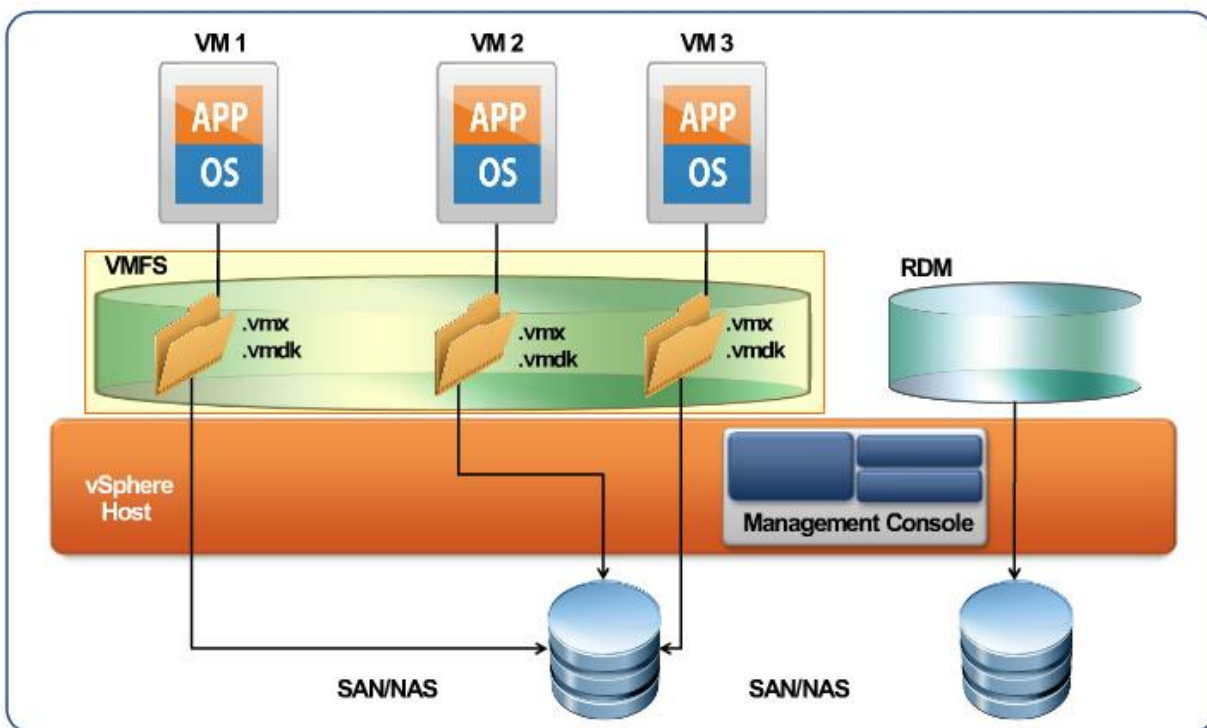
SANDEEP KUMAR SEERAM

VCA-DCV, VTSP – Cloud

OCTOBER 2013

VMware Data Recovery Overview

Virtual machines are important resources that change on a daily basis. You should create backups for all virtual machines – or VMs – in your environment. The information normally backed up for VMs includes the operating system, applications, and data. All of this information for each VM resides in one or more virtual machine disk files, which have the vmdk extension. In addition to virtual machine disk files, a VMware virtual machine has a configuration file, which has the vmx extension. These configuration files contain information about the VM configuration such as how many CPUs the VM has, how much memory the VM can use, and which vmdk files belong to the VM. As with physical machines, virtual machines need to be backed up periodically to recover from loss of data due to human error, technical malfunction, etc.



vSphere Data Protection (VDP) is VMware's backup and recovery solution designed for small- to medium-sized organizations. VDP offers several key features to make virtual machine backup and recovery rapid, reliable, manageable, and affordable. It provides a simple interface to quickly create, configure, and schedule backup jobs. It is an agent-less, pure disk-based solution, allowing for faster restores over solutions that write directly to tape.

