Dell Data Protection for VMware Horizon View Infrastructures

Options for backing up and recovering your VMware Horizon View environment

Dell Wyse Solutions Engineering
February 2014
## Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2014</td>
<td>Initial release v.6.0</td>
</tr>
</tbody>
</table>
# Table of contents

Revisions ........................................................................................................................................ 2

1  Disaster recovery overview ........................................................................................................ 5
   1.1  Introduction .......................................................................................................................... 5
   1.2  The Dell Data Protection portfolio ......................................................................................... 5
       1.2.1  Dell NetVault ............................................................................................................... 5
       1.2.2  Dell AppAssure ............................................................................................................ 6
       1.2.3  Dell vRanger ................................................................................................................. 6

2  Using vRanger to provide disaster recovery ............................................................................... 8

3  Options for backing up VDI management VMs in vSphere 5 environments ................................. 11

4  Conclusion .................................................................................................................................. 17
1 Disaster recovery overview

1.1 Introduction

In an era where so much depends on online services and up-to-date data, it is crucial to have a comprehensive plan for backup and recovery. A successful disaster recovery plan requires a holistic approach that considers business imperatives, current systems, staffing, procedures and technological choices.

Dell offers our customers the widest possible choice of robust and resilient infrastructure products that can be the foundation of any disaster recovery solution. Dell is dedicated to helping customers meet their critical challenges with solutions that help organizations achieve maximum efficiency, effective disaster recovery, and flexible scalability to meet the needs of the future.

Protecting virtual environments with traditional backup and replication software is no small feat. These agent-dependent solutions are slow, expensive, and difficult to manage; sapping virtual host CPU and I/O resources and often wasting large amounts of backup storage.

In many virtual desktop infrastructure (VDI) environments, customers will leverage their existing disaster recovery (DR) implementation to provide protection to the management hosts for the VDI environment. Below are a number of options from the Dell Data Protection portfolio that offer the best solutions to address the widest number of data protection challenges. The remainder of this document will focus on using Dell vRanger for protecting the management component of a VMware Horizon View environment.

This includes providing DR for the file server where user profiles and home directories reside, protect in the same way as you would protect a standard file server. This requires implementation of a corporate policy to centralize all data rather than trying to provide DR for data held within persistent desktops for example which would be considerably more difficult and costly to implement. Obviously, with a linked clone or non-persistent pool of desktop the user would not be in a position to store data locally on the image they are assigned anyway, but would rather store their information centrally on the designated file server.

1.2 The Dell Data Protection portfolio

Dell offers an extensive data protection software portfolio that addresses today’s key data protection challenges. In doing so, organizations are enabled to recover anything, every time, on time.

1.2.1 Dell NetVault

Dell NetVault backup and recovery products are cross-platform solutions that safeguard data and applications in both physical and virtual environments. Comprehensive platform and application support provides enterprise-class data protection. With NetVault solutions, organizations can protect a full range of mission-critical data and applications—such as Oracle Database, Microsoft SQL Server, Microsoft Exchange, MySQL, and IBM DB2— running on any major physical and virtual operating systems and processor architectures.
NetVault solutions support a wide range of disk and tape-based storage devices, enabling organizations to make the most of existing resources. Data deduplication helps enhance efficiency, minimizing the capacity required for backups and reducing backup windows.

NetVault solutions are designed to simplify backup and recovery. Administrators can manage data protection across environments from a single, well-thought-out administrative interface.

Granular recovery capabilities enable administrators to retrieve a single file, conduct a complete restoration, or choose anything in between. Data can be restored to the original host, a new host, or even a desktop.

### 1.2.2 Dell AppAssure

Dell AppAssure provides a unified approach to protecting physical, virtual, and cloud environments. It supports VMs running on Microsoft Hyper-V, VMware, and Citrix hypervisors. AppAssure is hardware-agnostic—organizations can recover data to physical or virtual machines regardless of the original machine’s configuration. Disk-image level snapshots and changed block tracking effectively eliminate backup windows. Business-critical virtual or physical machines can be backed up as frequently as every five minutes for near continuous system, data, and application protection. Integrated global data deduplication and compression reduces backup storage requirements by up to 80 percent compared with legacy backup technologies.