A VM that utilizes an agent for backup and recovery requires the VM to be powered on to perform a restore using that agent. With VDP, this is not the case - backups and recoveries can be performed regardless of the VM's power state.

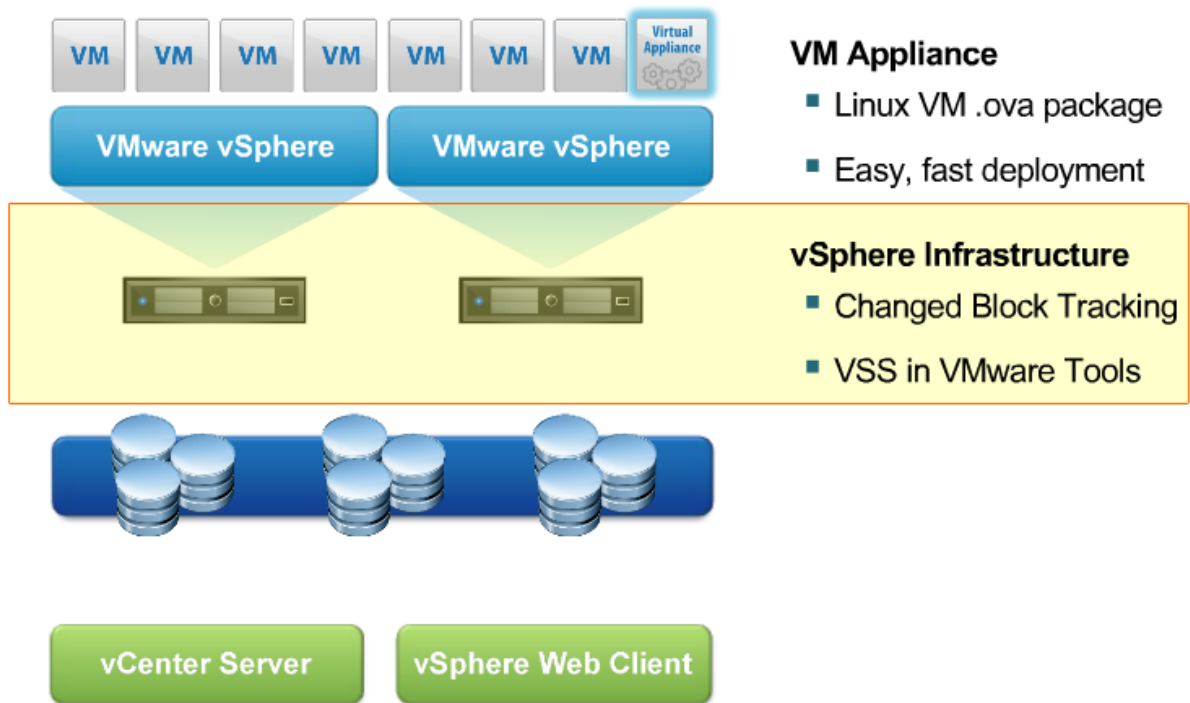
VDP provides a centralized management interface through VMware vCenter Server so scheduling of backup and recovery jobs are performed using the VMware vSphere Web Client. The vSphere Web Client allows an administrator to create, configure, schedule and execute backup and restore jobs through an intuitive wizard.

Additionally, VDP enables the recovery of an entire virtual machine image for virtual machines running any operating system. It also enables the recovery of individual files and directories for virtual machines running Microsoft Windows or Linux operating systems. Multiple restore points for each virtual machine are displayed to easily select a specific restore point.

VDP utilizes built-in data deduplication technology to help minimize disk space consumption. Deduplication eliminates duplicate storage blocks as backup data written to disk. Therefore, vSphere administrators can maintain multiple point-in-time copies of VMs using only a fraction of the storage that would normally be required versus storing multiple full copies of a VM.