Live Recovery technology delivers near-zero RTOs by recovering users’ access to an application in minutes, even if hundreds of gigabytes or several terabytes of data are being restored. Administrators can set up an automatically updated warm Virtual Standby in any location, including off-site or in the cloud. The standby is ready to be turned on within seconds after a failure has been detected.

Working from a single backup pass, administrators can choose anything from a highly granular restore of individual application elements or files all the way to a complete system recovery.

AppAssure can be broadly applied to environments ranging in size from a few servers to thousands. It supports data storage requirements that scale to exabyte levels. AppAssure is also available as a fully configured 1U backup appliance—the Dell PowerVault DL4000 powered by AppAssure. The DL4000 integrates 5.5 TB of storage capacity and two standby VMs with AppAssure software. The appliance can be scaled to 35.5 TB with a PowerVault MD1200 option. This appliance offers all the benefits of AppAssure software for Windows and Linux operating systems in a preconfigured, set-and-forget Dell hardware–based appliance.

### 1.2.3 Dell vRanger

Dell vRanger software provides simple, fast, and scalable data protection for VMware virtualized environments as well as Windows physical servers and files. vRanger can deliver high-speed backups while minimizing disruption to production systems. Multi-threaded processing executes multiple operations in parallel to minimize backup and replication windows. To accelerate performance, Active Block Mapping technology reduces the amount of data backed up, transferring only changed blocks. vRanger File Level Recovery engine enables administrators to browse archives and recover files directly from VM images in
the archives. It offers comprehensive protection of virtual and physical environments from a single, wizard-driven interface. Administrators can locate VMs, Windows servers, and even individual files quickly and restore them with a single click. The agentless architecture eliminates the need for administrators to install agents on each VM—vRanger automatically discovers and protects newly deployed VMs.

vRanger offers an excellent solution for organizations that need to protect an environment ranging in size from a few VMs to tens of thousands.
Dell vRanger Pro offers a simple, fast, and scalable data protection solution that deploys seamlessly into virtual environments. It provides a single console for managing backup, replication, and recovery. Built on our data protection platform, it's the only available architecture that's optimized for image handling.

Dell vRanger Pro scales with your virtual environment by maximizing resources through distributed processing, while simplifying management with central command and control.

Dell vRanger Pro is certified VMware Ready for vSphere 5, which means it has undergone and passed rigorous testing by VMware to ensure compatibility and support for vSphere 5.

**VMware VMFS and VMDK files**

vRanger Pro follows best practices by supporting VMFS-5, so you can continue to protect your virtual environment when upgrading to vSphere 5. In addition to its own scalable and high-performance engine, vRanger Pro also provides a resource manager that allows you to define the maximum number of tasks allowed to run concurrently on a vRanger server, off a LUN, on a host, or off a repository. This flexibility allows you to dial vRanger Pro’s performance up or down in accordance with available resources and bandwidth.

VMware virtual machine disk files, formatted in the virtual machine disk (VMDK) format, describe the entire virtual machine environment and are stored on VMFS volumes. VMDK files are the most critical component protected by vRanger Pro through backup and replication. Backing up VMDK files with vRanger Pro enables you to locate and restore individual files contained within the virtual machine or the entire virtual machine itself at high speed and with very little effort.

**VMware APIs**

vRanger Pro exploits a full range of VMware APIs to provide seamless integration with vSphere 5, enabling it to deliver highly optimized, efficient, and effective data protection services for virtual environments.

One of the most important integration points for vRanger Pro is the VMware vSphere Storage APIs – Data Protection (VADP). vRanger Pro integrates with VADP-5 as well as back-level VADP, ensuring uninterrupted data protection services as you upgrade to vSphere 5.