The built-in data deduplication works in conjunction with Changed Block Tracking in vSphere to minimize the amount of data to process. On vSphere hosts running 4.0 and later, a record of each virtual machine's changed blocks is maintained. This is called Changed Block Tracking. VDP utilizes this information and backs up only the blocks that have changed since the last backup of the VM. This helps reduce the amount of data to be transferred from the virtual machines to the VDP appliance for backup.

VDP Key Components



Now, you will look at components that are part of VDP solution and understand their functions. VDP is a virtual machine appliance deployed from an .ova or open virtual appliance file.

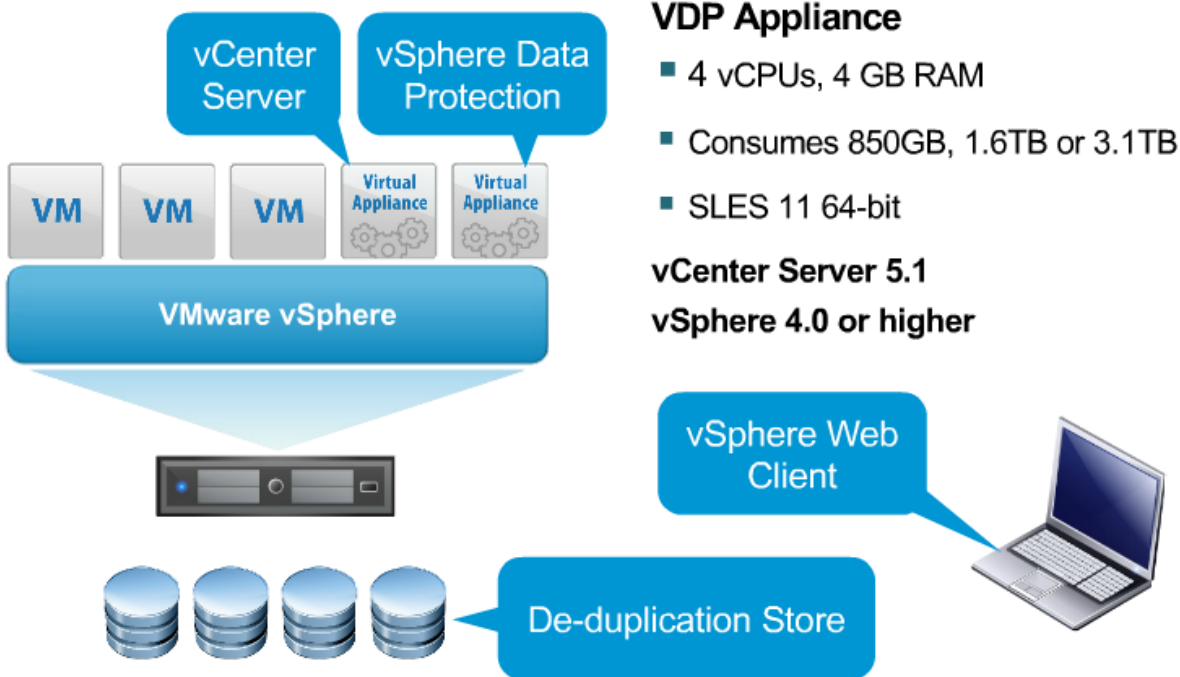
The VMware vStorage API for Data Protection (VADP) is utilized by VDP. This includes the Changed Block Tracking (CBT) mechanism. CBT tracks the changes made to a VM at the block level and provides this information to VDP so that only changed blocks are backed up. This significantly reduces storage consumption and speeds up backup and recovery times with VDP.

VMware Tools on Windows contains Microsoft Volume Shadow Copy Service (VSS) components to assist with guest OS and application quiescing when backing up Windows VMs.

The VDP appliances have three backup data destination storage capacities: .5 TB, 1 TB, 2 TB. Note that the actual amount of storage capacity consumed by the appliance will likely be greater than the backup data destination storage capacity. Please see the VDP Administration Guide for more information.

VDP is managed using the vSphere Web Client. Please note that the traditional vSphere Client cannot be used to manage VDP – you must use the vSphere Web Client.

VDP Architecture



The VDP appliance is deployed by default with four vCPUs and 4 GB of RAM. For the capacities of 0.5, one, or two terabytes, the amount of disk space (thick-provisioned) actually consumed by each appliance is 850 GB, 1.6TB and 3.1TB respectively. Thin provisioning can be used, but if it is, the administrator should actively monitor disk consumption.

It is important to note that once the VDP appliance is deployed, additional storage cannot be added.

The VDP appliance guest OS is SuSE Linux 11.

vCenter Server 5.1 or higher is required to use VDP.

VDP can backup VMs running on vSphere hosts 4.0 and higher. The VDP appliance connects to the hosts using port 902. If there is a firewall between the VDP appliance and the vSphere host, then port 902 must be opened. VDP management must be done via the vSphere Web Client.

Before installing the VDP appliance, it is recommended that you review the VMware Data Protection Administration Guide for a complete list of prerequisites.

VDP Considerations

When establishing VDP in your environment, there are special considerations to be aware of. Here are a few of them:

1. VDP does not support tape integration. It is a disk-based backup and recovery tool. It utilizes disk-based storage to enable speedy recovery of your virtual machines.
2. VDP cannot backup virtual machine protected by VMware Fault Tolerance – or FT. This is because there is no way to snapshot FT-protected virtual machines.
3. Each instance of vCenter Server can support a maximum of 10 VDP backup appliances per vCenter. Each VDP appliance supports backing up a maximum of 8 VMs concurrently.
4. VMware supports protecting a maximum of up to 100 VMs per appliance.
5. VDP appliances do not share information with each other. For example, if two VDP appliances are configured to protect the same VM, this could cause errors if both appliances try to back up the VM at the same time.

VDP Prerequisites

The VMware Data Protection Administration Guide lists VDP prerequisites in detail, but you will take a brief look at them now.

1. The VDP appliance is installed on a vSphere host version 4.x or 5.x.
2. The host that runs the backup appliance must be managed by vCenter Server 5.1.
3. The virtual machines to be backed up and the backup appliance must both connect to a vSphere host using port 902. If there is a firewall between the appliance and the vSphere host, port 902 must be open.
4. The VMware Client Integration Plug-in needs to be installed in your browser.

Before installing VDP, it is recommended that you review the VMware Data Protection Administration Guide for a complete list of prerequisites.

vSphere Data Protection Pre-Installation Steps

Before deploying VDP, it is important to properly size the appliance, as additional storage cannot be added after deployment. Sizing requirements are based on the number and types of virtual machines, the amount of data and retention periods, and data change rates. You can find general sizing guidelines in the Administration Guide.

DNS should be properly configured for vCenter Server and all vSphere hosts. A DNS host record for each VDP appliance should be added prior to deployment. Also, NTP must be configured for all vSphere hosts and vCenter Server.

A user account with administrative permissions in vCenter and the SSO server is required to deploy VDP.

With all these ready, you can proceed to deploy the VDP ova file.

Deploying the OVA Package

Deploy OVF Template, including an ova file, is an Action on the Objects tab of the Datacenters view of the vCenter Server. Ensure the pre-requisites have been met. You have to select the source where the VDP ova file is located. Next, you open the ova file and review the template details. After you read and accept the license agreement, you specify where you want the appliance deployed and select the host or cluster for the appliance.

Select the virtual disk format and the location of the storage for the appliance.

Browse to select the Destination Network for the appliance.

You can customize the template details. Verify the network configuration is correct.

Confirm that all of the options are correct and click Finish to deploy the VDP appliance.