VADP is a collection of APIs that enable vRanger to manage and manipulate VMDK files, including:

- Gaining block-level access to VMDK files from virtual machines running supported Microsoft Windows and Linux operating systems
- Gaining access to internal host data paths
- Performing full, incremental, or differential backups
- Using Microsoft Volume Shadow Copy Services (VSS) for virtual machines running supported Microsoft Windows operating systems to ensure data consistency
- Leveraging Change Block Tracking (CBT) which presents only the blocks that have changed since the last backup to vRanger, to help reduce backup storage requirements
In addition to CBT, vRanger Pro provides patented Active Block Mapping (ABM) which together with CBT can reduce the backup footprint by up to a third without extending job windows or adding resource overhead to the production environment. ABM enables vRanger Pro to skip zeroed and deleted blocks, so protected data includes only changed blocks with active data. When enabled, ABM applies to all backup jobs while CBT applies to incremental and differential backups.

vRanger Pro also provides enterprise-class data deduplication through NetVault SmartDisk – vRanger Edition (NVSD – vRanger Edition), an optional software-based deduplication engine. After applying CBT and ABM, protected virtual machine data can be streamed to the NVSD – vRanger Edition repository for deduplication. This implementation completely offloads the resource-intensive deduplication process from both your production host and vRanger environments.

vRanger Pro also utilizes available VMware web services to be able to query the vSphere server and individual hosts. This makes it simple to select which virtual machines to protect in each job; you can select groups of virtual machines associated with all vCenter objects or with specific data centers, clusters, hosts, resource pools, or your own custom groups.

**VMware data transport modes**

This extensive integration with vSphere 5 means not only that vRanger Pro delivers a simple, intuitive, and highly effective data protection experience, but also that vRanger Pro can utilize the full range of VMware transport modes available.

VMware transport modes include two advanced modes (SAN and Hot Add transports) and LAN transport. vRanger Pro provides added insurance by allowing you to configure backups that utilize primary and secondary transport modes. In the event the primary transport fails, vRanger can fail over to the secondary transport, ensuring that jobs will complete. The primary transport mode will be one of the advanced transport modes, when available, and the secondary transport mode will be LAN. If neither of the advanced transports is available, LAN will be the only transport mode.

**SAN transport**

The SAN transport mode involves vRanger Pro gathering information about the VMFS LUNs to read directly from the fibre SAN or iSCSI LUN where the virtual disk files are stored. SAN transport works only when vRanger Pro is installed on a physical machine and has access to fibre channel or iSCSI SAN storing the virtual disks being protected. In this case, backup data is transferred over the production SAN network.

**Hot add transport**

The Hot Add transport mode involves an SCSI Hot Add on the host where vRanger is running. vRanger must be installed in a virtual machine to leverage Hot Add transport. In addition, Hot Add works only for backing up virtual machines with SCSI disks, and not IDE disks. Hot Add works with storage area networks (SAN) or local storage (provided requisite Hot Add conditions are met), without using the LAN.

**LAN transport**
The LAN transport mode involves vRanger backing up virtual machines via the host over the network using a network block device (NBD) driver. LAN transport is necessary when vRanger cannot directly access the virtual machine disks. This transport method adds backup and restore traffic to the LAN, but does work with any storage device, including local or NAS.
Options for backing up VDI management VMs in vSphere 5 environments

Data movement, or the transferring of protected virtual machine data from the host to the backup destination, is the most important aspect of your data protection architecture.

LAN-Free Backup

Installing vRanger Pro on a physical machine with either a fibre channel or iSCSI SAN connected host environment provides maximum scalability and performance for backing up vSphere 5 environments. In this configuration, vRanger Pro can perform LAN-free backups by invoking VMware’s SAN transport mode. LAN-free backup can be utilized as the primary backup method, while network backup can be employed for fail-safe redundancy in the event LAN-free fails.