VDP Installation and Configuration Steps

The VDP .ova package must have deployed successfully, and you must be logged into the vCenter Server from the vSphere Web Client, before you start to install the VDP appliance.

In the vSphere Web Client, select vCenter Home > vCenter > VMs and Templates. Expand the vCenter tree and select the VDP appliance. Right-click the appliance and select Power On.

Then, you Right-click the appliance again and select Open Console.

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

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

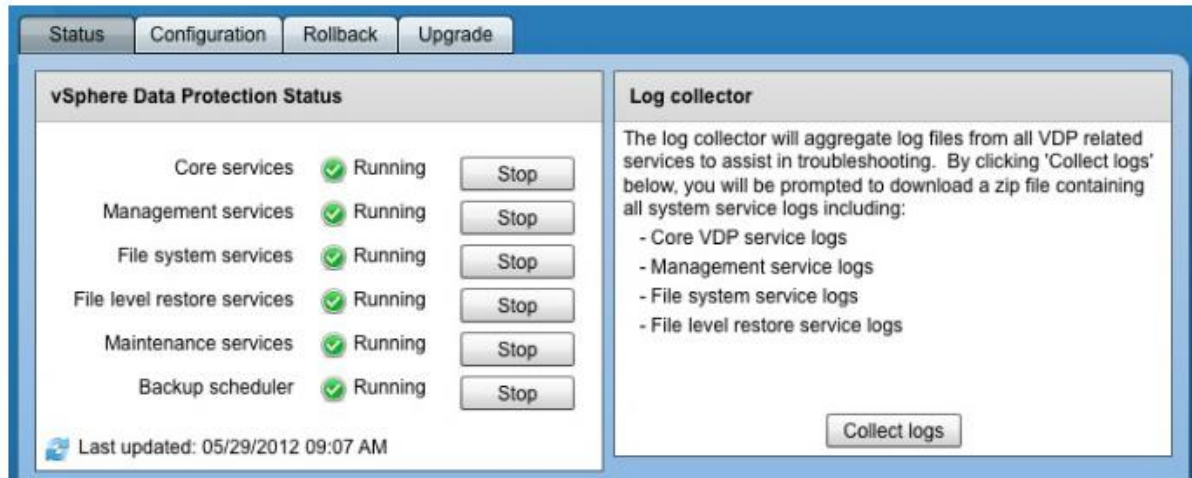
From the VMware Login screen, enter the User name: root, and Password: changeme (all lower case), then click Login. Over the next series of panels, you specify or confirm Network settings, Time Zone, VDP credentials, vCenter registration details and click Test connection.

At this stage, you may need to check your settings or user account parameters.

Once the connection is successful, click through to complete configuration.

Finally, you will need to return to the vSphere Web Client and reboot the appliance. The reboot can take up to 30 minutes.

VDP Post Installation



After initial configuration of the VDP appliance (“install mode”), subsequent web browser connections to the VDP appliance will show the “maintenance mode” GUI. There are four tabs: Status, Configuration, Rollback and Upgrade.

The Status tab is shown on the figure.

Core services comprise the backup engine of the appliance. If these services are disabled, no backup jobs will run – whether scheduled or “on demand”, and no restore activities can be initiated.

Management services should only be stopped under the direction of technical support.

File system services allow backups to be mounted for file-level restore operations.

File level restore services support the management of file-level restore operations.

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

Backup scheduler initiates schedule backup jobs. If this is stopped, no scheduled backups will run; however, “on demand” backups can still be initiated. There are several status levels that may appear in this tab. These are listed in the VDP administration guide.

Logs can also be collected here. You click the “Collect logs” button to create a LogBundle.zip file for convenient uploading to VMware Support in the event troubleshooting assistance is needed.

The Configuration tab provides an interface for changing configuration items on the VDP appliance – items such as network configuration and password. On the Rollback tab, you can access the list of checkpoints. The Upgrade tab is a simple interface for performing upgrades to the VDP appliance.

----- Thank You -----