The benefits of this configuration include:

- Leveraging your existing investment in SAN
- Isolating backup and restore traffic to the fibre channel or iSCSI network, completely offloading your production hosts and network from data protection overhead and traffic
- Enabling extreme high performance and scalability for data protection operations
  - Adding HBAs or NICs to the backup machine (one dedicated to reading and another to writing) further increases performance and scalability.

This configuration is illustrated below. Here vRanger Pro acts as a physical proxy server with storage connections to VMFS and the backup repository. The vRanger Pro machine must be attached to fibre channel or iSCSI SAN environment, and the VMFS volumes containing the protected virtual machines must also be presented to the vRanger Pro machine. vRanger Pro initiates the virtual machine snapshot and reads the VMDKs directly from the fibre SAN or iSCSI LUN that stores the virtual disks, the backup data traffic flows through the vRanger Pro server, and then is written to the repository.
The steps in LAN-free backup mode can be further broken down as follows:

1. vRanger Pro retrieves the job configuration from the database.
2. vRanger Pro establishes a connection to the repository.
3. vRanger Pro adds a temporary snapshot to the protected virtual machine.
4. vRanger Pro mounts the protected VMDKs to the vRanger physical machine using vStorage API’s proxy mount and SAN advanced transport mode.
5. vRanger Pro reads from the source disk, and transfers data from the protected host to the repository.
6. vRanger Pro deletes the temporary snapshot on the protected virtual machine.

There are a number of factors to consider in this configuration, including the number of virtual machines protected by each vRanger Pro physical proxy server. As a starting point, we recommend using one proxy server for every 10 hosts or every 100 virtual machines, obviously this is significantly higher than the number management VMs we will have for a VMware Horizon View deployment, so this deployment can encompass other VM’s in your infrastructure.

Coinciding with the number of protected virtual machines is the number of virtual machines that can be processed concurrently. The number of concurrent tasks running locally can be set between one through 20 via the Options menu, with the default set to three. As a starting point, we recommend one task per CPU core. If your server has eight cores, for example, start with the maximum number of tasks running locally set to eight.

Note that scalability will also depend on the amount of memory on the vRanger Pro machine and network bandwidth available to write to repositories.
Ensure to disable the auto-mount function on the vRanger machine so that Windows does not assign drive letters to protected VMDKs when they’re mounted to the vRanger machine. Do not initialize or format unknown or offline disks from the vRanger machine – these represent your VMFS volumes and any changes could potentially corrupt the VMFS volumes.

**LAN-free and Hot Add backup**

vRanger must be installed in a virtual machine to use Hot Add transport. The Hot Add transport mode involves a SCSI Hot Add on the host where vRanger is running. LAN-free/Hot Add backup works with SAN or local storage without using the LAN. You can use vRanger’s LAN-free/Hot Add backup as the primary method and use network backup as a secondary mode for redundancy.

The benefits of this configuration include:

- It is simple to deploy and configure.
- vRanger Pro is deployed in a virtual machine.
- vRanger Pro read speeds are extremely fast as they occur at native virtual machine performance.

In this configuration, illustrated below, vRanger is provided with direct access to protected VMDKs through vSphere’s I/O stack rather than through the network. The vRanger server in this configuration acts as a proxy server since the VMDKs are temporarily mounted directly to the vRanger virtual machine, and all backup data traffic flows through the vRanger virtual machine to shared or local storage.
The steps in the LAN-free/Hot Add backup mode can be broken down as follows:

1. vRanger Pro retrieves the job configuration from the database.
2. vRanger Pro establishes a connection to the repository.
3. vRanger Pro adds a temporary snapshot to the protected virtual machine.
4. vRanger Pro mounts the protected VMDKs to the vRanger virtual machine using vStorage API’s Hot Add advanced transport mode.
5. vRanger Pro reads from the source disk, and transfers data from the protected host to the repository.
6. vRanger Pro deletes the temporary snapshot on the protected virtual machine.

In order to employ Hot Add, the vRanger virtual machine must be able to access the datastores for all protected virtual machines. Make sure the protected virtual disks on the datastore have block sizes that match the block sizes for the vRanger virtual machine datastore. Hot Add works only for backing up virtual machines with iSCSI disks, and not IDE disks.

If the vRanger virtual machine can be moved using vMotion, all hosts that it can be moved to must be able to see the storage for all protected virtual machines as well. Also, be sure to disable auto mount on the vRanger virtual machine so that Windows does not assign drive letters to protected VMDKs when they’re mounted to the vRanger virtual machine.

vRanger can process a significant amount of data to the repository very quickly, provided it has enough available resources. As a guideline, allow for two concurrent jobs per vCPU. We recommend configuring the vRanger virtual machine with a minimum of four vCPUs: one for the vRanger server and three for job activities, which allows for up to six concurrent jobs. If you need to run a higher number of concurrent jobs, simply add additional vCPUs.

We also recommend adding a second SCSI controller to the vRanger virtual machine so that it can mount more protected disks at the same time during the Hot Add operation. vRanger Pro can mount as many virtual disks as vSphere allows.

**Network Backup**

In network backup, vRanger Pro backs up virtual machines via each host over the LAN utilizing either VMware’s LAN or Hot Add transport method.

The benefits of network backup include:

- vRanger Pro’s default configuration, so it’s the easiest to configure; it works out of the box.
- vRanger can be deployed in a virtual or physical machine.

This configuration is illustrated below. When vRanger Pro is installed on a virtual machine, it can leverage VMware’s Hot Add transport mode, provided the proper conditions are met for Hot Add. In this case, the VMDKs of the protected virtual machines will be mounted to the vRanger Pro virtual machine. This provides vRanger Pro with direct access to protected data, so reading occurs at native virtual machine
speeds, meaning it’s very fast. When vRanger Pro is installed on a physical machine, network backup will leverage VMware’s LAN transport mode.

When vRanger Pro is installed in a virtual machine, the steps included in network backup mode include:

1. vRanger Pro retrieves the job configuration from the database.
2. vRanger Pro establishes a connection to the repository.
3. vRanger Pro adds a temporary snapshot to the protected virtual machine.
4. vRanger Pro mounts the protected VMDKs to the vRanger virtual machine, using vStorage API’s Hot Add advanced transport mode.
5. vRanger Pro reads from the source disk, and transfers data from the protected host to the repository.
6. vRanger Pro deletes the temporary snapshot on the protected virtual machine.

When vRanger Pro is installed on a physical machine, after the snapshot is taken, the backup data is sent to the vRanger server and on to the repository.

Network backup mode can be utilized for redundancy when vRanger Pro is installed on a physical machine with fibre channel or iSCSI SAN connected hosts. When a LAN-free backup fails, vRanger Pro can fail over the transport mode to network based backup so that the job will complete although it will take longer to process. To ensure backup data traffic does not flow over the network at any time, you can
disable the option to perform a network backup on LANfree failure, in which case the backup job will fail upon LAN-free backup failure.

While vRanger’s performance is good for minimizing job windows, it can potentially degrade the performance of your production network, depending on the total traffic over your network during vRanger job activity and available resources and bandwidth. Best practice includes separation of vRanger data traffic from the production network by configuring a dedicated backup network through a second management NIC.
4 Conclusion

In an era where so much depends on online services and up-to-date data, it is crucial to have a comprehensive plan for backup and recovery. A successful disaster recovery plan requires a holistic approach that considers business imperatives, current systems, staffing, procedures and technological choices.

Dell offers our customers the widest possible choice of robust and resilient infrastructure products that can be the foundation of any disaster recovery solution. Dell is dedicated to helping customers meet their critical challenges with solutions that help organizations achieve maximum efficiency, effective disaster recovery, and flexible scalability to meet the needs of the future.